NCSA Special Publication 500 - 1
Version 1.0

(ร่าง) แนวปฏิบัติเกี่ยวกับเทคโนโลยี Secure Cloud Adoption

ร่างเพื่อรับฟังความคิดเห็นเท่านั้น ห้ามใช้อ้างอิง

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบริการคลาวด์ โดยครอบคลุมข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และแนวทางการนำไปปฏิบัติสำหรับหน่วยงานที่เกี่ยวข้อง เพื่อสนับสนุนการนำไปประยุกต์ใช้อย่างเหมาะสมและสอดคล้องกับกฎหมาย นโยบาย และมาตรฐานที่เกี่ยวข้อง

NOCSET - TASK FORCE 505
กันยายน 2569

สามารถดาวน์โหลดเอกสารฉบับนี้ได้ที่
https://www.ncsa.or.th/page/NOCSET
https://cloudsecurity.ncsa.or.th/team.html

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
เครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทย (คชซ.)

ที่มาและอำนาจหน้าที่

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้จัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทย โดยใช้ชื่อย่อว่า คชซ. (Network of Cyber Security Experts of Thailand: NOCSET) เพื่อเป็นเครือข่ายของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ในลักษณะสมัครใจ (Voluntary) จากหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในและต่างประเทศ รวมถึงผู้เชี่ยวชาญอื่นที่เกี่ยวข้อง โดย คชซ. ทำหน้าที่เป็นกลไกการดำเนินงานและประสานงานเชิงเทคนิครวมกับ สกมช. และมีคณะทำงานเฉพาะกิจ (Task Force) เป็นกลไกในการดำเนินภารกิจตามหัวข้อที่ได้รับมอบหมาย

การจัดตั้งและดำเนินงานของ คชซ. อาศัยอำนาจตามความในมาตรา 36 วรรคหนึ่ง (1) ประกอบมาตรา 22 วรรคหนึ่ง (11) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเป็นไปตามประกาศ สกมช. เรื่อง การดำเนินการของเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทย พ.ศ. 2568 ซึ่งกำหนดกรอบ โครงสร้าง หลักเกณฑ์ และแนวทางการดำเนินงานของ คชซ. และคณะทำงานเฉพาะกิจ (Task Force) เพื่อเป็นกลไกในการขับเคลื่อนภารกิจตามหัวข้อที่ได้รับมอบหมาย รวมทั้งจัดทำเอกสารและผลผลิตที่เป็นประโยชน์ต่อการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เอกสารฉบับนี้จัดทำขึ้นเพื่อรวบรวม ถ่ายทอด และเผยแพร่องค์ความรู้ แนวทางปฏิบัติ และข้อเสนอแนะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จากการศึกษา วิเคราะห์ และแลกเปลี่ยนความรู้และประสบการณ์ของผู้เชี่ยวชาญที่เกี่ยวข้อง เพื่อเป็นข้อมูลอ้างอิงและแนวทางสำหรับหน่วยงานและผู้ที่เกี่ยวข้องในการนำไปประยุกต์ใช้ให้เหมาะสมกับบริบท อันจะช่วยส่งเสริมและยกระดับขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนสนับสนุนการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

บทคัดย่อ

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางในการประยุกต์ใช้ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับบริการคลาวด์ สำหรับผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และหน่วยงานที่เกี่ยวข้อง โดยครอบคลุมหลักการ ข้อกำหนด ข้อพิจารณา และแนวทางการนำไปปฏิบัติในประเด็นสำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์ เช่น การกำหนดนโยบายและบทบาทหน้าที่ การควบคุมการเข้าถึง การบริหารทรัพย์สิน การเข้ารหัส การรักษาความมั่นคงปลอดภัยในการปฏิบัติการและเครือข่าย การบริหารผู้ให้บริการภายนอก การจัดการเหตุการณ์ และการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง เพื่อสนับสนุนให้หน่วยงานสามารถนำแนวทางไปปรับใช้ให้เหมาะสมกับลักษณะบริการ ระดับผลกระทบ ความเสี่ยง และบริบทของหน่วยงานได้อย่างเป็นระบบและมีประสิทธิภาพ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กิตติกรรมประกาศ

เอกสารฉบับนี้จัดทำขึ้นโดย คณะทำงานเฉพาะกิจ (Task Force 505) - จัดทำแนวปฏิบัติเกี่ยวกับเทคโนโลยี Secure Cloud Adoption ภายใต้เครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทย (NOCSET) ซึ่งได้รับการแต่งตั้งให้ศึกษา วิเคราะห์ จัดทำ และนำเสนอแนวปฏิบัติเกี่ยวกับเทคโนโลยี Secure Cloud Adoption ต่อคณะกรรมการบริหารเครือข่ายฯ

การจัดทำเอกสารฉบับนี้ได้รับความร่วมมือจากที่ปรึกษาคณะทำงาน หัวหน้าคณะทำงาน คณะทำงาน เลขานุการ ผู้ช่วยเลขานุการ ตลอดจนผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ หน่วยงาน และผู้มีส่วนเกี่ยวข้องในการให้ข้อคิดเห็น ข้อเสนอแนะ และทบทวนเนื้อหาอันเป็นประโยชน์ต่อการจัดทำเอกสารฉบับนี้ ทั้งนี้ สกมช. ขอขอบคุณผู้มีส่วนร่วมในการจัดทำเอกสารทุกท่านไว้ ณ โอกาสนี้

ลำดับที่	บทบาท	รายชื่อ	หน่วยงาน
1	ที่ปรึกษาคณะทำงาน	พล.อ.ต.จเด็ด คูหะก้องกิจ	สกมช.
2	คณะทำงานและเลขานุการ	พล.อ.ต.เนติภัทร ภัทรกุลชัย	สกมช.
3	คณะทำงานและผู้ช่วยเลขานุการ	น.ส.สุธาทิพย์ กลิ่นกลั่น	สกมช.
4	คณะทำงานและผู้ช่วยเลขานุการ	น.ส.แสงระวี ศรีจำรัส	สกมช.
5	คณะทำงานและผู้ช่วยเลขานุการ	น.ส.กุลฉัตร ตาลจรัส	สกมช.
6	คณะทำงานและผู้ช่วยเลขานุการ	นายพัฒนวัตร เรียงวงษ์	สกมช.

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้อ้างอิง

บทสรุปผู้บริหาร

ปัจจุบันหน่วยงานมีการนำบริการคลาวด์มาใช้ในการจัดเก็บ ประมวลผล และบริหารจัดการข้อมูลและระบบสารสนเทศเพิ่มมากขึ้น ซึ่งช่วยเพิ่มความยืดหยุ่นและประสิทธิภาพในการดำเนินงาน แต่ขณะเดียวกันก็ก่อให้เกิดความเสี่ยงและความท้าทายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านการกำหนดบทบาทและความรับผิดชอบ การควบคุมการเข้าถึง การบริหารทรัพย์สิน การเข้ารหัส การรักษาความมั่นคงปลอดภัยในการปฏิบัติการและเครือข่าย การบริหารผู้ให้บริการภายนอก ตลอดจนการจัดการเหตุการณ์และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง โดยการดำเนินการในสภาพแวดล้อมคลาวด์ต้องคำนึงถึงขอบเขตความรับผิดชอบระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ตามลักษณะและรูปแบบของบริการคลาวด์

เอกสารฉบับนี้จึงจัดทำขึ้นเพื่อเป็นแนวทางสำหรับการนำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มาประยุกต์ใช้กับบริการคลาวด์ โดยครอบคลุมข้อกำหนดและแนวทางสำหรับผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และหน่วยงานที่เกี่ยวข้อง รวมทั้งให้ความสำคัญกับการบริหารจัดการตามระดับความเสี่ยง ลักษณะของบริการ ขอบเขตความรับผิดชอบ และหลักฐานที่จำเป็นต่อการกำกับดูแลและการตรวจสอบ เช่น การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัย การประเมินความสามารถของผู้ให้บริการ การจัดการช่องว่างหรือความเสี่ยง และการบันทึกผลการตัดสินใจอย่างเหมาะสม

การนำแนวทางตามเอกสารฉบับนี้ไปประยุกต์ใช้ จะช่วยให้หน่วยงานสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบริการคลาวด์ได้อย่างเป็นระบบและสอดคล้องกับบริบทของหน่วยงาน ลดช่องว่างด้านความรับผิดชอบระหว่างผู้ใช้บริการและผู้ให้บริการคลาวด์ ตลอดจนสนับสนุนการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย นโยบาย และมาตรฐานที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้อ้างอิง

สารบัญ

หน้า

บทที่ 1 บทนำ....8

1.1 ความเป็นมา....8
1.2 วัตถุประสงค์และการนำไปใช้....8
1.3 กลุ่มเป้าหมาย....8
1.4 โครงสร้างของเอกสาร....8

บทที่ 2 หลักการพื้นฐาน....9

2.1 หลักการและแนวคิดสำคัญที่เกี่ยวข้อง....9
2.2 บริบทและประเด็นสำคัญของเรื่อง....9
2.3 บทบาทและความรับผิดชอบ....9
2.4 ความสัมพันธ์กับกฎหมาย นโยบาย มาตรฐาน หรือแนวปฏิบัติที่เกี่ยวข้อง....9
2.5 ข้อพิจารณาหรือหลักเกณฑ์สำคัญ....10

บทที่ 3 กระบวนการหรือแนวทางดำเนินการ

5.1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)....11
5.1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)....38
5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)....64
5.2.1 การบริหารทรัพยากรมนุษย์ (Human Resource Security)....92
5.2.2 การจัดการทรัพย์สิน (Asset Management)....98
5.2.3 การควบคุมการเข้าถึง (Access Control)....106
5.2.4 การเข้ารหัส (Cryptography)....151
5.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)....180
5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)....201
5.2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)....262
5.2.8 การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)....307
5.2.9 การจัดการผู้ให้บริการภายนอก (Supplier Relationships)....325
5.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)....343
5.3 การใช้ทรัพยากรคลาวด์อย่างมีประสิทธิภาพและยั่งยืน (Efficient and Sustainable Use of Cloud Resources)....357

ร่างเอกสาร Public Hearing เท่านั้น ห้ามใช้อ้างอิง

5.3.1 การเลือกประเภท ขนาด และรูปแบบการใช้ทรัพยากรให้เหมาะสมกับภาระงาน.....373
5.3.2 การบริหารระดับชั้นการจัดเก็บและวงจรชีวิตข้อมูล 383
5.3.3 การเลือกตำแหน่งของบริการและการลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น.....391
5.3.4 การวัด ติดตาม และปรับปรุงประสิทธิภาพการใช้ทรัพยากร.....398

ภาคผนวก ก (ประกอบหัวข้อ 5.2.4) แนวทางการคัดเลือกผู้ให้บริการคลาวด์ด้านการเข้ารหัสและการจัดการกุญแจ (Guidelines for Cloud Provider Selection: Cryptography and Key Management) 415

ภาคผนวก ข (ประกอบหัวข้อ 5.2.8) แบบตรวจสอบข้อกำหนดและความสามารถด้านความมั่นคงปลอดภัยของบริการคลาวด์ (Cloud Service Security Requirements and Capability Assessment Checklist).....419

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

บทที่ 1 บทนำ

1.1 ความเป็นมา

ปัจจุบันหน่วยงานมีการนำบริการคลาวด์มาใช้ในการจัดเก็บ ประมวลผล และบริหารจัดการข้อมูลและระบบสารสนเทศเพิ่มมากขึ้น เพื่อสนับสนุนการดำเนินงานและการให้บริการดิจิทัล อย่างไรก็ตาม การใช้บริการคลาวด์มีลักษณะการบริหารจัดการและขอบเขตความรับผิดชอบที่แตกต่างจากระบบสารสนเทศที่หน่วยงานดำเนินการเอง โดยอาจเกี่ยวข้องกับผู้ใช้บริการคลาวด์ (CSC) ผู้ให้บริการคลาวด์ (CSP) ผู้ให้บริการภายนอก ตลอดจนองค์ประกอบของบริการที่อยู่ภายใต้การควบคุมของแต่ละฝ่าย

การรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบริการคลาวด์จึงจำเป็นต้องพิจารณาทั้งมาตรการด้านการบริหารจัดการและมาตรการทางเทคนิค โดยคำนึงถึงรูปแบบบริการคลาวด์ ขอบเขตบริการ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ความเสี่ยง และการแบ่งบทบาทและความรับผิดชอบระหว่างผู้เกี่ยวข้อง เพื่อป้องกันช่องว่างหรือความซ้ำซ้อนในการดำเนินงาน

คณะทำงานเฉพาะกิจ (Task Force 505) จึงได้จัดทำแนวปฏิบัติเกี่ยวกับเทคโนโลยี Secure Cloud Adoption เพื่อสนับสนุนการนำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ไปประยุกต์ใช้ในทางปฏิบัติ โดยครอบคลุมข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ และแนวทางการนำไปปฏิบัติในประเด็นที่เกี่ยวข้อง

1.2 วัตถุประสงค์และการนำไปใช้

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อเป็นแนวทางในการประยุกต์ใช้ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับบริการคลาวด์ ให้ผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และหน่วยงานที่เกี่ยวข้องสามารถเข้าใจหลักการ ขอบเขตความรับผิดชอบ และแนวทางการดำเนินงานที่เกี่ยวข้องได้อย่างชัดเจน การนำแนวทางไปใช้ควรพิจารณาให้เหมาะสมกับรูปแบบบริการคลาวด์ ขอบเขตบริการ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ผลการประเมินความเสี่ยง ความสามารถและข้อจำกัดของบริการ รวมถึงกฎหมาย กฎ ระเบียบ ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดมาตรการหรือกระบวนการในลักษณะเดียวกันสำหรับทุกบริการ

1.3 กลุ่มเป้าหมาย

เอกสารฉบับนี้จัดทำขึ้นสำหรับผู้ใช้บริการคลาวด์ (CSC) ผู้ให้บริการคลาวด์ (CSP) ตลอดจนหน่วยงานและบุคลากรที่เกี่ยวข้องกับการวางแผน จัดหา ใช้งาน กำกับดูแล และรักษาความมั่นคงปลอดภัยของบริการคลาวด์

1.4 โครงสร้างของเอกสาร

เอกสารแบ่งเนื้อหาออกเป็น 3 บทหลัก ได้แก่ บทที่ 1 บทนำ ซึ่งอธิบายความเป็นมา วัตถุประสงค์ การนำไปใช้ และกลุ่มเป้าหมาย บทที่ 2 หลักการพื้นฐาน ซึ่งอธิบายแนวคิด บริบท บทบาทและความรับผิดชอบตลอดจนข้อพิจารณาที่เกี่ยวข้อง และบทที่ 3 กระบวนการหรือแนวทางดำเนินการ ซึ่งนำเสนอข้อกำหนดและแนวทางการนำไปปฏิบัติในรายละเอียดตามหัวข้อด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบริการคลาวด์

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

บทที่ 2 หลักการพื้นฐาน

2.1 หลักการและแนวคิดสำคัญที่เกี่ยวข้อง

การรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบริการคลาวด์ควรดำเนินการตามหลักการสำคัญ ได้แก่ ความรับผิดชอบร่วม (Shared Responsibility) ซึ่งกำหนดให้ผู้ใช้บริการคลาวด์ (CSC) ผู้ให้บริการคลาวด์ (CSP) มีบทบาทและความรับผิดชอบตามส่วนของบริการที่แต่ละฝ่ายควบคุมหรือรับผิดชอบ และการบริหารตามความเสี่ยง (Risk-based Approach) ซึ่งกำหนดระดับและลักษณะของมาตรการให้เหมาะสมกับความเสี่ยงและผลกระทบของข้อมูล ระบบ และบริการ ทั้งนี้ การแบ่งความรับผิดชอบอาจแตกต่างกันตามรูปแบบบริการคลาวด์ ขอบเขตบริการ สถาปัตยกรรม และข้อตกลงระหว่างคู่สัญญา

2.2 บริบทและประเด็นสำคัญของเรื่อง

บริการคลาวด์มีลักษณะที่ทรัพยากร ข้อมูล และองค์ประกอบของระบบอาจอยู่ภายใต้การควบคุมของหลายฝ่าย การกำหนดมาตรการรักษาความมั่นคงปลอดภัยจึงต้องพิจารณาความสามารถและข้อจำกัดของบริการ รวมถึงขอบเขตที่หน่วยงานสามารถควบคุม ตรวจสอบ หรือขอหลักฐานจากผู้ให้บริการได้

การดำเนินการควรมุ่งให้หน่วยงานสามารถระบุได้ว่า ส่วนใดต้องดำเนินการเอง ส่วนใดเป็นความรับผิดชอบของผู้ให้บริการ และส่วนใดต้องดำเนินการร่วมกัน เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างเหมาะสมและไม่เกิดช่องว่างด้านความรับผิดชอบ

2.3 บทบาทและความรับผิดชอบ

ผู้ใช้บริการคลาวด์ (CSC) ควรกำหนดข้อกำหนดด้านความมั่นคงปลอดภัย ประเมินความเหมาะสมของบริการ กำหนดและบริหารสิทธิ การตั้งค่า ข้อมูล และทรัพยากรที่อยู่ภายใต้การควบคุมของตน ตลอดจนติดตามและประเมินความเสี่ยงที่เกี่ยวข้อง

ผู้ให้บริการคลาวด์ (CSP) ควรดำเนินมาตรการด้านความมั่นคงปลอดภัยตามขอบเขตบริการที่รับผิดชอบและให้ข้อมูลที่จำเป็นแก่ CSC เพื่อประกอบการประเมินและกำกับดูแล ทั้งสองฝ่ายควรกำหนดบทบาท หน้าที่ ช่องทางการประสานงาน และความรับผิดชอบร่วมให้ชัดเจนตามรูปแบบบริการและข้อตกลงที่เกี่ยวข้อง เพื่อป้องกัน Responsibility Gap

2.4 ความสัมพันธ์กับกฎหมาย นโยบาย มาตรฐาน หรือแนวปฏิบัติที่เกี่ยวข้อง

การนำแนวทางตามเอกสารฉบับนี้ไปใช้ ต้องพิจารณาร่วมกับกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ นโยบาย มาตรฐาน และข้อกำหนดตามสัญญาที่เกี่ยวข้องกับหน่วยงาน ข้อมูล ระบบ และบริการคลาวด์นั้น โดยเฉพาะประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ตลอดจนข้อกำหนดด้านการคุ้มครองข้อมูล การบริหารความเสี่ยง และข้อผูกพันระหว่างผู้ใช้บริการและผู้ให้บริการ การปฏิบัติตามแนวทางในเอกสารนี้ไม่ควรตีความว่าเป็นการทดแทนกฎหมายหรือข้อกำหนดที่มีผลใช้บังคับ แต่เป็นแนวทางประกอบการดำเนินงานเพื่อช่วยให้หน่วยงานสามารถนำข้อกำหนดไปประยุกต์ใช้ได้อย่างเหมาะสมกับบริบทของตน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2.5 ข้อพิจารณาหรือหลักเกณฑ์สำคัญ

ในการนำแนวทางไปประยุกต์ใช้ หน่วยงานควรพิจารณาปัจจัยสำคัญ ได้แก่ รูปแบบบริการคลาวด์ (Cloud Service Model) ขอบเขตบริการ (Service Scope) ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ผลการประเมินความเสี่ยง ขอบเขตความรับผิดชอบร่วม ความสามารถและข้อจำกัดของบริการคลาวด์ รวมถึงข้อกำหนดทางกฎหมายและสัญญาที่เกี่ยวข้อง ทั้งนี้ มาตรการที่นำมาใช้ควรมีความเหมาะสมและได้สัดส่วนกับระดับความเสี่ยงและผลกระทบ โดยไม่ก่อให้เกิดภาระเกินความจำเป็น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

บทที่ 3 กระบวนการหรือแนวทางดำเนินการ

บทนี้นำเสนอข้อกำหนดและแนวทางการนำไปปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบริการคลาวด์ โดยจัดเรียงเนื้อหาตามลำดับและหมายเลขข้อกำหนดของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อให้สามารถเชื่อมโยงและอ้างอิงข้อกำหนดของมาตรฐานกับแนวทางการนำไปปฏิบัติได้อย่างชัดเจน ทั้งนี้ หมายเลขหัวข้อที่ปรากฏในบทนี้เป็นหมายเลขข้อกำหนดตามมาตรฐานดังกล่าว มิใช่หมายเลขหัวข้อย่อยของบทที่ 3

5.1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

การใช้บริการคลาวด์ทำให้ข้อมูล ระบบสารสนเทศ และทรัพย์สินขององค์กรอาจถูกจัดเก็บ ประมวลผล ส่งผ่าน สำรอง หรือบริหารจัดการบนโครงสร้างพื้นฐานที่อยู่นอกเหนือการควบคุมโดยตรงขององค์กร และอาจเกี่ยวข้องกับผู้ให้บริการคลาวด์ ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง ศูนย์ข้อมูล ตลอดจนประเทศและเขตอำนาจทางกฎหมายที่แตกต่างกัน

องค์กรจึงต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ต่อข้อมูลและทรัพย์สินอื่นขององค์กร โดยนโยบายควรกำหนดหลักการสำหรับการเลือกใช้ การกำกับดูแล การประเมินความเสี่ยง และการใช้มาตรการควบคุมที่เหมาะสมกับลักษณะของข้อมูล ระบบสารสนเทศ และบริการคลาวด์

การกำหนดนโยบายควรเชื่อมโยงกับ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ความอ่อนไหวของข้อมูล ความสำคัญต่อภารกิจ ปริมาณและการรวมศูนย์ของข้อมูล ตลอดจนผลกระทบที่อาจเกิดขึ้นต่อประชาชน การให้บริการสาธารณะ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือความมั่นคงของรัฐ เพื่อให้องค์กรสามารถกำหนดเงื่อนไขและระดับความเข้มงวดของการใช้บริการคลาวด์ได้อย่างเหมาะสม

สำหรับข้อมูลหรือระบบสารสนเทศที่มีความสำคัญหรืออาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญ การพิจารณาไม่ควรจำกัดเฉพาะผลกระทบด้านการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลแต่ละรายการ แต่ควรพิจารณาปัจจัยด้านปริมาณ การสะสม การรวมศูนย์ การเชื่อมโยง และความสามารถในการวิเคราะห์ข้อมูลร่วมกันด้วย เนื่องจากข้อมูลที่เมื่อพิจารณาเป็นรายรายการอาจมีผลกระทบจำกัด อาจก่อให้เกิดผลกระทบเพิ่มขึ้นอย่างมีนัยสำคัญเมื่อถูกรวบรวม สะสม หรือเชื่อมโยงกันในปริมาณมาก

ตัวอย่างข้อมูลหรือระบบที่ควรได้รับการพิจารณาเพิ่มเติมตามบริบทและผลการประเมิน ได้แก่ ระบบหรือข้อมูลที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ข้อมูลที่เกี่ยวข้องกับความมั่นคงของรัฐ ข้อมูลจากกล้องโทรทัศน์วงจรปิด (CCTV) ของพื้นที่สำคัญหรือหน่วยงานด้านความมั่นคง ข้อมูล CCTV ที่ใช้เทคโนโลยีรู้จำใบหน้าหรือชีวมิติ ฐานข้อมูลสุขภาพหรือเวชระเบียนจำนวนมาก ฐานข้อมูลส่วนบุคคลขนาดใหญ่ ตลอดจนข้อมูลจากยานยนต์ไฟฟ้าหรือยานยนต์เชื่อมต่อ (EV Data) เช่น ตำแหน่ง เส้นทาง เวลา และรูปแบบการเดินทาง ซึ่งเมื่อมีการรวบรวมอย่างต่อเนื่องอาจทำให้สามารถวิเคราะห์รูปแบบการเคลื่อนที่ของบุคคล ยานพาหนะ หรือหน่วยงานสำคัญได้

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น ห้ามนำไปอ้างอิง

ทั้งนี้ ตัวอย่างดังกล่าวมิได้หมายความว่าข้อมูลหรือระบบประเภทนั้นต้องถูกจัดเป็นระดับผลกระทบสูงโดยอัตโนมัติ แต่ควรนำลักษณะของข้อมูล ปริมาณ ระยะเวลาการสะสม ระดับการรวมศูนย์ ความสามารถในการเชื่อมโยง และผลกระทบที่อาจเกิดขึ้นมาประกอบการประเมินตามหลักเกณฑ์ที่เกี่ยวข้อง

นอกจากระดับผลกระทบแล้ว นโยบายควรคำนึงถึงตำแหน่งทางภูมิศาสตร์ของผู้ให้บริการคลาวด์ ประเทศที่ข้อมูลสามารถถูกจัดเก็บหรือประมวลผลได้ แม้เป็นการชั่วคราว เขตอำนาจทางกฎหมายที่เกี่ยวข้อง ตลอดจนความสามารถขององค์กรในการควบคุม เข้าถึง เคลื่อนย้าย กู้คืน หรือนำข้อมูลและบริการกลับมาใช้งานได้เมื่อเกิดเหตุการณ์ผิดปกติ ซึ่งเป็นองค์ประกอบสำคัญของการพิจารณาความเสี่ยงด้านอธิปไตยข้อมูล (Data Sovereignty) ตามบริบทขององค์กร

ทั้งนี้ การประเมินและจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศเป็นจุดเริ่มต้นสำคัญในการกำหนดข้อกำหนดขั้นต่ำและมาตรการควบคุมที่เกี่ยวข้องกับการใช้บริการคลาวด์ โดยข้อ 5.1.1 เป็นข้อกำหนดขั้นต่ำที่ใช้กับข้อมูลหรือระบบสารสนเทศทุกระดับผลกระทบ ขณะที่ข้อกำหนดด้านอื่นให้พิจารณาตามระดับผลกระทบและตารางข้อกำหนดขั้นต่ำท้ายประกาศ

สำหรับข้อมูลหรือระบบสารสนเทศที่ได้รับการจัดระดับผลกระทบเป็นระดับสูง ต้องดำเนินการตามข้อกำหนดส่วนที่ 1 และส่วนที่ 2 ทุกข้อ ซึ่งรวมถึงข้อ 5.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม โดยรายละเอียดเกี่ยวกับตำแหน่งของศูนย์ข้อมูลและการกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย ให้พิจารณาตามข้อ 5.2.5 โดยตรง

ดังนั้น ความสัมพันธ์ของข้อกำหนดสามารถสรุปได้ดังนี้

ข้อมูลหรือระบบสารสนเทศ ⟶ ประเมินความสำคัญและระดับผลกระทบ ⟶ กำหนดหลักการและเงื่อนไขตามนโยบาย 5.1.1 ⟶ กำหนดบทบาทและอำนาจการตัดสินใจตาม 5.1.2 ⟶ พิจารณากฎหมายและข้อกำหนดตาม 5.1.3 ⟶ นำข้อกำหนดขั้นต่ำตามระดับผลกระทบไปใช้กับมาตรการในข้อ 5.2

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของผู้ใช้บริการคลาวด์ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของผู้ใช้บริการคลาวด์ ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ขององค์กร	ก) ผู้ให้บริการคลาวด์ต้องเพิ่มนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์ โดยคำนึงถึงสิ่งต่อไปนี้ – ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์ – ความเสี่ยงจากบุคคลภายในที่ได้รับอนุญาต – การเช่าหลายรายและการแยก ผู้ใช้บริการคลาวด์ (รวมถึงการจำลองเสมือน) – การเข้าถึงทรัพย์สินของผู้ใช้บริการคลาวด์โดยเจ้าหน้าที่ของผู้ให้บริการคลาวด์

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ข) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับการประมวลผลบนคลาวด์ ผู้ใช้บริการคลาวด์ ต้องคำนึงถึงสิ่งต่อไปนี้ – ข้อมูลที่จัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงและการจัดการโดย ผู้ให้บริการคลาวด์ – ทรัพย์สินขององค์กรอาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชัน – กระบวนการต่าง ๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย – ผู้ใช้บริการคลาวด์และบริบทที่ใช้บริการคลาวด์ – ผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ที่ได้รับสิทธิพิเศษในการเข้าถึง – ตำแหน่งทางภูมิศาสตร์ขององค์กรของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ใช้บริการคลาวด์ ได้ (แม้จะเป็นการชั่วคราว) ค) นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการคลาวด์ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ใช้บริการคลาวด์ ง) ข้อตกลงทางสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง (Sub-contractors) และผู้ใช้บริการคลาวด์อย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaS หรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกันขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS	– ขั้นตอนการควบคุมการเข้าถึง เช่น การยืนยันตัวตนที่เข้มงวดสำหรับการเข้าถึงบริการคลาวด์ของผู้ดูแลระบบ – การสื่อสารกับผู้ใช้บริการคลาวด์ระหว่างการจัดการการเปลี่ยนแปลง – ความปลอดภัยของการจำลองเสมือน – การเข้าถึงและปกป้องข้อมูลของผู้ใช้บริการคลาวด์ – การจัดการวงจรชีวิตของบัญชีผู้ใช้บริการคลาวด์ – การสื่อสารกรณีเกิดเหตุละเมิดและแนวทางการแบ่งปันข้อมูลเพื่อช่วยในการสืบสวนและนิติเวช

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปที่ 1 กรอบการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์

ร่างเพื่อรับฟังความคิดเห็น Public Hearing

วัตถุประสงค์

1. เพื่อกำหนดกรอบและหลักการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้และระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

2. เพื่อให้องค์กรสามารถกำหนดเงื่อนไขในการเลือกใช้และกำกับดูแลบริการคลาวด์ให้เหมาะสมกับความสำคัญ ความอ่อนไหว ปริมาณ การรวมศูนย์ และลักษณะการใช้ข้อมูล

3. เพื่อสนับสนุนการประเมินและบริหารความเสี่ยงของข้อมูลหรือระบบสารสนเทศที่มีความสำคัญหรืออาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญ รวมถึงผลกระทบที่อาจเกิดจากการสะสม การรวมศูนย์ การเชื่อมโยง และการวิเคราะห์ข้อมูลจำนวนมาก

4. เพื่อให้องค์กรสามารถพิจารณาความเสี่ยงด้านสถานที่จัดเก็บและประมวลผลข้อมูล เขตอำนาจทางกฎหมาย อธิปไตยข้อมูล (Data Sovereignty) การพึ่งพาผู้ให้บริการ และความสามารถในการควบคุม เคลื่อนย้าย หรือกู้คืนข้อมูลและบริการได้อย่างเหมาะสม

5. เพื่อเชื่อมโยงการกำหนดนโยบายไปสู่การกำหนดบทบาทและอำนาจการตัดสินใจตามข้อ 5.1.2 การปฏิบัติตามกฎหมายและข้อกำหนดตามข้อ 5.1.3 และมาตรการควบคุมตามข้อ 5.2 ที่ใช้บังคับตามระดับผลกระทบ

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ โดยนโยบายดังกล่าวควรเชื่อมโยงกับนโยบายและกระบวนการบริหารความเสี่ยง การจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ การกำกับดูแลผู้ให้บริการ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่องค์กรมีอยู่ เพื่อให้การใช้บริการคลาวด์สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้

1. การกำหนดนโยบายสำหรับการใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ต่อข้อมูลและทรัพย์สินขององค์กร ตามข้อกำหนด 5.1.1 ของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

นโยบายควรครอบคลุมอย่างน้อยในเรื่องต่อไปนี้

1.1 การอนุญาตและเงื่อนไขในการนำข้อมูลหรือระบบสารสนเทศขึ้นใช้บริการคลาวด์

1.2 การประเมินความเสี่ยงและระดับผลกระทบก่อนใช้บริการคลาวด์

1.3 การพิจารณาความสำคัญและความอ่อนไหวของข้อมูล

1.4 การคุ้มครองข้อมูลและทรัพย์สินขององค์กร

1.5 การกำหนดขอบเขตความรับผิดชอบระหว่าง CSC และ CSP

1.6 การพิจารณาสถานที่จัดเก็บ ประมวลผล สำรอง และถ่ายโอนข้อมูล

1.7 การพิจารณาประเทศและเขตอำนาจทางกฎหมายที่เกี่ยวข้องกับบริการและข้อมูล

1.8 การบริหารความเสี่ยงด้านอธิปไตยข้อมูล

1.9 การกำกับดูแลผู้ให้บริการภายนอกและผู้รับจ้างช่วง

1.10 การบริหารการเปลี่ยนแปลง การย้ายบริการ และการยุติการใช้บริการคลาวด์

รายละเอียดมาตรการควบคุมเฉพาะด้าน เช่น การควบคุมการเข้าถึง การเข้ารหัส การจัดการกุญแจ การสำรองข้อมูล การบันทึกเหตุการณ์ และตำแหน่งศูนย์ข้อมูล ให้ดำเนินการตามข้อกำหนดเฉพาะในหัวข้อที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดรายละเอียดซ้ำไว้ในนโยบายนี้

2. การกำหนดแนวทางตามระดับความเสี่ยง ผู้ใช้บริการคลาวด์ควรใช้แนวทางตามระดับความเสี่ยงในการกำหนดเงื่อนไขและมาตรการสำหรับการใช้บริการคลาวด์ โดยพิจารณาร่วมกันจากลักษณะของข้อมูลระบบสารสนเทศ ประเภทบริการคลาวด์ ภัยคุกคาม ช่องโหว่ และผลกระทบที่อาจเกิดขึ้น

มาตรการสำหรับข้อมูลและระบบสารสนเทศแต่ละประเภทไม่จำเป็นต้องอยู่ในระดับเดียวกัน แต่ควรเพิ่มความเข้มงวดตามระดับผลกระทบ ความอ่อนไหว ความสำคัญต่อภารกิจ และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย

ประกาศมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศกำหนดให้พิจารณาวัตถุประสงค์ด้านการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน และจัดระดับผลกระทบเป็นระดับต่ำ ระดับกลาง และระดับสูง โดยคำนึงถึงผลกระทบด้านการเงินหรือทรัพย์สิน จำนวนผู้ได้รับผลกระทบ ความสามารถในการดำเนินภารกิจ และความมั่นคงหรือความสงบเรียบร้อยภายในประเทศ

ร่างสำหรับ Public Hearing ยกร่าง - ห้ามอ้างอิง

3. การพิจารณาความสำคัญและระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ก่อนนำข้อมูลหรือระบบสารสนเทศไปจัดเก็บ ประมวลผล หรือให้บริการผ่านระบบคลาวด์ ผู้ใช้บริการคลาวด์ควรประเมินความสำคัญ ความอ่อนไหว และระดับผลกระทบของข้อมูลหรือระบบสารสนเทศนั้น

การประเมินควรพิจารณาอย่างน้อยในมิติต่อไปนี้

3.1 ผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

3.2 ผลกระทบจากการแก้ไข ทำลาย หรือสูญเสียความถูกต้องของข้อมูล

3.3 ผลกระทบจากการไม่สามารถเข้าถึงข้อมูลหรือระบบได้

3.4 ผลกระทบต่อภารกิจและการให้บริการของหน่วยงาน

3.5 ผลกระทบต่อประชาชนหรือผู้ใช้บริการ

3.6 ผลกระทบต่อความเป็นส่วนตัว

3.7 ผลกระทบต่อความปลอดภัยของบุคคลและสาธารณะ

3.8 ผลกระทบต่อความมั่นคงของรัฐหรือความสงบเรียบร้อยภายในประเทศ

แนวทางดังกล่าวสอดคล้องกับหลักเกณฑ์การจัดระดับผลกระทบตามประกาศ พ.ศ. 2566

ร่าง ห้ามใช้อ้างอิง



รูปที่ 2 แนวทางการกำกับดูแลข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูงและความเสี่ยงด้านอธิปไตยข้อมูลข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง

สำหรับข้อมูลหรือระบบสารสนเทศที่ได้รับการประเมินว่ามีผลกระทบสูง หรือมีความสำคัญต่อภารกิจ ผู้ใช้บริการคลาวด์ควรพิจารณาเพิ่มเติมอย่างน้อยในเรื่องต่อไปนี้

- ความเหมาะสมของรูปแบบและประเภทบริการคลาวด์
- ความสามารถในการควบคุมการเข้าถึงข้อมูล
- ความสามารถในการรักษาความพร้อมใช้งานและความต่อเนื่องของบริการ
- สถานที่จัดเก็บ ประมวลผล สำรอง และถ่ายโอนข้อมูล
- ประเทศและเขตอำนาจทางกฎหมายที่เกี่ยวข้อง
- ความสามารถขององค์กรในการควบคุมและเรียกคืนข้อมูล
- ความสามารถในการย้ายข้อมูลหรือระบบไปยังสภาพแวดล้อมอื่น
- การพึ่งพา CSP ผู้ให้บริการภายนอก หรือผู้รับจ้างช่วง
- ผลกระทบกรณี CSP หรือบริการจากต่างประเทศไม่สามารถให้บริการได้
- ความจำเป็นในการกำหนดมาตรการเพิ่มเติมตามระดับความเสี่ยง

4. การจัดการความเสี่ยงด้านอธิปไตยข้อมูล ผู้ใช้บริการคลาวด์ควรประเมินความเสี่ยงด้านอธิปไตยข้อมูลโดยเฉพาะกรณีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง มีความสำคัญต่อภารกิจ เกี่ยวข้องกับความมั่นคง หรือ CII หรือเป็นข้อมูลที่มีความอ่อนไหวในปริมาณมาก

การประเมินควรครอบคลุมวงจรของข้อมูลทั้งการจัดเก็บ การประมวลผล การสำรอง การถ่ายโอน และการเข้าถึงจากระยะไกล รวมถึงพิจารณาประเทศและเขตอำนาจทางกฎหมายของ CSP และผู้รับจ้างช่วงที่สามารถเข้าถึงข้อมูลได้

การพิจารณาอธิปไตยข้อมูลไม่ควรจำกัดเฉพาะคำถามว่า “ข้อมูลอยู่ที่ใด” แต่ควรพิจารณาด้วยว่า “ผู้ใดสามารถควบคุมหรือเข้าถึงข้อมูลได้” “ข้อมูลอยู่ภายใต้กฎหมายของประเทศใด” และ “องค์กรยังสามารถควบคุม เข้าถึง ย้าย หรือกู้คืนข้อมูลและบริการได้หรือไม่เมื่อเกิดเหตุการณ์ผิดปกติ”

มาตรฐานคลาวด์กำหนดให้ CSC คำนึงถึงตำแหน่งทางภูมิศาสตร์ของ CSP และประเทศที่ CSP สามารถจัดเก็บข้อมูลได้ แม้เป็นการชั่วคราว และในหัวข้อ Compliance ยังกำหนดให้พิจารณาว่าบริการอาจอยู่ภายใต้กฎหมายของเขตอำนาจที่ควบคุม CSP นอกเหนือจากกฎหมายที่ควบคุม CSC

4.1 การพิจารณาสถานที่จัดเก็บและประมวลผลข้อมูล สำหรับข้อมูลหรือระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูง ผู้ใช้บริการคลาวด์ควรพิจารณาว่ามีความจำเป็นต้องกำหนดเงื่อนไขให้ข้อมูลหรือกระบวนการประมวลผลบางส่วนอยู่ภายในประเทศไทยหรือไม่ โดยพิจารณาจาก

4.1.1 ระดับผลกระทบของข้อมูลหรือระบบ
4.1.2 ความอ่อนไหวของข้อมูล
4.1.3 ความสำคัญต่อภารกิจหรือบริการสาธารณะ
4.1.4 ปริมาณและระดับการรวมศูนย์ของข้อมูล
4.1.5 ความสามารถในการเชื่อมโยงข้อมูลเพื่อวิเคราะห์บุคคล พฤติกรรม ตำแหน่ง หรือกิจกรรม
4.1.6 ผลกระทบต่อ CII
4.1.7 ผลกระทบต่อความมั่นคงของรัฐ

ร่างสำหรับการรับฟังความคิดเห็นสาธารณะ (Public Hearing) เท่านั้น ห้ามใช้อ้างอิง

4.1.8 กฎหมายหรือข้อกำหนดเฉพาะที่เกี่ยวข้อง

4.1.9 ความเสี่ยงจากเขตอำนาจทางกฎหมายต่างประเทศ

4.1.10 ความสามารถในการควบคุม เข้าถึง เคลื่อนย้าย และกู้คืนข้อมูล

ทั้งนี้ การกำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูลต้องพิจารณาตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ประกอบกับกฎหมาย มาตรฐาน ประกาศ และข้อกำหนดอื่นที่เกี่ยวข้อง โดยไม่ควรกำหนดเงื่อนไขเดียวกันสำหรับข้อมูลทุกประเภท เว้นแต่มีข้อกำหนดที่ใช้บังคับโดยตรง

สำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง ซึ่งต้องดำเนินการตามข้อกำหนดส่วนที่ 2 ทุกข้อ ข้อ 5.2.5.1 กำหนดให้ CSC ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย และกำหนดให้ CSP ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย ส่วนศูนย์ข้อมูลสำรองให้เป็นไปตามเงื่อนไขที่ข้อ 5.2.5.1 กำหนด

ดังนั้น ข้อ 5.1.1 ทำหน้าที่กำหนดหลักการเชิงนโยบายในการประเมินความจำเป็นด้านสถานที่จัดเก็บและประมวลผล อธิปไตยข้อมูล และเขตอำนาจทางกฎหมาย ส่วนข้อกำหนดเฉพาะด้านตำแหน่งศูนย์ข้อมูลให้พิจารณาตามข้อ 5.2.5.1

4.2 การพิจารณาผลกระทบจากปริมาณและการรวมข้อมูล การประเมินความสำคัญของข้อมูลไม่ควรพิจารณาเฉพาะข้อมูลแต่ละระเบียนหรือแต่ละรายการ แต่ควรพิจารณาผลกระทบที่เกิดจากการรวบรวมข้อมูลจำนวนมาก การรวมศูนย์ข้อมูล การเชื่อมโยงข้อมูลจากหลายแหล่ง และความสามารถในการวิเคราะห์ข้อมูลร่วมกัน

ข้อมูลที่เมื่อพิจารณาแยกเป็นรายรายการอาจมีผลกระทบไม่สูง สามารถมีระดับความเสี่ยงเพิ่มขึ้นอย่างมีนัยสำคัญเมื่อมีการสะสมเป็นระยะเวลานานหรือรวมกันเป็นฐานข้อมูลขนาดใหญ่ เนื่องจากอาจทำให้สามารถระบุตัวบุคคล วิเคราะห์พฤติกรรม ติดตามตำแหน่งหรือการเคลื่อนที่ วิเคราะห์ความสัมพันธ์ หรือค้นหารูปแบบกิจกรรมที่ไม่สามารถทราบได้จากข้อมูลแต่ละรายการ

ดังนั้น ผู้ใช้บริการคลาวด์ควรนำ ปริมาณ การรวมศูนย์ ระยะเวลาการสะสม ความสามารถในการเชื่อมโยง และศักยภาพในการวิเคราะห์ข้อมูล มาเป็นปัจจัยประกอบการกำหนดนโยบายและเงื่อนไขการใช้บริการคลาวด์ด้วย

4.3 ตัวอย่างข้อมูลหรือระบบที่ควรได้รับการพิจารณาเป็นกรณีพิเศษ ตัวอย่างต่อไปนี้เป็นกลุ่มข้อมูลหรือระบบที่ควรได้รับการพิจารณาความสำคัญ ผลกระทบ และความเสี่ยงเพิ่มเติมตามบริบท มิได้หมายความว่าข้อมูลหรือระบบดังกล่าวต้องถูกจัดเป็นระดับผลกระทบสูงโดยอัตโนมัติ หรือจำเป็นต้องจัดเก็บภายในประเทศไทยทุกกรณี การกำหนดระดับผลกระทบและข้อกำหนดที่ใช้บังคับให้เป็นไปตามประกาศและหลักเกณฑ์ที่เกี่ยวข้อง

ตัวอย่างข้อมูลหรือระบบ	ลักษณะความสำคัญและความเสี่ยง	เหตุผลที่ควรพิจารณาเป็นกรณีพิเศษ
ระบบและข้อมูลของหน่วยงาน CII	การหยุดชะงักหรือการถูกควบคุมอาจกระทบต่อบริการสำคัญ ประชาชน เศรษฐกิจ หรือความมั่นคง	ควรลดความเสี่ยงจากการพึ่งพาผู้ให้บริการหรือเขตอำนาจเดียว และรักษาความสามารถในการควบคุมและกู้คืนบริการ

เอกสารเผยแพร่ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ระบบควบคุมหรือข้อมูลที่เกี่ยวข้องกับ CII	อาจเปิดเผยโครงสร้าง การทำงาน จุดเชื่อมต่อ หรือรูปแบบการดำเนินงานของระบบสำคัญ	การเปิดเผยหรือถูกแก้ไขอาจสนับสนุนการโจมตีหรือทำให้บริการสำคัญหยุดชะงัก
CCTV ของหน่วยงานด้านความมั่นคงหรือพื้นที่สำคัญ	ข้อมูลจำนวนมากอาจเปิดเผยตำแหน่ง รูปแบบการรักษาความปลอดภัย การเข้าออก หรือการเคลื่อนที่	การรวมข้อมูลต่อเนื่องอาจทำให้สามารถวิเคราะห์รูปแบบการปฏิบัติงานหรือจุดที่มีความสำคัญด้านความมั่นคง
CCTV ที่ใช้การรู้จำใบหน้าหรือชีวมิติ	มีความสามารถในการระบุตัวบุคคลและอาจเกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว	ผลกระทบจากการรั่วไหลหรือการนำไปใช้ผิดวัตถุประสงค์สูงกว่าภาพ CCTV ทั่วไป
ฐานข้อมูลสุขภาพหรือเวชระเบียนจำนวนมาก	มีความอ่อนไหวสูงและเกี่ยวข้องกับประชาชนจำนวนมาก	การรวมศูนย์ข้อมูลทำให้ผลกระทบจากการรั่วไหล การเข้าถึงโดยมิชอบ หรือการสูญเสียการควบคุมเพิ่มสูงขึ้น
ข้อมูลยานยนต์ไฟฟ้าและยานยนต์เชื่อมต่อ (EV Data)	อาจประกอบด้วยตำแหน่ง เส้นทาง เวลา จุดชาร์จ และพฤติกรรมการเดินทาง	ข้อมูลสะสมสามารถใช้วิเคราะห์ตำแหน่งและรูปแบบการเคลื่อนที่ของบุคคล ยานพาหนะ หรือกลุ่มผู้ใช้งาน
ข้อมูลตำแหน่งของยานพาหนะหรือบุคลากรของหน่วยงานด้านความมั่นคง	สามารถสะท้อนตำแหน่ง เส้นทาง ฐานปฏิบัติการ หรือรูปแบบกิจกรรม	การวิเคราะห์ข้อมูลต่อเนื่องอาจเปิดเผยข้อมูลที่มีผลต่อการปฏิบัติภารกิจและความมั่นคง
ฐานข้อมูลส่วนบุคคลขนาดใหญ่	ผลกระทบอาจขยายจากระดับบุคคลไปสู่ประชาชนจำนวนมาก	ควรพิจารณาทั้งความอ่อนไหว จำนวนเจ้าของข้อมูล และความสามารถในการเชื่อมโยงข้อมูล
ข้อมูลจากหลายแหล่งที่สามารถเชื่อมโยงกันได้	ข้อมูลแต่ละชุดอาจไม่อ่อนไหว แต่เมื่อนำมารวมกันอาจสร้างข้อมูลใหม่ที่มีความอ่อนไหวสูงขึ้น	ควรประเมินผลกระทบจากการอนุมานและการวิเคราะห์ข้อมูลร่วมกัน ไม่ใช่พิจารณาเฉพาะข้อมูลต้นทาง

หมายเหตุ: ตัวอย่างข้างต้นมิได้หมายความว่าข้อมูลทุกประเภทต้องถูกจัดเก็บหรือประมวลผลภายในประเทศไทยโดยอัตโนมัติ แต่เป็นกลุ่มข้อมูลที่ควรได้รับการประเมินความจำเป็นด้านสถานที่จัดเก็บ การประมวลผล อธิปไตยข้อมูล และเขตอำนาจทางกฎหมายเป็นกรณีพิเศษ

ตัวอย่างการพิจารณา: CCTV ของหน่วยงานด้านความมั่นคง ภาพจากกล้อง CCTV เพียงกล้องเดียวและในช่วงเวลาสั้นอาจมีผลกระทบจำกัด อย่างไรก็ตาม หากมีการรวบรวมภาพจากกล้องจำนวนมากอย่างต่อเนื่อง อาจสามารถวิเคราะห์ตำแหน่งกล้อง จุดเข้าออก รูปแบบการเคลื่อนที่ของบุคลากร ช่วงเวลาปฏิบัติงาน หรือรูปแบบกิจกรรมของพื้นที่ได้

ร่างสำหรับ Public Hearing เท่านั้น - ยังไม่ใช่ฉบับจริง

หากเป็น CCTV ของพื้นที่ด้านความมั่นคงหรือพื้นที่ CII ผลกระทบจากการรวมข้อมูลอาจสูงกว่าการพิจารณาภาพแต่ละรายการ ดังนั้น หน่วยงานควรประเมินทั้งความอ่อนไหวของข้อมูล ปริมาณข้อมูล ระยะเวลาการจัดเก็บ และความสามารถในการวิเคราะห์ข้อมูลร่วมกัน ก่อนกำหนดรูปแบบบริการคลาวด์และสถานที่จัดเก็บข้อมูล

ตัวอย่างการพิจารณา: ข้อมูล EV ข้อมูลจากยานยนต์ไฟฟ้าหรือยานยนต์เชื่อมต่ออาจประกอบด้วยข้อมูลตำแหน่ง เวลา เส้นทางการเดินทาง จุดชาร์จ สถานะของยานพาหนะ และพฤติกรรมการใช้งาน

ข้อมูลตำแหน่งเพียงครั้งเดียวอาจมีผลกระทบจำกัด แต่เมื่อมีการเก็บข้อมูลต่อเนื่องสามารถนำมาวิเคราะห์รูปแบบการเดินทาง สถานที่ที่เดินทางเป็นประจำ ตำแหน่งของบุคคลหรือยานพาหนะ และรูปแบบการเคลื่อนที่ในพื้นที่ต่าง ๆ ได้ ดังนั้น หากมีการรวบรวม EV Data ในปริมาณมากหรือในระดับที่สามารถสะท้อนรูปแบบการเคลื่อนที่ของประชาชนหรือโครงสร้างการคมนาคม หน่วยงานควรประเมินความเสี่ยงด้านความเป็นส่วนตัว ความมั่นคง อธิปไตยข้อมูล และความจำเป็นในการกำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูลเป็นกรณีพิเศษ

5. การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลที่มีความอ่อนไหว ผู้ใช้บริการคลาวด์ควรกำหนดนโยบายและเงื่อนไขสำหรับการนำข้อมูลส่วนบุคคลและข้อมูลที่มีความอ่อนไหวไปประมวลผลบนคลาวด์ให้เหมาะสมกับลักษณะ ปริมาณ วัตถุประสงค์การประมวลผล และผลกระทบที่อาจเกิดขึ้น

มาตรฐานคลาวด์กำหนดว่ากรณีเป็นข้อมูลส่วนบุคคลต้องจัดระดับผลกระทบด้านการรักษาความลับเป็นระดับกลางอย่างน้อย และข้อ 5.1.1 กำหนดให้นโยบายคุ้มครองข้อมูลส่วนบุคคลของ CSC ระบุข้อตกลงทางสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ รวมถึงกำหนดความรับผิดชอบระหว่างผู้ประมวลผล ผู้รับจ้างช่วง และ CSC ให้ชัดเจน

สำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือข้อมูลส่วนบุคคลจำนวนมาก ควรพิจารณาเพิ่มเติมถึงสถานที่ประมวลผลและจัดเก็บ การถ่ายโอนข้อมูล การเข้าถึงจากต่างประเทศ ผู้รับจ้างช่วง และผลกระทบจากการรวมข้อมูลหรือการเชื่อมโยงข้อมูลหลายแหล่ง

6. การกำหนดความรับผิดชอบร่วมระหว่างผู้ใช้บริการและผู้ให้บริการคลาวด์ ผู้ใช้บริการคลาวด์ควรกำหนดขอบเขตความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศระหว่าง CSC และ CSP ให้ชัดเจน โดยพิจารณาตามประเภทบริการคลาวด์และองค์ประกอบของระบบที่แต่ละฝ่ายรับผิดชอบ

ความรับผิดชอบอาจแตกต่างกันระหว่าง IaaS, PaaS และ SaaS ดังนั้น การใช้บริการคลาวด์ไม่ควรถูกตีความว่าเป็นการโอนความรับผิดชอบด้านความมั่นคงปลอดภัยหรือการปฏิบัติตามกฎหมายทั้งหมดไปยัง CSP

มาตรฐานคลาวด์กำหนดให้ข้อตกลงทางสัญญาระบุความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง และ CSC อย่างชัดเจน โดยคำนึงถึงประเภทของบริการคลาวด์

7. การกำกับดูแลผู้ให้บริการภายนอกและผู้รับจ้างช่วง ผู้ใช้บริการคลาวด์ควรพิจารณาความเสี่ยงที่เกิดจากผู้ให้บริการภายนอกและผู้รับจ้างช่วงที่เกี่ยวข้องกับการจัดเก็บ ประมวลผล ส่งผ่าน สำรอง หรือสนับสนุนการให้บริการข้อมูลขององค์กร

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งาน

สำหรับข้อมูลหรือระบบที่มีผลกระทบสูง ควรพิจารณาอย่างน้อยถึง

7.1 ผู้ให้บริการและผู้รับจ้างช่วงที่สามารถเข้าถึงข้อมูล

7.2 ประเทศที่ผู้ให้บริการและผู้รับจ้างช่วงดำเนินงาน

7.3 สถานที่จัดเก็บและประมวลผลข้อมูล

7.4 เขตอำนาจทางกฎหมายที่เกี่ยวข้อง

7.5 การเปลี่ยนแปลงผู้ให้บริการหรือสถานที่ประมวลผล

7.6 ความเสี่ยงจากการพึ่งพาห่วงโซ่อุปทาน

7.7 ความสามารถในการย้ายข้อมูลหรือบริการเมื่อจำเป็น

8. การทบทวนและปรับปรุงนโยบาย ผู้ใช้บริการคลาวด์ควรทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์อย่างสม่ำเสมอ และเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น

8.1 การเปลี่ยนประเภทหรือรูปแบบบริการคลาวด์

8.2 การเปลี่ยน CSP หรือผู้รับจ้างช่วง

8.3 การเปลี่ยนประเทศหรือสถานที่จัดเก็บและประมวลผลข้อมูล

8.4 การนำข้อมูลประเภทใหม่ขึ้นสู่ระบบคลาวด์

8.5 การเปลี่ยนแปลงระดับผลกระทบหรือความอ่อนไหวของข้อมูล

8.6 การเพิ่มขึ้นอย่างมีนัยสำคัญของปริมาณหรือการรวมศูนย์ข้อมูล

8.7 การเปลี่ยนแปลงกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

8.8 การเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีนัยสำคัญ

8.9 การเปลี่ยนแปลงภารกิจหรือความสำคัญของระบบต่อองค์กร

ผลการทบทวนควรนำมาใช้ปรับปรุงนโยบาย เงื่อนไขการใช้บริการ การประเมินความเสี่ยง และมาตรการควบคุมที่เกี่ยวข้องให้เหมาะสมกับสภาพแวดล้อมและระดับความเสี่ยงที่เปลี่ยนแปลงไป

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ต้องกำหนดหรือเพิ่มเติมนโยบายด้านความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมการจัดหา การออกแบบ การให้บริการ การใช้งาน การเปลี่ยนแปลง การบำรุงรักษา และการยุติบริการคลาวด์ โดยนโยบายต้องคำนึงถึงข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศและความเสี่ยงที่เกิดจากลักษณะเฉพาะของบริการคลาวด์

ตามข้อ 5.1.1 ของประกาศ นโยบายของ CSP ต้องคำนึงถึงอย่างน้อยประเด็นต่อไปนี้

- ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์
- ความเสี่ยงจากบุคคลภายในที่ได้รับอนุญาต
- การใช้ทรัพยากรร่วมกัน การมีผู้ใช้บริการหลายราย และการแยกผู้ใช้บริการ รวมถึงการจำลองเสมือน
- การเข้าถึงทรัพย์สินของ CSC โดยเจ้าหน้าที่ของ CSP
- การควบคุมการเข้าถึงสำหรับผู้ดูแลระบบ รวมถึงการยืนยันตัวตนที่เข้มงวด
- การสื่อสารกับ CSC ระหว่างการจัดการการเปลี่ยนแปลง
- ความมั่นคงปลอดภัยของการจำลองเสมือน

ร่างประกาศ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

- การเข้าถึงและการปกป้องข้อมูลของ CSC
- การจัดการวงจรชีวิตของบัญชีผู้ใช้บริการคลาวด์
- การสื่อสารเมื่อเกิดเหตุละเมิด และการแบ่งปันข้อมูลที่จำเป็นเพื่อสนับสนุนการสืบสวนและนิติวิทยาศาสตร์ดิจิทัล

สำหรับบริการที่รองรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง หรือข้อมูลที่มีลักษณะ ปริมาณ หรือการรวมศูนย์ซึ่งอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญ เช่น ระบบหรือข้อมูลที่เกี่ยวข้องกับ CII ข้อมูลด้านความมั่นคง ฐานข้อมูลสุขภาพจำนวนมาก ข้อมูล CCTV ของพื้นที่สำคัญ หรือข้อมูล EV และข้อมูลตำแหน่งจำนวนมาก CSP ควรสามารถให้ข้อมูลเกี่ยวกับความสามารถและข้อจำกัดของบริการได้เพียงพอให้ CSC ใช้ประกอบการประเมินและกำหนดมาตรการตามข้อกำหนดที่เกี่ยวข้อง โดยไม่จำเป็นต้องเปิดเผยรายละเอียดภายในที่อาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัยของบริการ

1. การกำหนดนโยบายด้านความมั่นคงปลอดภัยสำหรับการให้บริการคลาวด์ นโยบายของ CSP ควรกำหนดหลักการและแนวทางสำหรับการนำข้อกำหนดข้างต้นไปปฏิบัติ และเชื่อมโยงไปยังมาตรการควบคุมเฉพาะด้านตามข้อ 5.2 ที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดรายละเอียดทางเทคนิคทั้งหมดซ้ำไว้ในนโยบาย

2. การรองรับข้อกำหนดตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ผู้ให้บริการคลาวด์ควรสามารถรองรับข้อกำหนดด้านความมั่นคงปลอดภัยที่แตกต่างกันตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศของ CSC

การให้บริการแก่ระบบหรือข้อมูลที่มีผลกระทบสูงควรพิจารณาความสามารถของบริการอย่างน้อยต่อไปนี้

2.1 การแยกข้อมูลและทรัพยากร
2.2 การจำกัดและตรวจสอบสิทธิการเข้าถึง
2.3 การเข้ารหัสและการบริหารกุญแจ
2.4 การบันทึกและตรวจสอบเหตุการณ์
2.5 การสำรองและกู้คืนข้อมูล
2.6 ความต่อเนื่องและความพร้อมใช้งานของบริการ
2.7 สถานที่จัดเก็บและประมวลผลข้อมูล
2.8 การสนับสนุนการย้ายหรือกู้คืนระบบ
2.9 การแจ้งเหตุการณ์และการสนับสนุนหลักฐาน
2.10 การจัดการผู้รับจ้างช่วงและห่วงโซ่อุปทาน

มาตรฐานคลาวด์กำหนดข้อกำหนดขั้นต่ำและรูปแบบการตรวจรับรองแตกต่างกันตามระดับผลกระทบต่ำ กลาง และสูง และสำหรับระดับสูงกำหนดให้ผู้ให้บริการได้รับการรับรองที่เกี่ยวข้องกับความมั่นคงปลอดภัยคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระดับที่สูงขึ้น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งาน

3. การแจ้งสถานที่จัดเก็บและประมวลผลข้อมูล ผู้ให้บริการคลาวด์ควรแจ้งข้อมูลเกี่ยวกับตำแหน่งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของ CSP และประเทศที่สามารถจัดเก็บข้อมูลของ CSC ได้ตามข้อ 5.1.2.2 รวมถึงให้ข้อมูลเพิ่มเติมเกี่ยวกับสถานที่จัดเก็บ ประมวลผล สำรอง หรือถ่ายโอนข้อมูลตามขอบเขตบริการและข้อกำหนดที่เกี่ยวข้อง เพื่อให้ CSC สามารถใช้ประกอบการประเมินความเสี่ยง เขตอำนาจทางกฎหมาย และอธิปไตยข้อมูลได้อย่างเหมาะสม

ข้อมูลดังกล่าวควรมีความชัดเจนเพียงพอให้ CSC สามารถประเมินความเสี่ยงด้านอธิปไตยข้อมูล เขตอำนาจทางกฎหมาย และความสอดคล้องกับข้อกำหนดเฉพาะของข้อมูลหรือระบบที่มีผลกระทบสูง

มาตรฐานกำหนดให้ CSP แจ้ง CSC ถึงที่ตั้งทางภูมิศาสตร์ขององค์กรและประเทศที่สามารถจัดเก็บข้อมูลของ CSC ได้ และกำหนดเรื่องตำแหน่งศูนย์ข้อมูลไว้โดยเฉพาะในข้อ 5.2.5.1

หากมีการเปลี่ยนแปลงสถานที่จัดเก็บหรือประมวลผลข้อมูลที่อาจส่งผลต่อข้อกำหนดด้านความมั่นคงปลอดภัย กฎหมาย หรืออธิปไตยข้อมูล CSP ควรแจ้ง CSC ตามเงื่อนไขที่กำหนดไว้ในสัญญาหรือข้อตกลง

สำหรับข้อมูลหรือระบบที่มีผลกระทบสูง การเปลี่ยนแปลงดังกล่าวควรได้รับการประเมินผลกระทบก่อนดำเนินการตามความเหมาะสม

4. การสนับสนุนการบริหารความเสี่ยงด้านอธิปไตยข้อมูล ผู้ให้บริการคลาวด์ควรให้ข้อมูลที่เพียงพอแก่ CSC เพื่อใช้ประเมินความเสี่ยงด้านอธิปไตยข้อมูล โดยอย่างน้อยควรสามารถระบุได้ว่า

4.1 ข้อมูลถูกจัดเก็บและประมวลผลในประเทศหรือภูมิภาคใด

4.2 มีผู้รับจ้างช่วงรายใดเกี่ยวข้องกับการประมวลผลข้อมูล

4.3 ผู้ให้บริการหรือผู้รับจ้างช่วงอยู่ภายใต้เขตอำนาจทางกฎหมายใด

4.4 บุคลากรของ CSP หรือผู้รับจ้างช่วงสามารถเข้าถึงข้อมูลจากประเทศใดได้บ้าง

4.5 มีข้อจำกัดใดในการกำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูล

4.6 มีความสามารถใดที่ช่วยให้ CSC ควบคุมข้อมูล กุญแจเข้ารหัส การสำรอง หรือการย้ายข้อมูลได้

4.7 มีเงื่อนไขใดที่อาจทำให้ข้อมูลหรือบริการได้รับผลกระทบจากคำสั่งหรือข้อกำหนดทางกฎหมายของต่างประเทศ

5. การรักษาความสามารถของ CSC ในการควบคุมข้อมูล สำหรับข้อมูลหรือระบบที่มีผลกระทบสูง CSP ควรสนับสนุนให้ CSC สามารถรักษาการควบคุมข้อมูลได้ในระดับที่เหมาะสมกับความเสี่ยง เช่น

5.1 การควบคุมสิทธิการเข้าถึง

5.2 การเข้ารหัสข้อมูล

5.3 การจัดการกุญแจเข้ารหัส

5.4 การบันทึกและตรวจสอบการเข้าถึง

5.5 การส่งออกหรือโอนย้ายข้อมูล

5.6 การสำรองและกู้คืนข้อมูล

5.7 การลบหรือทำลายข้อมูลเมื่อสิ้นสุดบริการ

ทั้งนี้ รายละเอียดทางเทคนิคของมาตรการดังกล่าวให้เป็นไปตามข้อกำหนดเฉพาะในหัวข้อที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

6. การคุ้มครองข้อมูลที่มีความอ่อนไหวและข้อมูลจำนวนมาก ผู้ให้บริการคลาวด์ควรกำหนดมาตรการและความสามารถของบริการให้เหมาะสมกับลักษณะและปริมาณของข้อมูลที่ CSC นำมาประมวลผล

กรณีที่บริการรองรับข้อมูลที่มีความอ่อนไหว ข้อมูลส่วนบุคคล หรือข้อมูลจำนวนมากที่สามารถนำมาเชื่อมโยงหรือวิเคราะห์ร่วมกัน CSP ควรพิจารณาความเสี่ยงที่เพิ่มขึ้นจากการรวมศูนย์ข้อมูลและการเข้าถึงข้อมูลในวงกว้าง

ในกรณีที่ CSP ทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล ควรกำหนดบทบาทและความรับผิดชอบตามข้อตกลงทางสัญญา และสนับสนุนให้ CSC สามารถปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม

ตัวอย่างข้อมูลที่ควรได้รับการพิจารณาเป็นพิเศษ

ตัวอย่างข้อมูล	ประเด็นที่ CSP ควรสามารถรองรับ
ข้อมูลสุขภาพหรือเวชระเบียนจำนวนมาก	การจำกัดสิทธิ การเข้ารหัส การบันทึกการเข้าถึง การกำหนดสถานที่ประมวลผล และการสนับสนุนการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัว
CCTV ที่ใช้การรู้จำใบหน้า	การคุ้มครองข้อมูลชีวมิติ การจำกัดการเข้าถึง การกำหนดระยะเวลาเก็บรักษา และการควบคุมสถานที่ประมวลผล
CCTV ของหน่วยงานด้านความมั่นคงหรือพื้นที่สำคัญ	การจำกัดการเข้าถึง การควบคุมการส่งออกข้อมูล การบันทึกการเข้าถึง และการกำหนดสถานที่จัดเก็บตามข้อกำหนดของ CSC
EV Data หรือข้อมูลยานยนต์เชื่อมต่อ	การควบคุมข้อมูลตำแหน่งและเส้นทาง การจำกัดการเข้าถึง การจัดการข้อมูลจำนวนมาก และการรองรับข้อกำหนดด้าน Data Localization ตามความจำเป็น
ข้อมูลหรือระบบของหน่วยงาน CII	การรองรับมาตรการควบคุมที่เข้มงวดขึ้น ความต่อเนื่อง การกู้คืน การตรวจสอบ และข้อกำหนดด้านสถานที่จัดเก็บข้อมูล

อ้างอิงตาม AI Security Guidelines ที่ระบุว่าข้อมูล CCTV ที่มีการรู้จำใบหน้าอาจเกี่ยวข้องกับข้อมูลชีวมิติ และข้อมูลจากยานยนต์ไฟฟ้าอาจประกอบด้วยตำแหน่งทางภูมิศาสตร์ เส้นทาง และพฤติกรรมการเดินทาง ควรพิจารณามาตรการด้านสถานที่จัดเก็บ การประมวลผล และอธิปไตยข้อมูลเพิ่มเติมตามความเสี่ยง

7. การควบคุมการเข้าถึงของบุคลากรและผู้ดูแลระบบ ผู้ให้บริการคลาวด์ควรกำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบของ CSC โดยบุคลากรของ CSP ให้สอดคล้องกับหลักการให้สิทธิเท่าที่จำเป็นและความจำเป็นตามหน้าที่ การเข้าถึงด้วยสิทธิพิเศษควรมีการควบคุมและบันทึกอย่างเหมาะสม เพื่อให้สามารถตรวจสอบย้อนหลังได้

สำหรับข้อมูลหรือระบบที่มีผลกระทบสูง ควรพิจารณามาตรการเพิ่มเติมตามระดับความเสี่ยง เช่น การจำกัดขอบเขตการเข้าถึง การจำกัดระยะเวลา และการเพิ่มระดับการตรวจสอบหรืออนุมัติ

มาตรฐานคลาวด์กำหนดให้ CSP คำนึงถึงการเข้าถึงทรัพย์สินของ CSC โดยเจ้าหน้าที่ของ CSP และกำหนดขั้นตอนการควบคุมการเข้าถึงที่เข้มงวดสำหรับผู้ดูแลระบบ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้อ้างอิง

8. การแยกผู้ใช้บริการและสภาพแวดล้อมการประมวลผล ผู้ให้บริการคลาวด์ควรกำหนดมาตรการเพื่อแยกข้อมูล ระบบ และทรัพยากรของ CSC แต่ละรายออกจากกันอย่างเหมาะสมกับสถาปัตยกรรมและระดับความเสี่ยง

ในกรณีที่ใช้โครงสร้างพื้นฐานร่วมกัน ควรมีมาตรการทางตรรกะหรือมาตรการอื่นที่เหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลข้ามระหว่างผู้ใช้บริการ

สำหรับระบบที่มีผลกระทบสูง อาจจำเป็นต้องพิจารณาความสามารถในการแยกทรัพยากรหรือสภาพแวดล้อมเพิ่มเติม หากผลการประเมินความเสี่ยงแสดงให้เห็นว่าการใช้ทรัพยากรร่วมกันไม่เพียงพอต่อระดับความเสี่ยงที่ยอมรับได้

9. การจัดการผู้รับจ้างช่วงและห่วงโซ่อุปทาน ผู้ให้บริการคลาวด์ควรกำหนดกระบวนการในการคัดเลือก ประเมิน และกำกับดูแลผู้รับจ้างช่วงหรือผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการคลาวด์

ควรสามารถแจ้งข้อมูลที่จำเป็นแก่ CSC เกี่ยวกับผู้รับจ้างช่วงที่สามารถเข้าถึง จัดเก็บ หรือประมวลผลข้อมูล รวมถึงการเปลี่ยนแปลงผู้รับจ้างช่วงที่อาจส่งผลต่อความเสี่ยงของ CSC

สำหรับข้อมูลหรือระบบที่มีผลกระทบสูง ควรพิจารณาเพิ่มเติมถึง

9.1 ประเทศที่ผู้รับจ้างช่วงดำเนินงาน

9.2 เขตอำนาจทางกฎหมายที่เกี่ยวข้อง

9.3 สถานที่จัดเก็บหรือประมวลผลข้อมูล

9.4 ความสามารถในการควบคุมและตรวจสอบผู้รับจ้างช่วง

9.5 ความต่อเนื่องของบริการ

9.6 ความเสี่ยงจากการพึ่งพาผู้ให้บริการรายย่อย

มาตรฐานคลาวด์กำหนดให้ CSP ที่ใช้ผู้ให้บริการรายย่อยต้องดูแลให้ระดับความมั่นคงปลอดภัยของผู้ให้บริการรายย่อยไม่น้อยกว่าระดับที่ CSC ต้องการ และต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยให้แก่ผู้ให้บริการภายนอกในห่วงโซ่อุปทาน

10. การสื่อสารการเปลี่ยนแปลงที่มีนัยสำคัญ ผู้ให้บริการคลาวด์ควรแจ้ง CSC เมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อความมั่นคงปลอดภัย ความพร้อมใช้งาน การปฏิบัติตามกฎหมาย หรืออธิปไตยข้อมูล
การเปลี่ยนแปลงที่ควรพิจารณา เช่น

10.1 สถาปัตยกรรมหรือเทคโนโลยีของบริการ

10.2 สถานที่จัดเก็บหรือประมวลผลข้อมูล

10.3 ผู้รับจ้างช่วง

10.4 เขตอำนาจทางกฎหมาย

10.5 มาตรการควบคุมที่มีนัยสำคัญ

10.6 ขอบเขตหรือรูปแบบบริการ

10.7 เงื่อนไขการสำรองหรือกู้คืนข้อมูล

มาตรฐานกำหนดให้ CSP สื่อสารกับ CSC ระหว่างการจัดการการเปลี่ยนแปลง และในข้อ 5.2.6.1 ยังกำหนดให้ CSP ให้ข้อมูลเกี่ยวกับการเปลี่ยนแปลงที่อาจส่งผลเสียต่อบริการคลาวด์

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

11. การสนับสนุนการยุติหรือเปลี่ยนบริการ ผู้ให้บริการคลาวด์ควรกำหนดแนวทางและความสามารถในการสนับสนุนการยุติหรือเปลี่ยนบริการ เพื่อให้ CSC สามารถนำข้อมูลกลับ โอนย้ายข้อมูล หรือนำระบบไปดำเนินงานในสภาพแวดล้อมอื่นได้อย่างมั่นคงปลอดภัย

ควรกำหนดเงื่อนไขเกี่ยวกับ

11.1 วิธีและรูปแบบการส่งคืนข้อมูล

11.2 ระยะเวลาที่ CSC สามารถเข้าถึงข้อมูลหลังแจ้งยุติบริการ

11.3 การลบหรือทำลายข้อมูลและสำเนาที่เหลืออยู่

11.4 การเพิกถอนบัญชีและสิทธิ

11.5 การสนับสนุนการโอนย้ายข้อมูลหรือระบบ

11.6 การเก็บรักษาบันทึกหรือหลักฐานที่ยังจำเป็น

11.7 การยืนยันการลบข้อมูลตามความเหมาะสม

สำหรับบริการที่รองรับข้อมูลหรือระบบที่มีผลกระทบสูง ควรพิจารณาความสามารถในการสนับสนุนการเปลี่ยนผ่านโดยลดผลกระทบต่อภารกิจของ CSC และลดความเสี่ยงจากการผูกติดกับผู้ให้บริการรายเดียว

12. การทบทวนและปรับปรุงนโยบาย ผู้ให้บริการคลาวด์ควรทบทวนนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศตามรอบระยะเวลาที่กำหนด และเมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อความเสี่ยงอย่างมีนัยสำคัญ

การทบทวนควรพิจารณาอย่างน้อยเมื่อมีการเปลี่ยนแปลง

12.1 รูปแบบหรือขอบเขตบริการ

12.2 สถาปัตยกรรมหรือเทคโนโลยี

12.3 สถานที่จัดเก็บหรือประมวลผลข้อมูล

12.4 ผู้รับจ้างช่วง

12.5 ข้อกำหนดทางกฎหมาย

12.6 ระดับความเสี่ยงของบริการ

12.7 เหตุการณ์ด้านความมั่นคงปลอดภัยที่มีนัยสำคัญ

13. หลักฐานที่ควรมี (Recommended Evidence) เพื่อสนับสนุนการแสดงการปฏิบัติตามข้อกำหนด CSP ควรสามารถแสดงหลักฐานตามความเหมาะสม เช่น

ประเด็น	ตัวอย่างหลักฐาน
นโยบายการใช้บริการคลาวด์	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ หรือนโยบายความมั่นคงปลอดภัยสำหรับบริการคลาวด์
ระดับผลกระทบ	ผลการจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
ความอ่อนไหวของข้อมูล	ผลการจำแนกประเภทหรือชั้นความลับของข้อมูล
ความเสี่ยง	ผลการประเมินความเสี่ยง หรือทะเบียนความเสี่ยง

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

อธิปไตยข้อมูล	ผลการพิจารณาสถานที่จัดเก็บหรือประมวลผลข้อมูล เขตอำนาจทางกฎหมาย และอธิปไตยข้อมูล
การประเมิน CSP	ผลการประเมินผู้ให้บริการคลาวด์ หรือผลการประเมินผู้ให้บริการ
ความรับผิดชอบร่วม	สัญญา ข้อตกลงระดับการให้บริการ หรือตารางความรับผิดชอบร่วม
สถานที่จัดเก็บและประมวลผลข้อมูล	ข้อมูลภูมิภาค ศูนย์ข้อมูล หรือสถานที่จัดเก็บและประมวลผลที่ CSP แจ้ง
ผู้รับจ้างช่วง	รายชื่อหรือข้อมูลผู้ประมวลผลช่วง ผู้รับจ้างช่วง หรือผู้ให้บริการภายนอกที่เกี่ยวข้อง
การคุ้มครองข้อมูลส่วนบุคคล	ผลการประเมินด้านความเป็นส่วนตัว ข้อตกลงการประมวลผลข้อมูล หรือข้อกำหนดตามสัญญาที่เกี่ยวข้อง
ความต่อเนื่อง	แผนความต่อเนื่อง การสำรองข้อมูล การกู้คืน หรือข้อมูลความสามารถของบริการที่เกี่ยวข้อง
การออกจากบริการ	แผนการออกจากบริการ หลักฐานการย้ายข้อมูล การส่งคืนข้อมูล หรือการลบข้อมูล
การตัดสินใจ	บันทึกอนุมัติ บันทึกการพิจารณาความเสี่ยง หรือหลักฐานประกอบการจัดซื้อจัดจ้าง

หมายเหตุ: ไม่จำเป็นต้องมีหลักฐานทุกประเภทในทุกกรณี และไม่จำเป็นต้องจัดทำเอกสารใหม่ หากเอกสาร ระบบ หรือหลักฐานที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดตาม 5.1.1 ไปปฏิบัติควรดำเนินการโดยเชื่อมโยงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ความอ่อนไหวของข้อมูล ลักษณะบริการคลาวด์ ขอบเขตความรับผิดชอบของ CSC และ CSP ตลอดจนความเสี่ยงด้านอธิปไตยข้อมูลและเขตอำนาจทางกฎหมายที่เกี่ยวข้อง

การดำเนินการควรประยุกต์ใช้ร่วมกับกระบวนการที่องค์กรมีอยู่เดิม เช่น การประเมินความเสี่ยง การจำแนกข้อมูล การจัดหา การประเมินผู้ให้บริการ การทบทวนสัญญา การบริหารความต่อเนื่อง และการบริหารการเปลี่ยนแปลง โดยไม่จำเป็นต้องสร้างกระบวนการใหม่ หากกระบวนการเดิมสามารถรองรับข้อกำหนดได้อย่างเพียงพอ แนวทางนี้ควรใช้ตามระดับความเสี่ยง โดยไม่กำหนดให้บริการคลาวด์ทุกประเภทต้องใช้มาตรการในระดับเดียวกัน

1. การนำไปใช้ตลอดวงจรชีวิตบริการคลาวด์ การกำกับดูแลควรครอบคลุมตั้งแต่ก่อนเริ่มใช้บริการ ระหว่างการใช้บริการ จนถึงการยุติหรือเปลี่ยนบริการ ตามวงจรชีวิตการกำกับดูแลบริการคลาวด์ ดังนี้

1.1 การประเมินและเตรียมความพร้อม (Assessment and Planning) ก่อนเริ่มใช้บริการคลาวด์ CSC ควรดำเนินการอย่างน้อย ดังนี้

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

- ระบุข้อมูล ระบบ และบริการที่จะนำไปใช้บนคลาวด์
- ประเมินระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
- พิจารณาความอ่อนไหว ปริมาณ และระดับการรวมศูนย์ของข้อมูล
- พิจารณาข้อกำหนดด้านกฎหมาย ความเป็นส่วนตัว และความมั่นคง
- พิจารณาความเสี่ยงด้านอธิปไตยข้อมูลและเขตอำนาจทางกฎหมาย
- กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยที่จำเป็น
- พิจารณาความต้องการด้านความต่อเนื่องและการกู้คืน
- กำหนดเงื่อนไขเบื้องต้นสำหรับการยุติหรือเปลี่ยนบริการ

สำหรับข้อมูลหรือระบบที่มีผลกระทบสูง หรือเกี่ยวข้องกับความมั่นคง CII หรือข้อมูลอ่อนไหวจำนวนมาก ควรเพิ่มระดับการประเมินและการอนุมัติให้เหมาะสมกับผลกระทบ

1.2 การคัดเลือกและจัดทำข้อตกลง (Selection and Contracting) ก่อนทำสัญญา CSC ควรประเมินความสามารถของ CSP เทียบกับข้อกำหนดที่กำหนดไว้ โดยพิจารณาอย่างน้อย

- ขอบเขตบริการและความรับผิดชอบ
- ความสามารถด้านความมั่นคงปลอดภัย
- สถานที่จัดเก็บและประมวลผลข้อมูล
- เขตอำนาจทางกฎหมาย
- ผู้รับจ้างช่วง
- การเข้าถึงข้อมูลโดยบุคลากร CSP
- การคุ้มครองข้อมูลส่วนบุคคล
- การแจ้งเหตุการณ์
- การแจ้งการเปลี่ยนแปลงบริการ
- การส่งคืน โอนย้าย และลบข้อมูลเมื่อยุติบริการ

หากบริการไม่สามารถตอบสนองข้อกำหนดบางประการได้ ควรพิจารณาช่องว่าง มาตรการเพิ่มเติม มาตรการทดแทน และความเสี่ยงที่เหลืออยู่ก่อนการตัดสินใจ

1.3 การใช้งานและกำกับติดตาม (Operation and Monitoring) ระหว่างการใช้บริการ CSC ควรติดตามการเปลี่ยนแปลงที่อาจส่งผลต่อความเสี่ยง เช่น

- การเปลี่ยนบริการหรือสถาปัตยกรรม
- การเปลี่ยนสถานที่ประมวลผล
- การเปลี่ยนผู้รับจ้างช่วง
- การเปลี่ยนข้อกำหนดทางกฎหมาย
- การเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
- การเปลี่ยนระดับความสำคัญของข้อมูลหรือระบบ
- การเพิ่มขึ้นของปริมาณหรือการรวมศูนย์ข้อมูล
- การเปลี่ยนแปลงความสามารถของบริการ

หากพบการเปลี่ยนแปลงที่มีนัยสำคัญ ควรทบทวนความเสี่ยงและมาตรการที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1.4 การยุติหรือเปลี่ยนบริการ (Exit and Termination) CSC ควรกำหนดแผนการออกจากบริการให้เหมาะสมกับความสำคัญของข้อมูลและระบบ โดยพิจารณาอย่างน้อย

- การส่งคืนหรือโอนย้ายข้อมูล
- รูปแบบข้อมูลและความสามารถในการนำไปใช้ต่อ
- การตรวจสอบความครบถ้วนของข้อมูลที่ได้รับคืน
- การลบหรือทำลายข้อมูลและสำเนาที่เหลืออยู่
- การเพิกถอนบัญชี สิทธิ และการเชื่อมต่อ
- การเก็บรักษาข้อมูลหรือหลักฐานตามข้อกำหนด
- การรักษาความต่อเนื่องของระบบหรือบริการ
- การยืนยันการสิ้นสุดหน้าที่และความรับผิดชอบของ CSP

สำหรับระบบที่มีผลกระทบสูง ควรพิจารณาความสามารถในการย้ายเวิร์กโหลด ระบบ หรือข้อมูลไปยังสภาพแวดล้อมอื่นได้ภายในระยะเวลาที่เหมาะสม

2. การประยุกต์ใช้ตามระดับผลกระทบและความอ่อนไหวของข้อมูล ระดับรายละเอียดและความเข้มงวดของการกำกับดูแลควรสัมพันธ์กับระดับผลกระทบ ความอ่อนไหว และบริบทของข้อมูลหรือระบบสารสนเทศ โดยให้ดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำที่ประกาศกำหนดสำหรับแต่ละระดับ

ลักษณะข้อมูลหรือระบบ	แนวทางการพิจารณา
ผลกระทบระดับต่ำ	ดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำที่ประกาศกำหนดสำหรับระดับต่ำ และสามารถใช้กระบวนการประเมินทั่วไปขององค์กรได้ หากไม่มีข้อกำหนดเฉพาะหรือปัจจัยความเสี่ยงเพิ่มเติม
ผลกระทบระดับปานกลาง	ดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำสำหรับระดับปานกลาง และพิจารณากฎหมายการคุ้มครองข้อมูลส่วนบุคคล เขตอำนาจทางกฎหมาย สถานที่จัดเก็บหรือประมวลผลข้อมูล ตลอดจนข้อมูลและหลักฐานที่จำเป็นต่อการประเมิน
ผลกระทบระดับสูง	ดำเนินการตามข้อกำหนดส่วนที่ 1 และส่วนที่ 2 ทุกข้อ และพิจารณาเชิงลึกเกี่ยวกับสถานที่จัดเก็บและประมวลผลข้อมูล เขตอำนาจทางกฎหมาย ความรับผิดชอบร่วม ความต่อเนื่องของบริการ แผนการออกจากบริการ และหลักฐานด้านความมั่นคงปลอดภัย
ข้อมูลที่มีความอ่อนไหวหรือมีปริมาณมาก	พิจารณาผลกระทบจากลักษณะข้อมูล ปริมาณ ระยะเวลาการสะสม การรวมศูนย์ การเชื่อมโยง และความสามารถในการวิเคราะห์ข้อมูลร่วมกัน โดยไม่สรุประดับผลกระทบจากประเภทข้อมูลเพียงอย่างเดียว
ระบบ CII หรือข้อมูลที่เกี่ยวข้องกับความมั่นคง	พิจารณาผลกระทบต่อภารกิจ ความต่อเนื่อง การควบคุมข้อมูล การพึ่งพาผู้ให้บริการ เขตอำนาจทางกฎหมาย และความสามารถในการกู้คืนหรือเคลื่อนย้ายบริการตามผลการประเมินและข้อกำหนดที่ใช้บังคับ

ร่างสำหรับประชาพิจารณ์ Public Hearing ห้ามใช้อ้างอิง

ประกาศมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์กำหนดให้ประเมินผลกระทบต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน รวมถึงผลกระทบด้านการเงิน จำนวนผู้ได้รับผลกระทบ ความสามารถในการดำเนินภารกิจ และความมั่นคงของรัฐ

3. การประเมินความจำเป็นด้านอธิปไตยข้อมูลและสถานที่จัดเก็บหรือประมวลผลข้อมูล

การพิจารณาความจำเป็นในการกำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูล (Data Localization) และความเสี่ยงด้านอธิปไตยข้อมูล (Data Sovereignty) ควรเป็นผลจากการประเมินระดับผลกระทบ ความเสี่ยง กฎหมายและข้อกำหนดที่เกี่ยวข้อง มิใช่การกำหนดเงื่อนไขเดียวกันสำหรับข้อมูลทุกประเภท เว้นแต่กฎหมาย มาตรฐานประกาศ หรือข้อกำหนดที่มีผลใช้บังคับกำหนดไว้เป็นการเฉพาะ โดย CSC ควรพิจารณาปัจจัยอย่างน้อย ดังนี้

ปัจจัย	แนวทางพิจารณา
ระดับผลกระทบ	หากข้อมูลหรือระบบมีผลกระทบสูง ควรเพิ่มระดับการควบคุมสถานที่จัดเก็บและประมวลผล
ความอ่อนไหว	ข้อมูลสุขภาพ ชีวมิติ หรือข้อมูลที่เปิดเผยพฤติกรรมและตำแหน่งควรได้รับการพิจารณาเพิ่มเติม
ปริมาณข้อมูล	ปริมาณมากอาจทำให้ผลกระทบจากการรั่วไหลหรือการวิเคราะห์เพิ่มสูงขึ้น
การรวมศูนย์	ฐานข้อมูลขนาดใหญ่หรือข้อมูลหลายแหล่งที่รวมกันอาจมีความสำคัญสูงกว่าข้อมูลแต่ละรายการ
ความสำคัญต่อภารกิจ	ระบบที่จำเป็นต่อการให้บริการสาธารณะหรือภารกิจหลักควรได้รับการควบคุมสูงขึ้น
ความเกี่ยวข้องกับ CII	ควรพิจารณาผลกระทบต่อความต่อเนื่องและความมั่นคงของประเทศ
เขตอำนาจทางกฎหมาย	พิจารณาว่ากฎหมายต่างประเทศอาจมีผลต่อการเข้าถึงหรือระงับบริการหรือไม่
การเข้าถึงจากต่างประเทศ	แม้ข้อมูลอยู่ในประเทศ แต่ควรพิจารณาว่าบุคลากรหรือระบบจากต่างประเทศสามารถเข้าถึงได้หรือไม่
ความสามารถในการควบคุมข้อมูล	พิจารณาความสามารถในการเข้ารหัส จัดการกุญแจ ส่งออก สำรอง กู้คืน และลบข้อมูล
ความสามารถในการออกจากบริการ	พิจารณาว่าสามารถย้ายข้อมูลหรือระบบได้เมื่อเกิดความจำเป็นหรือไม่

อ้างอิงตามแนวทาง Zero Trust ที่ระบุความเสี่ยงอธิปไตยข้อมูล (Data Sovereignty) กับความลับ ความถูกต้องความพร้อมใช้งาน และความเป็นส่วนตัว โดยยกตัวอย่างมาตรการ เช่น การถือครองกุญแจ การกระจายเขตอำนาจการสำรอง และความสามารถในการย้ายเวิร์กโหลดเมื่อบริการถูกจำกัด

4. ตัวอย่างการประยุกต์ใช้กับข้อมูลหรือระบบที่มีความสำคัญ

4.1 ระบบหรือข้อมูลของหน่วยงาน CII หากระบบคลาวด์รองรับบริการที่เป็นส่วนหนึ่งของ CII เช่น ระบบพลังงาน การเงิน โทรคมนาคม ขนส่ง หรือบริการสาธารณสุขที่สำคัญ ควรพิจารณาผลกระทบจากการหยุดชะงัก การถูกควบคุม การแก้ไขข้อมูล หรือการสูญเสียความสามารถในการเข้าถึงระบบ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้งานจริง

เหตุผลความจำเป็นในการกำหนดเงื่อนไขที่เข้มงวดขึ้น ได้แก่

- ระบบมีความสำคัญต่อบริการสาธารณะ
- การหยุดชะงักอาจกระทบประชาชนจำนวนมาก
- การถูกโจมตีอาจมีผลต่อความมั่นคงหรือเศรษฐกิจ
- การพึ่งพาผู้ให้บริการหรือเขตอำนาจเดียวอาจสร้างความเสี่ยงเชิงระบบ
- หน่วยงานต้องสามารถรักษาความต่อเนื่องและกู้คืนบริการได้

4.2 ข้อมูล CCTV ของหน่วยงานด้านความมั่นคงหรือพื้นที่สำคัญ การประเมิน CCTV ควรพิจารณามากกว่าความอ่อนไหวของภาพแต่ละรายการ โดยเฉพาะเมื่อมีการรวบรวมข้อมูลจำนวนมากหรือเชื่อมโยงกล้องจากหลายพื้นที่ โดยตัวอย่างผลกระทบที่อาจเกิดขึ้น ได้แก่

- เปิดเผยตำแหน่งหรือแนวทางติดตั้งกล้อง
- เปิดเผยจุดเข้าออกหรือพื้นที่ควบคุม
- แสดงรูปแบบการเคลื่อนที่ของบุคลากร
- แสดงช่วงเวลาการปฏิบัติงาน
- เปิดเผยรูปแบบการรักษาความปลอดภัยหรือจุดอ่อนของพื้นที่
- หากมีการรู้จำใบหน้า อาจเกี่ยวข้องกับข้อมูลชีวมิติ

ดังนั้น CCTV ของหน่วยงานด้านความมั่นคงหรือพื้นที่ CII ควรได้รับการประเมินเป็นกรณีพิเศษด้านสถานที่จัดเก็บ ผู้มีสิทธิเข้าถึง ระยะเวลาเก็บรักษา และความเสี่ยงจากการประมวลผลหรือเข้าถึงจากต่างประเทศ

AI Security Guidelines ที่แนบมาระบุว่าการประมวลผล CCTV เพื่อรู้จำใบหน้าสามารถเกี่ยวข้องกับข้อมูลชีวมิติ และเสนอให้พิจารณาการจัดเก็บหรือประมวลผลในประเทศเพื่อลดความเสี่ยงด้านกฎหมายและความเป็นส่วนตัว

4.3 ข้อมูลสุขภาพและเวชระเบียนจำนวนมาก ข้อมูลสุขภาพมีความอ่อนไหวสูง และเมื่อถูกรวมเป็นฐานข้อมูลขนาดใหญ่สามารถสร้างผลกระทบต่อประชาชนจำนวนมากได้ ควรพิจารณาอย่างน้อย

- ปริมาณข้อมูลและจำนวนเจ้าของข้อมูล
- ประเภทข้อมูลสุขภาพและความละเอียดของข้อมูล
- ความสามารถในการระบุตัวบุคคล
- การเข้าถึงโดย CSP และผู้รับจ้างช่วง
- สถานที่ประมวลผล
- การโอนข้อมูลข้ามประเทศ
- การเข้ารหัสและการควบคุมกุญแจ
- การสำรองและกู้คืน
- การลบข้อมูลเมื่อสิ้นสุดบริการ

AI Security Guidelines ยกตัวอย่างการใช้ข้อมูลประวัติการรักษาของผู้ป่วยกับ AI และเน้นความจำเป็นของมาตรการคุ้มครองข้อมูลที่เข้มงวดขึ้น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4.4 ข้อมูล EV และข้อมูลยานยนต์เชื่อมต่อ ข้อมูล EV อาจประกอบด้วยตำแหน่งทางภูมิศาสตร์ เวลา เส้นทางการเดินทาง จุดชาร์จ พฤติกรรมการขับขี่ และข้อมูลทางเทคนิคของยานพาหนะ การพิจารณาควรคำนึงถึงความเสี่ยงจากการรวบรวมข้อมูลต่อเนื่อง เพราะสามารถทำให้ทราบ

- ตำแหน่งของบุคคลหรือยานพาหนะ
- สถานที่ที่เดินทางเป็นประจำ
- เวลาและรูปแบบการเดินทาง
- เส้นทางที่ใช้เป็นประจำ
- รูปแบบการเคลื่อนที่ของกลุ่มผู้ใช้งาน
- รูปแบบการคมนาคมในพื้นที่หรือระดับมหภาค

หากข้อมูลดังกล่าวถูกเก็บในปริมาณมากหรือเกี่ยวข้องกับยานพาหนะของหน่วยงานสำคัญ อาจมีนัยต่อความเป็นส่วนตัว ความปลอดภัย และความมั่นคง จึงควรประเมินความจำเป็นของการจัดเก็บหรือประมวลผลในประเทศ รวมถึงการจำกัดสิทธิและการเข้าถึงข้อมูลจากต่างประเทศ

AI Security Guidelines ระบุโดยตรงว่าข้อมูลจากยานยนต์ไฟฟ้าสมัยใหม่อาจประกอบด้วยพฤติกรรมการขับขี่ ตำแหน่งทางภูมิศาสตร์ และเส้นทางการเดินทาง และเสนอให้พิจารณาสถาปัตยกรรมที่สนับสนุนอธิปไตยข้อมูลของประเทศ

5. ตัวอย่างการประเมินผลกระทบจากการรวมข้อมูล CSC ควรพิจารณาว่าข้อมูลหลายประเภทเมื่อแยกกันอาจมีผลกระทบไม่สูง แต่เมื่อรวมกันอาจเพิ่มระดับความเสี่ยงอย่างมีนัยสำคัญ

ตัวอย่าง

ข้อมูลตำแหน่งรถยนต์ 1 จุด

อาจมีผลกระทบจำกัด

↓

ข้อมูลตำแหน่งต่อเนื่องหลายเดือน

สามารถแสดงเส้นทางและสถานที่ที่เดินทางเป็นประจำ

↓

ข้อมูลจากยานพาหนะจำนวนมาก

สามารถวิเคราะห์รูปแบบการเคลื่อนที่ในระดับพื้นที่หรือประชากรได้

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามอ้างอิง

ในทำนองเดียวกัน

ภาพ CCTV 1 กล้อง

↓

ภาพ CCTV หลายกล้องในพื้นที่เดียวกัน

↓

ข้อมูล CCTV ของพื้นที่สำคัญหลายแห่งที่สะสมต่อเนื่อง

อาจทำให้สามารถวิเคราะห์โครงสร้างพื้นที่ การเคลื่อนที่ และรูปแบบการรักษาความปลอดภัยได้ ดังนั้น ปริมาณ ระยะเวลาการสะสม การรวมศูนย์ และความสามารถในการเชื่อมโยงข้อมูลควรถูกนำมาใช้ประกอบการประเมินระดับผลกระทบและข้อกำหนดด้านคลาวด์

6. การพิจารณามาตรการสำหรับความเสี่ยงด้านอธิปไตยข้อมูล เมื่อผลการประเมินแสดงว่ามีความเสี่ยงด้านอธิปไตยข้อมูลในระดับที่ต้องจัดการ CSC อาจพิจารณามาตรการเพิ่มเติมตามความเหมาะสม เช่น

6.1 กำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูล
6.2 จำกัดประเทศหรือภูมิภาคที่สามารถประมวลผลข้อมูล
6.3 จำกัดการเข้าถึงข้อมูลจากต่างประเทศ
6.4 ใช้การเข้ารหัสที่เหมาะสม
6.5 บริหารกุญแจเข้ารหัสภายใต้การควบคุมของ CSC ตามระดับความเสี่ยง
6.6 แยกข้อมูลสำรองจากบริการหลัก
6.7 กำหนดทางเลือกสำหรับการย้ายเวิร์กโหลดหรือบริการที่สำคัญ
6.8 กำหนดเงื่อนไขการแจ้งเมื่อมีการเปลี่ยนสถานที่ประมวลผลหรือผู้รับจ้างช่วง
6.9 กำหนดแผนการออกจากบริการ
6.10 ทดสอบความสามารถในการกู้คืนหรือโอนย้ายข้อมูลตามความเหมาะสม

มาตรการเหล่านี้เป็นตัวอย่างสำหรับการพิจารณาตามความเสี่ยง มิได้หมายความว่าต้องใช้ทุกมาตรการกับทุกบริการ

7. การเชื่อมโยงกับข้อกำหนดเฉพาะในหัวข้อ 5.2 การดำเนินการตาม 5.1.1 ควรทำหน้าที่เป็นกรอบการตัดสินใจระดับนโยบาย ส่วนมาตรการเชิงเทคนิคให้เชื่อมโยงกับข้อกำหนดเฉพาะ ดังนี้

ประเด็นจากการประเมิน	ข้อกำหนดที่เกี่ยวข้อง
การจำกัดและควบคุมสิทธิ	5.2.3 การควบคุมการเข้าถึง
การเข้ารหัสและการควบคุมกุญแจ	5.2.4 การเข้ารหัส
สถานที่ตั้งศูนย์ข้อมูล	5.2.5.1 ตำแหน่งของศูนย์ข้อมูล
การสำรองและกู้คืน	5.2.6.3 การสำรองข้อมูล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การบันทึกและปกป้อง Log	5.2.6.4–5.2.6.6
การถ่ายโอนข้อมูล	5.2.7.1 นโยบายและขั้นตอนการถ่ายโอนข้อมูล
การประเมินความสามารถ CSP	5.2.8.1 การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัย
ผู้รับจ้างช่วงและห่วงโซ่อุปทาน	5.2.9 การจัดการผู้ให้บริการภายนอก
การจัดการเหตุการณ์	5.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ

8. การใช้กระบวนการและเอกสารที่มีอยู่เดิม องค์กรสามารถใช้กระบวนการที่มีอยู่เดิมเพื่อสนับสนุนการปฏิบัติตาม 5.1.1 ได้ เช่น

8.1 การจำแนกข้อมูล
8.2 การประเมินความเสี่ยง
8.3 การประเมินผู้ให้บริการ
8.4 การจัดซื้อจัดจ้าง
8.5 การทบทวนสัญญา
8.6 การบริหารความต่อเนื่อง
8.7 การบริหารการเปลี่ยนแปลง
8.8 การบริหารข้อมูลส่วนบุคคล
8.9 การบริหารทรัพย์สิน
8.10 การบริหารข้อยกเว้น

ไม่จำเป็นต้องสร้างแบบฟอร์มหรือกระบวนการใหม่ หากระบบและเอกสารที่มีอยู่สามารถแสดงให้เห็นว่าได้มีการพิจารณาระดับผลกระทบ ความเสี่ยง Data Location, Jurisdiction, Data Sovereignty และความเหมาะสมของบริการอย่างเพียงพอ

9. หลักฐานที่ควรพิจารณา (Recommended Evidence) เพื่อสนับสนุนการตรวจสอบว่าการกำหนดและการนำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติมีความสอดคล้องกับข้อกำหนด องค์กรควรกำหนดและเก็บรักษาหลักฐานที่เหมาะสมกับลักษณะของบริการ ระดับผลกระทบความสำคัญของข้อมูลและระบบสารสนเทศ ตลอดจนความเสี่ยงที่เกี่ยวข้อง

หลักฐานควรสามารถแสดงให้เห็นอย่างน้อยว่า องค์กรได้กำหนดนโยบายที่เหมาะสม ประเมินระดับผลกระทบและความเสี่ยง พิจารณาความเหมาะสมของผู้ให้บริการและรูปแบบบริการ กำหนดความรับผิดชอบระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ ตลอดจนมีการพิจารณาและอนุมัติการใช้บริการตามอำนาจหน้าที่ที่กำหนด ตัวอย่างหลักฐานที่องค์กรอาจพิจารณา มีดังนี้

ลำดับ	ประเด็นที่ต้องสามารถยืนยันได้	ตัวอย่างหลักฐาน
1	การกำหนดนโยบายสำหรับบริการคลาวด์	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ หรือนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรที่มีข้อกำหนดสำหรับการใช้บริการคลาวด์อย่างชัดเจน

ร่างหลักเกณฑ์ฯ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2	การกำหนดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ	ผลการประเมินและจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ รวมถึงข้อมูลประกอบการพิจารณาระดับผลกระทบ
3	การจำแนกและพิจารณาความอ่อนไหวของข้อมูล	ทะเบียนข้อมูล ผลการจำแนกประเภทหรือชั้นความลับของข้อมูล และหลักฐานที่แสดงลักษณะหรือความอ่อนไหวของข้อมูลที่นำขึ้นใช้บริการคลาวด์
4	การประเมินความเสี่ยงจากการใช้บริการคลาวด์	ผลการประเมินความเสี่ยง ทะเบียนความเสี่ยง แผนจัดการความเสี่ยง และผลการพิจารณาความเสี่ยงที่เหลืออยู่ตามความเหมาะสม
5	การประเมินความเหมาะสมของผู้ให้บริการคลาวด์	ผลการประเมินผู้ให้บริการคลาวด์ แบบประเมินก่อนการจัดหาหรือใช้บริการ ข้อมูลความสามารถด้านความมั่นคงปลอดภัย ใบรับรอง หรือรายงานการประเมินที่เกี่ยวข้อง
6	การกำหนดความรับผิดชอบร่วมระหว่างผู้ใช้บริการและผู้ให้บริการ	สัญญา ข้อตกลงระดับการให้บริการ ตารางความรับผิดชอบร่วม หรือตารางกำหนดผู้รับผิดชอบตามบทบาท (RACI Matrix) ที่แสดงหน้าที่ของผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอกที่เกี่ยวข้อง
7	การพิจารณาสถานที่จัดเก็บและประมวลผลข้อมูล	ข้อมูลศูนย์ข้อมูล ภูมิภาคที่ให้บริการ ประเทศที่ข้อมูลอาจถูกจัดเก็บ ประมวลผล หรือสำรอง และข้อมูลเกี่ยวกับเขตอำนาจทางกฎหมายที่เกี่ยวข้อง
8	การพิจารณาความเสี่ยงด้านอธิปไตยข้อมูล	ผลการประเมินสถานที่และเขตอำนาจทางกฎหมายของข้อมูล การประเมินความเสี่ยงด้านอธิปไตยข้อมูล หรือบันทึกการพิจารณาความสามารถในการควบคุม เข้าถึง เคลื่อนย้าย และกู้คืนข้อมูลตามความเหมาะสม
9	การบริหารผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง	รายชื่อหรือข้อมูลผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง ขอบเขตบริการ สถานที่ประมวลผลข้อมูล และเงื่อนไขการแจ้งการเปลี่ยนแปลงที่เกี่ยวข้อง
10	การคุ้มครองข้อมูลส่วนบุคคล	ผลการประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ข้อกำหนดตามสัญญา หรือหลักฐานอื่นที่เกี่ยวข้องตามบทบาทของคู่สัญญา
11	การรักษาความต่อเนื่องและการกู้คืนบริการ	แผนความต่อเนื่องทางธุรกิจ แผนกู้คืนระบบ ข้อกำหนดหรือข้อมูลความสามารถในการสำรองและกู้คืนข้อมูล ผลการทดสอบ หรือหลักฐานอื่นที่แสดงความสามารถในการรักษาความต่อเนื่องของบริการ
12	การยุติ เปลี่ยน หรือเคลื่อนย้ายบริการคลาวด์	แผนการออกจากบริการ (Exit Plan) ขั้นตอนการเคลื่อนย้ายหรือส่งคืนข้อมูล หลักฐานการลบข้อมูล การเพิกถอนสิทธิ และบันทึกการดำเนินการเมื่อสิ้นสุดหรือเปลี่ยนบริการ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

13	การพิจารณาและอนุมัติการใช้บริการ	บันทึกการอนุมัติ บันทึกการประชุม ผลการพิจารณาความเสี่ยง การยอมรับความเสี่ยงที่เหลืออยู่ เอกสารการจัดซื้อจัดจ้าง หรือบันทึกการตัดสินใจของผู้มีอำนาจที่เกี่ยวข้อง
14	การทบทวนและติดตามภายหลังการนำบริการไปใช้	ผลการทบทวนนโยบาย ผลการประเมินความเสี่ยงซ้ำ บันทึกการเปลี่ยนแปลงที่มีนัยสำคัญ ผลการติดตามผู้ให้บริการ หรือหลักฐานการทบทวนตามรอบและเมื่อเกิดเหตุที่กำหนดไว้

หมายเหตุ: ตัวอย่างหลักฐานข้างต้นเป็นแนวทางประกอบการนำข้อกำหนดไปปฏิบัติ มิได้หมายความว่าองค์กรต้องจัดทำเอกสารแยกต่างหากสำหรับทุกประเด็น หรือมีหลักฐานครบทุกประเภทในทุกบริการ องค์กรสามารถใช้เอกสาร ระบบงาน ทะเบียน บันทึกการประชุม ข้อมูลจากผู้ให้บริการ หรือหลักฐานที่มีอยู่เดิมได้ หากสามารถแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอและสามารถตรวจสอบย้อนกลับได้

หลักฐานที่ใช้ควรมีความเหมาะสมกับ ระดับผลกระทบและความเสี่ยงของข้อมูลหรือระบบสารสนเทศ โดยข้อมูลหรือระบบที่มีระดับผลกระทบสูงย่อมต้องการหลักฐานที่มีรายละเอียดและความน่าเชื่อถือมากกว่ากรณีที่มีระดับผลกระทบต่ำ ทั้งนี้ การมีเอกสารหรือใบรับรองเพียงอย่างเดียวไม่ควรถือเป็นข้อยืนยันว่าความเสี่ยงได้รับการจัดการอย่างเพียงพอ หากหลักฐานดังกล่าวไม่ครอบคลุมบริการ ข้อมูล ระบบ หรือความเสี่ยงที่องค์กรกำลังพิจารณา

สรุปแนวทางการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ (Information Security Policy for Cloud Services Summary)

การกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ควรเริ่มจากการพิจารณาข้อมูล ระบบสารสนเทศ ภารกิจ และบริบทของการใช้บริการคลาวด์ขององค์กร โดยเชื่อมโยงกับระดับผลกระทบความเสี่ยงที่องค์กรยอมรับได้ ความอ่อนไหวของข้อมูล ปริมาณและการรวมศูนย์ของข้อมูล ตลอดจนลักษณะของบริการคลาวด์ที่นำมาใช้งาน

นโยบายไม่ควรกำหนดมาตรการเดียวกันสำหรับข้อมูลหรือระบบสารสนเทศทุกประเภท แต่ควรกำหนดหลักการและเงื่อนไขให้สามารถปรับระดับความเข้มงวดตามผลการประเมินได้ โดยเฉพาะกรณีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง มีความสำคัญต่อภารกิจ เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ข้อมูลด้านความมั่นคง ฐานข้อมูลสุขภาพหรือข้อมูลส่วนบุคคลจำนวนมาก ข้อมูลจากกล้องโทรทัศน์วงจรปิด (CCTV) ของพื้นที่สำคัญ ตลอดจนข้อมูลจากยานยนต์ไฟฟ้าหรือยานยนต์เชื่อมต่อ (EV Data) ที่สามารถนำมาเชื่อมโยงหรือวิเคราะห์ร่วมกันได้

อย่างไรก็ตาม การเป็นข้อมูลที่มีความอ่อนไหว มีปริมาณมาก หรืออยู่ในกลุ่มตัวอย่างข้างต้น มิได้หมายความว่าข้อมูลหรือระบบนั้นจะถูกจัดเป็นระดับผลกระทบสูงโดยอัตโนมัติ การกำหนดระดับผลกระทบต้องพิจารณาตามหลักเกณฑ์ที่เกี่ยวข้อง โดยคำนึงถึงลักษณะข้อมูล ปริมาณ ระยะเวลาการสะสม การรวมศูนย์ ความสามารถในการเชื่อมโยง ตลอดจนผลกระทบที่อาจเกิดขึ้นต่อบุคคล ภารกิจ การให้บริการสาธารณะ เศรษฐกิจ หรือความมั่นคงของรัฐ

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

นอกจากผลกระทบด้านการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานแล้ว องค์กรควรพิจารณาความเสี่ยงที่เกิดจากลักษณะเฉพาะของบริการคลาวด์ เช่น การใช้ทรัพยากรร่วมกัน การเข้าถึงข้อมูลโดยบุคลากรของผู้ให้บริการ การใช้ผู้รับจ้างช่วง สถานที่จัดเก็บและประมวลผลข้อมูล ประเทศและเขตอำนาจทางกฎหมาย การพึ่งพาผู้ให้บริการ ความสามารถในการเคลื่อนย้ายหรือกู้คืนข้อมูล และความเสี่ยงด้านอธิปไตยข้อมูล (Data Sovereignty) ตามความเหมาะสม

สรุปหน้าที่ของผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

ประเด็น	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
นโยบาย	กำหนดนโยบายสำหรับการประมวลผลบนคลาวด์ให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้และระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ	กำหนดหรือเพิ่มเติมนโยบายด้านความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมลักษณะเฉพาะของบริการคลาวด์
ระดับผลกระทบและความเสี่ยง	ประเมินระดับผลกระทบ ความอ่อนไหว ความสำคัญต่อภารกิจ และความเสี่ยงก่อนกำหนดเงื่อนไขการใช้บริการ	ให้ข้อมูลเกี่ยวกับความสามารถและข้อจำกัดของบริการเพื่อให้ CSC สามารถประเมินความเหมาะสมได้
ข้อมูลและทรัพย์สิน	กำหนดเงื่อนไขการนำข้อมูล ระบบ และทรัพย์สินขึ้นใช้บริการคลาวด์ตามระดับความเสี่ยง	จัดให้มีมาตรการคุ้มครองข้อมูลและทรัพย์สินของ CSC ตามขอบเขตบริการและความรับผิดชอบ
สถานที่จัดเก็บและประมวลผล	พิจารณาสถานที่จัดเก็บ ประมวลผล สำรอง และถ่ายโอนข้อมูล รวมถึงเขตอำนาจทางกฎหมายที่เกี่ยวข้อง	ให้ข้อมูลเกี่ยวกับสถานที่หรือประเทศที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลตามข้อกำหนดที่เกี่ยวข้อง
อธิปไตยข้อมูล	ประเมินความสามารถในการควบคุม เข้าถึง เคลื่อนย้าย กู้คืน และนำข้อมูลหรือบริการกลับมาใช้ได้เมื่อเกิดเหตุผิดปกติ	สนับสนุนข้อมูลและความสามารถที่จำเป็นต่อการควบคุม การส่งออก การย้าย การสำรอง และการกู้คืนข้อมูลตามขอบเขตบริการ
ความรับผิดชอบร่วม	กำหนดขอบเขตความรับผิดชอบของ CSC, CSP และผู้รับจ้างช่วงให้ชัดเจน	กำหนดและสื่อสารขอบเขตความรับผิดชอบของ CSP และผู้ให้บริการภายนอกที่เกี่ยวข้อง
ผู้ให้บริการภายนอกและผู้รับจ้างช่วง	พิจารณาความเสี่ยงที่เกิดจากผู้รับจ้างช่วงและห่วงโซ่อุปทาน	คัดเลือก ประเมิน กำกับดูแล และให้ข้อมูลเกี่ยวกับผู้รับจ้างช่วงตามความจำเป็น
การเปลี่ยนแปลง	ทบทวนความเสี่ยงและนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	แจ้งการเปลี่ยนแปลงที่อาจส่งผลต่อความมั่นคงปลอดภัย กฎหมาย ความพร้อมใช้งาน หรือความเสี่ยงของ CSC ตามข้อกำหนดที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การยุติหรือเปลี่ยนบริการ	วางแผนการส่งคืน โอนย้าย กู้คืน หรือลบข้อมูล และรักษาความต่อเนื่องของภารกิจ	สนับสนุนการส่งคืน โอนย้าย หรือลบข้อมูล และการยุติบริการอย่างมั่นคงปลอดภัย
การทบทวนและหลักฐาน	เก็บรักษาผลการประเมิน ความเสี่ยง ข้อตกลง การตัดสินใจ และหลักฐานที่เกี่ยวข้อง	จัดให้มีข้อมูลหรือหลักฐานที่เหมาะสมเพื่อสนับสนุนการประเมินและการปฏิบัติตามข้อกำหนดของ CSC

ความสัมพันธ์กับข้อกำหนดอื่น การดำเนินการตามข้อ 5.1.1 ไม่ควรแยกออกจากข้อกำหนดอื่นของมาตรฐาน แต่ควรเชื่อมโยงเป็นกระบวนการเดียวกัน โดยสามารถสรุปได้ดังนี้

ข้อมูลหรือระบบสารสนเทศ

- ประเมินระดับผลกระทบและความเสี่ยง
- กำหนดนโยบายและเงื่อนไขการใช้บริการตามข้อ 5.1.1
- กำหนดบทบาท ความรับผิดชอบ และอำนาจการตัดสินใจตามข้อ 5.1.2
- พิจารณากฎหมาย เขตอำนาจทางกฎหมาย และข้อกำหนดตามสัญญาตามข้อ 5.1.3
- กำหนดมาตรการควบคุมตามข้อ 5.2 ที่ใช้บังคับตามระดับผลกระทบ
- ติดตาม ทบทวน และปรับปรุงเมื่อมีการเปลี่ยนแปลง

สำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง ต้องดำเนินการตามข้อกำหนดส่วนที่ 1 และส่วนที่ 2 ทุกข้อของประกาศ ซึ่งรวมถึงข้อ 5.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม และข้อกำหนดอื่นที่เกี่ยวข้องกับระดับผลกระทบดังกล่าว

ในทางปฏิบัติ องค์กรไม่จำเป็นต้องจัดทำระบบเอกสารหรือกระบวนการใหม่สำหรับบริการคลาวด์ทั้งหมด หากนโยบาย การบริหารความเสี่ยง การจัดซื้อจัดจ้าง การบริหารผู้ให้บริการ การบริหารความต่อเนื่อง การจัดการการเปลี่ยนแปลง และระบบการกำกับดูแลที่มีอยู่สามารถรองรับข้อกำหนดดังกล่าวได้อย่างเพียงพอ ทั้งนี้ควรสามารถแสดงความเชื่อมโยงระหว่าง ข้อมูลหรือระบบ ระดับผลกระทบ ความเสี่ยง นโยบาย ข้อกำหนดความรับผิดชอบ มาตรการควบคุม หลักฐาน การตัดสินใจ และการติดตามผล ได้อย่างชัดเจนและตรวจสอบย้อนกลับได้

5.1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

การใช้บริการคลาวด์ทำให้ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศกระจายอยู่ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) และอาจรวมถึงผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง ดังนั้น การกำหนดโครงสร้างองค์กร บทบาท หน้าที่ อำนาจการตัดสินใจ และช่องทางการประสานงานที่ชัดเจน จึงเป็นองค์ประกอบสำคัญของการกำกับดูแลบริการคลาวด์

การกำหนดบทบาทไม่ควรมุ่งเพียงการระบุผู้รับผิดชอบการดำเนินมาตรการทางเทคนิค แต่ควรครอบคลุมถึงผู้มีอำนาจตัดสินใจเกี่ยวกับความเสี่ยง โดยเฉพาะกรณีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง มีความสำคัญต่อภารกิจ มีข้อมูลที่มีความอ่อนไหวในปริมาณมาก หรือมีความเสี่ยงด้านอธิปไตยข้อมูล เพื่อให้สามารถระบุได้ว่าใครเป็นผู้ประเมินผลกระทบ ใครมีอำนาจตัดสินใจ และใครเป็นเจ้าของความเสี่ยงที่เหลืออยู่

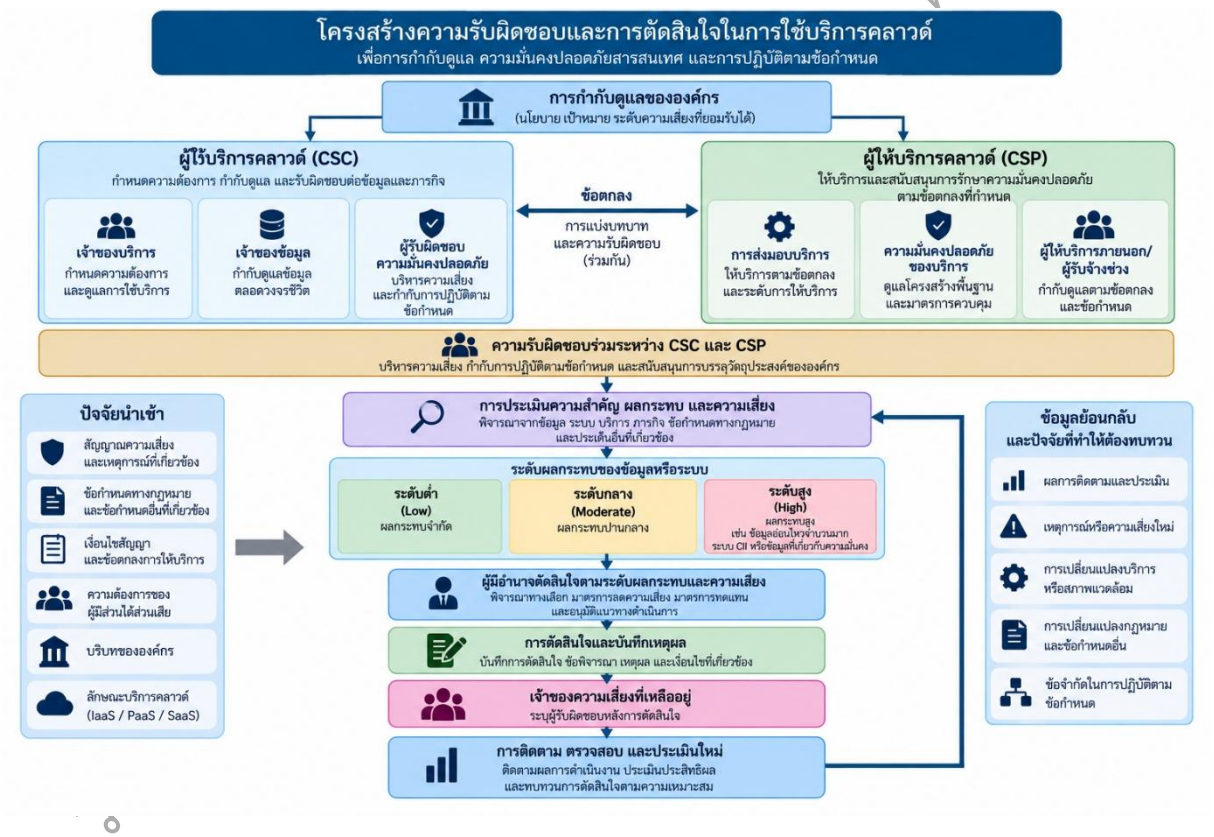
ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ประกาศกำหนดให้ CSC และ CSP ตกลงและบันทึกการแบ่งบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม โดย CSC ต้องสามารถปฏิบัติหน้าที่ที่ได้รับการจัดสรรและต้องจัดการความสัมพันธ์กับส่วนงานสนับสนุนของ CSP ขณะที่ CSP ต้องครอบคลุมความรับผิดชอบที่เกี่ยวข้องกับ CSC และผู้ให้บริการภายนอก รวมถึงแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล

หลักการดังกล่าวสอดคล้องกับแนวคิดความรับผิดชอบต่อการตัดสินใจ (Decision Accountability) ซึ่งให้ความสำคัญกับการเชื่อมโยงข้อมูลความเสี่ยงไปสู่การตัดสินใจที่ชัดเจน มีผู้รับผิดชอบ และสามารถตรวจสอบย้อนหลังได้ แทนการมีเพียงผลการประเมินความเสี่ยงหรือมาตรการควบคุมโดยไม่สามารถระบุได้ว่าใครเป็นผู้ตัดสินใจเกี่ยวกับความเสี่ยงนั้น

ในการกำหนดโครงสร้าง บทบาท ความรับผิดชอบ และการตัดสินใจ องค์กรควรพิจารณาว่าปัจจัยด้านสิ่งแวดล้อมและการเปลี่ยนแปลงสภาพภูมิอากาศมีความเกี่ยวข้องต่อการบรรลุวัตถุประสงค์ของบริการคลาวด์หรือไม่ ตามบริบทขององค์กร โดยรายละเอียดด้านสิ่งแวดล้อมและความยั่งยืนให้พิจารณาในข้อ 5.3

ห้ามใช้งานอ้างอิง



รูปที่ 3 โครงสร้างความรับผิดชอบและการตัดสินใจในการใช้บริการคลาวด์

5.1.2.1 บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

การใช้บริการคลาวด์ทำให้การควบคุมและการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศมิได้อยู่ภายใต้การควบคุมของหน่วยงานเพียงฝ่ายเดียว แต่กระจายอยู่ระหว่างผู้ใช้บริการคลาวด์ (CSC) ผู้ให้บริการคลาวด์ (CSP) และในบางกรณีอาจรวมถึงผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง

ขอบเขตความรับผิดชอบของแต่ละฝ่ายอาจแตกต่างกันตามรูปแบบบริการคลาวด์ ขอบเขตบริการ สถาปัตยกรรมของบริการ และข้อตกลงระหว่างคู่สัญญา ดังนั้น การกำหนดบทบาทและความรับผิดชอบจึงควรมุ่งให้แต่ละฝ่ายสามารถทราบได้อย่างชัดเจนว่า ตนมีหน้าที่ดำเนินการเรื่องใด เรื่องใดอยู่ภายใต้ความรับผิดชอบของอีกฝ่าย และเรื่องใดต้องดำเนินการร่วมกัน

การกำหนดความรับผิดชอบที่ไม่ชัดเจนอาจทำให้เกิดช่องว่างของความรับผิดชอบ (Responsibility Gap) เช่น CSC เข้าใจว่า CSP เป็นผู้รับผิดชอบการกำหนดสิทธิของผู้ใช้งาน ขณะที่ CSP กำหนดให้ CSC เป็นผู้รับผิดชอบ ส่งผลให้ไม่มีฝ่ายใดดำเนินการอย่างเพียงพอ หลักการนี้สอดคล้องกับแนวทางในข้อ 5.2.8 ซึ่งพิจารณาขอบเขตความรับผิดชอบและความสามารถของบริการตามส่วนที่ CSC และ CSP ควบคุม ทั้งนี้ สำหรับกิจกรรมการจัดการเหตุการณ์ที่ต้องดำเนินการร่วมกันให้เชื่อมโยงกับข้อ 5.2.10

นอกจากความรับผิดชอบในการดำเนินมาตรการแล้ว สำหรับประเด็นที่มีความเสี่ยงหรือผลกระทบอย่างมีนัยสำคัญ องค์กรควรกำหนดให้ชัดเจนว่า ใครมีอำนาจตัดสินใจ ใครเป็นผู้รับผิดชอบต่อผลของการตัดสินใจ และใครเป็นเจ้าของความเสี่ยงที่ยังคงเหลืออยู่ เพื่อให้สามารถติดตามและตรวจสอบย้อนกลับการตัดสินใจได้

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องมีการตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่า ผู้ใช้บริการคลาวด์ สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง ข) ผู้ใช้บริการคลาวด์ต้องระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับ ผู้ใช้บริการคลาวด์, ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก ข) ผู้ให้บริการคลาวด์ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อประสานงานกับผู้ใช้บริการคลาวด์

ร่างเอกสาร Public Hearing ไม่ใช่ฉบับประกาศใช้งาน

วัตถุประสงค์

1. เพื่อให้ CSC และ CSP กำหนดและจัดสรรบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์อย่างชัดเจน สอดคล้องกับรูปแบบบริการ ขอบเขตการควบคุม และความรับผิดชอบของแต่ละฝ่าย

2. เพื่อให้ CSC สามารถยืนยันได้ว่าองค์กรมีความสามารถในการปฏิบัติหน้าที่ที่ได้รับการจัดสรรและสามารถบริหารความสัมพันธ์กับส่วนงานสนับสนุนและส่วนงานที่เกี่ยวข้องของ CSP ได้อย่างเหมาะสม

3. เพื่อให้การตัดสินใจเกี่ยวกับความเสี่ยงที่มีนัยสำคัญ โดยเฉพาะกรณีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง สามารถระบุผู้มีอำนาจตัดสินใจ เจ้าของความเสี่ยงที่เหลืออยู่ และหลักฐานของการตัดสินใจได้อย่างเหมาะสม

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

CSC ควรกำหนดบทบาทและความรับผิดชอบที่เกี่ยวข้องกับบริการคลาวด์โดยใช้โครงสร้างการกำกับดูแลขององค์กรที่มีอยู่เป็นพื้นฐาน และเพิ่มเติมเฉพาะส่วนที่จำเป็นสำหรับบริบทของบริการคลาวด์

ไม่จำเป็นต้องจัดตั้งหน่วยงาน คณะกรรมการ หรือตำแหน่งใหม่สำหรับบริการคลาวด์โดยเฉพาะ หากโครงสร้างเดิมสามารถรองรับการกำหนดความรับผิดชอบ การประเมินความเสี่ยง การตัดสินใจ และการประสานงานกับ CSP ได้อย่างเพียงพอ

1. การกำหนดบทบาทและความรับผิดชอบภายในองค์กร CSC ควรกำหนดบทบาทที่เกี่ยวข้องกับบริการคลาวด์ให้ครอบคลุมทั้งด้านภารกิจ ข้อมูล ระบบ ความมั่นคงปลอดภัย กฎหมาย การบริหารบริการ และการบริหารความเสี่ยง โดยระดับรายละเอียดควรเหมาะสมกับความสำคัญและความซับซ้อนของบริการ ตัวอย่างการกำหนดบทบาท ได้แก่

ประเด็น	บทบาทที่อาจเกี่ยวข้อง	ตัวอย่างความรับผิดชอบ
ความต้องการของบริการ	เจ้าของบริการหรือเจ้าของภารกิจ	กำหนดวัตถุประสงค์ ความต้องการ และความสำคัญของบริการ
ข้อมูล	เจ้าของข้อมูล	กำหนดความสำคัญ การใช้ การเปิดเผย และข้อจำกัดของข้อมูล
ระบบสารสนเทศ	เจ้าของระบบ	กำกับดูแลระบบตลอดวงจรชีวิตและประสานการเปลี่ยนแปลง
ความมั่นคงปลอดภัย	ผู้รับผิดชอบด้านความมั่นคงปลอดภัย	ประเมินความเสี่ยงและให้ข้อเสนอแนะด้านมาตรการควบคุม
กฎหมายและข้อกำหนด	ผู้รับผิดชอบด้านกฎหมายหรือการกำกับดูแล	พิจารณากฎหมาย สัญญา เขตอำนาจทางกฎหมาย และข้อกำหนดที่เกี่ยวข้อง
ข้อมูลส่วนบุคคล	ผู้รับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล	พิจารณาประเด็นการประมวลผลและคุ้มครองข้อมูลส่วนบุคคล
การบริหารคลาวด์	ผู้ดูแลบริการคลาวด์	กำหนดค่า บริหารบัญชี ติดตามบริการ และประสาน CSP

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การบริหารความเสี่ยง	เจ้าของความเสี่ยงหรือผู้รับผิดชอบด้านความเสี่ยง	ติดตามและรายงานสถานะความเสี่ยง
การตัดสินใจ	ผู้มีอำนาจตามระดับความเสี่ยง	อนุมัติหรือพิจารณาความเสี่ยงที่อยู่ในอำนาจ

ตารางดังกล่าวเป็นแนวทาง มิได้หมายความว่าองค์กรต้องมีบุคลากรแยกกันสำหรับทุกบทบาท บุคคลหนึ่งอาจรับผิดชอบหลายบทบาทได้ หากเหมาะสมกับขนาด โครงสร้าง และการแบ่งแยกหน้าที่ขององค์กร

ตัวอย่าง หน่วยงานต้องการนำระบบรับคำร้องของประชาชนขึ้นใช้บริการ SaaS ฝ่ายเทคโนโลยีสารสนเทศไม่ควรเป็นผู้ตัดสินใจทุกประเด็นเพียงฝ่ายเดียว เนื่องจากฝ่ายเจ้าของบริการควรเป็นผู้กำหนดความสำคัญและความต้องการของระบบ เจ้าของข้อมูลควรพิจารณาลักษณะของข้อมูล ฝ่ายความมั่นคงปลอดภัยพิจารณาความเสี่ยง และฝ่ายกฎหมายหรือผู้รับผิดชอบด้านข้อมูลส่วนบุคคลพิจารณาข้อกำหนดที่เกี่ยวข้อง

หากผลการประเมินพบว่าระบบมีผลกระทบสูง การตัดสินใจยอมรับข้อจำกัดสำคัญของบริการควรอยู่กับผู้มีอำนาจตามระดับความเสี่ยงที่องค์กรกำหนด ไม่ควรตกอยู่กับผู้ดูแลระบบเพียงเพราะเป็นผู้ดำเนินการทางเทคนิค

2. การกำหนดความรับผิดชอบร่วมระหว่าง CSC และ CSP CSC ต้องตกลงกับ CSP เกี่ยวกับการแบ่งบทบาทและความรับผิดชอบ และควรสามารถจำแนกความรับผิดชอบได้อย่างน้อยเป็น

2.1 ความรับผิดชอบของ CSC

2.2 ความรับผิดชอบของ CSP

2.3 ความรับผิดชอบร่วมกัน

2.4 ความรับผิดชอบที่เกี่ยวข้องกับผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง

การแบ่งความรับผิดชอบควรพิจารณาตามรูปแบบและขอบเขตบริการ ไม่ควรกำหนดรูปแบบเดียวกันสำหรับโครงสร้างพื้นฐานเป็นบริการ (Infrastructure as a Service: IaaS) แพลตฟอร์มเป็นบริการ (Platform as a Service: PaaS) และซอฟต์แวร์เป็นบริการ (Software as a Service: SaaS) เนื่องจากระดับการควบคุมของแต่ละฝ่ายแตกต่างกัน ซึ่งเป็นหลักเดียวกับที่ใช้ในข้อ 5.2.8 ในการพิจารณาความสามารถของบริการและขอบเขตที่ CSC กับ CSP รับผิดชอบ ตัวอย่างในเชิงหลักการมีดังนี้

กิจกรรม	**IaaS**	**SaaS**
ความมั่นคงปลอดภัยของศูนย์ข้อมูล	CSP รับผิดชอบหลัก	CSP รับผิดชอบหลัก
โครงสร้างพื้นฐานคลาวด์	CSP รับผิดชอบหลัก	CSP รับผิดชอบหลัก
ระบบปฏิบัติการของเครื่องเสมือน	โดยทั่วไป CSC รับผิดชอบตามขอบเขตบริการ	โดยทั่วไป CSP รับผิดชอบ
โปรแกรมประยุกต์	CSC หรือร่วมกันตามบริการ	CSP รับผิดชอบส่วนบริการ CSC รับผิดชอบการใช้งานและการกำหนดค่าที่ตนควบคุม
บัญชีและสิทธิของผู้ใช้งาน CSC	CSC รับผิดชอบในส่วนที่ตนควบคุม	CSC รับผิดชอบในส่วนที่ตนควบคุม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การตอบสนองเหตุการณ์	แบ่งตามต้นเหตุและขอบเขตควบคุม	แบ่งตามต้นเหตุและขอบเขตควบคุม

ตารางนี้เป็นเพียงตัวอย่างเพื่ออธิบายหลักการ ไม่ควรนำไปใช้แทนข้อตกลงหรือรูปแบบความรับผิดชอบของ CSP แต่ละราย

ตัวอย่างช่องว่างของความรับผิดชอบ CSC ใช้บริการ IaaS และเข้าใจว่า CSP จะปรับปรุงระบบปฏิบัติการของเครื่องเสมือนให้โดยอัตโนมัติ ขณะที่เงื่อนไขบริการกำหนดว่า CSP รับผิดชอบเฉพาะโครงสร้างพื้นฐาน ส่วนระบบปฏิบัติการที่ CSC ติดตั้งเป็นความรับผิดชอบของ CSC

หากไม่มีการตรวจสอบความรับผิดชอบตั้งแต่ต้น ระบบอาจไม่ได้รับการปรับปรุงช่องโหว่เป็นระยะเวลานาน กรณีนี้เป็นตัวอย่างของช่องว่างของความรับผิดชอบที่การดำเนินการตาม 5.1.2.1 ควรช่วยป้องกัน

3. การยืนยันความสามารถของ CSC ในการปฏิบัติหน้าที่ที่ได้รับการจัดสรร สาระสำคัญของข้อกำหนดมิได้สิ้นสุดเพียงการระบุว่า “CSC รับผิดชอบอะไร” แต่ CSC ต้องพิจารณาด้วยว่าสามารถปฏิบัติหน้าที่ดังกล่าวได้จริงหรือไม่ โดย CSC ควรพิจารณาอย่างน้อยในประเด็นต่อไปนี้ตามความเกี่ยวข้อง

3.1 บุคลากรและความรู้ความสามารถ
3.2 เครื่องมือหรือความสามารถในการบริหารบริการ
3.3 สิทธิในการเข้าถึงข้อมูลและการตั้งค่าที่จำเป็น
3.4 ความสามารถในการติดตามและตรวจสอบบริการ
3.5 ความสามารถในการตอบสนองเหตุการณ์
3.6 ความสามารถในการสำรอง กู้คืน หรือย้ายข้อมูลตามขอบเขตที่ CSC รับผิดชอบ
3.7 ความสามารถในการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ตัวอย่าง CSP ระบุว่า CSC เป็นผู้รับผิดชอบการตรวจสอบบันทึกเหตุการณ์ของบัญชีผู้ดูแลระบบ แต่แพ็กเกจบริการที่ CSC เลือกไม่สามารถส่งออกบันทึกเหตุการณ์หรือเก็บรักษาไว้ตามระยะเวลาที่ CSC ต้องการได้

กรณีนี้ไม่ควรสรุปว่า “CSC รับผิดชอบแล้ว” เพียงเพราะมีการระบุไว้ในตารางความรับผิดชอบ แต่ต้องพิจารณาต่อว่า CSC มีความสามารถปฏิบัติหน้าที่นั้นได้จริงหรือไม่ หากไม่สามารถดำเนินการได้ ควรพิจารณาปรับระดับบริการ ใช้มาตรการเพิ่มเติม หรือประเมินความเสี่ยงก่อนตัดสินใจ

แนวทางนี้สอดคล้องกับวิธีพิจารณาในข้อ 5.2.8 คือ ข้อกำหนดของ CSC ⟶ ความสามารถของบริการ ⟶ ช่องว่างหรือข้อจำกัด ⟶ ความเสี่ยงที่ต้องพิจารณา

4. การจัดการความสัมพันธ์กับส่วนสนับสนุนและส่วนบริหารของ CSP CSC ควรทราบว่าต้องติดต่อส่วนใดของ CSP สำหรับกิจกรรมที่สำคัญ และไม่ควรพึ่งพาเพียงช่องทางสนับสนุนทั่วไปในทุกกรณี ตัวอย่างช่องทางที่อาจจำเป็น ได้แก่

กรณี	**ช่องทางหรือส่วนงานที่ควรระบุ**
ปัญหาการให้บริการทั่วไป	ส่วนสนับสนุนบริการ
เหตุการณ์ด้านความมั่นคงปลอดภัย	ช่องทางด้านความมั่นคงปลอดภัยหรือการจัดการเหตุการณ์

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

การยกระดับเหตุการณ์สำคัญ	ช่องทางยกระดับตามข้อตกลง
ประเด็นข้อมูลส่วนบุคคล	ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล
การเปลี่ยนแปลงบริการที่มีนัยสำคัญ	ผู้ดูแลบัญชีหรือส่วนบริหารบริการ
ประเด็นตามสัญญา	ผู้รับผิดชอบด้านสัญญาหรือการบริหารลูกค้า

รายละเอียดการติดต่อกับหน่วยงานของรัฐหรือหน่วยงานกำกับดูแลควรอยู่ในข้อ 5.1.2.2 ส่วนรายละเอียดการแจ้งและจัดการเหตุการณ์ควรเชื่อมโยงกับข้อ 5.2.10 ไม่จำเป็นต้องกำหนดซ้ำในหัวข้อนี้

5. การกำหนดอำนาจตัดสินใจตามระดับผลกระทบและความเสี่ยง การกำหนดผู้รับผิดชอบการดำเนินงานและการกำหนดผู้มีอำนาจตัดสินใจเป็นคนละประเด็นกัน ผู้ดูแลระบบอาจมีหน้าที่ดำเนินมาตรการ แต่ไม่ได้หมายความว่าผู้ดูแลระบบควรมีอำนาจยอมรับความเสี่ยงที่อาจส่งผลกระทบต่อภารกิจขององค์กร โดย CSC จึงควรกำหนดระดับอำนาจในการตัดสินใจให้เหมาะสมกับระดับผลกระทบและความเสี่ยง ตัวอย่างเชิงหลักการ มีดังนี้

ลักษณะกรณี	**แนวทางการตัดสินใจ**
การเปลี่ยนแปลงทั่วไปที่อยู่ในเกณฑ์ยอมรับ	ผู้รับผิดชอบบริการดำเนินการตามอำนาจที่ได้รับ
พบช่องว่างด้านความมั่นคงปลอดภัยที่สามารถลดความเสี่ยงได้ตามกระบวนการปกติ	เจ้าของระบบหรือเจ้าของความเสี่ยงพิจารณาตามเกณฑ์ขององค์กร
ความเสี่ยงที่เหลืออยู่เกินระดับที่ผู้ปฏิบัติงานมีอำนาจยอมรับ	ยกระดับไปยังผู้มีอำนาจตามเกณฑ์บริหารความเสี่ยง
ระบบผลกระทบสูงหรือการตัดสินใจที่อาจกระทบภารกิจสำคัญ	พิจารณาโดยผู้มีอำนาจในระดับที่เหมาะสมกับผลกระทบ

องค์กรไม่จำเป็นต้องกำหนดว่า “High Impact ต้องเข้าคณะกรรมการชุดใดชุดหนึ่งเสมอ” แต่ควรกำหนดระดับอำนาจให้ชัดเจนตามโครงสร้างขององค์กร

ในกรณีที่ผลการประเมินพบว่าหน่วยงานไม่สามารถดำเนินการให้เป็นไปตามข้อกำหนดของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่เกี่ยวข้องได้ ประเด็นดังกล่าวควรได้รับการยกระดับไปยังผู้มีอำนาจขององค์กร เพื่อพิจารณาข้อจำกัด ผลกระทบ ความเสี่ยง มาตรการทดแทนหรือมาตรการลดความเสี่ยง และแนวทางดำเนินการที่เหมาะสม ก่อนดำเนินการประสานหรือแจ้งหน่วยงานที่มีอำนาจตามข้อกำหนดที่เกี่ยวข้อง โดยให้เชื่อมโยงกับข้อ 5.1.2.2

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

CSP ควรกำหนดและสื่อสารบทบาทและความรับผิดชอบของตนให้ CSC สามารถเข้าใจขอบเขตการควบคุมของบริการได้อย่างเพียงพอ โดยเฉพาะส่วนที่ CSP รับผิดชอบ ส่วนที่ CSC ต้องดำเนินการเอง ส่วนที่ต้องดำเนินการร่วมกัน และส่วนที่เกี่ยวข้องกับผู้ให้บริการภายนอก

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้งานจริง

1. การกำหนดและบันทึกความรับผิดชอบ CSP ควรจัดให้มีข้อมูลที่อธิบายการแบ่งความรับผิดชอบตามรูปแบบบริการและขอบเขตบริการอย่างชัดเจน โดยข้อมูลดังกล่าวอาจปรากฏใน

1.1 ข้อตกลงการให้บริการ

1.2 ข้อตกลงระดับการให้บริการ

1.3 เงื่อนไขการใช้บริการ

1.4 คำอธิบายบริการ

1.5 เอกสารแสดงความรับผิดชอบร่วม

1.6 เอกสารทางเทคนิคหรือเอกสารความมั่นคงปลอดภัยที่เกี่ยวข้อง

ไม่จำเป็นต้องจัดทำเอกสารใหม่ หากเอกสารที่มีอยู่สามารถแสดงขอบเขตความรับผิดชอบได้เพียงพอ

2. การกำหนดความรับผิดชอบของผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง เมื่อบริการของ CSP พึ่งพาผู้ให้บริการภายนอก CSP ควรกำหนดความรับผิดชอบที่เกี่ยวข้องอย่างเหมาะสม และให้ข้อมูลแก่ CSC ในระดับที่จำเป็นต่อการประเมินความเสี่ยง โดยเฉพาะกรณีผู้ให้บริการภายนอกมีบทบาทเกี่ยวกับ

2.1 การจัดเก็บหรือประมวลผลข้อมูล

2.2 โครงสร้างพื้นฐานสำคัญของบริการ

2.3 การสำรองหรือกู้คืน

2.4 การสนับสนุนทางเทคนิค

2.5 การดำเนินงานด้านความมั่นคงปลอดภัย

ทั้งนี้ ไม่จำเป็นต้องเปิดเผยข้อมูลทางเทคนิคหรือข้อมูลภายในของ CSP ที่หากเปิดเผยแล้วอาจเพิ่มความเสี่ยงต่อบริการ

ตัวอย่าง CSP ให้บริการ SaaS แต่ใช้ผู้ให้บริการโครงสร้างพื้นฐานรายอื่นเป็นฐานในการให้บริการ CSC ไม่จำเป็นต้องบริหารผู้ให้บริการโครงสร้างพื้นฐานรายนั้นโดยตรง แต่ควรสามารถทราบขอบเขตที่มีนัยสำคัญต่อความเสี่ยงของบริการ และ CSP ต้องไม่ทำให้เกิดช่องว่างของความรับผิดชอบเพียงเพราะกิจกรรมบางส่วนดำเนินการโดยผู้ให้บริการภายนอก รายละเอียดการกำกับผู้ให้บริการภายนอกให้เชื่อมโยงกับข้อ 5.2.9

3. การกำหนดผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล CSP ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อประสานงานกับ CSC ตามข้อกำหนดของประกาศ

CSC ควรสามารถทราบช่องทางการติดต่อที่เหมาะสม โดยเฉพาะเมื่อบริการเกี่ยวข้องกับข้อมูลส่วนบุคคลหรือมีเหตุการณ์ที่อาจกระทบต่อข้อมูลดังกล่าว

คำว่า “ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล” ในข้อกำหนดนี้ไม่ควรถูกตีความโดยอัตโนมัติว่าต้องเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เว้นแต่มีข้อกำหนดทางกฎหมายที่เกี่ยวข้องกำหนดไว้เป็นการเฉพาะ

ร่างเอกสารเพื่อรับฟังความคิดเห็น (Public Hearing) เท่านั้น - ห้ามนำไปอ้างอิง

4. การให้ข้อมูลเพื่อสนับสนุนการปฏิบัติหน้าที่ของ CSC CSP ควรให้ข้อมูลที่เพียงพอเพื่อให้ CSC สามารถปฏิบัติหน้าที่ที่อยู่ในความรับผิดชอบของตนได้

ตัวอย่างเช่น หาก CSC มีหน้าที่ตรวจสอบการใช้งานบัญชีผู้ดูแลระบบ CSP ควรมีความสามารถหรือข้อมูลที่ทำให้ CSC สามารถดำเนินการดังกล่าวได้ตามขอบเขตบริการ หรืออย่างน้อยต้องทำให้ CSC ทราบข้อจำกัดของบริการก่อนการตัดสินใจ

สำหรับระบบที่มีผลกระทบสูง ระดับและความเพียงพอของข้อมูลที่ใช้ประกอบการประเมินควรสัมพันธ์กับความเสี่ยงของบริการ แต่ไม่จำเป็นต้องเปิดเผยข้อมูลภายในที่อาจเป็นประโยชน์ต่อผู้ไม่ประสงค์ดี ซึ่งเป็นหลักเดียวกับที่ข้อ 5.2.8 ใช้ในการขอข้อมูลความสามารถของ CSP

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การจัดทำแผนผังความรับผิดชอบ CSC และ CSP ควรสามารถแสดงความรับผิดชอบของกิจกรรมสำคัญได้อย่างชัดเจน โดยอาจใช้ตารางความรับผิดชอบร่วม หรือตารางกำหนดผู้รับผิดชอบตามบทบาท (RACI Matrix) หรือรูปแบบอื่นที่องค์กรใช้อยู่

ตัวอย่าง

กิจกรรม	CSC	CSP	ผู้ให้บริการภายนอก
กำหนดความสำคัญของข้อมูล	รับผิดชอบหลัก	ให้ข้อมูลสนับสนุน	-
กำหนดบัญชีและสิทธิของบุคลากร CSC	รับผิดชอบหลัก	จัดให้มีความสามารถตามบริการ	-
ความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน CSP	รับทราบ/ประเมินหลักฐาน	รับผิดชอบหลัก	อาจเกี่ยวข้อง
ประเมินความเสี่ยงต่อภารกิจของ CSC	รับผิดชอบหลัก	ให้ข้อมูลที่เกี่ยวข้อง	สนับสนุนตามขอบเขต
เหตุการณ์ที่เกิดจากโครงสร้างพื้นฐาน CSP	ประสานงานและประเมินผลกระทบ	รับผิดชอบหลักในขอบเขตตน	ตามขอบเขตบริการ
การตัดสินใจยอมรับความเสี่ยงของ CSC	รับผิดชอบหลัก	ให้ข้อมูลประกอบ	-

แนวทางนี้สอดคล้องกับรูปแบบของ 5.2.10 ซึ่งใช้ตารางแสดงกิจกรรมและผู้รับผิดชอบเพื่อป้องกันทั้งช่องว่างและความซ้ำซ้อนของความรับผิดชอบ

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2. การเชื่อมโยงระดับผลกระทบกับระดับการกำกับดูแล การกำหนดบทบาทควรสัมพันธ์กับผลการประเมินระดับผลกระทบที่ดำเนินการตามข้อ 5.1.1

ข้อมูลหรือระบบ ⟶ ระดับผลกระทบ ⟶ ความเสี่ยง ⟶ ระดับอำนาจตัดสินใจ ⟶ ผู้รับผิดชอบความเสี่ยง ⟶ การติดตาม

ระบบที่มีผลกระทบต่ำไม่ควรต้องใช้กระบวนการตัดสินใจที่ซับซ้อนเท่ากับระบบที่มีผลกระทบสูง เว้นแต่มีปัจจัยอื่นที่ทำให้ความเสี่ยงเพิ่มขึ้น

ในทางกลับกัน ระบบที่มีผลกระทบสูงไม่ควรปล่อยให้การตัดสินใจเกี่ยวกับข้อจำกัดสำคัญของบริการเป็นเพียงการตัดสินใจทางเทคนิคของผู้ดูแลระบบ

3. ความรับผิดชอบต่อการตัดสินใจ สำหรับความเสี่ยงที่มีนัยสำคัญ องค์กรควรประยุกต์ใช้หลักความรับผิดชอบต่อการตัดสินใจ (Decision Accountability) เพื่อให้สามารถตอบได้ว่า

มีข้อมูลหรือสัญญาณความเสี่ยงอะไร ⟶ เมื่อนำมาพิจารณาร่วมกันส่งผลอย่างไร ⟶ มีทางเลือกอะไร ⟶ ใครเป็นผู้ตัดสินใจ ⟶ เหตุใดจึงตัดสินใจเช่นนั้น ⟶ ใครรับผิดชอบความเสี่ยงที่ยังเหลืออยู่ ⟶ จะทบทวนเมื่อใด

สำหรับความเสี่ยงที่มีนัยสำคัญ หลักฐานการตัดสินใจควรสามารถระบุผู้มีอำนาจตัดสินใจ เหตุผลหรือข้อมูลสำคัญที่ใช้ประกอบการตัดสินใจ ทางเลือกที่ได้รับการพิจารณา เจ้าของความเสี่ยงที่เหลืออยู่ และเงื่อนไขหรือระยะเวลาสำหรับการทบทวนตามความเหมาะสม

องค์กรสามารถใช้กลไกการกำกับดูแลที่มีอยู่เดิม เช่น การประชุมบริหารความเสี่ยง การประชุมผู้บริหาร หรือคณะกรรมการพิจารณาการเปลี่ยนแปลง เพื่อบันทึกและติดตามการตัดสินใจดังกล่าว โดยไม่จำเป็นต้องจัดตั้งกลไกการกำกับดูแลขึ้นใหม่สำหรับบริการคลาวด์โดยเฉพาะ

ในเชิงกระบวนการ สามารถอธิบายได้ว่า

สัญญาณความเสี่ยง ⟶ การรวบรวมและประเมินความเสี่ยงในภาพรวม ⟶ การตัดสินใจของผู้มีอำนาจ ⟶ การกำหนดเจ้าของความเสี่ยงที่เหลืออยู่ ⟶ การติดตามและประเมินใหม่

ไม่จำเป็นต้องสร้างระบบใหม่ หากทะเบียนความเสี่ยง บันทึกการประชุม บันทึกอนุมัติ หรือระบบการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามข้อกำหนด (Governance, Risk and Compliance: GRC) สามารถแสดงความเชื่อมโยงดังกล่าวได้

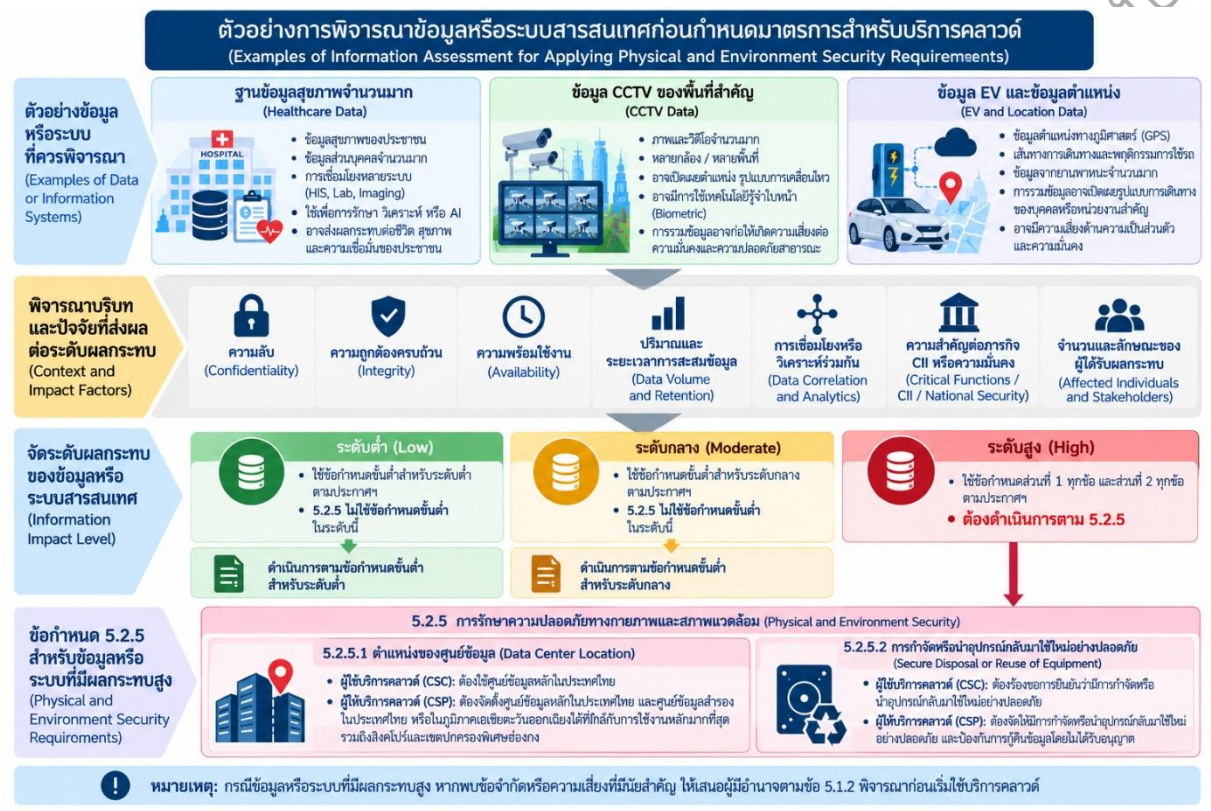
4. ตัวอย่างการนำไปใช้ในทางปฏิบัติ

4.1 กรณีระบบประชาสัมพันธ์บนบริการ SaaS หน่วยงานใช้บริการ SaaS เพื่อเผยแพร่ข้อมูลประชาสัมพันธ์ ไม่มีข้อมูลสำคัญหรือข้อมูลส่วนบุคคลที่มีนัยสำคัญ และผลการประเมินแสดงว่าระบบมีผลกระทบต่ำ

องค์กรอาจกำหนดเจ้าของบริการ ผู้ดูแลบริการ และผู้ประสานงาน CSP ให้ชัดเจน และให้อำนาจการตัดสินใจทั่วไปอยู่ในระดับหน่วยงานเจ้าของระบบตามเกณฑ์ที่องค์กรกำหนด โดยไม่จำเป็นต้องนำทุกการเปลี่ยนแปลงเข้าสู่คณะกรรมการระดับสูง

ร่างสำหรับ Public Hearing ห้ามนำไปอ้างอิง

ตัวอย่าง การกำกับดูแลควรเหมาะสมกับผลกระทบ ไม่ควรสร้างภาระเกินความจำเป็นสำหรับข้อมูลหรือระบบสารสนเทศที่มีความสำคัญหรือได้รับการประเมินว่ามีผลกระทบระดับสูง โดยเฉพาะข้อมูลหรือระบบที่เกี่ยวข้องกับบริการสำคัญ ข้อมูลส่วนบุคคลหรือข้อมูลที่มีความอ่อนไหวจำนวนมาก โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อมูลที่อาจมีผลต่อความมั่นคง หน่วยงานที่มีหน้าที่ควบคุมหรือกำกับดูแลที่เกี่ยวข้องควรพิจารณากำหนดแนวทางการควบคุม กำกับดูแล หรือติดตามให้เหมาะสมกับลักษณะข้อมูล ระดับผลกระทบ ความเสี่ยง และบริบทของภาคส่วนที่อยู่ภายใต้การกำกับดูแล ทั้งนี้ ตัวอย่างการพิจารณาข้อมูลหรือระบบสารสนเทศที่อาจนำมาใช้ประกอบการกำหนดแนวทางดังกล่าวแสดงดังรูปที่ 4



รูปที่ 4 ตัวอย่างการพิจารณาข้อมูลหรือระบบสารสนเทศที่มีความสำคัญ หรือมีผลกระทบระดับสูงสำหรับการกำกับดูแลบริการคลาวด์

หมายเหตุ: กรณีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง หากพบข้อจำกัดหรือความเสี่ยงที่มีนัยสำคัญ ควรเสนอผู้มีอำนาจตามข้อ 5.1.2 พิจารณาก่อนเริ่มใช้บริการ หรือเมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อระดับความเสี่ยงอย่างมีนัยสำคัญ

การกำกับดูแลดังกล่าวไม่ควรพิจารณาเฉพาะประเภทของข้อมูล แต่ควรพิจารณาร่วมกับความสำคัญของบริการ ปริมาณและการสะสมของข้อมูล ความสามารถในการเชื่อมโยงหรือวิเคราะห์ข้อมูล ผลกระทบต่อบุคคลหรือผู้มีส่วนได้เสีย ความต่อเนื่องของภารกิจ ตลอดจนประเด็นด้านอธิปไตยข้อมูลและเขตอำนาจทาง

กฎหมาย โดย CSC และ CSP ควรนำแนวทางของหน่วยงานที่เกี่ยวข้องมาใช้ประกอบการกำหนดความรับผิดชอบและมาตรการควบคุมตามขอบเขตที่แต่ละฝ่ายรับผิดชอบ

4.2 กรณีฐานข้อมูลสุขภาพจำนวนมาก หน่วยงานต้องการใช้บริการคลาวด์สำหรับระบบที่ประมวลผลฐานข้อมูลสุขภาพของประชาชนจำนวนมาก

การแบ่งหน้าที่ไม่ควรระบุเพียงว่า “ฝ่าย IT ดูแล Cloud” แต่ควรกำหนดอย่างน้อยว่าใครเป็นเจ้าของบริการ ใครเป็นเจ้าของข้อมูล ใครประเมินความมั่นคงปลอดภัย ใครพิจารณาการคุ้มครองข้อมูลส่วนบุคคล ใครพิจารณากฎหมายและเขตอำนาจทางกฎหมาย และใครมีอำนาจตัดสินใจหากพบข้อจำกัดที่มีนัยสำคัญ

หาก CSP สามารถตอบสนองข้อกำหนดส่วนใหญ่ แต่มีข้อจำกัดเกี่ยวกับสถานที่ประมวลผล ผู้รับจ้างช่วง หรือการควบคุมข้อมูลบางประการ ประเด็นดังกล่าวควรถูกประเมินเป็นความเสี่ยงและเสนอผู้มีอำนาจตามระดับที่กำหนด ไม่ควรให้ผู้จัดซื้อหรือผู้ดูแลระบบยอมรับเงื่อนไขดังกล่าวโดยลำพัง

4.3 กรณีข้อมูล CCTV ของพื้นที่สำคัญ หน่วยงานใช้บริการคลาวด์จัดเก็บและวิเคราะห์ข้อมูล CCTV จำนวนมากจากหลายพื้นที่

การกำหนดความรับผิดชอบควรครอบคลุมผู้รับผิดชอบข้อมูล ผู้รับผิดชอบระบบ ผู้ดูแลสิทธิ ผู้ประเมินความเสี่ยง และผู้มีอำนาจตัดสินใจ โดยเฉพาะเมื่อการรวมข้อมูลสามารถเปิดเผยตำแหน่ง จุดเข้าออก รูปแบบการเคลื่อนที่ หรือข้อมูลที่มีความสำคัญต่อการรักษาความปลอดภัย

หาก CSP มีการเปลี่ยนผู้รับจ้างช่วงหรือสถานที่ประมวลผลข้อมูล การประเมินไม่ควรจำกัดอยู่ที่การเปลี่ยนแปลงทางเทคนิค แต่ควรมีผู้รับผิดชอบประเมินผลกระทบด้านข้อมูล กฎหมาย ความมั่นคงปลอดภัย และอธิปไตยข้อมูล และยกระดับการตัดสินใจตามความเสี่ยง

4.4 กรณีข้อมูล EV และข้อมูลตำแหน่งจำนวนมาก ระบบรวบรวมข้อมูลตำแหน่งและเส้นทางของยานพาหนะจำนวนมากอย่างต่อเนื่อง แม้ข้อมูลตำแหน่งแต่ละรายการอาจไม่ทำให้ระบบมีผลกระทบสูงโดยอัตโนมัติ แต่การสะสมและเชื่อมโยงข้อมูลอาจทำให้สามารถวิเคราะห์รูปแบบการเดินทาง พฤติกรรม หรือตำแหน่งของบุคคลหรือหน่วยงานสำคัญได้

จึงควรกำหนดผู้รับผิดชอบการประเมินผลกระทบในภาพรวมก่อนกำหนดระดับอำนาจในการตัดสินใจ หากผลการประเมินเป็นระดับสูง การยอมรับข้อจำกัดเกี่ยวกับสถานที่จัดเก็บ การเข้าถึง การถ่ายโอน หรือเขตอำนาจทางกฎหมายควรได้รับการพิจารณาจากผู้มีอำนาจตามระดับความเสี่ยง

4.5 กรณีความเสี่ยงหลายรายการรวมกัน ระบบบริการประชาชนที่มีความสำคัญพบประเด็นดังต่อไปนี้

- พึ่งพา CSP รายเดียว
- ศูนย์ข้อมูลสำรองเกี่ยวข้องกับต่างเขตอำนาจทางกฎหมาย
- การกู้คืนบริการยังไม่ได้รับการทดสอบในสถานการณ์ที่เพียงพอ
- CSC มีข้อจำกัดในการควบคุมกุญแจเข้ารหัสสำหรับข้อมูลบางส่วน

ความเสี่ยงแต่ละรายการอาจได้รับการประเมินแยกกันในระดับที่ยังยอมรับได้ แต่เมื่อพิจารณาร่วมกันอาจส่งผลต่อความต่อเนื่องของภารกิจ การคุ้มครองข้อมูล และอธิปไตยข้อมูลอย่างมีนัยสำคัญ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ในกรณีดังกล่าว ผู้รับผิดชอบด้านความเสี่ยงควรรวบรวมประเด็นในระดับบริการและเสนอทางเลือกแก่ผู้มีอำนาจตัดสินใจ เช่น ยอมรับความเสี่ยง เพิ่มมาตรการ เปลี่ยนรูปแบบบริการ หรือเลือกทางเลือกอื่น พร้อมกำหนดเจ้าของความเสี่ยงที่ยังคงเหลืออยู่หลังการตัดสินใจ

กรณีตัวอย่างข้างต้นสะท้อนให้เห็นว่า การกำกับดูแลตามข้อ 5.1.2 มิได้สิ้นสุดเพียงการระบุหรือบันทึกความเสี่ยง แต่ควรทำให้สามารถเชื่อมโยงความเสี่ยงที่มีนัยสำคัญไปสู่การตัดสินใจ ผู้มีอำนาจตัดสินใจ เจ้าของความเสี่ยงที่เหลืออยู่ และการติดตามผลได้อย่างชัดเจนและตรวจสอบย้อนกลับได้

5. การบันทึกและตรวจสอบย้อนกลับ สำหรับการตัดสินใจที่มีนัยสำคัญ ควรสามารถตรวจสอบความเชื่อมโยงได้อย่างน้อยดังนี้

ความเสี่ยง ⟶ ผลกระทบต่อข้อมูล ระบบ บริการ หรือภารกิจ ⟶ ทางเลือก ⟶ การตัดสินใจ ⟶ ผู้มีอำนาจตัดสินใจ ⟶ เจ้าของความเสี่ยงที่เหลืออยู่ ⟶ การติดตามและประเมินใหม่

หลักฐานอาจอยู่ในทะเบียนความเสี่ยง รายงานการประชุม บันทึกอนุมัติ ระบบบริหารความเสี่ยงระบบ GRC หรือเอกสารอื่นที่องค์กรใช้อยู่ ไม่จำเป็นต้องจัดทำเอกสารชุดใหม่หากสามารถตรวจสอบย้อนกลับได้อย่างเพียงพอ

6. ตัวอย่างหลักฐาน

ประเด็น	ตัวอย่างหลักฐาน
บทบาทภายใน CSC	นโยบาย ระเบียบปฏิบัติ คำสั่ง หรือเอกสารกำหนดหน้าที่
ความรับผิดชอบ CSC–CSP	สัญญา SLA เงื่อนไขบริการ หรือเอกสารความรับผิดชอบร่วม
ความรับผิดชอบของผู้ให้บริการภายนอก	สัญญา ข้อมูลผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง หรือเอกสารบริการตามความเหมาะสม
ผู้ประสานงาน	รายชื่อและช่องทางการติดต่อ
ผู้มีอำนาจตัดสินใจ	ตารางอำนาจอนุมัติหรือหลักเกณฑ์การยอมรับความเสี่ยง
เจ้าของความเสี่ยง	ทะเบียนความเสี่ยง
การตัดสินใจ	บันทึกอนุมัติ รายงานการประชุม หรือบันทึกการตัดสินใจ
การติดตาม	รายงานทบทวนความเสี่ยงหรือการทบทวนบริการ

7. การวัดผลในทางปฏิบัติ เพื่อให้สามารถแสดงผลของการนำแนวทางไปใช้ องค์กรอาจพิจารณาตัวชี้วัด เช่น

7.1 สัดส่วนบริการคลาวด์สำคัญที่มีการกำหนดเจ้าของบริการและเจ้าของข้อมูลอย่างชัดเจน

7.2 สัดส่วนบริการคลาวด์ที่มีการระบุความรับผิดชอบระหว่าง CSC และ CSP

7.3 จำนวนช่องว่างของความรับผิดชอบที่ตรวจพบและได้รับการแก้ไข

7.4 สัดส่วนความเสี่ยงระดับสูงที่สามารถระบุผู้มีอำนาจตัดสินใจได้

7.5 สัดส่วนความเสี่ยงที่เหลืออยู่ระดับสูงที่มีเจ้าของความเสี่ยง

7.6 สัดส่วนการตัดสินใจที่มีนัยสำคัญซึ่งสามารถตรวจสอบย้อนกลับจากความเสี่ยงไปยังการตัดสินใจและผู้รับผิดชอบได้

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ตัวชี้วัดดังกล่าวเป็นเพียงตัวอย่าง องค์กรควรกำหนดค่าเป้าหมายและวิธีการวัดให้เหมาะสมกับบริบทและระดับความพร้อมของตน

5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)

การใช้บริการคลาวด์อาจเกี่ยวข้องกับหน่วยงานภายนอกหลายประเภท เช่น หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล หน่วยงานบังคับใช้กฎหมาย หรือหน่วยงานอื่นที่มีอำนาจหน้าที่ตามกฎหมาย ทั้งนี้ หน่วยงานที่เกี่ยวข้องอาจแตกต่างกันตามภารกิจ ประเภทของข้อมูลหรือระบบสารสนเทศ ระดับผลกระทบ และลักษณะของบริการคลาวด์

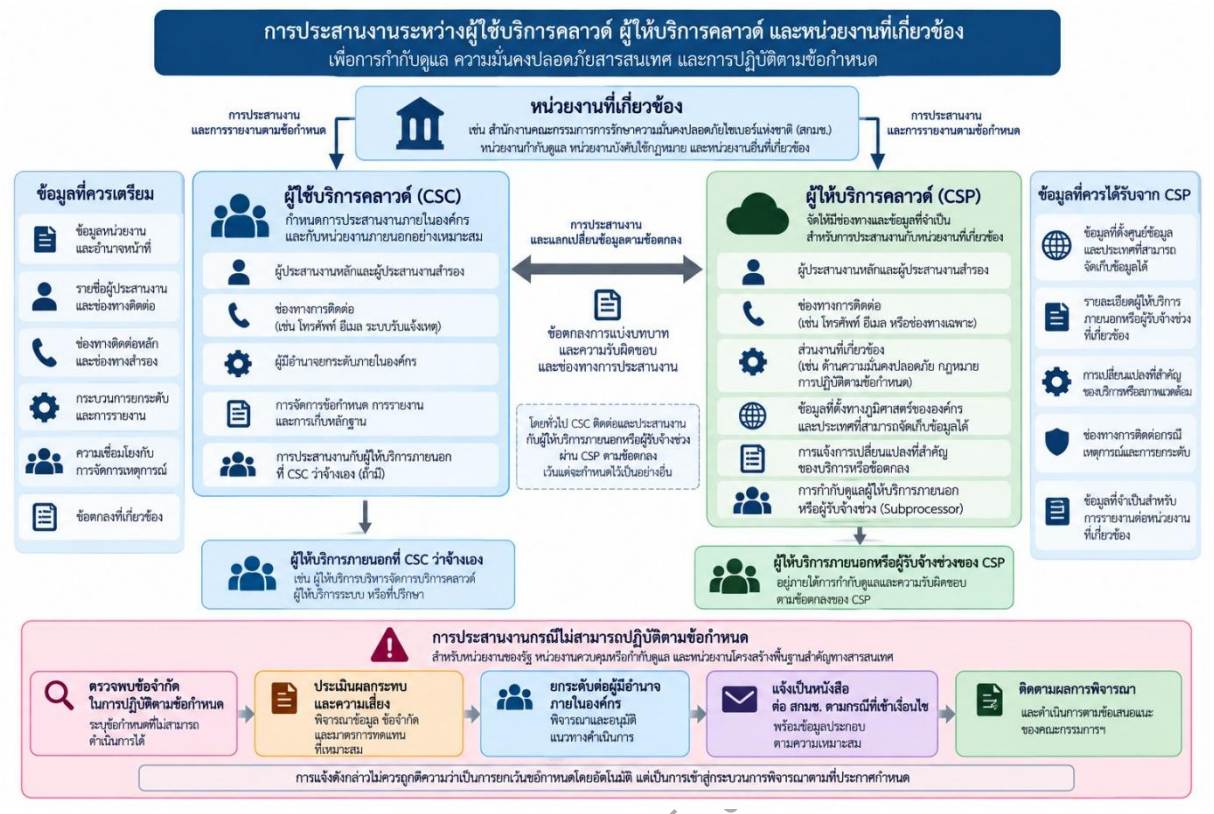
การระบุหน่วยงานที่เกี่ยวข้องไว้ล่วงหน้ามีวัตถุประสงค์เพื่อให้ CSC และ CSP สามารถประสานงานได้อย่างเหมาะสมเมื่อมีเหตุหรือสถานการณ์ที่จำเป็น โดยไม่ต้องเริ่มค้นหาหน่วยงาน ผู้รับผิดชอบ หรือช่องทางการติดต่อภายหลังจากเกิดเหตุแล้ว

ในบริบทของบริการคลาวด์ การประสานงานดังกล่าวมีความเกี่ยวข้องกับที่ตั้งทางภูมิศาสตร์ของ CSP และประเทศที่ข้อมูลของ CSC อาจถูกจัดเก็บ เนื่องจากปัจจัยดังกล่าวอาจทำให้เกิดความเกี่ยวข้องกับหน่วยงานกฎหมาย หรือเขตอำนาจทางกฎหมายที่แตกต่างกัน โดยเฉพาะกรณีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง หรือมีข้อกำหนดเฉพาะด้านที่ตั้งและการควบคุมข้อมูล

อย่างไรก็ตาม ข้อ 5.1.2.2 มุ่งเน้นที่ การระบุหน่วยงาน การกำหนดช่องทางและความพร้อมในการประสานงาน ส่วนการวิเคราะห์กฎหมาย เขตอำนาจทางกฎหมาย และข้อกำหนดตามสัญญาให้พิจารณาตามข้อ 5.1.3 และการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศให้พิจารณาตามข้อ 5.2.10 เพื่อหลีกเลี่ยงความซ้ำซ้อนของข้อกำหนด

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ควรแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูล ผู้ใช้บริการคลาวด์ได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปที่ 5 แนวทางการประสานงานระหว่างผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และหน่วยงานที่เกี่ยวข้อง

วัตถุประสงค์

1. เพื่อให้ CSC สามารถระบุหน่วยงานที่อาจจำเป็นต้องติดต่อหรือประสานงานเกี่ยวกับบริการคลาวด์ได้อย่างเหมาะสมกับภารกิจ ลักษณะบริการ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และข้อกำหนดที่เกี่ยวข้อง

2. เพื่อให้มีการกำหนดผู้รับผิดชอบและช่องทางการประสานงานระหว่าง CSC, CSP และหน่วยงานที่เกี่ยวข้องอย่างเหมาะสม เพื่อสนับสนุนการดำเนินงาน การกำกับดูแล และการตอบสนองต่อสถานการณ์ที่จำเป็น

3. เพื่อให้ CSC ได้รับข้อมูลเกี่ยวกับที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของ CSP และประเทศที่ข้อมูลของ CSC สามารถถูกจัดเก็บ เพื่อใช้เป็นข้อมูลประกอบการพิจารณากฎหมาย เขตอำนาจทางกฎหมาย อธิปไตยข้อมูล และข้อกำหนดด้านตำแหน่งของข้อมูลในหัวข้อที่เกี่ยวข้อง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การระบุหน่วยงานที่เกี่ยวข้อง CSC ต้องระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่าง CSC และ CSP โดยพิจารณาตามบริบทขององค์กร ภารกิจ ประเภทของบริการ ข้อมูลหรือระบบสารสนเทศ และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง หน่วยงานที่อาจเกี่ยวข้อง ตัวอย่างเช่น

ร่างสำหรับ Public Hearing

ประเภทหน่วยงาน	ตัวอย่างกรณีที่อาจเกี่ยวข้อง
หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์	การประสานงานเกี่ยวกับภัยคุกคามหรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
หน่วยงานควบคุมหรือกำกับดูแลเฉพาะภาคส่วน	ระบบหรือบริการอยู่ภายใต้การกำกับดูแลเฉพาะด้าน
หน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล	กรณีเกี่ยวข้องกับการประมวลผลหรือเหตุการณ์ที่กระทบข้อมูลส่วนบุคคล
หน่วยงานบังคับใช้กฎหมาย	กรณีมีเหตุหรือคำร้องขอที่อยู่ภายใต้อำนาจตามกฎหมาย
หน่วยงานตอบสนองหรือประสานงานเหตุการณ์	กรณีจำเป็นต้องประสานเพื่อรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย
หน่วยงานอื่นที่มีอำนาจหน้าที่ตามกฎหมาย	ตามลักษณะภารกิจ ข้อมูล ระบบ หรือบริการของ CSC

CSC ไม่จำเป็นต้องกำหนดหน่วยงานทุกประเภทสำหรับบริการคลาวด์ทุกบริการ แต่ควรสามารถระบุหน่วยงานที่มีความเกี่ยวข้องจริงและเหตุผลของความเกี่ยวข้องได้

ตัวอย่าง หน่วยงานใช้ SaaS สำหรับระบบงานสนับสนุนภายในที่ไม่มีข้อมูลสำคัญ การระบุหน่วยงานที่เกี่ยวข้องอาจใช้โครงสร้างการประสานงานตามปกติขององค์กร โดยไม่จำเป็นต้องสร้างรายชื่อหน่วยงานจำนวนมากเฉพาะสำหรับบริการดังกล่าว

ในทางกลับกัน หากบริการคลาวด์รองรับระบบที่เกี่ยวข้องกับ CII CSC ควรระบุหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานที่เกี่ยวข้องกับภาคส่วนนั้นไว้ล่วงหน้า เนื่องจากการประสานงานอาจมีความสำคัญต่อการดำเนินภารกิจและการปฏิบัติตามกฎหมาย

2. การกำหนดผู้รับผิดชอบในการประสานงาน CSC ควรกำหนดผู้รับผิดชอบหรือบทบาทที่ทำหน้าที่ประสานงานกับ CSP และหน่วยงานที่เกี่ยวข้อง โดยสามารถใช้บทบาทที่องค์กรมีอยู่เดิมได้ ควรพิจารณาอย่างน้อยว่า

2.1 ใครเป็นผู้ประสานงานหลัก
2.2 ใครสามารถปฏิบัติหน้าที่แทนได้เมื่อผู้ประสานงานหลักไม่พร้อม
2.3 ใครมีอำนาจให้หรือรับข้อมูลที่เกี่ยวข้อง
2.4 ใครมีหน้าที่ยกระดับเรื่องไปยังผู้มีอำนาจตัดสินใจ
2.5 ช่องทางใดใช้สำหรับการติดต่อในกรณีปกติและกรณีเร่งด่วน

ไม่จำเป็นต้องกำหนดบุคคลเดียวให้ประสานงานทุกเรื่อง ตัวอย่างเช่น ประเด็นด้านความมั่นคงปลอดภัยอาจอยู่กับหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศ ขณะที่ประเด็นข้อมูลส่วนบุคคลอาจต้องประสานกับผู้รับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การกำหนดช่องทางการติดต่อ CSC ควรจัดให้มีข้อมูลการติดต่อที่เพียงพอและเป็นปัจจุบันสำหรับ CSP และหน่วยงานที่เกี่ยวข้อง โดยระดับรายละเอียดควรเหมาะสมกับความสำคัญของบริการ

ข้อมูลอาจประกอบด้วยชื่อหน่วยงาน บทบาทหรือส่วนงานที่ต้องติดต่อ ช่องทางการติดต่อ เวลาที่สามารถติดต่อได้ และช่องทางสำหรับกรณีเร่งด่วนตามความจำเป็น

สำหรับระบบที่มีผลกระทบสูงหรือสนับสนุนภารกิจสำคัญ ควรพิจารณาว่าช่องทางดังกล่าวสามารถรองรับการประสานงานภายในระยะเวลาที่เหมาะสมกับความสำคัญของบริการหรือไม่

ตัวอย่าง ระบบบริการประชาชนที่ให้บริการตลอด 24 ชั่วโมงไม่ควรพึ่งพาเพียงอีเมลสนับสนุนทั่วไปที่มีเวลาตอบกลับหลายวัน หากลักษณะของบริการอาจจำเป็นต้องประสาน CSP อย่างเร่งด่วน CSC ควรตรวจสอบว่ามีช่องทางยกระดับที่เหมาะสมตามข้อตกลงหรือระดับบริการหรือไม่

4. การทบทวนข้อมูลการประสานงาน CSC ควรทบทวนข้อมูลหน่วยงาน ผู้ประสานงาน และช่องทางการติดต่อเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้อง เช่น

4.1 การเปลี่ยน CSP หรือรูปแบบบริการ
4.2 การเปลี่ยนผู้ประสานงาน
4.3 การเปลี่ยนขอบเขตของระบบหรือบริการ
4.4 การเปลี่ยนหน่วยงานกำกับดูแลที่เกี่ยวข้อง
4.5 การเปลี่ยนแปลงกฎหมายหรือข้อกำหนด
4.6 การเปลี่ยนแปลงประเทศที่เกี่ยวข้องกับการจัดเก็บหรือประมวลผลข้อมูล
4.7 ผลจากเหตุการณ์หรือการทดสอบที่พบว่าช่องทางเดิมไม่เพียงพอ

ไม่จำเป็นต้องกำหนดรอบทบทวนเฉพาะขึ้นใหม่ หากองค์กรมีการทบทวนข้อมูลผู้ติดต่อ สัญญาบริการ หรือความเสี่ยงเป็นระยะอยู่แล้ว

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การแจ้งที่ตั้งทางภูมิศาสตร์ขององค์กร CSP ควรแจ้ง CSC ให้ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของ CSP ตามที่ประกาศกำหนด เพื่อให้ CSC มีข้อมูลเพียงพอสำหรับพิจารณาข้อกำหนดที่อาจเกี่ยวข้องกับบริการ

ข้อมูลดังกล่าวมีความสำคัญเนื่องจากที่ตั้งขององค์กรที่เป็นเจ้าของ CSP อาจเกี่ยวข้องกับกฎหมาย เขตอำนาจทางกฎหมาย หรือข้อกำหนดอื่นที่ CSC จำเป็นต้องพิจารณา อย่างไรก็ตาม การวิเคราะห์ว่ากฎหมายหรือเขตอำนาจดังกล่าวมีผลอย่างไรต่อ CSC เป็นสาระของข้อ 5.1.3 ไม่ควรขยายรายละเอียดทางกฎหมายในข้อ 5.1.2.2

2. การแจ้งประเทศที่สามารถจัดเก็บข้อมูลของ CSC โดย CSP ควรแจ้ง CSC ให้ทราบถึงประเทศที่ CSP สามารถจัดเก็บข้อมูลของ CSC ได้ตามที่ประกาศกำหนด ข้อมูลนี้ควรมีความชัดเจนเพียงพอให้ CSC สามารถนำไปประกอบการพิจารณาความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง โดยเฉพาะในกรณีที่บริการสามารถย้าย ทำสำเนา สำรอง หรือจัดเก็บข้อมูลในหลายประเทศตามสถาปัตยกรรมหรือเงื่อนไขของบริการ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่าง บริการ SaaS ระบุเพียงว่าให้บริการใน “ภูมิภาคเอเชีย” แต่ไม่ได้ทำให้ CSC ทราบว่าข้อมูลสามารถถูกจัดเก็บในประเทศใดได้บ้าง หากข้อมูลดังกล่าวมีความจำเป็นต่อการประเมินข้อกำหนดของ CSC ควรมีข้อมูลเพิ่มเติมในระดับที่ทำให้ CSC สามารถประเมินได้ว่าบริการสอดคล้องกับข้อกำหนดของตนหรือไม่

ประเด็นนี้ไม่ควรถูกตีความว่าข้อ 5.1.2.2 เป็นข้อกำหนดเรื่องตำแหน่งศูนย์ข้อมูลโดยตรง เนื่องจากข้อกำหนดด้านตำแหน่งของศูนย์ข้อมูลสำหรับระบบที่เข้าเกณฑ์ให้พิจารณาตามข้อ 5.2.5.1

3. การแจ้งการเปลี่ยนแปลงที่มีนัยสำคัญ ในกรณีที่ข้อมูลเกี่ยวกับที่ตั้งขององค์กรหรือประเทศที่สามารถจัดเก็บข้อมูลมีการเปลี่ยนแปลง และการเปลี่ยนแปลงนั้นอาจมีผลต่อข้อกำหนดหรือความเสี่ยงของ CSC ควรมีกลไกที่ทำให้ CSC สามารถรับทราบและนำไปประเมินผลกระทบได้ตามความเหมาะสม ทั้งนี้ รายละเอียดและระยะเวลาการแจ้งควรพิจารณาตามสัญญา ลักษณะบริการ และข้อกำหนดที่เกี่ยวข้อง ไม่ควรกำหนดระยะเวลาตายตัวเพิ่มเติมในแนวทางนี้หากประกาศมิได้กำหนดไว้

ตัวอย่าง เดิมบริการกำหนดให้ข้อมูลของ CSC สามารถจัดเก็บได้เฉพาะในประเทศที่ CSC ได้ประเมินไว้แล้ว ต่อมา CSP เพิ่มประเทศใหม่เข้าสู่ขอบเขตการให้บริการ หากการเปลี่ยนแปลงดังกล่าวอาจมีผลต่อกฎหมาย สัญญา หรือความเสี่ยงของ CSC ควรทำให้ CSC สามารถรับทราบก่อนหรือภายในระยะเวลาที่เหมาะสมตามข้อตกลง เพื่อประเมินว่าจำเป็นต้องดำเนินการเพิ่มเติมหรือไม่

4. การสนับสนุนการประสานงาน CSP ควรจัดให้มีช่องทางที่เหมาะสมสำหรับการประสานงานกับ CSC ตามลักษณะบริการและข้อตกลง โดยเฉพาะกรณีที่ CSC จำเป็นต้องประสานงานกับหน่วยงานภายนอกในเรื่องที่เกี่ยวข้องกับบริการของ CSP

CSP ควรสามารถให้ข้อมูลหรือสนับสนุนการประสานงานในขอบเขตที่ตนรับผิดชอบ โดยคำนึงถึงข้อจำกัดด้านกฎหมาย สัญญา ความลับ และความมั่นคงปลอดภัยของบริการ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines) การนำข้อกำหนดนี้ไปปฏิบัติควรมุ่งให้ CSC สามารถตอบคำถามพื้นฐานได้ว่า

บริการนี้เกี่ยวข้องกับหน่วยงานใด ⟶ ใครเป็นผู้ประสานงาน ⟶ ติดต่อผ่านช่องทางใด ⟶ CSP ต้องให้ข้อมูลอะไร ⟶ หากข้อมูลหรือเงื่อนไขเปลี่ยนแปลง ใครต้องนำไปพิจารณาต่อ

ไม่จำเป็นต้องสร้างกระบวนการใหม่แยกต่างหาก หากองค์กรสามารถใช้ทะเบียนผู้ติดต่อ แผนตอบสนองเหตุการณ์ กระบวนการบริหารบริการ สัญญา หรือระบบบริหารความเสี่ยงที่มีอยู่เพื่อรองรับข้อกำหนดนี้ได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. การจัดทำแผนผังการประสานงาน องค์กรอาจจัดทำแผนผังหรือตารางอย่างง่ายเพื่อแสดงความสัมพันธ์ระหว่าง CSC, CSP และหน่วยงานที่เกี่ยวข้อง เช่น

ประเด็น	CSC	CSP	หน่วยงานที่เกี่ยวข้อง
ความมั่นคงปลอดภัยไซเบอร์	ผู้ประสานงานด้านความมั่นคงปลอดภัย	ช่องทางด้านความมั่นคงปลอดภัยหรือส่วนสนับสนุน (Security/Support)	หน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้อง
ข้อมูลส่วนบุคคล	ผู้รับผิดชอบด้านการคุ้มครองข้อมูล	ผู้ประสานงานด้านการคุ้มครองข้อมูลของ CSP	หน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้อง
การหยุดชะงักของบริการ	เจ้าของบริการ/ผู้ดูแลระบบ	ส่วนสนับสนุนบริการและช่องทางยกระดับ (Service Support/Escalation)	หน่วยงานที่เกี่ยวข้อง หากเข้าเงื่อนไข
คำร้องหรือคำสั่งตามกฎหมาย	ฝ่ายกฎหมายหรือผู้ได้รับมอบหมาย	ส่วนกฎหมายและการปฏิบัติตามข้อกำหนด (Legal/Compliance) ของ CSP	หน่วยงานผู้มีอำนาจตามกฎหมาย
การเปลี่ยนประเทศที่จัดเก็บข้อมูล	เจ้าของบริการ/ความเสี่ยง/กฎหมาย	CSP แจ้งข้อมูลการเปลี่ยนแปลง	พิจารณาตามกฎหมายและบริบท

ตารางนี้เป็นเพียงตัวอย่าง ไม่ได้กำหนดว่าทุกองค์กรต้องใช้บทบาทหรือช่องทางตามที่ระบุ

2. การเชื่อมโยงกับระดับผลกระทบ เนื่องจาก 5.1.2 เป็นข้อกำหนดขั้นต่ำตั้งแต่ระดับผลกระทบต่ำ การมีช่องทางประสานงานจึงไม่ควรจำกัดเฉพาะระบบผลกระทบสูง อย่างไรก็ตาม ระดับความเข้มข้นของการเตรียมการประสานงานสามารถแตกต่างกันตามผลกระทบ เช่น

ระดับผลกระทบ	ตัวอย่างแนวทาง
ต่ำ	ระบุผู้ประสานงานและช่องทางพื้นฐานตามกระบวนการปกติ
กลาง	เพิ่มการพิจารณาหน่วยงานกำกับดูแล กฎหมาย ข้อมูลส่วนบุคคล และช่องทางยกระดับตามความเกี่ยวข้อง
สูง	กำหนดเส้นทางประสานงานและการยกระดับที่ชัดเจน ตรวจสอบความพร้อมของช่องทาง และเชื่อมโยงผู้มีอำนาจตัดสินใจตาม 5.1.2.1

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้งานจริง

3. การเชื่อมโยงกับที่ตั้งและอธิปไตยข้อมูล ข้อมูลที่ CSP แจ้งเกี่ยวกับที่ตั้งขององค์กรและประเทศที่สามารถจัดเก็บข้อมูลควรถูกนำไปใช้เป็นข้อมูลนำเข้าสำหรับการประเมินในหัวข้ออื่นที่เกี่ยวข้อง มิใช่เก็บไว้เพียงเพื่อเป็นหลักฐานว่ามีการแจ้ง แนวทางการเชื่อมโยงสามารถแสดงได้ดังนี้

ประเทศที่สามารถจัดเก็บข้อมูล ⟶ กฎหมายและเขตอำนาจที่เกี่ยวข้อง ⟶ ข้อกำหนดตามสัญญา ⟶ ความเสี่ยงต่อข้อมูลและภารกิจ ⟶ การตัดสินใจและมาตรการที่เหมาะสม

โดย

- 5.1.1 กำหนดหลักการด้านความเสี่ยงและอธิปไตยข้อมูล
- 5.1.2 กำหนดผู้รับผิดชอบและการประสานงาน
- 5.1.3 พิจารณากฎหมาย เขตอำนาจ และข้อกำหนดตามสัญญา
- 5.2.5.1 กำหนดมาตรการด้านตำแหน่งศูนย์ข้อมูลสำหรับกรณีที่ข้อกำหนดดังกล่าวบังคับใช้

4. การเชื่อมโยงกับการจัดการเหตุการณ์ หากการประสานงานเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ให้ใช้ช่องทางและผู้รับผิดชอบที่กำหนดตาม 5.1.2.2 เป็นองค์ประกอบสนับสนุนการดำเนินการตามข้อ 5.2.10 “เมื่อเกิดเหตุการณ์แล้วต้องประเมิน รายงาน ตอบสนอง เรียนรู้ และจัดการหลักฐานอย่างไร”

5. ตัวอย่างการนำไปใช้ในทางปฏิบัติ

5.1 กรณีระบบงานทั่วไป หน่วยงานใช้ SaaS สำหรับระบบสนับสนุนภายในที่มีผลกระทบต่ำ CSC ระบุผู้ประสานงานของหน่วยงาน ช่องทางสนับสนุนของ CSP และหน่วยงานที่อาจเกี่ยวข้องตามบริบทไว้ในทะเบียนผู้ติดต่อ ในกรณีนี้ ไม่จำเป็นต้องจัดทำโครงสร้างประสานงานที่ซับซ้อนหรือกำหนดการยกระดับถึงผู้บริหารระดับสูงสำหรับทุกเหตุการณ์ การเตรียมการควรเหมาะสมกับระดับผลกระทบ

5.2 กรณีระบบที่เกี่ยวข้องกับ CII โดย CSC ใช้บริการคลาวด์รองรับระบบที่มีความสำคัญต่อ CII จึงระบุหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ประสานงานของ CSP และผู้มีอำนาจภายในองค์กรไว้ล่วงหน้า หากเกิดเหตุการณ์ที่มีนัยสำคัญ เส้นทางการประสานงานจึงสามารถดำเนินจาก

ผู้ตรวจพบ ⟶ ผู้รับผิดชอบระบบ/ความมั่นคงปลอดภัย ⟶ CSP ⟶ ผู้มีอำนาจภายใน ⟶ หน่วยงานที่เกี่ยวข้อง

ตามเงื่อนไขและหน้าที่ที่กฎหมายหรือกระบวนการขององค์กรกำหนด โดยรายละเอียดการจัดการเหตุให้ดำเนินการตามข้อ 5.2.10

5.3 กรณี CSP เปลี่ยนประเทศที่สามารถจัดเก็บข้อมูล CSC ใช้บริการคลาวด์สำหรับข้อมูลสำคัญ โดยได้ประเมินกฎหมายและความเสี่ยงจากประเทศที่ CSP แจ้งไว้แล้ว ต่อมา CSP แจ้งว่าบริการอาจจัดเก็บข้อมูลในประเทศเพิ่มเติม

ผู้ประสานงานไม่ควรเพียงรับทราบการแจ้งแล้วปิดเรื่อง แต่ควรส่งต่อข้อมูลไปยังผู้รับผิดชอบที่เกี่ยวข้องเพื่อพิจารณาว่าการเปลี่ยนแปลงดังกล่าวมีผลต่อกฎหมาย สัญญา อธิปไตยข้อมูล หรือความเสี่ยงของบริการหรือไม่ และหากมีนัยสำคัญให้เชื่อมโยงกับผู้มีอำนาจตัดสินใจตามข้อ 5.1.2.1

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

5.4 กรณีข้อมูลสุขภาพจำนวนมาก หน่วยงานใช้บริการคลาวด์สำหรับฐานข้อมูลสุขภาพจำนวนมาก โดย CSP แจ้งว่าข้อมูลสามารถจัดเก็บในหลายประเทศ

ในกรณีนี้ 5.1.2.2 ไม่ได้ทำหน้าที่ตัดสินว่าแต่ละประเทศ “ใช้ได้หรือไม่ได้” แต่ทำหน้าที่ให้ CSC ได้รับข้อมูลที่จำเป็นและมีผู้รับผิดชอบในการนำข้อมูลนั้นไปพิจารณาต่อ

CSC จึงควรเชื่อมข้อมูลประเทศที่จัดเก็บข้อมูลไปยังการพิจารณากฎหมายและข้อกำหนดตามข้อ 5.1.3 รวมทั้งเชื่อมโยงกับการประเมินความเสี่ยงและอธิปไตยข้อมูลตาม 5.1.1 และหากเป็นระบบที่เข้าข่ายผลกระทบสูง ให้พิจารณาข้อกำหนด 5.2.5 ที่เกี่ยวข้องต่อไป

ตัวอย่างนี้ช่วยให้เห็นความแตกต่างชัดเจนว่า 5.1.2.2 = ผู้เกี่ยวข้องและการประสานงาน ไม่ใช่ การวิเคราะห์กฎหมาย หรือ การกำหนดตำแหน่งศูนย์ข้อมูล

6. การประสานงานกรณีไม่สามารถปฏิบัติตามข้อกำหนด ในกรณีที่หน่วยงานตรวจพบว่าไม่สามารถดำเนินการให้เป็นไปตามข้อกำหนดของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่เกี่ยวข้องได้ หน่วยงานควรกำหนดกระบวนการยกระดับและผู้รับผิดชอบในการประสานงานให้ชัดเจน

สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ดำเนินการตามประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย พ.ศ. 2567 ซึ่งกำหนดให้กรณีไม่สามารถดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้ต้องแจ้งเป็นหนังสือมายังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อดำเนินการตามกระบวนการที่กำหนดต่อไป ก่อนการแจ้งหน่วยงานควรมีข้อมูลประกอบที่เพียงพอตามความเหมาะสม เช่น

- ข้อกำหนดที่ไม่สามารถปฏิบัติตามได้
- ระบบหรือบริการคลาวด์ที่เกี่ยวข้อง
- สาเหตุหรือข้อจำกัด
- ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
- ความเสี่ยงที่เกิดขึ้นหรืออาจเกิดขึ้น
- มาตรการทดแทนหรือมาตรการลดความเสี่ยงที่ได้ดำเนินการหรือเสนอไว้
- ผู้มีอำนาจที่ได้พิจารณาประเด็นดังกล่าว
- แนวทางการติดตามหรือแก้ไขต่อไป

7. หลักฐานที่ควรมี

ประเด็น	ตัวอย่างหลักฐาน
หน่วยงานที่เกี่ยวข้อง	รายชื่อหน่วยงานหรือทะเบียนผู้ติดต่อ
ผู้ประสานงาน CSC	เอกสารกำหนดบทบาท รายชื่อผู้ประสานงาน หรือแผนการติดต่อ
ช่องทาง CSP	SLA, Support Plan, Escalation Matrix หรือข้อมูลติดต่อ
ที่ตั้งองค์กรของ CSP	ข้อมูลบริการ สัญญา เอกสารกำกับดูแล หรือข้อมูลที่ CSP แจ้ง
ประเทศที่สามารถจัดเก็บข้อมูล	ข้อมูลตำแหน่งหรือภูมิภาคที่จัดเก็บข้อมูล (Data Location/Region Information), สัญญาหรือข้อตกลง (Contract/Agreement) หรือเอกสารบริการ

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การเปลี่ยนแปลง	การแจ้งการเปลี่ยนแปลง (Change Notification) หรือบันทึกการแจ้ง
การทบทวน	รายงานทบทวนบริการ ทะเบียนผู้ติดต่อ หรือหลักฐานการปรับปรุงข้อมูล

หลักฐานไม่จำเป็นต้องจัดทำเป็นเอกสารใหม่ หากข้อมูลที่องค์กรมีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

8. การวัดผลในทางปฏิบัติ เพื่อประเมินว่าการประสานงานสามารถใช้งานได้จริง องค์กรอาจกำหนดตัวชี้วัดตามบริบท เช่น

- สัดส่วนบริการคลาวด์สำคัญที่ระบุผู้ประสานงาน CSC และช่องทางติดต่อ CSP แล้ว
- สัดส่วนระบบที่เกี่ยวข้องกับหน่วยงานกำกับดูแลซึ่งระบุช่องทางประสานงานไว้แล้ว
- สัดส่วนบริการที่มีข้อมูลประเทศซึ่งสามารถจัดเก็บข้อมูลของ CSC
- สัดส่วนข้อมูลผู้ติดต่อที่ได้รับการทบทวนตามเงื่อนไขที่กำหนด
- จำนวนกรณีที่พบว่าช่องทางประสานงานไม่สามารถใช้งานได้หรือไม่เป็นปัจจุบัน และได้รับการแก้ไขแล้ว

ไม่จำเป็นต้องกำหนดค่าเป้าหมายเดียวกันสำหรับทุกองค์กร แต่ควรกำหนดให้สัมพันธ์กับความสำคัญของบริการและระดับความเสี่ยง

สรุปข้อกำหนดและความรับผิดชอบด้านโครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security Requirements and Responsibility Summary)

หลักการการกำหนดโครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ควรดำเนินการตามหลักการสำคัญ ดังต่อไปนี้

1.1 ความรับผิดชอบร่วม (Shared Responsibility) CSC และ CSP ควรกำหนดและตกลงขอบเขตบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้ชัดเจนตามรูปแบบบริการคลาวด์ ขอบเขตบริการ สถาปัตยกรรมของบริการ และข้อตกลงที่เกี่ยวข้อง

การกำหนดความรับผิดชอบควรทำให้สามารถระบุได้ว่า กิจกรรมใดอยู่ภายใต้ความรับผิดชอบของ CSC กิจกรรมใดอยู่ภายใต้ความรับผิดชอบของ CSP กิจกรรมใดต้องดำเนินการร่วมกัน และกิจกรรมใดเกี่ยวข้องกับผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง เพื่อป้องกันช่องว่างของความรับผิดชอบ (Responsibility Gap)

1.2 การกำหนดบทบาทและอำนาจตัดสินใจตามความเสี่ยง การกำหนดผู้รับผิดชอบการดำเนินงานไม่ควรถูกตีความว่าเป็นการให้อำนาจบุคคลดังกล่าวยอมรับความเสี่ยงทุกประเภท องค์กรควรกำหนดระดับอำนาจในการตัดสินใจให้เหมาะสมกับระดับผลกระทบ ความสำคัญของบริการ และระดับความเสี่ยง

สำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง หรือการตัดสินใจที่อาจมีผลต่อภารกิจสำคัญ ความมั่นคง ความต่อเนื่องของบริการ ข้อมูลที่มีความอ่อนไหวจำนวนมาก หรืออธิปไตยข้อมูล ควรยกระดับการพิจารณาไปยังผู้มีอำนาจในระดับที่เหมาะสม

1.3 ความรับผิดชอบต่อการตัดสินใจ (Decision Accountability) สำหรับความเสี่ยงที่มีนัยสำคัญ องค์กรควรสามารถเชื่อมโยงข้อมูลหรือสัญญาณความเสี่ยงไปสู่การประเมินในภาพรวม การตัดสินใจ ผู้มีอำนาจตัดสินใจ เจ้าของความเสี่ยงที่เหลืออยู่ และการติดตามผลได้อย่างชัดเจน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักฐานการตัดสินใจควรสามารถแสดงเหตุผลหรือข้อมูลสำคัญที่ใช้ประกอบการตัดสินใจ ทางเลือกที่ได้รับการพิจารณา ผู้มีอำนาจตัดสินใจ เจ้าของความเสี่ยงที่เหลืออยู่ และเงื่อนไขหรือระยะเวลาสำหรับการทบทวนตามความเหมาะสม

1.4 การประสานงานกับหน่วยงานที่เกี่ยวข้อง (Coordination with Relevant Authorities) CSC ควรระบุหน่วยงานที่อาจจำเป็นต้องติดต่อหรือประสานงานเกี่ยวกับบริการคลาวด์ให้เหมาะสมกับภารกิจ ลักษณะข้อมูลหรือระบบ ระดับผลกระทบ และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

สำหรับข้อมูลหรือระบบสารสนเทศที่มีความสำคัญหรือได้รับการประเมินว่ามีผลกระทบระดับสูง หน่วยงานควบคุมหรือกำกับดูแลที่เกี่ยวข้องอาจพิจารณากำหนดแนวทางการควบคุม กำกับดูแล หรือติดตามให้เหมาะสมกับลักษณะข้อมูล ระดับผลกระทบ ความเสี่ยง และบริบทของภาคส่วนที่อยู่ภายใต้การกำกับดูแล

1.5 การใช้ข้อมูลตำแหน่งและเขตอำนาจทางกฎหมายในการกำกับดูแล CSP ควรแจ้งข้อมูลเกี่ยวกับที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของ CSP และประเทศที่สามารถจัดเก็บข้อมูลของ CSC ตามข้อกำหนดที่เกี่ยวข้อง

CSC ควรนำข้อมูลดังกล่าวไปใช้เป็นข้อมูลนำเข้าสำหรับการพิจารณากฎหมาย เขตอำนาจทางกฎหมาย ข้อกำหนดตามสัญญา อธิปไตยข้อมูล และความเสี่ยงของบริการ โดยรายละเอียดการวิเคราะห์ให้เชื่อมโยงกับข้อ 5.1.3 และมาตรการที่เกี่ยวข้องในข้อ 5.2

1.6 การยกระดับกรณีไม่สามารถปฏิบัติตามข้อกำหนด เมื่อพบว่าไม่สามารถดำเนินการให้เป็นไปตามข้อกำหนดที่เกี่ยวข้องได้ ควรมีการประเมินข้อจำกัด ผลกระทบ ความเสี่ยง มาตรการทดแทนหรือมาตรการลดความเสี่ยง และยกระดับไปยังผู้มีอำนาจขององค์กรก่อนดำเนินการตามกระบวนการประสานหรือแจ้งหน่วยงานที่มีอำนาจตามที่กำหนด

สำหรับกรณีที่อยู่ภายใต้ข้อกำหนดให้แจ้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้ดำเนินการตามกระบวนการที่กำหนด ทั้งนี้ การแจ้งดังกล่าวไม่ควรถูกตีความว่าเป็นการได้รับยกเว้นจากข้อกำหนดโดยอัตโนมัติ

สรุปข้อกำหนดและความรับผิดชอบ (Requirements and Responsibility Summary)

ประเด็น	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
การกำหนดบทบาทและความรับผิดชอบ	กำหนดบทบาทภายในองค์กร และตกลงขอบเขตความรับผิดชอบกับ CSP	กำหนด บันทึก และสื่อสารขอบเขตความรับผิดชอบของตน รวมถึงส่วนที่เกี่ยวข้องกับ CSC และผู้ให้บริการภายนอก
ความรับผิดชอบร่วม	ตรวจสอบว่าความรับผิดชอบที่ได้รับการจัดสรรสามารถปฏิบัติได้จริง	จัดให้มีข้อมูลและความสามารถของบริการที่สนับสนุนการปฏิบัติหน้าที่ของ CSC ตามขอบเขตบริการ
รูปแบบบริการคลาวด์	พิจารณาความรับผิดชอบตาม IaaS, PaaS หรือ SaaS	ระบุขอบเขตการควบคุมและความรับผิดชอบตามรูปแบบบริการ

ร่างคำสั่ง Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เจ้าของบริการ ข้อมูล และระบบ	กำหนดบทบาทที่เหมาะสมภายในองค์กร	สนับสนุนข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ของ CSC
ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง	ประเมินผลกระทบต่อความเสี่ยงตามข้อมูลที่ได้รับ	กำหนดและกำกับความรับผิดชอบของผู้ให้บริการภายนอกหรือผู้รับจ้างช่วงภายในขอบเขตของตน
ผู้ประสานงานด้านข้อมูลส่วนบุคคล	ทราบและใช้ช่องทางประสานงานตามความจำเป็น	แต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลตามข้อกำหนด
การประเมินระดับผลกระทบ	ใช้ผลการประเมินข้อมูลหรือระบบเป็นข้อมูลนำเข้าสำหรับกำหนดระดับการกำกับดูแล	สนับสนุนข้อมูลเกี่ยวกับบริการที่จำเป็นต่อการประเมิน
ผู้มีอำนาจตัดสินใจ	กำหนดอำนาจตัดสินใจให้เหมาะสมกับระดับผลกระทบและความเสี่ยง	ให้ข้อมูลที่จำเป็นเพื่อสนับสนุนการตัดสินใจของ CSC
เจ้าของความเสี่ยงที่เหลืออยู่	กำหนดผู้รับผิดชอบต่อความเสี่ยงที่ยังคงเหลืออยู่หลังการตัดสินใจ	สนับสนุนข้อมูลและการดำเนินการในขอบเขตบริการตามความเหมาะสม
การตรวจสอบย้อนกลับการตัดสินใจ	บันทึกเหตุผล ทางเลือก การตัดสินใจ ผู้มีอำนาจ และการติดตาม	ให้ข้อมูลประกอบการตัดสินใจตามขอบเขตที่รับผิดชอบ
การระบุหน่วยงานที่เกี่ยวข้อง	ระบุหน่วยงานควบคุม กำกับดูแล หรือหน่วยงานอื่นที่เกี่ยวข้องกับบริการตามบริบท	สนับสนุนข้อมูลที่จำเป็นต่อการประสานงานในขอบเขตบริการ
ช่องทางการประสานงาน	กำหนดผู้ประสานงานหลัก ผู้แทน และช่องทางติดต่อ	จัดให้มีช่องทางและผู้ประสานงานที่เหมาะสม
ที่ตั้งทางภูมิศาสตร์ขององค์กร	นำข้อมูลไปใช้ประกอบการพิจารณาความเสี่ยงและข้อกำหนด	แจ้งที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของ CSP ตามข้อกำหนด
ประเทศที่สามารถจัดเก็บข้อมูล	ประเมินกฎหมาย เขตอำนาจอธิปไตยข้อมูล และความเสี่ยงที่เกี่ยวข้อง	แจ้งประเทศที่สามารถจัดเก็บข้อมูลของ CSC
การเปลี่ยนแปลงที่มีนัยสำคัญ	ประเมินผลกระทบและยกระดับการพิจารณาเมื่อจำเป็น	มีกลไกแจ้งการเปลี่ยนแปลงที่อาจมีผลต่อข้อกำหนดหรือความเสี่ยงตามความเหมาะสม
กรณีไม่สามารถปฏิบัติตามข้อกำหนด	ประเมิน ยกระดับ ตัดสินใจ และดำเนินการแจ้งหรือประสานตามข้อกำหนดที่ใช้บังคับ	ให้ข้อมูลหรือสนับสนุน CSC ในส่วนที่เกี่ยวข้องกับบริการตามขอบเขตความรับผิดชอบ

ตารางนี้เป็น สรุปความรับผิดชอบในระดับแนวทาง ไม่ใช่ตารางกำหนดความรับผิดชอบแบบตายตัว เนื่องจากความรับผิดชอบจริงอาจแตกต่างกันตามรูปแบบบริการคลาวด์ ขอบเขตบริการ สถาปัตยกรรม ข้อตกลง และระดับการควบคุมของแต่ละฝ่าย

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

หลักฐานขั้นต่ำที่ควรพิจารณา (Minimum Evidence) เพื่อสนับสนุนการตรวจสอบการนำข้อกำหนดไปปฏิบัติ CSC และ CSP ควรมีหลักฐานที่เหมาะสมกับลักษณะบริการ ความสำคัญของข้อมูลหรือระบบ และระดับความเสี่ยง โดยอาจประกอบด้วย

ประเด็น	ตัวอย่างหลักฐาน
บทบาทและความรับผิดชอบภายใน	นโยบาย ระเบียบปฏิบัติ คำสั่ง หรือเอกสารกำหนดหน้าที่
ความรับผิดชอบระหว่าง CSC และ CSP	สัญญา ข้อตกลงระดับการให้บริการ (SLA) เงื่อนไขบริการ หรือเอกสารความรับผิดชอบร่วม
ความรับผิดชอบของผู้ให้บริการภายนอก	สัญญา ข้อมูลผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง หรือเอกสารบริการ
ความสามารถของ CSC	หลักฐานด้านบุคลากร เครื่องมือ สิทธิการเข้าถึง หรือความสามารถในการปฏิบัติหน้าที่ที่ได้รับการจัดสรร
ผู้มีอำนาจตัดสินใจ	ตารางอำนาจอนุมัติ หลักเกณฑ์การยอมรับความเสี่ยง หรือเอกสารกำหนดอำนาจ
เจ้าของความเสี่ยง	ทะเบียนความเสี่ยงหรือบันทึกความเสี่ยง
การตัดสินใจ	บันทึกอนุมัติ รายงานการประชุม หรือบันทึกการตัดสินใจ
การติดตามและทบทวน	รายงานทบทวนความเสี่ยง การทบทวนบริการ หรือรายงานติดตามผล
หน่วยงานที่เกี่ยวข้อง	รายชื่อหน่วยงานหรือทะเบียนผู้ติดต่อ
ผู้ประสานงาน CSC/CSP	รายชื่อผู้ประสานงาน แผนการติดต่อ หรือข้อมูลช่องทางยกระดับ
ที่ตั้งและประเทศที่จัดเก็บข้อมูล	ข้อมูลตำแหน่งหรือภูมิภาคที่จัดเก็บข้อมูล (Data Location/Region Information) สัญญา หรือข้อมูลบริการ
การแจ้งการเปลี่ยนแปลง	การแจ้งการเปลี่ยนแปลง (Change Notification) หรือบันทึกการแจ้ง
กรณีไม่สามารถปฏิบัติตามข้อกำหนด	บันทึกข้อจำกัด ผลการประเมินความเสี่ยง การพิจารณาของผู้มีอำนาจ หนังสือแจ้ง หรือหลักฐานการติดตามตามกรณี

หลักฐานดังกล่าวเป็นตัวอย่างหลักฐาน (Examples of Evidence) ไม่ใช่รายการเอกสารบังคับทั้งหมด และองค์กรสามารถใช้ระบบหรือเอกสารที่มีอยู่เดิมได้ หากสามารถแสดงให้เห็นถึงการดำเนินงานตามข้อกำหนดได้อย่างเพียงพอ

หลักการประยุกต์ใช้ (Application Considerations) การนำข้อกำหนดด้านโครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศไปใช้ ควรพิจารณาปัจจัยต่อไปนี้

1.1 รูปแบบบริการคลาวด์ (Cloud Service Model) ควรพิจารณาความแตกต่างระหว่าง IaaS, PaaS และ SaaS เนื่องจากระดับการควบคุมและความรับผิดชอบของ CSC และ CSP แตกต่างกัน ความรับผิดชอบที่เหมาะสมกับบริการประเภทหนึ่งไม่ควรถูกนำไปใช้กับบริการประเภทอื่นโดยอัตโนมัติ

เอกสารสำหรับ Public Hearing ภายนอก - ห้ามใช้อ้างอิง

1.2 ความสำคัญของบริการและระดับผลกระทบ (Service Criticality and Impact Level) ระดับการกำกับดูแล อำนาจตัดสินใจ การประสานงาน และหลักฐานที่ต้องใช้ควรสัมพันธ์กับความสำคัญของบริการและระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ควรพิจารณาอย่างน้อยถึง

- ความลับ (Confidentiality)
- ความถูกต้องครบถ้วน (Integrity)
- ความพร้อมใช้งาน (Availability)
- ปริมาณและระยะเวลาการสะสมข้อมูล
- ความสามารถในการเชื่อมโยงหรือวิเคราะห์ข้อมูลร่วมกัน
- จำนวนและลักษณะของบุคคลหรือผู้มีส่วนได้เสียที่ได้รับผลกระทบ
- ความสำคัญต่อภารกิจหรือบริการสำคัญ
- ความเกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือความมั่นคง

การกำหนดว่าข้อมูลหรือระบบมีผลกระทบสูงไม่ควรพิจารณาจากชื่อประเภทข้อมูลเพียงอย่างเดียว แต่ควรพิจารณาจากบริบท ปริมาณ การรวมข้อมูล การนำไปใช้ และผลกระทบที่อาจเกิดขึ้น

1.3 ข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง (High-Impact Information or Information Systems) สำหรับข้อมูลหรือระบบสารสนเทศที่ได้รับการประเมินว่ามีผลกระทบระดับสูง ควรเพิ่มระดับความเข้มข้นของการกำกับดูแลให้เหมาะสม โดยเฉพาะการกำหนดผู้มีอำนาจตัดสินใจ การระบุเจ้าของความเสี่ยงที่เหลืออยู่ การพิจารณาข้อจำกัดของบริการ และการประสานกับหน่วยงานที่เกี่ยวข้อง

ตัวอย่างอาจรวมถึงฐานข้อมูลสุขภาพจำนวนมาก ข้อมูล CCTV ของพื้นที่สำคัญ ข้อมูลตำแหน่งหรือเส้นทางของยานพาหนะจำนวนมาก ระบบที่เกี่ยวข้องกับ CII หรือข้อมูลที่เมื่อสะสมและวิเคราะห์ร่วมกันแล้วอาจส่งผลต่อความมั่นคงหรือภารกิจสำคัญ ทั้งนี้ ตัวอย่างดังกล่าวไม่ควรถูกตีความว่าข้อมูลทุกกรณีในประเภทเดียวกันเป็นข้อมูลผลกระทบสูงโดยอัตโนมัติ

1.4 กฎหมาย เขตอำนาจทางกฎหมาย และอธิปไตยข้อมูล (Legal Jurisdiction and Data Sovereignty) เมื่อบริการคลาวด์เกี่ยวข้องกับการจัดเก็บ ประมวลผล สำรอง หรือถ่ายโอนข้อมูลข้ามประเทศ CSC ควรพิจารณากฎหมาย เขตอำนาจทางกฎหมาย ข้อกำหนดตามสัญญา และความเสี่ยงด้านอธิปไตยข้อมูลตามความเหมาะสม

รายละเอียดการวิเคราะห์ข้อกำหนดดังกล่าวให้พิจารณาตามข้อ 5.1.3 และข้อกำหนดอื่นที่เกี่ยวข้องเพื่อหลีกเลี่ยงการกำหนดเนื้อหาซ้ำในข้อ 5.1.2

1.5 หน่วยงานควบคุมหรือกำกับดูแลที่เกี่ยวข้อง หน่วยงานควบคุมหรือกำกับดูแลที่รับผิดชอบภาคส่วนซึ่งมีข้อมูลหรือระบบสารสนเทศที่มีผลกระทบสูง ควรพิจารณาความจำเป็นในการกำหนดแนวทางควบคุม กำกับดูแลหรือติดตามเพิ่มเติมให้เหมาะสมกับระดับความเสี่ยงและบริบทของภาคส่วน แนวทางดังกล่าวอาจนำมาใช้ประกอบการกำหนดเงื่อนไขด้านบริการคลาวด์ การประเมินความเสี่ยง การกำหนดตำแหน่งหรือการจัดเก็บข้อมูล การประสานงาน การรายงาน หรือมาตรการควบคุมอื่นที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดมาตรการเดียวกันสำหรับข้อมูลหรือระบบทุกประเภท

ร่างเอกสารสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

1.6 การเปลี่ยนแปลงและการประเมินใหม่ (Change and Reevaluation) การกำกับดูแลบริการคลาวด์ไม่ควรสิ้นสุดเมื่อเริ่มใช้บริการแล้ว แต่ควรมีการประเมินใหม่เมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อความเสี่ยงอย่างมีนัยสำคัญ เช่น

- การเปลี่ยนรูปแบบหรือขอบเขตบริการ
- การเปลี่ยน CSP หรือผู้ให้บริการภายนอก
- การเปลี่ยนประเทศที่จัดเก็บหรือประมวลผลข้อมูล
- การเปลี่ยนข้อกำหนดทางกฎหมายหรือสัญญา
- เหตุการณ์ด้านความมั่นคงปลอดภัยที่มีนัยสำคัญ
- การเปลี่ยนระดับผลกระทบของข้อมูลหรือระบบ
- การพบข้อจำกัดในการปฏิบัติตามข้อกำหนด

ผลจากการประเมินใหม่ควรเชื่อมโยงกลับไปยังผู้มีอำนาจตัดสินใจ เจ้าของความเสี่ยง และมาตรการควบคุมที่เกี่ยวข้อง

1.7 การใช้กลไกการกำกับดูแลที่มีอยู่เดิม องค์กรสามารถใช้โครงสร้างหรือกลไกการกำกับดูแลที่มีอยู่เดิม เช่น การประชุมบริหารความเสี่ยง การประชุมผู้บริหาร คณะกรรมการพิจารณาการเปลี่ยนแปลง ระบบ GRC หรือกระบวนการบริหารบริการ เพื่อรองรับการกำกับดูแลบริการคลาวด์ได้

ไม่จำเป็นต้องจัดตั้งคณะกรรมการ ตำแหน่ง หรือระบบใหม่เฉพาะสำหรับบริการคลาวด์ หากโครงสร้างเดิมสามารถแสดงบทบาท ความรับผิดชอบ อำนาจตัดสินใจ และการติดตามได้อย่างเพียงพอ

1.8 ปัจจัยด้านสิ่งแวดล้อมและการเปลี่ยนแปลงสภาพภูมิอากาศ องค์กรควรพิจารณาว่าปัจจัยด้านสิ่งแวดล้อมและการเปลี่ยนแปลงสภาพภูมิอากาศมีความเกี่ยวข้องต่อการบรรลุวัตถุประสงค์ของบริการคลาวด์หรือไม่ ตามบริบทขององค์กร รายละเอียดด้านสิ่งแวดล้อมและความยั่งยืนให้พิจารณาเพิ่มเติมในข้อ 5.3

5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

การใช้บริการคลาวด์ทำให้ข้อมูล ระบบสารสนเทศ และกระบวนการดำเนินงานขององค์กรอาจเกี่ยวข้องกับกฎหมาย กฎ ระเบียบ ข้อบังคับ ข้อกำหนดตามสัญญา และเขตอำนาจทางกฎหมายหลายประการ เนื่องจากการให้บริการอาจเกี่ยวข้องกับผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ ผู้ให้บริการภายนอก ตลอดจนสถานที่และประเทศที่เกี่ยวข้องกับการจัดเก็บ ประมวลผล หรือให้บริการข้อมูล

การปฏิบัติตามข้อกำหนดสำหรับบริการคลาวด์จึงไม่ควรพิจารณาเฉพาะว่าผู้ให้บริการคลาวด์มีมาตรการด้านความมั่นคงปลอดภัยหรือได้รับการรับรองมาตรฐานหรือไม่ แต่ควรพิจารณาว่า ข้อกำหนดใดมีผลใช้กับข้อมูล ระบบ และบริการขององค์กร ผู้ใดมีหน้าที่รับผิดชอบ และมีข้อมูลหรือหลักฐานเพียงพอที่จะแสดงถึงการปฏิบัติตามข้อกำหนดดังกล่าวหรือไม่ มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์กำหนดข้อ 5.1.3 ครอบคลุมการระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา สิทธิในทรัพย์สินทางปัญญา การปกป้องบันทึกข้อมูล กฎระเบียบที่เกี่ยวข้องกับมาตรการควบคุมการเข้ารหัสข้อมูล และการทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ โดยกำหนดหน้าที่ของผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ตามหลักความรับผิดชอบร่วมกัน

ร่างประกาศ Public Hearing ไทยนิยม - ห้ามใช้อ้างอิง

การพิจารณาว่าข้อกำหนดใดเป็นข้อกำหนดขั้นต่ำที่ต้องดำเนินการ ให้พิจารณาตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศและตารางข้อกำหนดขั้นต่ำท้ายประกาศ โดยสามารถเชื่อมโยงกับผลการประเมินและแนวทางการกำกับดูแลตามข้อ 5.1.1 และ 5.1.2 ที่ได้ดำเนินการไว้แล้ว ทั้งนี้ องค์กรยังคงต้องปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ และข้อผูกพันอื่นที่มีผลใช้บังคับกับองค์กรโดยไม่ขึ้นอยู่กับการกำหนดข้อกำหนดขั้นต่ำของมาตรฐานฉบับนี้

ในทางปฏิบัติ องค์กรควรสามารถเชื่อมโยง ข้อกำหนดที่เกี่ยวข้องกับบริการคลาวด์ ข้อมูลหรือหลักฐานที่ใช้ยืนยันการปฏิบัติตาม ช่องว่างหรือข้อจำกัดที่ตรวจพบ และการดำเนินการหรือการตัดสินใจที่เกี่ยวข้อง เพื่อให้สามารถติดตามและตรวจสอบย้อนกลับได้ โดยใช้กระบวนการและเอกสารที่องค์กรมีอยู่เดิมได้ตามความเหมาะสม และไม่จำเป็นต้องจัดทำระบบเอกสารแยกขึ้นใหม่หากสามารถแสดงความเชื่อมโยงดังกล่าวได้อย่างเพียงพอ

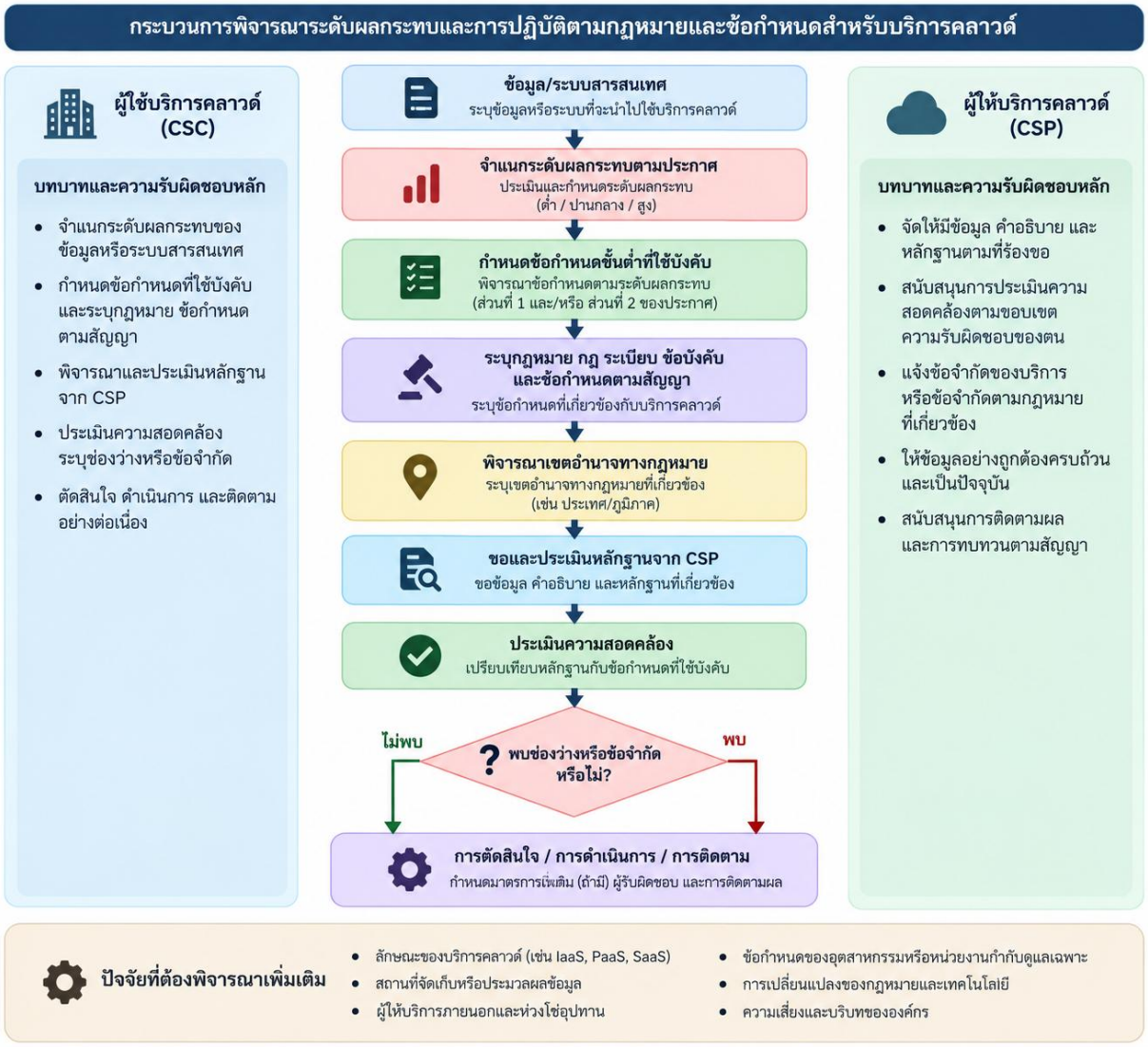
การเชื่อมโยงระดับผลกระทบกับข้อกำหนดด้านการปฏิบัติตาม ก่อนดำเนินการตามข้อ 5.1.3 องค์กรควรนำผลการจำแนกระดับผลกระทบของข้อมูลหรือระบบสารสนเทศมาใช้กำหนดข้อกำหนดขั้นต่ำที่เกี่ยวข้องตามตารางท้ายประกาศ โดยไม่ควรเริ่มจากการพิจารณาว่าผู้ให้บริการคลาวด์มีใบรับรองหรือมาตรการควบคุมใดแล้วจึงย้อนกลับมากำหนดระดับของระบบ

สำหรับข้อมูลหรือระบบสารสนเทศที่มีระดับผลกระทบ ต่ำ ข้อกำหนดขั้นต่ำในส่วนที่ 1 กำหนดให้ดำเนินการตามข้อ 5.1.1 และ 5.1.2 ส่วนข้อมูลหรือระบบสารสนเทศที่มีระดับผลกระทบ ปานกลาง ต้องดำเนินการตามข้อกำหนดในส่วนที่ 1 ทั้งหมด ซึ่งรวมถึงข้อ 5.1.3 และข้อมูลหรือระบบสารสนเทศที่มีระดับผลกระทบ สูง ต้องดำเนินการตามข้อกำหนดในส่วนที่ 1 และส่วนที่ 2 ทั้งหมด

อย่างไรก็ตาม การที่ข้อ 5.1.3 มิได้เป็นข้อกำหนดขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศระดับผลกระทบต่ำ มิได้หมายความว่าองค์กรได้รับยกเว้นจากกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือข้อผูกพันตามสัญญาที่มีผลใช้บังคับกับองค์กร ดังนั้น ลำดับการพิจารณาควรเป็นดังนี้

ข้อมูลหรือระบบสารสนเทศ ⟶ ระดับผลกระทบ ⟶ ข้อกำหนดขั้นต่ำที่ใช้บังคับ ⟶ กฎหมาย กฎ ระเบียบ ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้อง ⟶ หลักฐาน ⟶ การประเมินความสอดคล้อง ⟶ ช่องว่างหรือข้อจำกัด ⟶ การดำเนินการและการตัดสินใจ ⟶ การติดตามและทบทวน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปที่ 6 กระบวนการพิจารณาระดับผลกระทบและการปฏิบัติตามข้อกำหนดสำหรับบริการคลาวด์

5.1.3.1 การระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา (Identification of Applicable Legislation and Contractual Requirements)

การใช้บริการคลาวด์อาจทำให้องค์กรต้องพิจารณากฎหมายและข้อบังคับที่เกี่ยวข้องมากกว่ากฎหมายที่ใช้บังคับกับองค์กรโดยตรง เนื่องจากผู้ให้บริการคลาวด์ องค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ ตลอดจนองค์ประกอบของการให้บริการ อาจอยู่ภายใต้เขตอำนาจทางกฎหมายที่แตกต่างกัน

การระบุกฎหมายที่บังคับใช้จึงควรพิจารณาทั้งข้อกำหนดที่มีผลต่อผู้ใช้บริการคลาวด์ และข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับผู้ให้บริการคลาวด์ โดยใช้ข้อมูลที่ได้รับจากผู้ให้บริการคลาวด์ประกอบการพิจารณา รวมถึงควรพิจารณาข้อกำหนดตามสัญญาที่กำหนดสิทธิ หน้าที่ ความรับผิดชอบ และเงื่อนไขที่เกี่ยวข้องกับการให้บริการ

ประกาศกำหนดให้ผู้ใช้บริการคลาวด์พิจารณาว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจทางกฎหมายที่ควบคุมผู้ให้บริการคลาวด์ นอกเหนือจากกฎหมายที่ควบคุมผู้ใช้บริการคลาวด์ และต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้อง ขณะที่ผู้ให้บริการคลาวด์ต้องแจ้งเขตอำนาจทางกฎหมายที่ควบคุมบริการ ระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับตนเอง และแสดงหลักฐานการปฏิบัติตามกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา

ดังนั้น การดำเนินการตามข้อ 5.1.3.1 ควรพิจารณาต่อเนื่องจากผลการจำแนกระดับผลกระทบและข้อกำหนดขั้นต่ำที่ใช้บังคับ เพื่อให้สามารถตอบคำถามสำคัญได้อย่างน้อยว่า

ข้อมูลหรือระบบมีระดับผลกระทบใด ⟶ ข้อกำหนดใดใช้บังคับ ⟶ มีกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือข้อกำหนดตามสัญญาใดเกี่ยวข้อง ⟶ เขตอำนาจทางกฎหมายใดเกี่ยวข้อง ⟶ CSC และ CSP ต้องดำเนินการอะไร ⟶ มีข้อมูลหรือหลักฐานใดยืนยันการปฏิบัติตาม ⟶ มีช่องว่างหรือข้อจำกัดใด ⟶ ต้องดำเนินการ ตัดสินใจ หรือติดตามอย่างไร

แนวทางดังกล่าวช่วยให้องค์กรพิจารณาการปฏิบัติตามข้อกำหนดจากบริบทและระดับความสำคัญของข้อมูลหรือระบบที่นำไปใช้บริการคลาวด์ แทนการเริ่มต้นจากใบรับรองหรือมาตรการที่ CSP มีอยู่เพียงอย่างเดียว

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องพิจารณาประเด็นที่ว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์นอกเหนือจากกฎหมายที่ควบคุมผู้ใช้บริการคลาวด์ ข) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์ โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก	ก) ผู้ให้บริการคลาวด์ต้องแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงเขตอำนาจศาลทางกฎหมายที่ควบคุมบริการคลาวด์ ข) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องของตนเอง (เช่น เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลส่วนบุคคล) และต้องให้ข้อมูลนี้แก่ผู้ใช้บริการคลาวด์เมื่อได้รับการร้องขอ ค) ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานให้ ผู้ใช้บริการคลาวด์ทราบถึงการปฏิบัติตามกฎหมายที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา

วัตถุประสงค์

1. เพื่อให้ผู้ใช้บริการคลาวด์สามารถระบุกฎหมาย กฎ ระเบียบ ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้องกับการใช้บริการคลาวด์ได้อย่างเหมาะสม

2. เพื่อให้สามารถพิจารณาเขตอำนาจทางกฎหมายที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และการให้บริการคลาวด์ ซึ่งอาจมีผลต่อข้อมูล ระบบสารสนเทศ หรือการดำเนินงานขององค์กร

3. เพื่อให้ผู้ใช้บริการคลาวด์สามารถขอและประเมินข้อมูลหรือหลักฐานจากผู้ให้บริการคลาวด์ เพื่อสนับสนุนการพิจารณาการปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ มาตรฐาน และข้อกำหนดตามสัญญาที่เกี่ยวข้อง

สงวนสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานอื่น

4. เพื่อให้สามารถระบุช่องว่างหรือข้อจำกัดในการปฏิบัติตามข้อกำหนด และเชื่อมโยงประเด็นที่มีนัยสำคัญเข้าสู่กระบวนการบริหารความเสี่ยง การตัดสินใจ และการติดตามตามข้อ 5.1.1 และ 5.1.2

5. เพื่อสนับสนุนให้การพิจารณาการปฏิบัติตามข้อกำหนดสามารถตรวจสอบย้อนกลับได้ตั้งแต่ข้อกำหนดที่ใช้บังคับ หลักฐานที่เกี่ยวข้อง ผลการประเมิน ช่องว่างหรือข้อจำกัด การตัดสินใจ และการติดตามผล

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การพิจารณากฎหมายและข้อบังคับที่เกี่ยวข้อง ผู้ใช้บริการคลาวด์ต้องพิจารณากฎหมายและข้อบังคับที่เกี่ยวข้องกับการใช้บริการคลาวด์ โดยคำนึงว่ากฎหมายที่เกี่ยวข้องอาจมิได้จำกัดเฉพาะกฎหมายที่ใช้บังคับกับผู้ใช้บริการคลาวด์ แต่อาจรวมถึงกฎหมายของเขตอำนาจทางกฎหมายที่ควบคุมผู้ให้บริการคลาวด์ด้วย ตามที่ประกาศกำหนด ในทางปฏิบัติ การพิจารณาอาจครอบคลุมตามความเกี่ยวข้อง เช่น

1. กฎหมาย กฎ ระเบียบ และข้อบังคับที่ใช้บังคับกับองค์กร
2. กฎหมายหรือข้อกำหนดเฉพาะภาคส่วนที่เกี่ยวข้องกับภารกิจหรือบริการขององค์กร
3. กฎหมายและข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
4. กฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล
5. ข้อกำหนดเกี่ยวกับการจัดเก็บ ประมวลผล เข้าถึง เปิดเผย ถ่ายโอน เก็บรักษา ส่งคืน หรือลบข้อมูล
6. ข้อกำหนดตามสัญญา ข้อตกลงระดับการให้บริการ และเงื่อนไขการใช้บริการ
7. กฎหมายหรือข้อกำหนดของเขตอำนาจทางกฎหมายอื่นที่อาจมีผลต่อข้อมูลหรือบริการคลาวด์

รายการดังกล่าวเป็นแนวทางประกอบการพิจารณาตามความเกี่ยวข้อง มิใช่ข้อกำหนดว่าทุกบริการคลาวด์ต้องอยู่ภายใต้กฎหมายหรือข้อกำหนดทุกประเภท

2. การพิจารณาเขตอำนาจทางกฎหมาย ผู้ใช้บริการคลาวด์ควรนำข้อมูลเกี่ยวกับเขตอำนาจทางกฎหมายที่ควบคุมบริการคลาวด์มาพิจารณาร่วมกับกฎหมายและข้อกำหนดที่ใช้บังคับกับองค์กร ข้อมูลที่อาจนำมาพิจารณาตามความเกี่ยวข้อง ได้แก่ ประเทศหรือเขตอำนาจทางกฎหมายขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ ประเทศที่เกี่ยวข้องกับการจัดเก็บหรือประมวลผลข้อมูล และเขตอำนาจทางกฎหมายอื่นที่อาจมีผลต่อการให้บริการหรือการจัดการข้อมูล

การพิจารณาดังกล่าวไม่ควรสรุปเพียงจากตำแหน่งของศูนย์ข้อมูล เนื่องจากตำแหน่งทางภูมิศาสตร์ของข้อมูลและเขตอำนาจทางกฎหมายที่มีผลต่อบริการเป็นประเด็นที่เกี่ยวข้องกัน แต่ไม่จำเป็นต้องเป็นเรื่องเดียวกันเสมอไป

หากผลการพิจารณาพบประเด็นทางกฎหมายหรือข้อจำกัดที่อาจส่งผลอย่างมีนัยสำคัญต่อข้อมูล ระบบ หรือภารกิจขององค์กร ควรนำประเด็นดังกล่าวเข้าสู่กระบวนการประเมินความเสี่ยงและการตัดสินใจตามข้อ 5.1.1 และ 5.1.2

3. การพิจารณาข้อกำหนดตามสัญญาผู้ใช้บริการคลาวด์ควรตรวจสอบว่าข้อกำหนดตามสัญญาและเงื่อนไขการให้บริการสอดคล้องกับกฎหมาย กฎ ระเบียบ ข้อบังคับ และความต้องการขององค์กรที่เกี่ยวข้องกับบริการคลาวด์ ประเด็นที่ควรพิจารณาตามความเกี่ยวข้องอาจรวมถึง

ร่างสำหรับ Public Hearing เท่านั้น _ห้ามใช้อ้างอิง

- สิทธิและหน้าที่ของคู่สัญญา
- บทบาทและความรับผิดชอบของ CSC และ CSP
- การใช้ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง
- สถานที่หรือประเทศที่เกี่ยวข้องกับข้อมูลและบริการ
- การเข้าถึง การเปิดเผย หรือการถ่ายโอนข้อมูล
- การแจ้งการเปลี่ยนแปลงที่อาจมีผลต่อข้อกำหนด
- การจัดการข้อมูลเมื่อสิ้นสุดหรือยกเลิกบริการ
- สิทธิในการได้รับข้อมูลหรือหลักฐานที่จำเป็นต่อการตรวจสอบการปฏิบัติตามข้อกำหนด

รายละเอียดด้านความมั่นคงปลอดภัยที่ต้องกำหนดในข้อตกลงกับผู้ให้บริการภายนอกให้เชื่อมโยงกับข้อ 5.2.9

4. การขอหลักฐานการปฏิบัติตามข้อกำหนดผู้ใช้บริการคลาวด์ต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์ โดยประกาศระบุว่าหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก

การพิจารณาหลักฐานไม่ควรจำกัดเฉพาะการตรวจสอบว่ามีเอกสารหรือใบรับรองอยู่หรือไม่ แต่ควรพิจารณาว่าหลักฐานนั้น เกี่ยวข้องกับข้อกำหนดที่ต้องการยืนยัน มีความเป็นปัจจุบัน และเพียงพอต่อการนำมาใช้ประกอบการพิจารณาขององค์กรหรือไม่

ทั้งนี้ รายละเอียดเกี่ยวกับการทบทวนอย่างเป็นอิสระและหลักฐานการนำมาตรการด้านความมั่นคงปลอดภัยไปปฏิบัติ ให้พิจารณาร่วมกับข้อ 5.1.3.5 และการตรวจรับรองตามที่ประกาศกำหนด

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การแจ้งเขตอำนาจทางกฎหมาย ผู้ให้บริการคลาวด์ต้องแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงเขตอำนาจทางกฎหมายที่ควบคุมบริการคลาวด์ เพื่อให้ผู้ใช้บริการคลาวด์สามารถนำข้อมูลดังกล่าวไปใช้ในการพิจารณากฎหมาย ข้อบังคับ และข้อกำหนดที่เกี่ยวข้องกับบริการ

ข้อมูลดังกล่าวควรมีความสอดคล้องกับข้อมูลที่ผู้ให้บริการคลาวด์แจ้งตามข้อ 5.1.2.2 เกี่ยวกับตำแหน่งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์และประเทศที่สามารถจัดเก็บข้อมูลของผู้ใช้บริการคลาวด์ เพื่อสนับสนุนให้การพิจารณาด้านกฎหมายและการประสานงานเป็นไปในทิศทางเดียวกัน

2. การระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับตนเอง และต้องให้ข้อมูลดังกล่าวแก่ผู้ใช้บริการคลาวด์เมื่อได้รับการร้องขอ

ประกาศยกตัวอย่างข้อกำหนดเกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลส่วนบุคคล ซึ่งแสดงให้เห็นว่าข้อมูลที่ CSP ต้องให้แก่ CSC ควรช่วยให้ CSC สามารถพิจารณาได้ว่า ข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับ CSP อาจมีผลต่อบริการหรือมาตรการที่ CSC ใช้งานอย่างไร

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การแสดงหลักฐานการปฏิบัติตามข้อกำหนด ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานให้ผู้ใช้บริการคลาวด์ทราบถึงการปฏิบัติตามกฎหมายที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา

หลักฐานที่ใช้ควรมีความเหมาะสมกับข้อกำหนดที่ต้องการยืนยัน และสามารถใช้ประกอบการพิจารณาของผู้ใช้บริการคลาวด์ได้ โดยอาจเชื่อมโยงกับหลักฐานจากการตรวจประเมิน การตรวจรับรอง หรือการทบทวนอย่างเป็นอิสระตามที่เกี่ยวข้อง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การจัดทำความเชื่อมโยงของข้อกำหนด องค์กรควรสามารถระบุความสัมพันธ์ระหว่างบริการคลาวด์กับข้อกำหนดที่เกี่ยวข้องได้อย่างเป็นระบบ โดยอาจใช้ทะเบียนกฎหมาย ทะเบียนข้อกำหนด รายการตรวจสอบ หรือระบบบริหารการปฏิบัติตามข้อกำหนดที่องค์กรมีอยู่เดิม แนวทางการเชื่อมโยงสามารถแสดงโดยสรุปได้ดังนี้

ข้อมูลหรือระบบสารสนเทศ ⟶ ระดับผลกระทบ ⟶ ข้อกำหนดขั้นต่ำที่ใช้บังคับ ⟶ บริการคลาวด์ที่เกี่ยวข้อง ⟶ กฎหมายและข้อกำหนดที่เกี่ยวข้อง ⟶ เขตอำนาจทางกฎหมาย ⟶ ข้อกำหนดตามสัญญา ⟶ ข้อมูลหรือหลักฐานจาก CSP ⟶ ผลการประเมินความสอดคล้อง ⟶ ช่องว่างหรือข้อจำกัด ⟶ การดำเนินการและติดตาม

องค์กรไม่จำเป็นต้องจัดทำทะเบียนสำหรับบริการคลาวด์แยกต่างหาก หากทะเบียนกฎหมาย ทะเบียนข้อกำหนด ระบบบริหารความเสี่ยง หรือระบบการกำกับดูแลที่มีอยู่สามารถแสดงความสัมพันธ์ดังกล่าวได้อย่างชัดเจนและตรวจสอบย้อนกลับได้

2. การพิจารณาการเปลี่ยนแปลง การปฏิบัติตามข้อกำหนดไม่ควรเป็นการประเมินเพียงครั้งเดียวก่อนเริ่มใช้บริการ เนื่องจากกฎหมาย ข้อกำหนดตามสัญญา รูปแบบการให้บริการ ผู้ให้บริการภายนอก สถานที่ที่เกี่ยวข้องกับข้อมูล หรือเขตอำนาจทางกฎหมายอาจเปลี่ยนแปลงได้ องค์กรจึงควรกำหนดเหตุที่ทำให้ต้องทบทวนตามความเหมาะสม เช่น

- การเปลี่ยนแปลงกฎหมายหรือข้อบังคับที่เกี่ยวข้อง
- การเปลี่ยนแปลงเงื่อนไขสำคัญของบริการหรือสัญญา
- การเปลี่ยนแปลงประเทศหรือสถานที่ที่เกี่ยวข้องกับข้อมูล
- การเปลี่ยนแปลงผู้ให้บริการภายนอกหรือผู้รับจ้างช่วงที่มีนัยสำคัญ
- การเปลี่ยนแปลงลักษณะข้อมูล ระบบ หรือบริการที่ใช้งาน
- การพบข้อจำกัดหรือประเด็นจากการตรวจประเมิน

การเปลี่ยนแปลงด้านบริการคลาวด์ที่มีผลต่อการปฏิบัติตามข้อกำหนดควรเชื่อมโยงกับกระบวนการจัดการการเปลี่ยนแปลงและกระบวนการกำกับดูแลที่องค์กรมีอยู่ โดยไม่จำเป็นต้องสร้างกระบวนการแยกต่างหาก

3. การจัดการช่องว่างหรือข้อจำกัดในการปฏิบัติตามข้อกำหนด เมื่อพบว่าบริการคลาวด์ไม่สามารถตอบสนองกฎหมาย ข้อบังคับ ข้อกำหนดตามสัญญา หรือข้อกำหนดอื่นที่มีผลใช้กับองค์กรได้ครบถ้วน ไม่ควรสรุปเพียงว่าความเสี่ยงดังกล่าวสามารถยอมรับได้ แต่ควรระบุให้ชัดเจนว่า ข้อกำหนดใดไม่สามารถปฏิบัติได้ สาเหตุหรือข้อจำกัดคืออะไร และส่งผลต่อองค์กรอย่างไร

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ก่อนสรุปว่ามีช่องว่างหรือไม่สามารถปฏิบัติตามข้อกำหนด องค์กรควรตรวจสอบก่อนว่าข้อกำหนดดังกล่าวเป็นข้อกำหนดที่มีผลใช้บังคับกับข้อมูล ระบบ หรือบริการนั้นจริงหรือไม่ โดยพิจารณาจากระดับผลกระทบ กฎหมาย กฎ ระเบียบ ข้อบังคับ และข้อผูกพันอื่นที่เกี่ยวข้อง แนวทางในการพิจารณาสามารถดำเนินการตามลำดับดังนี้

ระดับผลกระทบ ⟶ ข้อกำหนดที่ใช้บังคับ ⟶ หลักฐาน ⟶ ช่องว่างหรือข้อจำกัด ⟶ ผลกระทบและความเสี่ยง ⟶ ทางเลือกหรือมาตรการเพิ่มเติม ⟶ การตัดสินใจของผู้มีอำนาจ ⟶ การดำเนินการ ⟶ การติดตามและทบทวน

แนวทางดังกล่าวช่วยป้องกันการนำข้อกำหนดที่มิได้เป็นข้อกำหนดขั้นต่ำสำหรับระดับผลกระทบนั้นมาใช้เป็นเกณฑ์ตัดสินโดยอัตโนมัติ ทั้งนี้ หากข้อกำหนดดังกล่าวมีผลใช้บังคับจากกฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา หรือนโยบายขององค์กร ก็ยังคงต้องนำมาพิจารณาตามฐานของข้อกำหนดนั้น

กรณีที่เป็นประเด็นซึ่งต้องได้รับการตัดสินใจในระดับองค์กร ควรเชื่อมโยงกับบทบาท อำนาจ และความรับผิดชอบตามข้อ 5.1.2 เพื่อให้สามารถระบุได้ว่าใครเป็นผู้ตัดสินใจ เหตุผลประกอบการตัดสินใจคืออะไร และใครเป็นผู้รับผิดชอบต่อความเสี่ยงที่เหลืออยู่ภายหลังการตัดสินใจ

สำหรับกรณีที่กฎหมาย กฎ ระเบียบ ประกาศ หรือข้อกำหนดที่เกี่ยวข้องกำหนดกระบวนการแจ้งขออนุมัติ หรือประสานงานกับหน่วยงานที่มีอำนาจ องค์กรต้องดำเนินการตามกระบวนการดังกล่าว โดยการตัดสินใจยอมรับความเสี่ยงภายในองค์กรไม่สามารถใช้แทนหน้าที่ตามกฎหมายหรือข้อกำหนดที่มีผลใช้บังคับได้

4. ตัวอย่างการนำไปใช้

ตัวอย่างที่ 1 การพิจารณาเขตอำนาจทางกฎหมาย หน่วยงานมีแผนใช้บริการคลาวด์จาก CSP ซึ่งองค์กรเจ้าของ CSP ตั้งอยู่ในต่างประเทศ และการให้บริการอาจเกี่ยวข้องกับการจัดเก็บหรือประมวลผลข้อมูลในหลายประเทศ

ก่อนใช้บริการ หน่วยงานขอข้อมูลเกี่ยวกับเขตอำนาจทางกฎหมายที่ควบคุมบริการประเทศที่เกี่ยวข้องกับการจัดเก็บหรือประมวลผลข้อมูล และข้อกำหนดทางกฎหมายที่ CSP ระบุว่าเกี่ยวข้องกับการให้บริการ จากนั้นนำข้อมูลดังกล่าวมาพิจารณาร่วมกับกฎหมายและข้อกำหนดที่ใช้บังคับกับหน่วยงาน

หากพบว่ามีกฎหมายหรือข้อกำหนดของต่างประเทศที่อาจมีผลต่อการเข้าถึง เปิดเผย ถ่ายโอน หรือควบคุมข้อมูล หน่วยงานนำประเด็นดังกล่าวเข้าสู่การประเมินความเสี่ยงและกระบวนการตัดสินใจตามข้อ 5.1.1 และ 5.1.2 ก่อนกำหนดแนวทางดำเนินการที่เหมาะสม

ตัวอย่างที่ 2 การเปลี่ยนแปลงเงื่อนไขของบริการ ระหว่างการใช้บริการ CSP แจ้งการเปลี่ยนแปลงที่อาจทำให้ประเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลหรือผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการเปลี่ยนแปลงไปจากเดิม หน่วยงานไม่ควรพิจารณาการเปลี่ยนแปลงดังกล่าวเป็นเพียงการเปลี่ยนแปลงทางเทคนิค แต่ควรตรวจสอบว่าการเปลี่ยนแปลงมีผลต่อกฎหมาย เขตอำนาจทางกฎหมาย ข้อกำหนดตามสัญญา หรือความเสี่ยงที่องค์กรเคยประเมินไว้หรือไม่ และดำเนินการทบทวนหรือยกระดับการพิจารณาตามความเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างที่ 3 หลักฐานไม่เพียงพอต่อการยืนยันข้อกำหนด หน่วยงานกำหนดข้อกำหนดที่ CSP ต้องปฏิบัติและขอหลักฐานเพื่อใช้ยืนยันการปฏิบัติตาม แต่หลักฐานที่ได้รับสามารถยืนยันได้เพียงบางส่วน หรือไม่สามารถแสดงความสัมพันธ์กับข้อกำหนดที่หน่วยงานต้องการตรวจสอบได้อย่างเพียงพอ

หน่วยงานควรขอข้อมูลหรือหลักฐานเพิ่มเติม หรือใช้หลักฐานจากการทบทวนและการตรวจประเมินที่เกี่ยวข้องตามความเหมาะสม หากยังมีช่องว่างที่มีนัยสำคัญ ควรบันทึกประเด็น ประเมินความเสี่ยง และนำเข้าสู่กระบวนการพิจารณาตัดสินใจ แทนการสรุปว่าผู้ให้บริการปฏิบัติตามข้อกำหนดเพียงเพราะมีใบรับรองหรือรายงานการตรวจประเมินบางประเภท

ตัวอย่างที่ 4 การพิจารณาข้อกำหนดและหลักฐานตามระดับผลกระทบ หน่วยงานประเมินข้อมูลหรือระบบสารสนเทศที่จะนำไปใช้บริการคลาวด์และได้ผลเป็นระดับผลกระทบปานกลาง หน่วยงานจึงพิจารณาข้อกำหนดขั้นต่ำที่ใช้บังคับกับระดับดังกล่าวก่อนกำหนดรายการหลักฐานที่ต้องขอจาก CSP

จากนั้น หน่วยงานตรวจสอบว่าหลักฐานและการรับรองที่ CSP จัดให้สามารถสนับสนุนข้อกำหนดที่มีผลใช้กับบริการระดับผลกระทบปานกลางได้หรือไม่ รวมถึงพิจารณาขอบเขต ความเป็นปัจจุบัน และความเกี่ยวข้องของหลักฐานกับบริการที่จะใช้งาน หาก CSP มีหลักฐานบางประเภทแต่ไม่สามารถยืนยันข้อกำหนดที่มีผลใช้กับระดับผลกระทบดังกล่าวได้ครบถ้วน หน่วยงานควรระบุเป็นช่องว่าง ขอข้อมูลหรือหลักฐานเพิ่มเติม และประเมินผลกระทบก่อนตัดสินใจดำเนินการต่อไป

ในทางกลับกัน ข้อกำหนดที่ประกาศกำหนดเป็นข้อกำหนดขั้นต่ำเฉพาะสำหรับระดับผลกระทบสูง ไม่ควรถูกนำมาใช้ตัดสินว่าบริการระดับผลกระทบปานกลางไม่สอดคล้องโดยอัตโนมัติ เว้นแต่ข้อกำหนดดังกล่าวมีผลใช้จากกฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา หรือนโยบายอื่นขององค์กร

5. หลักฐานที่ควรมี องค์กรอาจใช้หลักฐานที่มีอยู่เดิมหรือหลักฐานจาก CSP เพื่อสนับสนุนการดำเนินการตามข้อ 5.1.3.1 โดยไม่จำเป็นต้องจัดทำเอกสารทุกประเภทแยกต่างหาก

ประเด็น	ตัวอย่างหลักฐาน
กฎหมายและข้อกำหนดที่เกี่ยวข้อง	ทะเบียนกฎหมาย ทะเบียนข้อกำหนด หรือผลการทบทวน Compliance
เขตอำนาจทางกฎหมาย	ข้อมูลจาก CSP เกี่ยวกับเขตอำนาจทางกฎหมายและประเทศที่เกี่ยวข้องกับบริการ
ข้อกำหนดตามสัญญา	สัญญา ข้อตกลงระดับการให้บริการ เงื่อนไขการให้บริการ หรือข้อตกลงที่เกี่ยวข้อง
การปฏิบัติตามของ CSP	หนังสือรับรอง รายงานการตรวจประเมิน หลักฐานการรับรอง หรือเอกสารยืนยันอื่นที่เกี่ยวข้อง
ช่องว่างหรือข้อจำกัด	รายงานผลการประเมิน บันทึกประเด็น หรือทะเบียนความเสี่ยง
การตัดสินใจ	บันทึกอนุมัติ มติที่ประชุม หรือหลักฐานการพิจารณาของผู้มีอำนาจ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การติดตาม	ผลการทบทวน การติดตามการแก้ไข หรือหลักฐานการประเมินใหม่เมื่อมีการเปลี่ยนแปลง

หมายเหตุ: รายการข้างต้นเป็นตัวอย่างของหลักฐานที่สามารถใช้สนับสนุนการดำเนินการ มิใช่การกำหนดเอกสารบังคับเพิ่มเติมจากประกาศ

6. การวัดผลในทางปฏิบัติ องค์กรอาจกำหนดตัวชี้วัดเพื่อสนับสนุนการติดตามประสิทธิผลของการปฏิบัติตามข้อกำหนด เช่น

1. ร้อยละของบริการคลาวด์ที่สามารถระบุกฎหมายและข้อกำหนดที่เกี่ยวข้องได้
2. ร้อยละของบริการคลาวด์ที่มีข้อมูลเกี่ยวกับเขตอำนาจทางกฎหมายที่จำเป็นต่อการประเมิน
3. ร้อยละของข้อกำหนดสำคัญที่มีหลักฐานสนับสนุนการปฏิบัติตามอย่างเพียงพอ
4. ร้อยละของช่องว่างหรือข้อจำกัดที่มีนัยสำคัญซึ่งได้รับการพิจารณาโดยผู้มีอำนาจและมีผู้รับผิดชอบติดตาม
5. ร้อยละของการเปลี่ยนแปลงที่มีนัยสำคัญซึ่งได้รับการทบทวนผลกระทบต่อกฎหมาย

ข้อกำหนดตามสัญญา หรือเขตอำนาจทางกฎหมาย องค์กรควรกำหนดตัวชี้วัดและค่าเป้าหมายให้เหมาะสมกับบริบท ความสำคัญของบริการ และระบบการกำกับดูแลที่มีอยู่ โดยตัวชี้วัดดังกล่าวเป็นเครื่องมือสนับสนุนการบริหารจัดการ มิใช่ข้อกำหนดเพิ่มเติมจากประกาศ

5.1.3.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

การใช้บริการคลาวด์อาจเกี่ยวข้องกับซอฟต์แวร์ ระบบปฏิบัติการ ฐานข้อมูล หรือองค์ประกอบอื่นที่อยู่ภายใต้สิทธิในทรัพย์สินทางปัญญาและเงื่อนไขการอนุญาตให้ใช้สิทธิ โดยลักษณะของบริการคลาวด์ที่มีความยืดหยุ่นและสามารถเพิ่มหรือลดทรัพยากรได้ อาจทำให้รูปแบบการใช้ซอฟต์แวร์แตกต่างจากระบบสารสนเทศแบบดั้งเดิม ตัวอย่างเช่น การเพิ่มจำนวนเครื่องเสมือนหรือหน่วยประมวลผลโดยอัตโนมัติอาจทำให้การใช้งานเกินขอบเขตที่เงื่อนไขการอนุญาตให้ใช้สิทธิกำหนดไว้ หากไม่ได้พิจารณาข้อกำหนดดังกล่าวก่อนการติดตั้งหรือการเปลี่ยนแปลงบริการ

ประกาศจึงกำหนดหน้าที่ของ CSC ในการระบุข้อกำหนดด้านสิทธิการใช้งานที่เกี่ยวข้องกับสภาพแวดล้อมคลาวด์ก่อนอนุญาตให้ติดตั้งซอฟต์แวร์ และกำหนดหน้าที่ของ CSP ในการมีกระบวนการตอบสนองต่อข้อร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) การติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์ในบริการคลาวด์อาจทำให้เกิดการละเมิดเงื่อนไขการอนุญาตให้ใช้สิทธิสำหรับซอฟต์แวร์ได้ ผู้ใช้บริการคลาวด์ต้องมีขั้นตอนในการระบุข้อกำหนดในการให้สิทธิการใช้งานเฉพาะระบบคลาวด์ก่อนที่จะ	ก) ผู้ให้บริการคลาวด์ต้องกำหนดกระบวนการในการตอบสนองต่อการร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา

ร่างเพื่อรับฟัง Public Hearing ไม่ใช่ฉบับจริง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
อนุญาตให้ติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในบริการคลาวด์ และต้องให้ความสนใจเป็นพิเศษกับกรณีที่บริการคลาวด์มีความยืดหยุ่นและสามารถปรับขนาดได้ และสามารถใช้งานซอฟต์แวร์บนระบบหรือแกนประมวลผลได้มากกว่าที่อนุญาตโดยเงื่อนไขการอนุญาตให้ใช้สิทธิ	

วัตถุประสงค์

1. เพื่อให้การติดตั้งและใช้งานซอฟต์แวร์บนบริการคลาวด์เป็นไปตามสิทธิและเงื่อนไขการอนุญาตให้ใช้สิทธิที่เกี่ยวข้อง
2. เพื่อป้องกันความเสี่ยงจากการใช้ซอฟต์แวร์เกินขอบเขตที่ได้รับอนุญาต อันเนื่องมาจากความยืดหยุ่นและการขยายขนาดของบริการคลาวด์
3. เพื่อให้ CSP มีกระบวนการที่เหมาะสมสำหรับรับและตอบสนองต่อข้อร้องเรียนเกี่ยวกับสิทธิในทรัพย์สินทางปัญญา

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

CSC ต้องมีขั้นตอนในการระบุและตรวจสอบข้อกำหนดด้านสิทธิการใช้งานที่เกี่ยวข้องกับสภาพแวดล้อมคลาวด์ก่อนอนุญาตให้ติดตั้งซอฟต์แวร์ โดยเฉพาะซอฟต์แวร์ที่มีเงื่อนไขการอนุญาตให้ใช้สิทธิตามจำนวนระบบเครื่องเสมือน แกนประมวลผล ผู้ใช้ หรือทรัพยากรที่ใช้งาน ตามความเกี่ยวข้อง

การพิจารณาควรครอบคลุมอย่างน้อยตามความเกี่ยวข้องว่า ซอฟต์แวร์สามารถใช้งานในสภาพแวดล้อมคลาวด์ที่เลือกได้หรือไม่ และการเพิ่มหรือลดทรัพยากรของบริการอาจทำให้การใช้งานเกินสิทธิที่ได้รับหรือไม่

ไม่จำเป็นต้องสร้างกระบวนการใหม่ หากองค์กรมีการบริหารสินทรัพย์ซอฟต์แวร์หรือการบริหารใบอนุญาตให้ใช้สิทธิที่สามารถครอบคลุมบริการคลาวด์ได้อยู่แล้ว

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

CSP ต้องมีกระบวนการสำหรับรับและตอบสนองต่อข้อร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา โดยกระบวนการควรทำให้สามารถรับเรื่อง ตรวจสอบ และดำเนินการตามกฎหมาย ข้อกำหนดตามสัญญา และลักษณะของบริการที่เกี่ยวข้อง

หากข้อร้องเรียนเกี่ยวข้องกับซอฟต์แวร์หรือทรัพยากรที่ CSC นำมาใช้บนบริการ CSP ควรมีกลไกประสานงานกับ CSC ตามขอบเขตความรับผิดชอบที่ตกลงกัน

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การตรวจสอบก่อนติดตั้ง ก่อนอนุญาตให้ติดตั้งซอฟต์แวร์ CSC ควรตรวจสอบ

ซอฟต์แวร์ ⟶ เงื่อนไขการอนุญาตให้ใช้สิทธิ ⟶ รูปแบบการใช้บนคลาวด์ ⟶ ทรัพยากรที่อาจเพิ่มหรือลด ⟶ ความสอดคล้องของการใช้งาน

ร่างสำหรับ Public Hearing ท่านนำไปอ้างอิงได้

หากพบข้อจำกัด ควรแก้ไขหรือกำหนดเงื่อนไขการใช้งานก่อนนำซอฟต์แวร์ไปใช้จริง

การติดตามเมื่อบริการสามารถขยายขนาดได้ กรณีบริการมีการเพิ่มหรือลดทรัพยากรโดยอัตโนมัติ ควรพิจารณาว่าการเปลี่ยนแปลงดังกล่าวมีผลต่อเงื่อนไขการอนุญาตให้ใช้สิทธิหรือไม่ และกำหนดวิธีติดตามตามความเหมาะสม

ตัวอย่างการนำไปใช้ในทางปฏิบัติ องค์กรมีซอฟต์แวร์ที่อนุญาตให้ใช้งานตามจำนวนแกนประมวลผล และนำซอฟต์แวร์ดังกล่าวไปติดตั้งบนเครื่องเสมือนในบริการคลาวด์ที่สามารถเพิ่มทรัพยากรโดยอัตโนมัติ

หากระบบเพิ่มจำนวนแกนประมวลผลเกินกว่าจำนวนที่ได้รับอนุญาต องค์กรอาจใช้ซอฟต์แวร์เกินสิทธิที่ได้รับแม้การเพิ่มทรัพยากรเกิดขึ้นโดยอัตโนมัติ ดังนั้น ก่อนเปิดใช้งานการขยายทรัพยากร ควรตรวจสอบเงื่อนไขการอนุญาตให้ใช้สิทธิและกำหนดวิธีควบคุมหรือติดตามการใช้งานให้เหมาะสม

อีกกรณีหนึ่ง องค์กรมีใบอนุญาตซอฟต์แวร์ที่เดิมใช้กับระบบภายในองค์กร การมีใบอนุญาตดังกล่าวไม่ควรตีความโดยอัตโนมัติว่าสามารถนำไปใช้บนบริการคลาวด์ได้ แต่ควรตรวจสอบว่าเงื่อนไขอนุญาตให้ใช้งานในสภาพแวดล้อมคลาวด์และรูปแบบการจำลองเสมือนที่องค์กรเลือกใช้หรือไม่

หลักฐานที่ควรมี

ประเด็น	ตัวอย่างหลักฐาน
สิทธิในการใช้งาน	สัญญา ใบอนุญาต หรือหลักฐานการจัดซื้อ
เงื่อนไขการอนุญาต	ข้อกำหนดและเงื่อนไขการใช้สิทธิ
ซอฟต์แวร์ที่ใช้งาน	ทะเบียนซอฟต์แวร์หรือทะเบียนสินทรัพย์
การเปลี่ยนแปลงทรัพยากร	บันทึกการเปลี่ยนแปลงหรือข้อมูลการใช้งานที่เกี่ยวข้อง
การตอบสนองข้อร้องเรียน	ขั้นตอนและบันทึกการรับ/ตอบสนองข้อร้องเรียนของ CSP

ร่างเอกสารเพื่อรับฟังความคิดเห็น - Public Hearing Draft - ห้ามใช้อ้างอิง

5.1.3.3 การปกป้องบันทึกข้อมูล (Protection of Records)

การใช้บริการคลาวด์ทำให้บันทึกข้อมูลบางประเภทที่เกี่ยวข้องกับการใช้บริการของผู้ใช้บริการคลาวด์อาจถูกสร้าง รวบรวม จัดเก็บ หรือดูแลโดยผู้ให้บริการคลาวด์ บันทึกดังกล่าวอาจมีความสำคัญต่อการตรวจสอบ การพิสูจน์การดำเนินงาน การปฏิบัติตามข้อกำหนด การบริหารบริการ หรือการจัดการเหตุการณ์ที่เกี่ยวข้องกับบริการคลาวด์

ผู้ใช้บริการคลาวด์จึงควรทราบว่าผู้ให้บริการคลาวด์มีวิธีการปกป้องบันทึกข้อมูลที่เกี่ยวข้องกับการใช้บริการของตนอย่างไร เพื่อให้สามารถประเมินได้ว่าการปกป้องบันทึกดังกล่าวมีความเหมาะสมกับข้อกำหนดขององค์กร กฎหมาย ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้องหรือไม่

ข้อ 5.1.3.3 มุ่งเน้นที่ การได้รับข้อมูลเกี่ยวกับการปกป้องบันทึกที่ CSP รวบรวมและจัดเก็บมิใช่การกำหนดรายละเอียดทางเทคนิคของการบันทึกเหตุการณ์ การจัดเก็บ Log หรือการเฝ้าระวังระบบซึ่งให้พิจารณาตามข้อ 5.2.6 ที่เกี่ยวข้อง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์

วัตถุประสงค์

1. เพื่อให้ผู้ใช้บริการคลาวด์ได้รับข้อมูลเกี่ยวกับวิธีการปกป้องบันทึกข้อมูลที่ผู้ให้บริการคลาวด์รวบรวมและจัดเก็บซึ่งเกี่ยวข้องกับการใช้บริการของตน
2. เพื่อให้ผู้ใช้บริการคลาวด์สามารถประเมินได้ว่าการปกป้องบันทึกข้อมูลดังกล่าวมีความเหมาะสมกับกฎหมาย ข้อบังคับ ข้อกำหนดตามสัญญา และความต้องการขององค์กรที่เกี่ยวข้องหรือไม่
3. เพื่อให้ผู้ให้บริการคลาวด์สามารถให้ข้อมูลที่เพียงพอเกี่ยวกับการปกป้องบันทึกข้อมูลในส่วนที่อยู่ภายใต้ความรับผิดชอบของตน
4. เพื่อสนับสนุนให้บันทึกข้อมูลที่เกี่ยวข้องสามารถนำมาใช้ในการตรวจสอบ การพิสูจน์การดำเนินงาน หรือการปฏิบัติตามข้อกำหนดได้ตามความจำเป็น

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับวิธีการปกป้องบันทึกข้อมูลที่ผู้ให้บริการคลาวด์รวบรวมและจัดเก็บซึ่งเกี่ยวข้องกับการใช้บริการของผู้ใช้บริการคลาวด์ ข้อมูลที่ขอควรเพียงพอให้ผู้ใช้บริการคลาวด์สามารถประเมินได้ว่า บันทึกดังกล่าวได้รับการปกป้องในระดับที่เหมาะสมกับข้อกำหนดที่เกี่ยวข้องหรือไม่ โดยอาจพิจารณาตามความเหมาะสมถึง

1. ประเภทหรือขอบเขตของบันทึกข้อมูลที่ผู้ให้บริการคลาวด์รวบรวมและจัดเก็บ
2. แนวทางในการควบคุมการเข้าถึงบันทึกข้อมูล
3. แนวทางในการป้องกันการเปลี่ยนแปลง สูญหาย หรือเปิดเผยบันทึกข้อมูลโดยไม่ได้รับอนุญาต
4. ระยะเวลาเก็บรักษาบันทึกข้อมูลตามที่เกี่ยวข้องกับบริการและข้อกำหนดที่ใช้บังคับ
5. ความสามารถในการเรียกดู ส่งออก หรือส่งมอบบันทึกข้อมูลเมื่อผู้ใช้บริการคลาวด์จำเป็นต้องใช้
6. แนวทางการลบหรือทำลายบันทึกข้อมูลเมื่อครบกำหนดหรือเมื่อสิ้นสุดบริการตามความเหมาะสม

รายการดังกล่าวเป็นแนวทางประกอบการพิจารณา มิใช่การกำหนดให้ CSP ต้องมีรูปแบบการควบคุมแบบเดียวกันทุกบริการ

ผู้ใช้บริการคลาวด์สามารถใช้ข้อมูลที่ได้รับจาก CSP ร่วมกับกระบวนการบริหารบันทึก การกำกับดูแลข้อมูล การตรวจประเมิน หรือการบริหารการปฏิบัติตามข้อกำหนดที่มีอยู่เดิม โดยไม่จำเป็นต้องจัดทำกระบวนการใหม่สำหรับบริการคลาวด์โดยเฉพาะ

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่ตนรวบรวมและจัดเก็บซึ่งเกี่ยวข้องกับการใช้บริการของผู้ใช้บริการคลาวด์ตามที่ประกาศกำหนด

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

ข้อมูลดังกล่าวควรมีรายละเอียดในระดับที่เพียงพอให้ผู้ใช้บริการคลาวด์สามารถนำไปใช้ประกอบการพิจารณาการปฏิบัติตามข้อกำหนดได้ โดยไม่จำเป็นต้องเปิดเผยรายละเอียดภายในที่อาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัยของระบบหรือบริการ

ในกรณีที่ลักษณะของบริการมีบันทึกข้อมูลหลายประเภท ผู้ให้บริการคลาวด์ควรสามารถอธิบายได้ว่าบันทึกประเภทใดอยู่ภายใต้ความรับผิดชอบของ CSP บันทึกประเภทใดผู้ใช้บริการคลาวด์สามารถเข้าถึงหรือจัดการได้ และมีข้อจำกัดใดที่ผู้ใช้บริการคลาวด์ควรทราบ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การระบุบันทึกข้อมูลที่เกี่ยวข้อง

ผู้ใช้บริการคลาวด์ควรเริ่มจากการระบุว่าบันทึกข้อมูลประเภทใดที่ CSP รวบรวมและจัดเก็บซึ่งเกี่ยวข้องกับการใช้บริการของตน โดยไม่จำเป็นต้องครอบคลุมบันทึกภายในทั้งหมดของ CSP
ตัวอย่างบันทึกที่อาจเกี่ยวข้องตามลักษณะบริการ ได้แก่

- บันทึกเกี่ยวกับการใช้บริการ
- บันทึกการบริหารบริการหรือการเปลี่ยนแปลงที่เกี่ยวข้องกับ CSC
- บันทึกการเข้าถึงหรือกิจกรรมที่ CSP จัดเก็บในขอบเขตบริการ
- บันทึกเกี่ยวกับเหตุการณ์หรือการสนับสนุนบริการที่เกี่ยวข้องกับ CSC
- บันทึกอื่นที่มีความจำเป็นต่อการตรวจสอบหรือการปฏิบัติตามข้อกำหนดของ CSC

การระบุประเภทของบันทึกควรอ้างอิงบริการที่ใช้งานจริง ไม่ควรสรุปว่าทุก CSP ต้องรวบรวมบันทึกประเภทเดียวกันทั้งหมด

2. การประเมินความเพียงพอของการปกป้องบันทึก

เมื่อได้รับข้อมูลจาก CSP แล้ว CSC ควรพิจารณาว่าการปกป้องบันทึกดังกล่าวสามารถรองรับข้อกำหนดขององค์กรได้หรือไม่ โดยอาจพิจารณาความเชื่อมโยงดังนี้

บันทึกที่เกี่ยวข้อง ⟶ ข้อกำหนดที่ต้องปฏิบัติ ⟶ แนวทางการปกป้องของ CSP ⟶ ข้อจำกัดหรือช่องว่าง ⟶ การดำเนินการที่เหมาะสม

หากข้อมูลที่ CSP ให้ไม่เพียงพอต่อการประเมิน CSC ควรขอข้อมูลเพิ่มเติมตามความเหมาะสม หรือใช้หลักฐานอื่นที่เกี่ยวข้อง เช่น รายงานการตรวจประเมิน เอกสารบริการ หรือหลักฐานการตรวจรับรอง เพื่อประกอบการพิจารณา

3. การเชื่อมโยงกับข้อกำหนดอื่น

หากบันทึกข้อมูลดังกล่าวเป็นบันทึกเหตุการณ์หรือข้อมูลบันทึกที่ใช้เพื่อวัตถุประสงค์ด้านความมั่นคงปลอดภัย รายละเอียดทางเทคนิคเกี่ยวกับการบันทึกเหตุการณ์ การปกป้องข้อมูลในบันทึก และระยะเวลาการเก็บรักษา ให้เชื่อมโยงกับข้อ 5.2.6.4 และ 5.2.6.5 ตามความเกี่ยวข้อง โดยไม่ควรเขียนข้อกำหนดดังกล่าวซ้ำในข้อ 5.1.3.3

หากบันทึกข้อมูลมีข้อมูลส่วนบุคคล ควรพิจารณากฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องร่วมด้วยตามข้อ 5.1.3.1

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. ตัวอย่างการนำไปใช้ในทางปฏิบัติ

ตัวอย่างที่ 1 บันทึกการใช้บริการที่ CSP เป็นผู้จัดเก็บ หน่วยงานใช้บริการ SaaS และ CSP เป็นผู้จัดเก็บบันทึกเกี่ยวกับกิจกรรมการใช้งานของผู้ใช้และการบริหารบริการ

CSC ควรขอข้อมูลจาก CSP ว่าบันทึกดังกล่าวได้รับการปกป้องอย่างไร สามารถเข้าถึง เรียกดู หรือส่งออกได้ภายใต้เงื่อนไขใด มีระยะเวลาการเก็บรักษาเท่าใด และมีข้อจำกัดใดที่ CSC จำเป็นต้องทราบ

หากองค์กรมีข้อกำหนดให้เก็บบันทึกเป็นระยะเวลานานกว่าที่ CSP รองรับ CSC ควรระบุช่องว่างดังกล่าวและพิจารณาทางเลือก เช่น การส่งออกบันทึกไปจัดเก็บในระบบที่องค์กรควบคุม หรือปรับระดับบริการตามความเหมาะสม

ตัวอย่างที่ 2 บันทึกที่จำเป็นต่อการตรวจสอบภายหลัง องค์กรจำเป็นต้องใช้บันทึกบางประเภทเพื่อสนับสนุนการตรวจสอบหรือการพิสูจน์เหตุการณ์ แต่ CSP ให้ข้อมูลว่าบันทึกดังกล่าวมีระยะเวลาเก็บรักษาจำกัดและไม่สามารถเรียกคืนได้หลังจากพ้นระยะเวลาที่กำหนด

กรณีนี้ CSC ควรพิจารณาว่าข้อจำกัดดังกล่าวสอดคล้องกับข้อกำหนดขององค์กร กฎหมาย หรือสัญญาหรือไม่ หากไม่สอดคล้องควรกำหนดแนวทางเพิ่มเติมก่อนที่จะพึ่งพาบันทึกดังกล่าวเป็นหลักฐานสำคัญ

5. หลักฐานที่ควรมี

ประเด็น	ตัวอย่างหลักฐาน
ประเภทของบันทึก	เอกสารบริการหรือข้อมูลที่ CSP แจ้ง
การปกป้องบันทึก	เอกสารอธิบายมาตรการหรือแนวทางการปกป้องบันทึกของ CSP
การเข้าถึงและส่งออก	คู่มือบริการ เงื่อนไขบริการ หรือข้อมูลความสามารถของระบบ
ระยะเวลาเก็บรักษา	นโยบายหรือข้อมูลเกี่ยวกับการเก็บรักษาบันทึก
ช่องว่างหรือข้อจำกัด	ผลการประเมิน บันทึกข้อจำกัด หรือทะเบียนความเสี่ยง
การดำเนินการเพิ่มเติม	การกำหนดคาบริการ ข้อตกลงเพิ่มเติม หรือหลักฐานการจัดเก็บบันทึกเพิ่มเติม

หมายเหตุ: รายการดังกล่าวเป็นตัวอย่างหลักฐาน ไม่ใช่การกำหนดเอกสารบังคับเพิ่มเติมจากประกาศ

5.1.3.4 กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls)

การใช้มาตรการควบคุมการเข้ารหัสข้อมูลในบริการคลาวด์มีทั้งมิติด้านความมั่นคงปลอดภัยและมิติด้านการปฏิบัติตามข้อกำหนด เนื่องจากการเข้ารหัส การใช้กุญแจเข้ารหัส การถ่ายโอนข้อมูล และการจัดการข้อมูลที่ได้รับการเข้ารหัสอาจอยู่ภายใต้ข้อกำหนดตามกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือข้อตกลงที่เกี่ยวข้อง

ดังนั้น การพิจารณาในข้อ 5.1.3.4 จึงมุ่งเน้นว่า มาตรการควบคุมการเข้ารหัสที่นำมาใช้สอดคล้องกับข้อกำหนดทางกฎหมายและข้อผูกพันที่เกี่ยวข้องหรือไม่ มากกว่าการกำหนดรายละเอียดทางเทคนิคของอัลกอริทึม วิธีการเข้ารหัส หรือการจัดการกุญแจ ซึ่งให้พิจารณาเพิ่มเติมในข้อ 5.2.4

ประกาศกำหนดให้ CSC ตรวจสอบให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสที่ใช้กับบริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง และกำหนดให้ CSP ให้คำอธิบายเกี่ยวกับ

เอกสารสำหรับ Public Hearing ร่างประกาศ... ห้ามใช้อ้างอิง

มาตรการควบคุมการเข้ารหัสที่ตนดำเนินการ เพื่อให้ CSC สามารถใช้ประกอบการทบทวนการปฏิบัติตามข้อกำหนดได้

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้กับการใช้บริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง	ก) ผู้ให้บริการคลาวด์ต้องให้คำอธิบายกับ ผู้ใช้บริการคลาวด์เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูลที่ดำเนินการโดยผู้ให้บริการคลาวด์ เพื่อใช้ในการทบทวนการปฏิบัติตามข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้อง

วัตถุประสงค์

1. เพื่อให้มาตรการควบคุมการเข้ารหัสที่ใช้กับบริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้อง
2. เพื่อให้ CSC ได้รับข้อมูลเพียงพอจาก CSP สำหรับใช้ทบทวนความสอดคล้องของมาตรการควบคุมการเข้ารหัส
3. เพื่อให้สามารถระบุข้อจำกัดหรือความแตกต่างระหว่างมาตรการที่ CSP จัดให้กับข้อกำหนดของ CSC ได้อย่างชัดเจน
4. เพื่อเชื่อมโยงผลการทบทวนด้านการปฏิบัติตามข้อกำหนดกับมาตรการทางเทคนิคในข้อ 5.2.4 โดยไม่กำหนดรายละเอียดซ้ำซ้อน

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

CSC ต้องตรวจสอบว่ามาตรการควบคุมการเข้ารหัสที่ใช้กับบริการคลาวด์สอดคล้องกับข้อกำหนดที่เกี่ยวข้องกับองค์กร โดยควรพิจารณาทั้งมาตรการที่องค์กรเป็นผู้กำหนดเองและมาตรการที่ CSP จัดให้เป็นส่วนหนึ่งของบริการ

การทบทวนอาจพิจารณาตามความเกี่ยวข้องถึง

1. ข้อกำหนดตามกฎหมายหรือกฎระเบียบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล
2. ข้อกำหนดตามสัญญาหรือข้อตกลงที่เกี่ยวข้องกับการปกป้องข้อมูล
3. ข้อกำหนดขององค์กรเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส
4. ขอบเขตข้อมูลหรือกิจกรรมที่ต้องใช้การเข้ารหัส
5. ข้อจำกัดที่อาจเกิดจากบริการหรือรูปแบบการให้บริการของ CSP

หากพบว่ามาตรการที่ CSP จัดให้ไม่สามารถรองรับข้อกำหนดที่เกี่ยวข้องได้ครบถ้วน CSC ควรระบุช่องว่างดังกล่าวและพิจารณามาตรการหรือทางเลือกเพิ่มเติมตามความเหมาะสม

รายละเอียดเกี่ยวกับความแข็งแรงของการเข้ารหัส การจัดการกุญแจ และความสามารถทางเทคนิคของบริการ ให้พิจารณาตามข้อ 5.2.4 โดยข้อ 5.1.3.4 มุ่งเน้นการตรวจสอบความสอดคล้องของมาตรการควบคุมการเข้ารหัสกับข้อกำหนดที่เกี่ยวข้องเป็นหลัก

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

CSP ต้องให้คำอธิบายเกี่ยวกับมาตรการควบคุมการเข้ารหัสที่ตนดำเนินการ เพื่อให้ CSC สามารถนำข้อมูลดังกล่าวไปใช้ทบทวนการปฏิบัติตามข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้องได้
ข้อมูลที่ CSP ให้ควรมีความเพียงพอให้ CSC เข้าใจอย่างน้อยว่า

- CSP มีมาตรการควบคุมการเข้ารหัสในส่วนใดของบริการ
- ขอบเขตการใช้มาตรการดังกล่าวครอบคลุมข้อมูลหรือกิจกรรมประเภทใด
- มีข้อจำกัดหรือเงื่อนไขใดที่ CSC ควรทราบ
- มีความสามารถใดที่ CSC สามารถกำหนดหรือเลือกใช้เพิ่มเติมได้ตามขอบเขตบริการ

ทั้งนี้ การให้ข้อมูลควรอยู่ในระดับที่เพียงพอสำหรับการทบทวนการปฏิบัติตามข้อกำหนด โดยไม่จำเป็นต้องเปิดเผยรายละเอียดภายในที่อาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัยของบริการ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การเชื่อมโยงข้อกำหนดกับมาตรการเข้ารหัส

CSC ควรเริ่มจากการระบุข้อกำหนดที่เกี่ยวข้องก่อน แล้วจึงพิจารณาว่ามาตรการที่ CSP จัดให้สามารถรองรับข้อกำหนดดังกล่าวได้หรือไม่

แนวทางสามารถสรุปได้ดังนี้

ข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้อง ⟶ ข้อกำหนดด้านการเข้ารหัส ⟶ มาตรการที่ CSC หรือ CSP ใช้ ⟶ ผลการทบทวนความสอดคล้อง ⟶ ช่องว่างหรือข้อจำกัด ⟶ การดำเนินการเพิ่มเติม

แนวทางนี้ช่วยแยกบทบาทของ 5.1.3.4 ออกจาก 5.2.4 อย่างชัดเจน กล่าวคือ ข้อ 5.1.3.4 ตอบคำถามว่า “ต้องสอดคล้องกับข้อกำหนดอะไร” ส่วนข้อ 5.2.4 ตอบคำถามว่า “จะใช้มาตรการเข้ารหัสและจัดการกุญแจอย่างไร”

2. การใช้ข้อมูลจาก CSP ประกอบการทบทวน

CSC ควรใช้คำอธิบายและข้อมูลจาก CSP ประกอบการพิจารณาว่ามาตรการที่ให้บริการอยู่สามารถตอบสนองข้อกำหนดขององค์กรได้หรือไม่

หากข้อมูลที่ได้รับยังไม่เพียงพอ CSC ควรขอข้อมูลเพิ่มเติมตามความเหมาะสม หรือใช้เอกสารทางเทคนิค รายงานการตรวจประเมิน หรือหลักฐานอื่นที่เกี่ยวข้องเพื่อประกอบการพิจารณา

ไม่ควรสรุปว่าการมีฟังก์ชันเข้ารหัสในบริการเพียงอย่างเดียวเท่ากับการปฏิบัติตามข้อกำหนดครบถ้วน โดยควรตรวจสอบความสัมพันธ์ระหว่างข้อกำหนดกับขอบเขตและวิธีใช้มาตรการดังกล่าวด้วย

3. การจัดการเมื่อพบข้อจำกัด

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

หากพบว่ามาตรการควบคุมการเข้ารหัสที่ใช้กับบริการไม่สอดคล้องกับกฎหมาย ข้อบังคับ หรือข้อกำหนดตามสัญญาที่เกี่ยวข้อง CSC ควรระบุประเด็นดังกล่าวให้ชัดเจน และพิจารณาแนวทาง เช่น

- ปรับการกำหนดค่าหรือใช้ความสามารถเพิ่มเติมของบริการ
- ใช้มาตรการที่ CSC จัดหาเองตามขอบเขตที่บริการรองรับ
- ปรับข้อกำหนดหรือสถาปัตยกรรมของบริการ หากกฎหมายหรือข้อผูกพันเปิดให้ดำเนินการได้
- พิจารณาทางเลือกบริการอื่นเมื่อไม่สามารถตอบสนองข้อกำหนดที่มีผลใช้บังคับได้

หากข้อจำกัดมีนัยสำคัญ ควรเชื่อมโยงกับการพิจารณาความเสี่ยงและผู้มีอำนาจตัดสินใจตามข้อ 5.1.1 และ 5.1.2 รวมถึงกระบวนการจัดการกรณีไม่สามารถปฏิบัติตามข้อกำหนดตามข้อ 5.1.3.1 หากเข้าเงื่อนไข

4. ตัวอย่างการนำไปใช้ในทางปฏิบัติ

ตัวอย่างที่ 1 ข้อกำหนดตามสัญญากำหนดให้ข้อมูลต้องได้รับการเข้ารหัส องค์กรมีข้อตกลงที่กำหนดให้ข้อมูลบางประเภทต้องได้รับการเข้ารหัสระหว่างการจัดเก็บและการส่งผ่านเครือข่าย ก่อนเลือกหรือกำหนดค่าบริการคลาวด์ CSC ควรขอข้อมูลจาก CSP ว่าบริการมีมาตรการเข้ารหัสในขอบเขตใด และตรวจสอบว่าความสามารถดังกล่าวสามารถรองรับข้อกำหนดตามข้อตกลงขององค์กรได้หรือไม่ หาก CSP รองรับเฉพาะการเข้ารหัสระหว่างส่งข้อมูลแต่ไม่สามารถรองรับการเข้ารหัสข้อมูลขณะจัดเก็บตามข้อกำหนดที่มีผลใช้ CSC ควรระบุช่องว่างและกำหนดแนวทางเพิ่มเติมก่อนใช้บริการดังกล่าวกับข้อมูลที่อยู่ภายใต้ข้อกำหนดนั้น

ตัวอย่างที่ 2 การใช้มาตรการเข้ารหัสของ CSP เพื่อรองรับข้อกำหนดทางกฎหมาย องค์กรใช้บริการคลาวด์ที่เกี่ยวข้องกับข้อมูลซึ่งอยู่ภายใต้ข้อกำหนดทางกฎหมายด้านการคุ้มครองข้อมูล และ CSP เป็นผู้จัดให้มีมาตรการเข้ารหัสส่วนหนึ่งของบริการ CSC ควรขอคำอธิบายจาก CSP เกี่ยวกับมาตรการที่ใช้ ขอบเขตที่ครอบคลุม และข้อจำกัดที่เกี่ยวข้อง เพื่อนำมาพิจารณาว่าการใช้มาตรการดังกล่าวสามารถสนับสนุนการปฏิบัติตามข้อกำหนดขององค์กรได้หรือไม่ การมีข้อความว่า “ข้อมูลได้รับการเข้ารหัส” ในเอกสารบริการเพียงอย่างเดียวไม่ควรใช้แทนการทบทวนว่ามาตรการดังกล่าวสอดคล้องกับข้อกำหนดที่องค์กรต้องปฏิบัติจริงหรือไม่

5. หลักฐานที่ควรมี

ประเด็น	ตัวอย่างหลักฐาน
ข้อกำหนดที่เกี่ยวข้อง	กฎหมาย กฎ ระเบียบ ข้อกำหนดตามสัญญา หรือนโยบายที่เกี่ยวข้อง
คำอธิบายของ CSP	เอกสารอธิบายความสามารถหรือมาตรการควบคุมการเข้ารหัส
ขอบเขตการเข้ารหัส	เอกสารบริการ การกำหนดค่า หรือข้อมูลความสามารถที่เกี่ยวข้อง
ผลการทบทวน	รายการตรวจสอบ ผลการประเมิน หรือบันทึกการพิจารณาความสอดคล้อง
ช่องว่างหรือข้อจำกัด	บันทึกข้อจำกัด ผลการประเมินความเสี่ยง หรือทะเบียนความเสี่ยง
การดำเนินการเพิ่มเติม	การกำหนดค่าบริการ มาตรการเพิ่มเติม หรือบันทึกการตัดสินใจ

หมายเหตุ: รายการดังกล่าวเป็นตัวอย่างหลักฐาน ไม่ใช่การกำหนดเอกสารบังคับเพิ่มเติมจากประกาศ

ร่างประกาศ Public Hearing ไม่ใช่ – ห้ามใช้อ้างอิง

5.1.3.5 การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)

การใช้บริการคลาวด์ทำให้ CSC อาจไม่สามารถตรวจสอบมาตรการควบคุมภายในของ CSP ได้โดยตรงในลักษณะเดียวกับระบบที่องค์กรเป็นผู้บริหารจัดการเอง เนื่องจากโครงสร้างพื้นฐาน ระบบ และกระบวนการบางส่วนอยู่ภายใต้การควบคุมของ CSP และอาจให้บริการแก่ผู้ใช้บริการหลายรายร่วมกัน

ดังนั้น การพิจารณาความมั่นคงปลอดภัยของบริการคลาวด์จึงไม่ควรอาศัยเพียงคำกล่าวอ้างหรือเอกสารประชาสัมพันธ์ของ CSP แต่ต้องมีหลักฐานที่สามารถยืนยันได้ว่ามาตรการควบคุมและแนวทางปฏิบัติที่กล่าวอ้างนั้นมีการนำไปปฏิบัติจริง

ประกาศจึงกำหนดให้ CSC ขอหลักฐานที่เป็นเอกสารเกี่ยวกับการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศไปปฏิบัติ ขณะที่ CSP ต้องจัดให้มีหลักฐานเพื่อยืนยันการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล รวมถึงกำหนดแนวทางสำหรับกรณีที่การตรวจสอบโดย CSC โดยตรงไม่สามารถกระทำได้หรืออาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ และมีความสอดคล้องกับที่ผู้ให้บริการคลาวด์กล่าวอ้าง ทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย	ก) ผู้ให้บริการคลาวด์ต้องให้หลักฐานที่เป็นเอกสารแก่ผู้ใช้บริการคลาวด์เพื่อยืนยันข้อเรียกร้องของ ผู้ให้บริการคลาวด์ในการนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้ ข) ในกรณีที่การตรวจสอบโดยผู้ใช้บริการคลาวด์แต่ละรายการไม่สามารถกระทำได้หรืออาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและขั้นตอนของผู้ให้บริการคลาวด์ ทั้งนี้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานดังกล่าวให้กับผู้ที่คาดว่าจะเป็น ผู้ใช้บริการคลาวด์ก่อนเข้าทำสัญญา โดยปกติแล้วการตรวจสอบอิสระที่เกี่ยวข้องตามที่ผู้ให้บริการคลาวด์เลือก ควรเป็นวิธีการที่เป็นที่ยอมรับเพื่อตอบสนองความต้องการของ ผู้ใช้บริการคลาวด์ ในการตรวจสอบการดำเนินงานของ ผู้ให้บริการคลาวด์ หากมีความโปร่งใสเพียงพอ เมื่อการตรวจสอบที่เป็นอิสระ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้งานอื่น

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ไม่สามารถทำได้ ผู้ให้บริการคลาวด์ ต้องทำการประเมินตนเอง และเปิดเผยกระบวนการและผลลัพธ์ต่อผู้ใช้บริการคลาวด์

วัตถุประสงค์

1. เพื่อให้ CSC มีหลักฐานที่เหมาะสมสำหรับยืนยันว่ามาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ได้มีการนำไปปฏิบัติจริง
2. เพื่อให้สามารถตรวจสอบความสอดคล้องระหว่างสิ่งที่ CSP กล่าวอ้างกับการดำเนินงานจริง
3. เพื่อให้มีหลักฐานที่เป็นอิสระสำหรับสนับสนุนการประเมิน CSP ในกรณีที่ CSC ไม่สามารถตรวจสอบ CSP ได้โดยตรง หรือการตรวจสอบโดยตรงอาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
4. เพื่อให้ผู้ที่คาดว่าจะเป็น CSC สามารถได้รับหลักฐานที่เกี่ยวข้องก่อนเข้าทำสัญญาและใช้ประกอบการพิจารณาเลือกใช้บริการ
5. เพื่อให้มีกลไกรองรับกรณีที่ไม่สามารถจัดให้มีการตรวจสอบอย่างเป็นอิสระ โดย CSP ต้องดำเนินการประเมินตนเองและเปิดเผยกระบวนการและผลลัพธ์ต่อ CSC ตามที่ประกาศกำหนด

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

CSC ต้องขอหลักฐานที่เป็นเอกสารเพื่อยืนยันว่ามาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ CSP กล่าวอ้างสำหรับบริการคลาวด์นั้นมีการนำไปปฏิบัติจริง และมีความสอดคล้องกับข้อมูลที่ CSP ได้แจ้งไว้

หลักฐานที่นำมาใช้ไม่จำเป็นต้องอยู่ในรูปแบบเดียวกันทั้งหมด โดยประกาศระบุว่าหลักฐานดังกล่าว อาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้อง ดังนั้น การมีใบรับรองมาตรฐานจึงเป็นหลักฐานรูปแบบหนึ่ง แต่ CSC ควรพิจารณาความเหมาะสมของหลักฐานกับสิ่งที่ต้องการยืนยันด้วย

การกำหนดว่าต้องขอหรือประเมินหลักฐานประเภทใดควรเริ่มจาก ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และข้อกำหนดการตรวจรับรองที่ประกาศกำหนดสำหรับระดับนั้น แล้วจึงพิจารณาว่าหลักฐานที่ CSP จัดให้สามารถรองรับข้อกำหนดดังกล่าวได้หรือไม่ ดังนั้น ลำดับการพิจารณาควรเป็น

ระดับผลกระทบ ⟶ ข้อกำหนดที่ใช้บังคับ ⟶ ข้อกำหนดการตรวจรับรองหรือหลักฐานที่ต้องพิจารณา ⟶ หลักฐานที่ CSP จัดให้ ⟶ ขอบเขตและความเป็นปัจจุบัน ⟶ ข้อจำกัดหรือข้อค้นพบ ⟶ ผลการประเมิน

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ไม่ควรใช้แนวทางย้อนกลับโดยเริ่มจากใบรับรองที่ CSP มีอยู่แล้วจึงสรุปว่าบริการดังกล่าวเหมาะสมสำหรับข้อมูลหรือระบบสารสนเทศทุกระดับผลกระทบ เนื่องจากข้อกำหนดขั้นต่ำและข้อกำหนดการตรวจรับรองอาจแตกต่างกันตามระดับผลกระทบ

ในทางปฏิบัติ CSC ควรพิจารณาอย่างน้อยว่า

1. หลักฐานที่ได้รับสามารถยืนยันข้อกล่าวอ้างหรือมาตรการที่ต้องการตรวจสอบได้หรือไม่
2. หลักฐานยังมีผลหรือเป็นปัจจุบันหรือไม่
3. ขอบเขตของหลักฐานครอบคลุมบริการหรือองค์ประกอบที่ CSC ใช้งานหรือไม่
4. มีข้อยกเว้น ข้อจำกัด หรือข้อค้นพบที่อาจมีผลต่อการใช้บริการของ CSC หรือไม่

ทั้งนี้ การพิจารณาหลักฐานตามข้อนี้ควรดำเนินการร่วมกับข้อกำหนดการตรวจรับรองที่ประกาศกำหนด โดยไม่ควรตีความว่าหลักฐานประเภทใดประเภทหนึ่งสามารถใช้แทนข้อกำหนดการตรวจรับรองที่มีผลใช้บังคับได้โดยอัตโนมัติ

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดให้มีหลักฐานที่เป็นเอกสาร

CSP ต้องให้หลักฐานที่เป็นเอกสารแก่ CSC เพื่อยืนยันข้อกล่าวอ้างเกี่ยวกับการนำมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้

หลักฐานควรมีความสัมพันธ์กับมาตรการหรือแนวทางปฏิบัติที่ CSP กล่าวอ้าง และอยู่ในระดับที่ทำให้ CSC สามารถนำไปใช้ประกอบการประเมินบริการได้อย่างเหมาะสม

2. กรณี CSC ไม่สามารถตรวจสอบ CSP โดยตรง

การให้ CSC แต่ละรายเข้าตรวจสอบระบบ กระบวนการ หรือสถานที่ของ CSP โดยตรงอาจไม่สามารถดำเนินการได้ในทางปฏิบัติ หรืออาจทำให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การเปิดเผยรายละเอียดของระบบหรือข้อมูลที่เกี่ยวข้องกับผู้ใช้บริการรายอื่น

ในกรณีดังกล่าว ประกาศกำหนดให้ CSP แสดง หลักฐานที่เป็นอิสระ ว่ามีการนำมาตรการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปปฏิบัติและดำเนินการตามนโยบายและขั้นตอนของ CSP

การใช้หลักฐานจากการตรวจสอบอย่างเป็นอิสระจึงเป็นกลไกที่ช่วยให้ CSC สามารถได้รับความเชื่อมั่นในมาตรการของ CSP โดยไม่จำเป็นต้องเข้าตรวจสอบระบบของ CSP โดยตรงทุกกรณี

3. การให้หลักฐานก่อนเข้าทำสัญญา

ประกาศกำหนดเพิ่มเติมว่า CSP ต้องแสดงหลักฐานดังกล่าวแก่ ผู้ที่คาดว่าจะเป็น CSC ก่อนเข้าทำสัญญา

ประเด็นนี้มีความสำคัญในทางปฏิบัติ เนื่องจากหมายความว่าการประเมินหลักฐานด้านความมั่นคงปลอดภัยไม่ควรเกิดขึ้นเฉพาะหลังจากเริ่มใช้บริการแล้ว แต่ควรเป็นส่วนหนึ่งของการประเมินและคัดเลือก CSP ก่อนเกิดข้อผูกพันตามสัญญา

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

4. กรณีไม่สามารถจัดให้มีการตรวจสอบอย่างเป็นอิสระ

เมื่อไม่สามารถดำเนินการตรวจสอบอย่างเป็นอิสระได้ ประกาศกำหนดให้ CSP ดำเนินการประเมินตนเองและเปิดเผยกระบวนการและผลลัพธ์ต่อ CSC

ดังนั้น การประเมินตนเองตามกรณีนี้ไม่ควรมีเพียงคำรับรองว่ามีการปฏิบัติตาม แต่ควรทำให้ CSC สามารถทราบได้อย่างน้อยว่าการประเมินดำเนินการอย่างไร ครอบคลุมเรื่องใด และมีผลการประเมินอย่างไร เพื่อใช้ประกอบการพิจารณาความเพียงพอของหลักฐาน

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การพิจารณาหลักฐานตามวัตถุประสงค์ของการตรวจสอบ

CSC ควรเริ่มจากการกำหนดว่า ต้องการยืนยันเรื่องใด แล้วจึงพิจารณาว่าหลักฐานที่ CSP ให้สามารถตอบวัตถุประสงค์ดังกล่าวได้หรือไม่

แนวทางสามารถสรุปได้ดังนี้

ข้อกำหนดหรือมาตรการที่ต้องการยืนยัน ⟶ ข้อกล่าวอ้างของ CSP ⟶ หลักฐาน ⟶ ขอบเขตและความเป็นปัจจุบัน ⟶ ข้อจำกัดหรือข้อค้นพบ ⟶ ผลการพิจารณา

แนวทางดังกล่าวช่วยลดการพิจารณาหลักฐานในลักษณะเพียงตรวจสอบว่ามีใบรับรองหรือรายงานอยู่หรือไม่ โดยให้ความสำคัญกับความสัมพันธ์ระหว่างหลักฐานกับสิ่งที่ CSC ต้องการยืนยัน

2. การใช้หลักฐานจากการทบทวนอย่างเป็นอิสระ

กรณีที่การตรวจสอบ CSP โดยตรงไม่เหมาะสม CSC สามารถพิจารณาหลักฐานจากการตรวจสอบหรือการประเมินอย่างเป็นอิสระที่ CSP จัดให้ โดยควรพิจารณาตามความเหมาะสมถึง

- ผู้ดำเนินการตรวจสอบหรือประเมิน
- ขอบเขตของการตรวจสอบ
- ช่วงเวลาที่ดำเนินการและความเป็นปัจจุบัน
- บริการหรือองค์ประกอบที่อยู่ในขอบเขต
- ข้อจำกัดหรือข้อยกเว้นของรายงาน
- ข้อค้นพบที่อาจเกี่ยวข้องกับบริการที่ CSC ใช้งาน

การพิจารณาดังกล่าวไม่ได้หมายความว่า CSC ต้องสามารถเข้าถึงรายงานฉบับเต็มทุกกรณี หากมีข้อจำกัดด้านการรักษาความลับหรือความมั่นคงปลอดภัย แต่ควรได้รับข้อมูลเพียงพอต่อการตัดสินใจตามข้อกำหนดที่เกี่ยวข้อง

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การติดตามข้อจำกัดหรือข้อค้นพบ

หากหลักฐานที่ได้รับมีข้อจำกัด ข้อยกเว้น หรือข้อค้นพบที่เกี่ยวข้องกับบริการของ CSC ไม่ควรพิจารณาเฉพาะสถานะว่า “ผ่านการตรวจประเมิน” แต่ควรพิจารณาว่าประเด็นดังกล่าวมีผลต่อข้อกำหนดหรือการใช้บริการขององค์กรหรือไม่

กรณีที่มีนัยสำคัญ ควรกำหนดการดำเนินการ ผู้รับผิดชอบ และการติดตามผล หรือเชื่อมโยงเข้าสู่กระบวนการบริหารความเสี่ยงและการตัดสินใจตามข้อ 5.1.1 และ 5.1.2

4. ตัวอย่างการนำไปใช้ในทางปฏิบัติ

ตัวอย่างที่ 1 CSP ไม่อนุญาตให้ CSC เข้าตรวจสอบศูนย์ข้อมูลโดยตรง

CSC ขอเข้าตรวจสอบศูนย์ข้อมูลและกระบวนการควบคุมของ CSP แต่ CSP ไม่สามารถอนุญาตให้ผู้ใช้บริการแต่ละรายเข้าตรวจสอบได้ เนื่องจากสภาพแวดล้อมดังกล่าวรองรับผู้ใช้บริการหลายรายและการเปิดให้ตรวจสอบอาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัย กรณีนี้ ไม่ได้หมายความโดยอัตโนมัติว่า CSP ไม่ผ่านข้อกำหนด แต่ CSP ต้องสามารถแสดงหลักฐานที่เป็นอิสระเกี่ยวกับการนำมาตรการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปปฏิบัติตามที่ประกาศกำหนด CSC จึงควรตรวจสอบว่าหลักฐานดังกล่าวมีขอบเขตเกี่ยวข้องกับบริการที่กำลังพิจารณา มีความเป็นปัจจุบัน และมีข้อมูลเพียงพอต่อการประเมินหรือไม่

ตัวอย่างที่ 2 การประเมิน CSP ก่อนเข้าทำสัญญา

หน่วยงานอยู่ระหว่างคัดเลือก CSP และผู้ให้บริการระบุว่าบริการของตนมีมาตรการด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานที่เกี่ยวข้อง หน่วยงานไม่ควรรอจนเริ่มใช้บริการแล้วจึงตรวจสอบหลักฐาน แต่ควรขอหลักฐานที่เกี่ยวข้องในขั้นตอนการประเมินก่อนเข้าทำสัญญา เพื่อพิจารณาว่าข้อกล่าวอ้างของ CSP มีหลักฐานรองรับและเหมาะสมกับบริการที่จะใช้หรือไม่ ซึ่งสอดคล้องกับข้อกำหนดของประกาศที่ให้ CSP แสดงหลักฐานแก่ผู้ที่คาดว่าจะเป็น CSC ก่อนเข้าทำสัญญา

ตัวอย่างที่ 3 ไม่มีหลักฐานการตรวจสอบอย่างเป็นอิสระ

CSP ไม่สามารถจัดให้มีหลักฐานจากการตรวจสอบอย่างเป็นอิสระสำหรับบริการที่ CSC กำลังพิจารณาได้ ในกรณีดังกล่าว CSP ต้องดำเนินการประเมินตนเองและเปิดเผย ทั้งกระบวนการและผลลัพธ์ ต่อ CSC ตามประกาศ ไม่ใช่เพียงส่งข้อความหรือหนังสือรับรองว่าตนปฏิบัติตามข้อกำหนด CSC ควรนำข้อมูลดังกล่าวมาพิจารณาความเพียงพอและข้อจำกัดของหลักฐานก่อนตัดสินใจดำเนินการต่อไป

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5. หลักฐานที่ควรมี

ประเด็น	ตัวอย่างหลักฐาน
การนำมาตรการไปปฏิบัติ	เอกสารหรือรายงานที่ยืนยันการดำเนินมาตรการควบคุม
การรับรอง	ใบรับรองหรือหลักฐานการรับรองมาตรฐานที่เกี่ยวข้อง
การตรวจสอบอย่างเป็นอิสระ	รายงานหรือผลการประเมินจากหน่วยงานอิสระ
ขอบเขตของหลักฐาน	ขอบเขตบริการ ระบบ สถานที่ หรือช่วงเวลาที่หลักฐานครอบคลุม
การประเมินก่อนทำสัญญา	แบบประเมิน CSP รายงานการตรวจสอบสถานะและความเหมาะสมของ CSP (Due Diligence) หรือบันทึกการพิจารณาหลักฐาน
กรณีไม่มีการตรวจสอบอย่างเป็นอิสระ	กระบวนการประเมินตนเองและผลลัพธ์ที่ CSP เปิดเผย
ข้อจำกัดหรือข้อค้นพบ	รายการข้อยกเว้น ข้อจำกัด ผลการประเมินความเสี่ยง หรือแผนติดตามแก้ไข

หมายเหตุ: ตัวอย่างหลักฐานข้างต้นเป็นแนวทางสำหรับสนับสนุนการดำเนินการ ไม่ใช่การกำหนดเอกสารเพิ่มเติมจากประกาศ

สรุปแนวทางการปฏิบัติตามข้อ 5.1.3

การปฏิบัติตามกฎ ระเบียบ และข้อบังคับสำหรับบริการคลาวด์ควรดำเนินการอย่างเป็นระบบตั้งแต่การระบุข้อกำหนดที่เกี่ยวข้อง การพิจารณาเขตอำนาจทางกฎหมายและข้อกำหนดตามสัญญา การจัดการสิทธิในทรัพย์สินทางปัญญา การปกป้องบันทึกข้อมูล การตรวจสอบความสอดคล้องของมาตรการควบคุมการเข้ารหัส ตลอดจนการได้รับหลักฐานที่เพียงพอเพื่อยืนยันว่ามาตรการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลได้มีการนำไปปฏิบัติจริง

การดำเนินการดังกล่าวควรอยู่บนหลักความรับผิดชอบร่วมกันระหว่าง CSC และ CSP โดย CSC ยังคงมีหน้าที่พิจารณาว่าการใช้บริการคลาวด์สามารถตอบสนองข้อกำหนดที่มีผลใช้กับองค์กรได้หรือไม่ ขณะที่ CSP มีหน้าที่ให้ข้อมูล คำอธิบาย และหลักฐานในส่วนที่อยู่ภายใต้ความรับผิดชอบของตนตามที่ประกาศกำหนด

หลักการสำคัญ

การดำเนินการตามข้อ 5.1.3 ควรยึดหลักสำคัญ ดังนี้

1. เริ่มจากระดับผลกระทบและข้อกำหนดที่ใช้บังคับ

องค์กรควรนำผลการจำแนกระดับผลกระทบของข้อมูลหรือระบบสารสนเทศมาใช้กำหนดข้อกำหนดขั้นต่ำที่ต้องดำเนินการตามประกาศ ก่อนพิจารณารายละเอียดด้านการปฏิบัติตามข้อกำหนด ทั้งนี้ การที่ข้อกำหนดใดมิได้เป็นข้อกำหนดขั้นต่ำสำหรับระดับผลกระทบนั้น มิได้ทำให้องค์กรได้รับยกเว้นจากกฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา หรือข้อผูกพันอื่นที่มีผลใช้บังคับ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

2. ระบุข้อกำหนดก่อนประเมินความสอดคล้อง

เมื่อทราบข้อกำหนดที่ใช้บังคับแล้ว องค์กรควรระบุว่ามีกฎหมาย กฎ ระเบียบ ข้อบังคับ ข้อกำหนดตามสัญญา หรือข้อผูกพันใดเกี่ยวข้องกับบริการคลาวด์ ก่อนพิจารณาว่ามาตรการหรือหลักฐานที่มีอยู่สามารถรองรับข้อกำหนดดังกล่าวได้หรือไม่

3. พิจารณาทั้ง CSC และ CSP รวมถึงเขตอำนาจทางกฎหมายที่เกี่ยวข้อง

การใช้บริการคลาวด์อาจเกี่ยวข้องกับข้อกำหนดและเขตอำนาจทางกฎหมายที่มีผลต่อทั้ง CSC และ CSP ตลอดจนผู้ให้บริการภายนอกที่เกี่ยวข้อง จึงควรพิจารณาความสัมพันธ์ดังกล่าวตามขอบเขตของบริการและข้อมูลที่ใช้งานจริง

4. ใช้หลักฐานที่สัมพันธ์กับข้อกำหนดที่ต้องการยืนยัน

ใบรับรอง รายงานการตรวจประเมิน ผลการทบทวนอย่างเป็นอิสระ หรือคำอธิบายของ CSP ควรได้รับการพิจารณาจากขอบเขต ความเป็นปัจจุบัน ความเกี่ยวข้อง และข้อจำกัดของหลักฐาน ไม่ควรพิจารณาเพียงว่ามีเอกสารหรือใบรับรองดังกล่าวอยู่หรือไม่

5. พิจารณาการปฏิบัติตามข้อกำหนดอย่างต่อเนื่อง

การเปลี่ยนแปลงกฎหมาย สัญญา รูปแบบบริการ ผู้ให้บริการภายนอก สถานที่จัดเก็บหรือประมวลผลข้อมูล เขตอำนาจทางกฎหมาย หรือองค์ประกอบสำคัญของบริการ อาจทำให้ผลการประเมินเดิมเปลี่ยนแปลง จึงควรกำหนดเหตุหรือเงื่อนไขสำหรับการทบทวนใหม่ตามความเหมาะสม

6. เชื่อมโยงช่องว่างกับความเสี่ยง การตัดสินใจ และการติดตาม

เมื่อพบข้อจำกัดหรือความไม่สอดคล้อง องค์กรควรระบุข้อกำหนดที่ได้รับผลกระทบ หลักฐานที่เกี่ยวข้อง ผลกระทบและความเสี่ยง ทางเลือกหรือมาตรการเพิ่มเติม ตลอดจนผู้มีอำนาจตัดสินใจและผู้รับผิดชอบต่อการติดตาม โดยเชื่อมโยงกับบทบาทและอำนาจตามข้อ 5.1.2

7. การยอมรับความเสี่ยงไม่ใช้แทนหน้าที่ตามกฎหมายหรือข้อกำหนดที่มีผลบังคับ

ก่อนใช้การยอมรับความเสี่ยงหรือมาตรการทดแทน องค์กรควรตรวจสอบว่าข้อกำหนดที่เกี่ยวข้องเปิดให้ดำเนินการในลักษณะดังกล่าวได้หรือไม่ หากกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือประกาศกำหนดกระบวนการเฉพาะ องค์กรยังคงต้องดำเนินการตามกระบวนการนั้น แนวทางดังกล่าวสามารถสรุปเป็นความสัมพันธ์ได้ดังนี้

ระดับผลกระทบ ⟶ ข้อกำหนดที่ใช้บังคับ ⟶ ข้อมูลและหลักฐาน ⟶ การประเมินความสอดคล้อง ⟶ ช่องว่างหรือข้อจำกัด ⟶ ผลกระทบและความเสี่ยง ⟶ การดำเนินการ/การตัดสินใจ ⟶ ผู้รับผิดชอบ ⟶ การติดตามและทบทวน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. สรุปความรับผิดชอบของ CSC และ CSP

ข้อ	ประเด็น	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
5.1.3.1	กฎหมายและข้อกำหนดตามสัญญา	พิจารณากฎหมายและข้อบังคับที่เกี่ยวข้อง รวมถึงเขตอำนาจทางกฎหมายที่ควบคุม CSP และขอหลักฐานการปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้อง	แจ้งเขตอำนาจทางกฎหมายที่ควบคุมบริการ ระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับตน และแสดงหลักฐานการปฏิบัติตามกฎหมายและข้อกำหนดตามสัญญา
5.1.3.2	สิทธิในทรัพย์สินทางปัญญา	มีขั้นตอนระบุข้อกำหนดการอนุญาตให้ใช้สิทธิเฉพาะระบบคลาวด์ก่อนอนุญาตให้ติดตั้งซอฟต์แวร์ โดยคำนึงถึงความยืดหยุ่นและการปรับขนาดของบริการ	มีกระบวนการตอบสนองต่อข้อร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา
5.1.3.3	การปกป้องบันทึกข้อมูล	ขอข้อมูลเกี่ยวกับการปกป้องบันทึกที่ CSP รวบรวมและจัดเก็บซึ่งเกี่ยวข้องกับการใช้บริการของ CSC	ให้ข้อมูลเกี่ยวกับการปกป้องบันทึกดังกล่าวแก่ CSC
5.1.3.4	มาตรการควบคุมการเข้ารหัส	ตรวจสอบให้มาตรการควบคุมการเข้ารหัสที่ใช้กับบริการสอดคล้องกับข้อตกลง กฎหมายและข้อบังคับที่เกี่ยวข้อง	ให้คำอธิบายเกี่ยวกับมาตรการควบคุมการเข้ารหัสที่ CSP ดำเนินการ เพื่อให้ CSC ใช้ทบทวนการปฏิบัติตามข้อกำหนด
5.1.3.5	การทบทวนอย่างเป็นอิสระ	ขอหลักฐานที่เป็นเอกสารว่ามาตรการควบคุมและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยได้มีการนำไปปฏิบัติและสอดคล้องกับที่ CSP กล่าวอ้าง	ให้หลักฐานที่เป็นเอกสาร และเมื่อ CSC ตรวจสอบโดยตรงไม่ได้หรือการตรวจสอบอาจเพิ่มความเสี่ยง ต้องแสดงหลักฐานที่เป็นอิสระ รวมถึงดำเนินการประเมินตนเองและเปิดเผยกระบวนการกับผลลัพธ์เมื่อไม่สามารถจัดให้มีการตรวจสอบอย่างเป็นอิสระได้

ตารางนี้เป็นการสรุปสาระจากข้อกำหนด 5.1.3.1–5.1.3.5 เพื่อให้เห็นความสัมพันธ์ของความรับผิดชอบ โดยรายละเอียดให้พิจารณาตามข้อกำหนดแต่ละข้อ

ไม่ใช่สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2. หลักฐานสำคัญที่ควรพิจารณา

หลักฐานสำหรับการปฏิบัติตามข้อ 5.1.3 ไม่จำเป็นต้องจัดทำเป็นเอกสารชุดใหม่ทั้งหมด หากองค์กรมีเอกสารหรือระบบบริหารจัดการที่สามารถแสดงข้อมูลและความเชื่อมโยงที่จำเป็นได้อยู่แล้ว

ประเด็น	ตัวอย่างหลักฐาน
กฎหมายและข้อกำหนด	ทะเบียนกฎหมาย ทะเบียนข้อกำหนด หรือผลการทบทวนการปฏิบัติตาม
เขตอำนาจทางกฎหมาย	ข้อมูลที่ CSP แจ้งเกี่ยวกับเขตอำนาจทางกฎหมายที่ควบคุมบริการ
ข้อกำหนดตามสัญญา	สัญญา ข้อตกลงระดับการให้บริการ และเงื่อนไขการใช้บริการ
สิทธิในทรัพย์สินทางปัญญา	ใบอนุญาตให้ใช้สิทธิ สัญญาซอฟต์แวร์ ทะเบียนซอฟต์แวร์
การปกป้องบันทึกข้อมูล	เอกสารหรือคำอธิบายจาก CSP เกี่ยวกับการปกป้องบันทึก
การควบคุมการเข้ารหัส	คำอธิบายมาตรการควบคุมการเข้ารหัสของ CSP และผลการทบทวนความสอดคล้อง
การทบทวนอย่างเป็นอิสระ	ใบรับรอง รายงานการตรวจประเมิน หรือหลักฐานจากการประเมินอย่างเป็นอิสระ
กรณีไม่มีการตรวจสอบอย่างเป็นอิสระ	กระบวนการและผลการประเมินตนเองที่ CSP เปิดเผย
ช่องว่างและการดำเนินการ	ผลการประเมินความเสี่ยง แผนการดำเนินการ บันทึกการอนุมัติ หรือมติที่เกี่ยวข้อง
การติดตาม	ผลการทบทวน หลักฐานการแก้ไข และการประเมินใหม่เมื่อมีการเปลี่ยนแปลง

หมายเหตุ: รายการดังกล่าวเป็นตัวอย่างหลักฐานที่อาจใช้สนับสนุนการปฏิบัติตามข้อกำหนด มิใช่การกำหนดให้ต้องจัดทำเอกสารทุกประเภทเพิ่มเติมจากประกาศ

3. การนำไปประยุกต์ใช้ในทางปฏิบัติ

การดำเนินการตามข้อ 5.1.3 ไม่ควรแยกออกจากกระบวนการบริหารจัดการที่องค์กรมีอยู่ แต่ควรเชื่อมโยงกับการกำหนดนโยบายตามข้อ 5.1.1 การกำหนดบทบาทและอำนาจการตัดสินใจตามข้อ 5.1.2 ตลอดจนมาตรการควบคุมด้านเทคนิคและการปฏิบัติการตามข้อ 5.2 ที่เกี่ยวข้อง

ตัวอย่างเช่น เมื่อ CSC พบจากการทบทวนสัญญาว่า CSP ไม่สามารถให้ข้อมูลหรือหลักฐานที่จำเป็นต่อการยืนยันข้อกำหนดทางกฎหมายบางประการได้ CSC ควรระบุให้ชัดว่า ข้อกำหนดใดได้รับผลกระทบ หลักฐานใดขาดหาย และข้อจำกัดดังกล่าวมีผลอย่างไร จากนั้นจึงพิจารณาทางเลือก มาตรการเพิ่มเติม หรือการเปลี่ยนแปลงบริการ และนำประเด็นที่มีนัยสำคัญเข้าสู่กระบวนการตัดสินใจของผู้มีอำนาจ

ในทำนองเดียวกัน หาก CSP มีใบรับรองหรือรายงานการตรวจประเมิน ไม่ควรพิจารณาเพียงสถานะว่า “ได้รับการรับรองแล้ว” แต่ควรพิจารณาว่าหลักฐานดังกล่าวเกี่ยวข้องกับสิ่งที่องค์กรต้องการยืนยัน มีขอบเขตและระยะเวลาที่เหมาะสม และมีข้อจำกัดหรือข้อค้นพบที่ต้องติดตามหรือไม่

ร่างประกาศ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

แนวทางดังกล่าวช่วยให้การปฏิบัติตามข้อกำหนดไม่เป็นเพียงการรวบรวมเอกสาร แต่สามารถแสดงความเชื่อมโยงระหว่าง ข้อกำหนด หลักฐาน ผลการประเมิน การตัดสินใจ และการติดตามผล ได้อย่างตรวจสอบย้อนกลับได้

4. การวัดผลในทางปฏิบัติ

องค์กรอาจพิจารณาตัวชี้วัดในภาพรวมของข้อ 5.1.3 แทนการกำหนดตัวชี้วัดแยกสำหรับทุกข้อย่อย เช่น

1. ร้อยละของบริการคลาวด์ที่มีการระบุกฎหมาย ข้อกำหนดตามสัญญา และเขตอำนาจทางกฎหมายที่เกี่ยวข้อง
2. ร้อยละของข้อกำหนดสำคัญที่มีข้อมูลหรือหลักฐานสนับสนุนการปฏิบัติตามอย่างเพียงพอ
3. ร้อยละของ CSP ที่มีหลักฐานด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการทบทวนก่อนเข้าทำสัญญา
4. ร้อยละของช่องว่างหรือข้อจำกัดที่มีนัยสำคัญซึ่งได้รับการกำหนดผู้รับผิดชอบและติดตามการดำเนินการ
5. ร้อยละของการเปลี่ยนแปลงที่มีนัยสำคัญซึ่งได้รับการทบทวนผลกระทบต่อการปฏิบัติตามข้อกำหนด

ตัวชี้วัดดังกล่าวเป็นแนวทางสำหรับสนับสนุนการบริหารจัดการ องค์กรสามารถเลือกใช้หรือปรับให้เหมาะสมกับบริบทของตน โดยมิใช่ข้อกำหนดเพิ่มเติมจากประกาศ

5. ข้อพิจารณาสำหรับการนำไปใช้

ในการนำข้อ 5.1.3 ไปใช้ องค์กรควรให้ความสำคัญกับ ความเพียงพอและความสัมพันธ์ของหลักฐานกับข้อกำหนดมากกว่าปริมาณเอกสารที่จัดทำขึ้น และควรใช้กระบวนการที่องค์กรมีอยู่เดิมให้มากที่สุด เพื่อลดความซ้ำซ้อนและทำให้การปฏิบัติตามข้อกำหนดสามารถดำเนินการได้จริง

เมื่อมีการใช้ผู้ให้บริการภายนอกหลายรายหรือบริการคลาวด์หลายรูปแบบ องค์กรควรสามารถระบุได้ว่าแต่ละฝ่ายรับผิดชอบต่อข้อกำหนดใด และหลักฐานใดอยู่ภายใต้การควบคุมของ CSC หรือ CSP โดยเชื่อมโยงกับหลักความรับผิดชอบร่วมกันและบทบาทที่กำหนดไว้ในข้อ 5.1.2

หากพบข้อกำหนดที่ไม่สามารถปฏิบัติได้หรือหลักฐานไม่เพียงพอ องค์กรควรหลีกเลี่ยงการสรุปเพียงว่า “ยอมรับความเสี่ยง” แต่ควรตรวจสอบก่อนว่าข้อกำหนดดังกล่าวเปิดให้ใช้การยอมรับความเสี่ยงหรือมาตรการทดแทนได้หรือไม่ หากเป็นหน้าที่ตามกฎหมาย กฎ ระเบียบ หรือประกาศที่กำหนดกระบวนการเฉพาะ องค์กรยังคงต้องดำเนินการตามกระบวนการนั้น

โดยสรุป การปฏิบัติตามข้อ 5.1.3 ควรทำให้องค์กรสามารถแสดงความเชื่อมโยงได้อย่างตรวจสอบย้อนกลับตั้งแต่ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ข้อกำหนดที่ใช้บังคับ ข้อมูลและหลักฐานที่ได้รับจาก CSP ผลการประเมินความสอดคล้อง ช่องว่างหรือข้อจำกัดที่ตรวจพบ ตลอดจนการดำเนินการ การตัดสินใจ ผู้รับผิดชอบ และการติดตามผล

CSC ยังคงมีหน้าที่พิจารณาว่าบริการคลาวด์ที่เลือกใช้สามารถรองรับข้อกำหนดที่มีผลใช้กับองค์กรและระดับผลกระทบของข้อมูลหรือระบบได้หรือไม่ ขณะที่ CSP ต้องสามารถให้ข้อมูล คำอธิบาย และหลักฐานตามขอบเขต

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ความรับผิดชอบของตนตามข้อ 5.1.3.1–5.1.3.5 ทั้งนี้ การมีใบรับรอง รายงานการตรวจประเมิน หรือมาตรการควบคุมของ CSP ไม่ควรถูกใช้แทนการพิจารณาข้อกำหนดที่มีผลใช้กับ CSC โดยอัตโนมัติ

สาระสำคัญจึงมิใช่ปริมาณเอกสารที่องค์กรจัดทำขึ้น แต่คือความสามารถในการแสดงว่า “ข้อกำหนดใดใช้บังคับ มีหลักฐานใดรองรับ พบช่องว่างใด ใครเป็นผู้ตัดสินใจ และมีการติดตามผลอย่างไร” ซึ่งทำให้การปฏิบัติตามข้อกำหนดสามารถเชื่อมโยงกับการกำกับดูแล การบริหารความเสี่ยง และการตัดสินใจขององค์กรได้อย่างเป็นระบบ

5.2.1 การบริหารทรัพยากรมนุษย์ (Human Resource Security)

5.2.1.1 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรม (Information Security Awareness, Education and Training)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องเพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง – มาตรฐานและขั้นตอนการใช้บริการคลาวด์ – ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น – ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์ – การคุ้มครองข้อมูลส่วนบุคคล – ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)	ก) ผู้ให้บริการคลาวด์ ต้องสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษา และการฝึกอบรมแก่พนักงาน รวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกันเกี่ยวกับการจัดการข้อมูลของผู้ใช้บริการคลาวด์ และข้อมูลที่ได้จากบริการคลาวด์อย่างเหมาะสม โดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อผู้ใช้บริการคลาวด์หรืออยู่ภายใต้ข้อจำกัดเฉพาะ รวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึงและใช้งานโดย ผู้ให้บริการคลาวด์

วัตถุประสงค์ (Objective) เพื่อลดความเสี่ยงที่เกิดจากความผิดพลาดของมนุษย์ (Human Error), การโจรกรรมข้อมูลจากภายใน (Insider Threat), และการใช้งานระบบในทางที่ผิด โดยการสร้างความมั่นใจว่าบุคลากรที่เกี่ยวข้องกับบริการคลาวด์มีความรู้ความเข้าใจ ตระหนักถึงความรับผิดชอบ และมีความน่าเชื่อถือตลอดวงจรการจ้างงาน ตั้งแต่ก่อนเริ่มงาน ระหว่างปฏิบัติงาน จนถึงพ้นสภาพการจ้างงาน

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ก) ผู้ใช้บริการคลาวด์ ต้องเพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง

– มาตรฐานและขั้นตอนการใช้บริการคลาวด์

– ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น

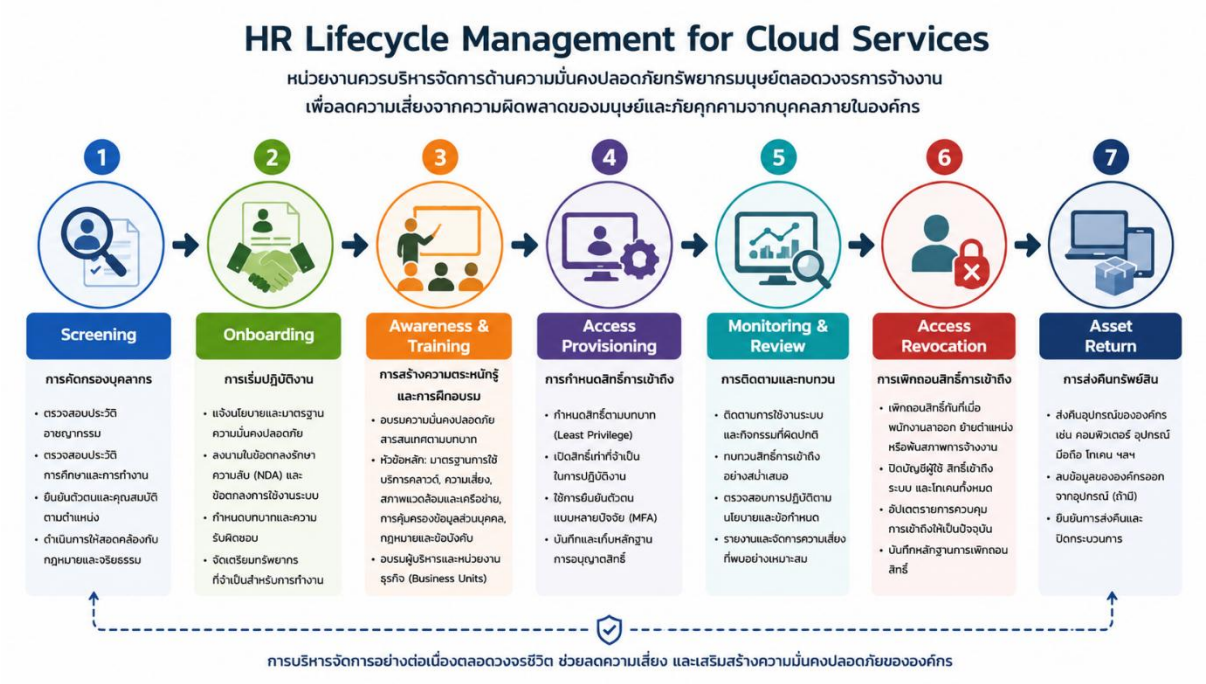
– ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์

– การคุ้มครองข้อมูลส่วนบุคคล

– ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง

ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)

หน่วยงานควรบริหารจัดการด้านความมั่นคงปลอดภัยทรัพยากรมนุษย์ตลอดวงจรการจ้างงาน ตั้งแต่การคัดกรองบุคลากร การเริ่มปฏิบัติงาน การสร้างความตระหนักรู้ การกำหนดสิทธิ์การเข้าถึง การติดตามและทบทวนการใช้งาน ไปจนถึงการเพิกถอนสิทธิ์และการส่งคืนทรัพย์สินเมื่อพ้นสภาพการจ้างงาน เพื่อให้สามารถลดความเสี่ยงจากความผิดพลาดของมนุษย์และภัยคุกคามจากบุคคลภายในองค์กรได้อย่างเหมาะสม



รูปที่ 7 ตัวอย่างวงจรการบริหารจัดการด้านความมั่นคงปลอดภัยทรัพยากรมนุษย์ (HR Security Lifecycle)

โดยควรดำเนินการให้ครอบคลุม 3 ระยะ ดังนี้

1. ระยะก่อนการจ้างงาน (Prior to Employment)

- **การคัดกรองบุคลากร (Background Verification)**

สำหรับตำแหน่งงานที่มีสิทธิ์เข้าถึงข้อมูลสำคัญหรือเป็นผู้ดูแลระบบ (Administrator) บนคลาวด์ หน่วยงาน**ควร**ดำเนินการตรวจสอบประวัติ (Background Checks) เช่น ประวัติอาชญากรรม ประวัติการศึกษา และประวัติการทำงานย้อนหลัง ให้สอดคล้องกับกฎหมายและจริยธรรม

เหตุผลและความจำเป็น (Rationale) ผู้ดูแลระบบคลาวด์เป็นผู้มีสิทธิ์เข้าถึงระบบและข้อมูลสำคัญขององค์กรในระดับสูง หากรับบุคคลที่มีประวัติทุจริตเข้ามา อาจนำไปสู่ความเสียหายร้ายแรงเกินกว่าที่ระบบป้องกันทางเทคนิคจะรับมือได้

- **ข้อตกลงรักษาความลับ (Confidentiality Agreements)**

พนักงานและผู้รับจ้าง (Contractors) ทุกคนที่มีสิทธิ์เข้าถึงระบบคลาวด์ ควรลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement: NDA) หรือข้อตกลงการรักษาความลับ ที่ระบุขอบเขตความรับผิดชอบและบทลงโทษทางกฎหมายหากนำข้อมูลองค์กรไปเผยแพร่

2. ระยะระหว่างการจ้างงาน (During Employment)

- **การสร้างความตระหนักรู้และการฝึกอบรม (Awareness, Education and Training)**

หน่วยงานควรจัดอบรมให้แก่พนักงาน (รวมถึงผู้รับจ้าง) อย่างสม่ำเสมอ โดยเนื้อหาต้องครอบคลุม 5 หัวข้อหลักตามข้อกำหนด

1. **มาตรฐานและขั้นตอนปฏิบัติ** วิธีการใช้บริการคลาวด์อย่างปลอดภัย (เช่น การตั้งค่าความเป็นส่วนตัว)
2. **ความเสี่ยงด้านสารสนเทศ** รู้ทันภัยคุกคาม เช่น การหลอกลวงทางอีเมล (Phishing) หรือวิศวกรรมสังคม (Social Engineering)
3. **ความเสี่ยงด้านสภาพแวดล้อม** ความเสี่ยงจากการใช้งานผ่านเครือข่ายสาธารณะหรืออุปกรณ์ส่วนตัว (BYOD)
4. **การคุ้มครองข้อมูลส่วนบุคคล** หน้าที่ในการดูแลข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)
5. **กฎหมายและข้อบังคับ** ความรับผิดชอบตามกฎหมายที่เกี่ยวข้อง
6. **การแจ้งเหตุผิดปกติและเหตุละเมิดด้านความมั่นคงปลอดภัย (Security Incident and Breach Reporting)** หน้าที่ในการแจ้งเหตุผิดปกติ เหตุสงสัย หรือเหตุละเมิดด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงานที่รับผิดชอบโดยไม่ล่าช้า เช่น การตรวจพบการเข้าถึงโดยไม่ได้รับอนุญาต การส่งข้อมูลผิดผู้รับ การสูญหายของอุปกรณ์ หรือพฤติกรรมที่อาจบ่งชี้ถึงการโจมตีทางไซเบอร์

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- **การอบรมสำหรับผู้บริหาร (Executive Training)**

หน่วยงานควรสร้างความตระหนักรู้แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units) เพื่อให้เข้าใจความเสี่ยงในภาพรวมและการกำกับดูแล (Governance) โดยควรได้รับการสร้างความตระหนักรู้เกี่ยวกับ

- ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จากการใช้บริการคลาวด์
- ผลกระทบทางธุรกิจและกฎหมายจากเหตุข้อมูลรั่วไหล
- หลักการกำกับดูแลบริการคลาวด์ (Cloud Governance)
- หลักการแบ่งความรับผิดชอบ (Shared Responsibility Model)
- บทบาทของผู้บริหารในการกำกับดูแลความเสี่ยงและการตัดสินใจด้านคลาวด์
- หน้าที่และกระบวนการรายงานเหตุละเมิดข้อมูลหรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident/Breach Reporting)

เหตุผลและความจำเป็น (Rationale) การตัดสินใจด้านคลาวด์จำนวนมากเป็นการตัดสินใจเชิงธุรกิจและการกำกับดูแล หากผู้บริหารขาดความเข้าใจด้านความเสี่ยง อาจนำไปสู่การกำหนดนโยบายหรือการลงทุนที่ไม่เหมาะสม และส่งผลกระทบต่อความมั่นคงปลอดภัยขององค์กรในภาพรวม

3. ระยะพ้นสภาพการจ้างงานหรือเปลี่ยนหน้าที่ (Termination and Change of Employment)

- **การเพิกถอนสิทธิ์ (Access Revocation)**

หน่วยงานควรมีกระบวนการเพิกถอนสิทธิ์การเข้าถึงระบบคลาวด์และแอปพลิเคชันที่เกี่ยวข้องภายในระยะเวลาที่องค์กรกำหนด (แนะนำภายใน 24 ชั่วโมง) เมื่อพนักงานลาออกหรือถูกเลิกจ้าง หรือปรับปรุงสิทธิ์เมื่อมีการย้ายตำแหน่งงาน (Change of Employment)

เหตุผลและความจำเป็น (Rationale) อดีตพนักงานที่ยังเข้าถึงระบบได้คือความเสี่ยงอันดับต้น ๆ ของข้อมูลรั่วไหล (Data Leakage) หรือการลบหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต

- **การส่งคืนทรัพย์สิน (Return of Assets)**

พนักงานที่พ้นสภาพควรส่งคืนอุปกรณ์ที่หน่วยงานจัดหาให้ (เช่น คอมพิวเตอร์พกพา, อุปกรณ์ยืนยันตัวตน Hardware Token) และส่งมอบรหัสผ่านสำหรับการบริหารจัดการระบบทั้งหมดคืนแก่หน่วยงาน

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

- **การอบรมเจ้าหน้าที่ของผู้ให้บริการ (CSP Staff Training)**

ผู้ให้บริการคลาวด์ควรอบรมพนักงานของตนเองเกี่ยวกับขั้นตอนการจัดการข้อมูลของผู้ใช้บริการอย่างเคร่งครัด โดยเฉพาะข้อมูลความลับและข้อมูลส่วนบุคคล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access)

- **การคัดกรองบุคลากรของผู้ให้บริการ (CSP Personnel Screening)**

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ผู้ให้บริการควรมีกระบวนการตรวจสอบประวัติอาชญากรรมและประวัติการทำงานของพนักงานที่มีสิทธิ์เข้าถึงศูนย์ข้อมูล (Physical Access) หรือระบบบริหารจัดการโครงสร้างพื้นฐาน (Logical Access) ตามกฎหมายแรงงานท้องถิ่น

- **มาตรการลงโทษทางวินัย (Disciplinary Process)**

ผู้ให้บริการควรมีระเบียบวินัยและบทลงโทษที่ชัดเจนสำหรับพนักงานที่ละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

เพื่อให้การบริหารทรัพยากรมนุษย์มีประสิทธิภาพและสอดคล้องกับการใช้งานคลาวด์จริง ขอแนะนำแนวทางปฏิบัติดังนี้

1. การจัดทำหลักสูตรอบรมตามบทบาท (Role-Based Training Curriculum) เนื้อหาการอบรมควรปรับให้เหมาะกับหน้าที่ของแต่ละกลุ่ม

- **สำหรับผู้ใช้งานทั่วไป (End Users)** เน้นเรื่อง "แนวปฏิบัติด้านความมั่นคงปลอดภัยที่เหมาะสมและไม่เหมาะสม"

แนวปฏิบัติที่เหมาะสม	**แนวปฏิบัติที่ไม่เหมาะสม**
เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับบัญชีที่เข้าถึงบริการคลาวด์	ไม่เปิดใช้งาน MFA สำหรับบัญชีที่เข้าถึงบริการคลาวด์
จัดเก็บข้อมูลในระบบหรือบริการคลาวด์ที่องค์กรอนุญาต	นำไฟล์งานสำคัญไปจัดเก็บบนคลาวด์ส่วนตัว (Personal Cloud Storage)
ใช้งานเฉพาะเครื่องมือหรือบริการที่องค์กรอนุมัติ	ใช้เครื่องมือหรือบริการที่องค์กรไม่ได้รับรอง (Shadow IT)
ตรวจสอบความถูกต้องของผู้ส่งและลิงก์ก่อนเปิดอีเมลหรือเอกสารแนบ	เปิดลิงก์หรือไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือโดยไม่ตรวจสอบ
รายงานเหตุผิดปกติหรือเหตุสงสัยด้านความมั่นคงปลอดภัยต่อหน่วยงานที่รับผิดชอบโดยไม่ล่าช้า	ละเลยหรือไม่แจ้งเหตุผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์
ใช้อุปกรณ์และเครือข่ายที่องค์กรกำหนดมาตรการรักษาความมั่นคงปลอดภัยไว้แล้ว	ใช้งานระบบคลาวด์ผ่านอุปกรณ์ส่วนตัวหรือเครือข่ายสาธารณะที่ไม่มีมาตรการป้องกันที่เหมาะสม
ปฏิบัติตามนโยบายการจัดชั้นข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลขององค์กร	เปิดเผยหรือส่งต่อข้อมูลสำคัญโดยไม่ได้รับอนุญาต
ออกจากระบบ (Sign Out) และล็อกอุปกรณ์ทุกครั้งเมื่อเลิกใช้งาน	ปล่อยบัญชีผู้ใช้งานหรืออุปกรณ์ให้อยู่ในสถานะพร้อมใช้งานโดยไม่มีการป้องกัน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- **สำหรับผู้ดูแลระบบและนักพัฒนา (Admins & Developers)** เน้นเรื่องเทคนิคความมั่นคงปลอดภัย
    - การตั้งค่าความมั่นคงปลอดภัย (Secure Configuration)
    - การจัดการกุญแจเข้ารหัส (Key Management)
    - หลักการแบ่งความรับผิดชอบ (Shared Responsibility Model)

2. การเชื่อมโยงกระบวนการทรัพยากรบุคคลและไอที (HR & IT Process Integration) ควรใช้ระบบอัตโนมัติเพื่อลดความผิดพลาดในการจัดการสิทธิ์ (Joiner, Mover, Leaver Process)

- **เริ่มงาน (Joiner)** เมื่อฝ่ายทรัพยากรบุคคล (HR) สร้างข้อมูลพนักงานใหม่ ระบบบริหารจัดการสิทธิ์ (Identity Management System) ควรสร้างบัญชีผู้ใช้งานและกำหนดสิทธิ์ขั้นต่ำที่จำเป็น (Least Privilege) ให้อัตโนมัติ
- **ลาออก (Leaver)** เมื่อ HR ระบุสถานะ "ลาออก" ในระบบ ระบบต้องสั่งระงับบัญชี (Disable Account) ในทุกบริการคลาวด์ที่เชื่อมต่ออยู่ภายในระยะเวลาที่องค์กรกำหนด เพื่อลดช่องว่างเวลาที่อาจเกิดความเสียหาย

3. การตรวจสอบสัญญาผู้ให้บริการ (Vendor Contract Review) ในสัญญาหรือข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement: DPA) ควรระบุข้อความยืนยันว่า *"ผู้ให้บริการรับรองว่าบุคลากรทุกคนที่ทำหน้าที่ประมวลผลข้อมูล ได้ผ่านการลงนามในข้อตกลงรักษาความลับ (Commitment to Confidentiality) และได้รับการอบรมด้านความมั่นคงปลอดภัยแล้ว"*

ตัวอย่างสรุปการดำเนินการตามระดับผลกระทบ (Summary by Impact Level)

หัวข้อการดำเนินการ (Action Item)	ผลกระทบต่ำ (Low Impact)	ผลกระทบปานกลาง (Medium Impact)	ผลกระทบสูง (High Impact)
1. การอบรม (Awareness)	พื้นฐาน (ออนไลน์)	อบรมประจำปี + ทดสอบ	อบรมเข้มข้น + จำลองการโจมตี (Phishing Drill)
2. การคัดกรองประวัติ (Screening)	เอกสารสมัครงานปกติ	ตรวจสอบบุคคลอ้างอิง	ตรวจสอบประวัติอาชญากรรมเชิงลึก
3. การเพิกถอนสิทธิ์ (Revocation)	ภายใน 3 วันทำการ	ภายใน 24 ชั่วโมง	แบบอัตโนมัติและใกล้เคียงเวลาจริง (Automated / Near Real-Time)
4. สัญญาความลับ (NDA)	ระบุในสัญญาจ้าง	แยกฉบับเฉพาะ	ทบทวนสัญญาทุกปี

ข้อผิดพลาดที่พบบ่อย (Common Human Risks)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- ใช้รหัสผ่านร่วมกัน
- ไม่เปิดใช้ MFA
- ใช้ Cloud Storage ส่วนตัว
- พนักงานลาออกแต่ยังไม่ปิดบัญชี
- ผู้ดูแลระบบมีสิทธิ์มากเกินความจำเป็น
- ไม่อบรมผู้รับจ้างภายนอก
- ให้สิทธิแก่ผู้รับจ้างภายนอกสูงเกินไปและตลอดเวลา
- การเลือกผู้รับจ้างภายนอกโดยไม่ผ่านกระบวนการประเมินด้านความมั่นคงปลอดภัยอย่างเหมาะสม
- ไม่รายงานเหตุผิดปกติหรือเหตุสงสัยด้านความมั่นคงปลอดภัยไซเบอร์ภายในระยะเวลาที่เหมาะสม

5.2.2 การจัดการทรัพย์สิน (Asset Management)

5.2.2.1 ทะเบียนทรัพย์สิน (Inventory of Assets)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ทะเบียนทรัพย์สินของผู้ใช้บริการคลาวด์ต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของผู้ให้บริการคลาวด์	ก) ทะเบียนทรัพย์สินของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง - ข้อมูลของผู้ใช้บริการคลาวด์ - ข้อมูลที่เกิดจากการใช้บริการคลาวด์

วัตถุประสงค์ (Objective)

เพื่อให้หน่วยงานสามารถระบุ ติดตาม และบริหารจัดการทรัพย์สินสารสนเทศที่จัดเก็บหรือประมวลผลอยู่บนระบบคลาวด์ได้อย่างเหมาะสม ครอบคลุม และเป็นปัจจุบัน

ทั้งนี้ เนื่องจากทรัพย์สินบนระบบคลาวด์ (Virtual Assets) สามารถถูกสร้าง แก้ไข ย้าย หรือยกเลิกการใช้งานได้อย่างรวดเร็ว การจัดทำทะเบียนทรัพย์สินที่ถูกต้องจึงถือเป็นพื้นฐานสำคัญของการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงขององค์กร

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

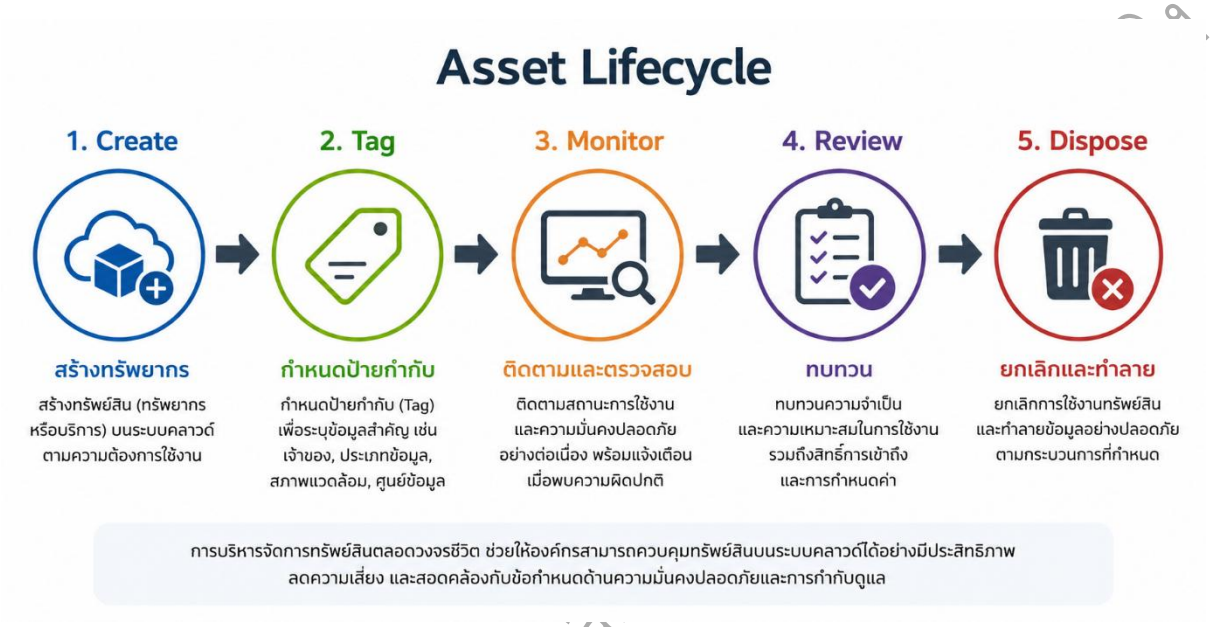
ก) ทะเบียนทรัพย์สินของผู้ใช้บริการคลาวด์ ต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของผู้ให้บริการคลาวด์

โดยควรดำเนินการดังต่อไปนี้

- **การบริหารจัดการทรัพย์สินบนระบบคลาวด์ตลอดวงจรชีวิต (Asset Lifecycle)**

ร่างประกาศ Public Hearing ฉบับที่ 2 - ห้ามใช้อ้างอิง

หน่วยงานควรบริหารจัดการทรัพย์สินบนระบบคลาวด์ตลอดวงจรชีวิต ตั้งแต่การสร้างทรัพยากร การกำหนดป้ายกำกับ การติดตามตรวจสอบ และการทบทวนความจำเป็นในการใช้งาน
ทั้งนี้ ควรมีแนวทางการยกเลิกการใช้งานและทำลายข้อมูลอย่างเหมาะสม เพื่อให้สามารถกำกับดูแลทรัพย์สินได้อย่างต่อเนื่องและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างแนวคิดวงจรชีวิตของทรัพย์สินบนระบบคลาวด์สามารถแสดงได้ดังรูปต่อไปนี้



รูปที่ 8 ตัวอย่างวงจรชีวิตการบริหารจัดการทรัพย์สินบนระบบคลาวด์ (Asset Lifecycle)

ร่างสำหรับ Public Hea

- **การจัดทำและปรับปรุงทะเบียนทรัพย์สิน (Inventory Maintenance)**

หน่วยงานควรจัดทำบัญชีรายชื่อทรัพย์สินสารสนเทศที่อยู่บนระบบคลาวด์ โดยระบุรายละเอียดสำคัญอย่างน้อยดังนี้

1. **เอกลักษณ์และประเภท (Identity & Type)** เช่น รหัสเครื่องเสมือน (Virtual Machine ID), ชื่อถังเก็บข้อมูล (Storage Bucket Name), หรืออินสแตนซ์ฐานข้อมูล (Database Instance)
2. **เจ้าของทรัพย์สิน (Asset Owner)** ระบุชื่อบุคคลหรือหน่วยงานที่รับผิดชอบดูแลทรัพย์สินนั้น
3. **ระดับชั้นความลับ (Information Classification)** ระบุว่าทรัพย์สินนั้นจัดเก็บข้อมูลระดับใด (เช่น ลับ, ใช้งานภายใน, สาธารณะ)

- **สถานที่จัดเก็บ (Physical Location)** ระบุภูมิภาค (Region) หรือศูนย์ข้อมูล (Data Center) ที่ทรัพย์สินนั้นตั้งอยู่

หน่วยงานควรพิจารณาระดับผลกระทบของข้อมูลหรือระบบสารสนเทศตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 ประกอบการกำหนดสถานที่จัดเก็บและประมวลผลข้อมูลบนระบบคลาวด์

สำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง หน่วยงานควรพิจารณาเลือกใช้บริการคลาวด์ที่มีศูนย์ข้อมูลหลัก (Primary Data Center) อยู่ภายในประเทศไทย และศูนย์ข้อมูลสำรอง (Disaster Recovery Site) อยู่ภายในประเทศไทยหรืออยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของผู้ใช้บริการคลาวด์ เช่น สาธารณรัฐสิงคโปร์ หรือเขตบริหารพิเศษฮ่องกงแห่งสาธารณรัฐประชาชนจีน เพื่อสนับสนุนการกำกับดูแลข้อมูล การปฏิบัติตามกฎหมาย การบริหารความต่อเนื่องทางธุรกิจ และการลดผลกระทบจากความหน่วงของเครือข่าย (Network Latency)
ทั้งนี้ ควรสอดคล้องกับข้อกำหนดเรื่องตำแหน่งของศูนย์ข้อมูล (Data Center Location) ตามข้อ 5.2.5.1 ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
เหตุผลและความจำเป็น (Rationale) การระบุและจัดทำทะเบียนทรัพย์สินอย่างครบถ้วนถือเป็นพื้นฐานสำคัญของการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ เนื่องจากหน่วยงานไม่สามารถกำหนดมาตรการคุ้มครองทรัพย์สินที่ไม่สามารถตรวจสอบหรือระบุได้อย่างชัดเจน การระบุสถานที่จัดเก็บมีความสำคัญอย่างยิ่งต่อการปฏิบัติตามกฎหมายเกี่ยวกับการโอนข้อมูลส่วนบุคคลข้ามพรมแดน

- **การระบุความเป็นเจ้าของ (Ownership Assignment)**

ทรัพย์สินบนคลาวด์ควรมีผู้รับผิดชอบที่ชัดเจน และเมื่อพนักงานผู้เป็นเจ้าของพ้นสภาพการปฏิบัติงาน หน่วยงานควรมีกระบวนการโอนย้ายความเป็นเจ้าของ (Re-assign Ownership) ไปยังผู้อื่นโดยไม่ล่าช้าจนส่งผลกระทบต่อการกำกับดูแลทรัพย์สิน เพื่อป้องกันการเกิดทรัพย์สินที่ไม่มีผู้รับผิดชอบกำกับดูแล (Orphaned Assets)

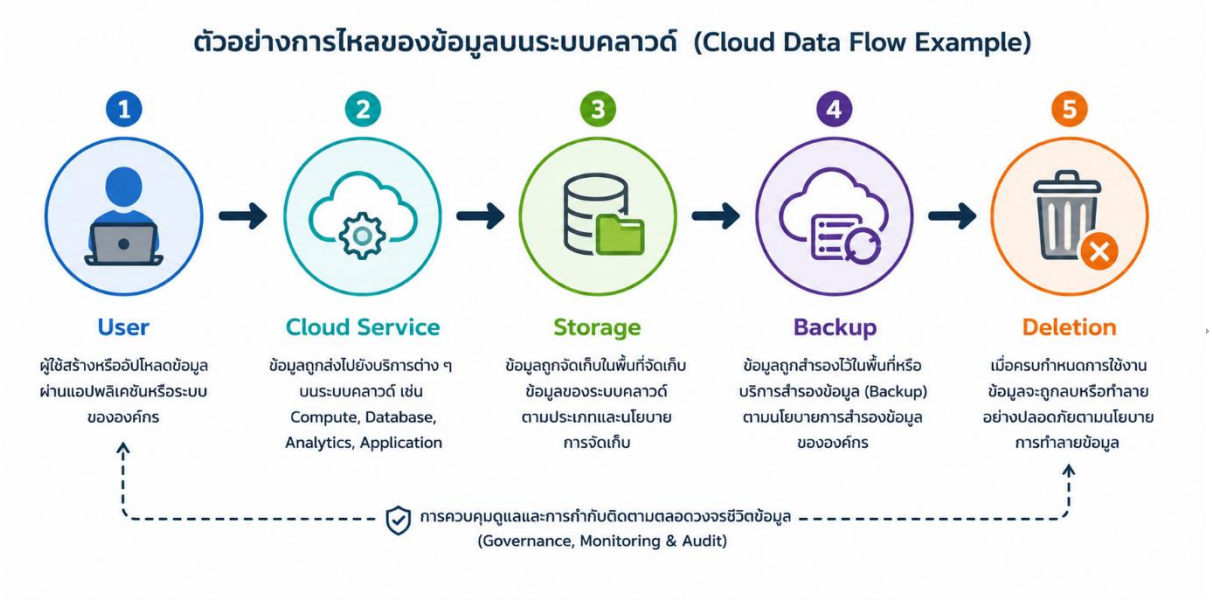
- **การส่งคืนและการทำลายทรัพย์สิน (Return and Disposal of Assets)**

เมื่อเลิกสัญญาหรือเลิกใช้บริการคลาวด์ หน่วยงานควรมีขั้นตอนที่ชัดเจนในการนำข้อมูลกลับคืน (Data Retrieval) และดำเนินการทำลายข้อมูล (Data Sanitization) จากฝั่งผู้ให้บริการ เพื่อไม่ให้ข้อมูลตกค้าง

- **เข้าใจเส้นทางการไหลของข้อมูล (Data Flow)**

หน่วยงานควรเข้าใจเส้นทางการไหลของข้อมูล (Data Flow) บนระบบคลาวด์ เพื่อใช้ประกอบการกำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัย การสำรองข้อมูล และการกำหนดสิทธิ์การเข้าถึง
รวมถึงการลบหรือทำลายข้อมูลเมื่อสิ้นสุดระยะเวลาการใช้งานตามนโยบายขององค์กร
ตัวอย่างการไหลของข้อมูลบนระบบคลาวด์สามารถแสดงได้ดังรูปต่อไปนี้

ร่างเอกสารเพื่อรับฟังความคิดเห็น (Public Hearing) ไม่ใช่ฉบับจริง



รูปที่ 9 ตัวอย่างการไหลของข้อมูลบนระบบคลาวด์ (Cloud Data Flow Example)

ตัวอย่างแนวทางการดำเนินการด้านทะเบียนทรัพย์สินบนระบบคลาวด์

ประเด็น	แนวทางการดำเนินการ
Asset Inventory	มีทะเบียนทรัพย์สินบนคลาวด์
Asset Owner	ระบุผู้รับผิดชอบ
Classification	ระบุระดับชั้นข้อมูล
Location	ระบุ Region/Data Center
Disposal	มีขั้นตอนลบข้อมูล

ตัวอย่างแนวทางการจัดทำทะเบียนทรัพย์สินบนระบบคลาวด์ (Asset Inventory Example)

ประเภท	ตัวอย่าง
Virtual Machine	Web-Server-Prod-01
Storage Bucket	citizen-data-prod
Database	HR-Personnel-DB

ร่างเอกสารสำหรับ Public Hearing เท่านั้น

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ก) ทะเบียนทรัพย์สิน (Inventory) ของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง
- ข้อมูลของผู้ใช้บริการคลาวด์
- ข้อมูลที่เกิดจากการใช้บริการคลาวด์
โดยควรดำเนินการดังต่อไปนี้

- **ความโปร่งใสของข้อมูลทรัพย์สิน (Asset Visibility)**

ผู้ให้บริการคลาวด์ควรจัดเตรียมเครื่องมือ ระบบแสดงผลภาพรวมทรัพย์สิน (Dashboard) หรือรายงาน ที่ช่วยให้ผู้ใช้บริการสามารถตรวจสอบรายการทรัพย์สินทั้งหมด รวมถึงระบุตำแหน่งที่ตั้งทางกายภาพ (Physical Location) ของทรัพย์สินเหล่านั้นได้อย่างชัดเจน

- **นโยบายการทำลายข้อมูล (Secure Disposal Policy)**

ผู้ให้บริการควรมีกระบวนการทำลายสื่อบันทึกข้อมูลหรือทรัพยากรที่เลิกใช้งานแล้วอย่างปลอดภัยและถาวร เพื่อให้มั่นใจว่าข้อมูลจะไม่สามารถถูกกู้คืนกลับมาได้

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

(เฉพาะเรื่องการจัดการทะเบียนและการตรวจสอบทรัพย์สิน)

1. การใช้เครื่องมือค้นหาอัตโนมัติ (Automated Discovery)

เนื่องจากทรัพยากรบนคลาวด์มีการเปลี่ยนแปลงตลอดเวลา การจดบันทึกด้วยมือ (Manual) ลงในตารางคำนวณ (Excel) อาจไม่สอดคล้องกับการเปลี่ยนแปลงของสภาพแวดล้อมคลาวด์และเกิดข้อผิดพลาดได้ง่าย
แนวทางการดำเนินการ ใช้ฟีเจอร์การค้นหาทรัพยากร (Resource Inventory/Explorer) ของผู้ให้บริการหรือเครื่องมือบริหารจัดการสถานะความมั่นคงปลอดภัยคลาวด์ (Cloud Security Posture Management: CSPM) เพื่อค้นหาและรวบรวมข้อมูลทรัพย์สินและอัปเดตทะเบียนโดยอัตโนมัติ

2. การจัดการ "ไอทีเงา" (Shadow IT Discovery)

แนวปฏิบัติที่เหมาะสม	แนวปฏิบัติที่ไม่เหมาะสม
ใช้งานบริการคลาวด์ผ่านกระบวนการอนุมัติและจัดซื้อขององค์กร	เปิดใช้บริการคลาวด์โดยไม่ผ่านกระบวนการกำกับดูแลขององค์กร
ลงทะเบียนทรัพย์สินคลาวด์เข้าสู่ระบบ Inventory กลางขององค์กร	ใช้งานบริการคลาวด์โดยไม่มีการบันทึกในทะเบียนทรัพย์สิน
ใช้บริการคลาวด์ที่ผ่านการประเมินความมั่นคงปลอดภัยแล้ว	ใช้บริการคลาวด์ที่องค์กรไม่ได้อนุมัติ (Shadow IT)

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตรวจสอบและทบทวนรายการบริการคลาวด์ที่ใช้งานอย่างสม่ำเสมอ	ไม่ติดตามหรือไม่ทราบว่ามีการใช้งานบริการคลาวด์ใดภายในองค์กร

แนวทางการดำเนินการ ผู้ดูแลระบบควรตรวจสอบบันทึกข้อมูลจราจร (Log) จากอุปกรณ์รักษาความมั่นคงปลอดภัยเครือข่าย (Firewall) หรือเว็บพร็อกซี (Web Proxy) ขององค์กร เพื่อดูว่ามีการเชื่อมต่อออกไปยังบริการคลาวด์ที่ไม่ได้รับอนุญาตหรือไม่ และนำเข้าระบบบริหารจัดการให้ถูกต้อง

3. การตรวจสอบเมื่อเลิกสัญญา (Decommissioning Verification)

เมื่อมีการสั่งลบเครื่องเสมือน (Virtual Machine) หรือพื้นที่จัดเก็บข้อมูล (Storage Volume) หน่วยงานควรทำการบันทึกหลักฐาน เช่น บันทึกเหตุการณ์จากระบบ (System Log) รายงานการลบข้อมูล (Deletion Report) หรือหลักฐานการดำเนินการอื่นที่สามารถตรวจสอบย้อนหลังได้ว่าทรัพย์สินถูกทำลายแล้วจริงตามระเบียบปฏิบัติ

4. เกณฑ์การคัดเลือกผู้ให้บริการ (Selection Criteria)

ในการจัดซื้อจัดจ้าง ควรเลือกผู้ให้บริการที่มี **"หน้าจอสรุปภาพรวมทรัพย์สินแบบรวมศูนย์" (Unified Asset Dashboard)** ที่สามารถแสดงผลทรัพยากรทั้งหมดในมุมมองเดียว และสามารถกรองหรือระบุตำแหน่งที่ตั้งของทรัพยากรตามภูมิภาค (Region) หรือประเทศที่เกี่ยวข้องได้ เพื่อลดภาระของผู้ดูแลระบบในการทำทะเบียนทรัพย์สินส่งหน่วยงานกำกับดูแล

หน่วยงานควรตรวจสอบให้ชัดเจนว่าผู้ให้บริการคลาวด์มีการจัดเก็บ สำรอง หรือประมวลผลข้อมูลข้ามภูมิภาคหรือข้ามประเทศหรือไม่ รวมถึงควรพิจารณาผลกระทบด้านกฎหมาย เขตอำนาจศาล และข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

5.2.2.2 การบ่งชี้ข้อมูล (Labelling of Information)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องบ่งชี้ข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร	ก) ผู้ให้บริการคลาวด์ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการใด ๆ ที่ผู้ใช้บริการคลาวด์ สามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้

วัตถุประสงค์ (Objective)

เพื่อให้สามารถจำแนกและระบุคุณลักษณะของข้อมูลหรือทรัพยากรบนคลาวด์ได้ผ่านการ "ติดป้ายกำกับ" (Tagging/Labelling) ซึ่งจะช่วยให้ระบบรักษาความมั่นคงปลอดภัยสามารถนำข้อมูลป้ายกำกับเหล่านี้ไปใช้ในการบังคับใช้นโยบาย (Policy Enforcement) การตรวจสอบ และการบริหารจัดการต้นทุนได้อย่างมีประสิทธิภาพ

ร่างเพื่อรับฟังความคิดเห็น (Public Hearing) - ห้ามอ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ก) ผู้ใช้บริการคลาวด์ต้องบ่งชี้ข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร

โดยควรดำเนินการดังต่อไปนี้

- **การติดป้ายระบุข้อมูลเมตา (Metadata Tagging)**

หน่วยงานควรกำหนดมาตรฐานและดำเนินการติดป้ายกำกับ (Tags) บนทรัพยากรคลาวด์ เพื่อบ่งชี้ระดับชั้นความลับและบริบทการใช้งานของข้อมูล ให้สอดคล้องกับนโยบายการจัดชั้นข้อมูล (Data Classification Policy) ขององค์กร

เหตุผลและความจำเป็น (Rationale) ในระบบคลาวด์ที่มีทรัพยากรจำนวนมหาศาล การตรวจสอบด้วยคนเป็นเรื่องยาก การติดป้ายกำกับช่วยให้สามารถใช้ระบบอัตโนมัติในการตรวจสอบได้ เช่น กำหนดให้ทรัพยากรที่มีป้ายกำกับระดับ Confidential ไม่ให้ถูกเปิดเผยสู่สาธารณะ

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ก) ผู้ให้บริการคลาวด์ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการใด ๆ ที่ผู้ใช้บริการคลาวด์ สามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้

โดยควรดำเนินการดังต่อไปนี้

- **ความสามารถในการติดป้ายกำกับ (Tagging Capability)**

ผู้ให้บริการคลาวด์ควรจัดเตรียมฟังก์ชันการทำงานที่ช่วยให้ผู้ใช้บริการสามารถสร้าง แก้ไข และลบป้ายกำกับ (Tags) บนทรัพยากรต่าง ๆ ได้ และข้อมูลป้ายกำกับเหล่านี้ต้องสามารถนำไปใช้ในการค้นหา (Search) หรือกรองข้อมูล (Filter) ในรายงานได้

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

(เฉพาะเรื่องเทคนิคการติดป้ายกำกับ)

1. กลยุทธ์มาตรฐานการติดป้ายกำกับ (Tagging Strategy)

หน่วยงานควรกำหนด "โครงสร้างป้ายกำกับ" (Tagging Schema) ให้เป็นมาตรฐานเดียวกันทั้งองค์กร เพื่อให้ง่ายต่อการตรวจสอบและบริหารจัดการ โดยควรพิจารณาป้ายกำกับพื้นฐานดังนี้

ชื่อป้ายกำกับ (Tag Key)	คำอธิบาย (Description)	ตัวอย่างค่า (Value Examples)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

Data-Classification	ระดับความลับของข้อมูลในทรัพยากรนั้น	Public, Internal, Confidential, Restricted
Environment	สภาพแวดล้อมการใช้งาน	Production, UAT, Development, Disaster-Recovery
Owner	ผู้รับผิดชอบ (ใช้ติดต่อเมื่อเกิดเหตุผิดปกติหรือปัญหาด้านความมั่นคงปลอดภัย)	user@example.com, Team-A
Cost-Center	รหัสหน่วยงานสำหรับบริหารงบประมาณ	IT-001, MKT-2024
Project-ID	รหัสโครงการหรือชื่อระบบงาน	PRJ-XYZ, Mobile-App

แนวปฏิบัติที่เหมาะสม	**แนวปฏิบัติที่ไม่เหมาะสม**
กำหนดมาตรฐานการตั้งชื่อและการติดป้ายกำกับร่วมกันทั้งองค์กร	ใช้รูปแบบการตั้งชื่อหรือ Tag ที่แตกต่างกันในแต่ละหน่วยงาน
กำหนด Tag สำหรับ Asset Owner และระดับชั้นข้อมูล	ไม่ระบุผู้รับผิดชอบหรือระดับชั้นข้อมูลของทรัพย์สิน
ใช้ระบบอัตโนมัติช่วยตรวจสอบความครบถ้วนของ Tag	อาศัยการตรวจสอบด้วยตนเองเพียงอย่างเดียว
ทบทวนและปรับปรุง Tag ตามการเปลี่ยนแปลงของระบบงาน	ปล่อยให้ข้อมูล Tag ไม่เป็นปัจจุบัน
กำหนดสิทธิ์ควบคุมการแก้ไข Tag ที่สำคัญ	อนุญาตให้ผู้ใช้งานทุกคนแก้ไข Tag สำคัญได้โดยไม่มีการควบคุม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้อ้างอิง

2. การบังคับใช้นโยบายการติดป้าย (Enforcement Policy)

- **แนวทางการดำเนินการ** ใช้เครื่องมือนโยบายของผู้ให้บริการคลาวด์ (Cloud Policy Management) เพื่อบังคับว่า "หากจะสร้างทรัพยากรใหม่ ต้องใส่ Tag ที่กำหนดให้ครบถ้วน มิเช่นนั้นจะสร้างไม่สำเร็จ" (Deny creation if tags are missing) เพื่อเพิ่มความครบถ้วนและความสอดคล้องของการกำหนดป้ายกำกับทรัพย์สินภายในองค์กร

ตัวอย่างระดับชั้นข้อมูลและประเภทข้อมูลที่เกี่ยวข้อง

Classification	**ตัวอย่างข้อมูล**

Public	ข้อมูลประชาสัมพันธ์
Internal	เอกสารภายใน
Confidential	ข้อมูลบุคลากร
Restricted	ข้อมูลสำคัญของรัฐ

ตัวอย่างโครงสร้างป้ายกำกับ (Tagging Schema)

Tag Key	Example Value
Environment	Production
Data-Classification	Confidential
Owner	security-team

ข้อผิดพลาดที่พบบ่อย (Common Misconfigurations)

องค์กรควรตระหนักถึงข้อผิดพลาดที่มักพบในการบริหารจัดการทรัพย์สินบนระบบคลาวด์ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลข้อมูล ดังต่อไปนี้

- เปิด Public Access ให้ Storage Bucket โดยไม่ได้ตั้งใจ
- ไม่มีการกำหนด Asset Owner
- ใช้งานหลาย Cloud Account โดยไม่มี Inventory กลาง
- ลบ VM แล้วแต่ Snapshot ยังอยู่
- ใช้ Tag ไม่เป็นมาตรฐานเดียวกัน

หมายเหตุ

แม้ผู้ให้บริการคลาวด์จะจัดเตรียมมาตรการรักษาความมั่นคงปลอดภัยพื้นฐานไว้แล้ว ผู้ใช้บริการคลาวด์ยังคงมีหน้าที่รับผิดชอบในการกำหนดค่าความมั่นคงปลอดภัย การบริหารสิทธิ์การเข้าถึง และการกำกับดูแลข้อมูลของตนเอง ตามหลักการแบ่งความรับผิดชอบ (Shared Responsibility Model)

5.2.3 การควบคุมการเข้าถึง (Access Control)

การควบคุมการเข้าถึงเป็นกระบวนการสำคัญในการจำกัดและกำกับการเข้าถึงข้อมูล ระบบสารสนเทศ และบริการคลาวด์ ให้เฉพาะบุคคล ระบบ หรือองค์ประกอบที่ได้รับอนุญาตสามารถเข้าถึงและใช้งานได้ตามขอบเขตที่กำหนด เพื่อป้องกันการเข้าถึง การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

สำหรับบริการคลาวด์ การควบคุมการเข้าถึงเกี่ยวข้องกับทั้งผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยขอบเขตความรับผิดชอบของแต่ละฝ่ายอาจ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

แตกต่างกันตามประเภทบริการคลาวด์ ขอบเขตบริการ สถาปัตยกรรมที่ใช้ และความสามารถในการควบคุมของแต่ละฝ่าย ดังนั้น การกำหนดและบริหารจัดการการเข้าถึงจึงควรพิจารณาตามหลักความรับผิดชอบร่วม (Shared Responsibility) และระดับความเสี่ยงของข้อมูลหรือระบบสารสนเทศ

การควบคุมการเข้าถึงควรครอบคลุมตั้งแต่การกำหนดสิทธิในการเข้าถึงเครือข่ายและบริการ การลงทะเบียนและยกเลิกผู้ใช้งาน การจัดสรรและทบทวนสิทธิ การควบคุมบัญชีหรือสิทธิพิเศษ การจัดการข้อมูลที่ใช้ในการพิสูจน์และยืนยันตัวตน การจำกัดการเข้าถึงข้อมูล การควบคุมการใช้โปรแกรมอรรถประโยชน์พิเศษ ตลอดจนการกำหนดขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย ซึ่งสอดคล้องกับหัวข้อย่อยตามข้อ 5.2.3.1 ถึง 5.2.3.8 ของประกาศ

แนวทางการควบคุมควรกำหนดให้เหมาะสมกับหน้าที่ ความจำเป็นในการใช้งาน ระดับผลกระทบของข้อมูลหรือระบบ และความเสี่ยงที่เกี่ยวข้อง โดยมุ่งให้ผู้ใช้งานได้รับสิทธิเท่าที่จำเป็นต่อการปฏิบัติงาน และให้สามารถทบทวน เปลี่ยนแปลง ระงับ หรือเพิกถอนสิทธิได้เมื่อสิ้นสุดความจำเป็นหรือเมื่อพบความเสี่ยงที่เกี่ยวข้อง

ทั้งนี้ การดำเนินการตามข้อกำหนดด้านการควบคุมการเข้าถึงไม่จำเป็นต้องจัดทำเป็นระบบหรือกระบวนการแยกต่างหากสำหรับบริการคลาวด์ หากหน่วยงานมีกระบวนการบริหารจัดการตัวตนและสิทธิการเข้าถึงที่สามารถรองรับบริบทของบริการคลาวด์ได้อย่างเพียงพอ โดยควรเพิ่มเติมเฉพาะประเด็นที่เกี่ยวข้องกับขอบเขตการควบคุม ความสามารถของผู้ให้บริการคลาวด์ และการแบ่งความรับผิดชอบระหว่าง CSC และ CSP

หลักการสำคัญในการควบคุมการเข้าถึง

การนำข้อกำหนดด้านการควบคุมการเข้าถึงไปปฏิบัติควรพิจารณาหลักการสำคัญดังต่อไปนี้

1. **การกำหนดสิทธิตามความจำเป็นในการใช้งาน** การเข้าถึงข้อมูล ระบบ และบริการควรกำหนดตามหน้าที่และความจำเป็นในการปฏิบัติงาน โดยหลีกเลี่ยงการให้สิทธิที่กว้างเกินความจำเป็น
2. **การบริหารจัดการสิทธิตลอดวงจรชีวิต** สิทธิการเข้าถึงควรได้รับการจัดการตั้งแต่การเริ่มใช้งาน การเปลี่ยนแปลงบทบาทหรือหน้าที่ การทบทวนสิทธิ ไปจนถึงการระงับหรือยกเลิกสิทธิเมื่อหมดความจำเป็น
3. **การควบคุมสิทธิพิเศษตามระดับความเสี่ยง** บัญชีหรือสิทธิที่สามารถบริหารจัดการระบบหรือเข้าถึงทรัพยากรสำคัญควรได้รับการควบคุมที่เหมาะสมและใช้กลไกการยืนยันตัวตนที่สอดคล้องกับระดับความเสี่ยง
4. **การคุ้มครองข้อมูลที่ใช้ในการพิสูจน์ตัวตน** ข้อมูลที่ใช้ในการพิสูจน์และยืนยันตัวตนควรได้รับการจัดการอย่างเหมาะสมตลอดช่วงการใช้งาน และมีมาตรการรองรับเมื่อข้อมูลดังกล่าวถูกเปิดเผย สูญหาย หรือถูกคุกคาม
5. **การจำกัดการเข้าถึงข้อมูลและบริการ** การเข้าถึงข้อมูลและบริการคลาวด์ควรสอดคล้องกับนโยบายการควบคุมการเข้าถึง และสามารถจำกัดขอบเขตการใช้งานตามความเหมาะสม

ร่างเพื่อการรับฟังความคิดเห็น Public Hearing เท่านั้น ยังไม่ใช่ฉบับที่ใช้งาน

6. **การติดตามและทบทวนความเหมาะสมของสิทธิ**
   ควรมีการทบทวนสิทธิและเงื่อนไขการเข้าถึงตามความเหมาะสม เพื่อให้มั่นใจว่าสิทธิยังคงสอดคล้องกับหน้าที่และความจำเป็นในการใช้งาน

หลักการดังกล่าวเป็นแนวทางสำหรับการประยุกต์ใช้ข้อกำหนด และไม่ควรตีความเป็นการกำหนดเทคโนโลยีรูปแบบสถาปัตยกรรม หรือวิธีการเฉพาะที่ต้องใช้ในทุกกรณี โดยหน่วยงานควรเลือกมาตรการให้เหมาะสมกับบริบทความเสี่ยง และความสามารถของบริการคลาวด์

หมายเหตุ เพื่อไม่ให้เกิดความซ้ำซ้อนกับข้อกำหนดส่วนอื่น หัวข้อการควบคุมการเข้าถึงควรมุ่งเน้นเฉพาะการกำหนด บริหาร และควบคุมสิทธิในการเข้าถึงข้อมูลและบริการเป็นหลัก โดยประเด็นที่เกี่ยวข้องกับการบันทึกเหตุการณ์ การปกป้องบันทึก การแบ่งแยกเครือข่าย การเข้ารหัส การจัดการช่องโหว่ และการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ให้พิจารณาตามข้อกำหนดที่เกี่ยวข้องในหมวดอื่นของประกาศ

ห้ามใช้งาน



รูปที่ 10 ภาพรวมกระบวนการควบคุมการเข้าถึง

5.2.3.1 การควบคุมเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่ายมีวัตถุประสงค์เพื่อให้ผู้ใช้งานสามารถเข้าถึงบริการคลาวด์ได้เฉพาะบริการและช่องทางที่ได้รับอนุญาต โดยสอดคล้องกับหน้าที่ ความจำเป็นในการใช้งาน และนโยบายการควบคุมการเข้าถึงของหน่วยงาน

ในบริบทของบริการคลาวด์ การเข้าถึงอาจเกิดขึ้นผ่านช่องทางที่แตกต่างกัน เช่น ส่วนติดต่อสำหรับผู้ใช้งาน ระบบบริหารจัดการบริการคลาวด์ หรือช่องทางเชื่อมต่อระหว่างระบบ ดังนั้น ผู้ใช้บริการคลาวด์ควรกำหนดข้อกำหนดการเข้าถึงให้เหมาะสมกับบริการที่ใช้งาน โดยไม่จำเป็นต้องกำหนดรูปแบบหรือเทคโนโลยีการเชื่อมต่อเป็นการเฉพาะ หากสามารถบรรลุวัตถุประสงค์ด้านการควบคุมการเข้าถึงได้

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) นโยบายการควบคุมการเข้าถึงของผู้ใช้บริการคลาวด์สำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริการที่ใช้งาน	

วัตถุประสงค์ (Objective)

เพื่อให้ผู้ใช้บริการคลาวด์กำหนดและควบคุมการเข้าถึงบริการคลาวด์แต่ละบริการอย่างเหมาะสม โดยผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการและช่องทางที่ได้รับอนุญาตตามหน้าที่และความจำเป็นในการใช้งาน และลดความเสี่ยงจากการเข้าถึงบริการคลาวด์โดยไม่ได้รับอนุญาตหรือเกินกว่าขอบเขตที่กำหนด

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1.1 การกำหนดข้อกำหนดการเข้าถึงตามบริการ

CSC ต้องกำหนดข้อกำหนดสำหรับการเข้าถึงบริการคลาวด์ที่หน่วยงานใช้งาน โดยข้อกำหนดดังกล่าวควรเป็นส่วนหนึ่งของนโยบายการควบคุมการเข้าถึง หรือเอกสารที่เกี่ยวข้องของหน่วยงาน

การกำหนดข้อกำหนดควรพิจารณาตามลักษณะของบริการและความเสี่ยงที่เกี่ยวข้อง โดยอย่างน้อยควรสามารถระบุได้ว่า

- ผู้ใช้งานหรือกลุ่มผู้ใช้งานใดได้รับอนุญาตให้เข้าถึงบริการ
- บริการหรือส่วนของบริการใดที่ได้รับอนุญาตให้เข้าถึง
- การเข้าถึงมีวัตถุประสงค์หรือความจำเป็นในการใช้งานอย่างไร
- มีเงื่อนไขหรือข้อจำกัดในการเข้าถึงหรือไม่

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หน่วยงานไม่จำเป็นต้องจัดทำเอกสารแยกสำหรับบริการคลาวด์ทุกบริการ หากนโยบายหรือกระบวนการควบคุมการเข้าถึงที่มีอยู่สามารถระบุข้อกำหนดดังกล่าวได้อย่างเพียงพอ

ตัวอย่าง กรณีหน่วยงานใช้บริการคลาวด์สำหรับระบบงานทั่วไปและระบบที่มีข้อมูลสำคัญ หน่วยงานอาจกำหนดให้ผู้ใช้งานทั่วไปเข้าถึงเฉพาะระบบงานที่เกี่ยวข้องกับหน้าที่ ขณะที่การเข้าถึงส่วนบริหารจัดการบริการคลาวด์จำกัดเฉพาะผู้ดูแลระบบที่ได้รับมอบหมาย

ตัวอย่างดังกล่าวเป็นเพียงแนวทางในการประยุกต์ใช้ มิได้หมายความว่าหน่วยงานต้องแบ่งกลุ่มผู้ใช้งานหรือบริการในรูปแบบเดียวกันทุกกรณี

1.2 การกำหนดผู้ที่ได้รับอนุญาตให้เข้าถึง

CSC ควรกำหนดการเข้าถึงบริการตามบทบาท หน้าที่ หรือความจำเป็นในการปฏิบัติงาน โดยให้สิทธิเฉพาะเท่าที่จำเป็นต่อการใช้งานบริการนั้น

การกำหนดสิทธิอาจดำเนินการเป็นรายบุคคล รายกลุ่ม หรือตามบทบาท ขึ้นอยู่กับลักษณะและความสามารถของบริการคลาวด์ ทั้งนี้ ควรสามารถเชื่อมโยงการได้รับสิทธิกับการอนุมัติหรือการมอบหมายหน้าที่ของหน่วยงานได้อย่างเหมาะสม

รายละเอียดเกี่ยวกับการจัดสรร การเปลี่ยนแปลง และการถอนสิทธิของผู้ใช้งาน ให้พิจารณาตามข้อ 5.2.3.3 การจัดสรรการเข้าถึงของผู้ใช้

1.3 การกำหนดบริการที่อนุญาตให้เข้าถึง

CSC ควรทราบว่าบริการคลาวด์ที่หน่วยงานใช้งานประกอบด้วยบริการหรือส่วนการทำงานใดบ้างที่ผู้ใช้งานสามารถเข้าถึง และกำหนดขอบเขตการเข้าถึงให้เหมาะสม

ในกรณีที่บริการเดียวประกอบด้วยส่วนการใช้งานที่มีระดับความสำคัญแตกต่างกัน เช่น ส่วนสำหรับผู้ใช้งานทั่วไปและส่วนสำหรับการบริหารจัดการระบบ หน่วยงานควรพิจารณาแยกข้อกำหนดการเข้าถึงตามความเหมาะสม

ทั้งนี้ ไม่จำเป็นต้องจัดทำรายการทางเทคนิคของพอร์ต โพรโทคอล หรือองค์ประกอบเครือข่ายทั้งหมด เว้นแต่ข้อมูลดังกล่าวจำเป็นต่อการกำหนดหรือควบคุมการเข้าถึงของหน่วยงาน

1.4 การกำหนดช่องทางและเงื่อนไขการเข้าถึง

CSC ควรพิจารณาว่าการเข้าถึงบริการคลาวด์สามารถดำเนินการผ่านช่องทางใด และมีเงื่อนไขใดที่จำเป็นต่อการควบคุมความเสี่ยง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างเงื่อนไขที่อาจนำมาพิจารณา ได้แก่

- การเข้าถึงผ่านช่องทางที่หน่วยงานหรือ CSP จัดให้
- การเข้าถึงส่วนบริหารจัดการเฉพาะผู้ที่ได้รับอนุญาต
- การกำหนดกลไกการยืนยันตัวตนที่เหมาะสมกับความเสี่ยง
- การจำกัดการเข้าถึงจากสภาพแวดล้อมหรืออุปกรณ์บางประเภท เมื่อมีความจำเป็น

มาตรการดังกล่าวควรกำหนดตามความเสี่ยงและความสามารถของบริการ โดยไม่จำเป็นต้องใช้เทคโนโลยีหรือรูปแบบเดียวกันสำหรับบริการคลาวด์ทุกประเภท

1.5 การทบทวนข้อกำหนดการเข้าถึง

CSC ควรทบทวนข้อกำหนดการเข้าถึงเมื่อมีการเปลี่ยนแปลงที่อาจมีผลต่อความเหมาะสมของการควบคุม เช่น

- มีการนำบริการคลาวด์ใหม่มาใช้งาน
- มีการเปลี่ยนแปลงหน้าที่หรือกลุ่มผู้ใช้งาน
- มีการเปลี่ยนแปลงลักษณะหรือความสำคัญของข้อมูล
- มีการเปลี่ยนแปลงบริการหรือความสามารถที่ CSP จัดให้
- พบความเสี่ยงหรือเหตุการณ์ที่แสดงว่ามาตรการเดิมอาจไม่เพียงพอ

ไม่จำเป็นต้องกำหนดวงรอบการทบทวนใหม่เฉพาะสำหรับข้อ 5.2.3.1 หากหน่วยงานมีกระบวนการทบทวนนโยบาย สิทธิ หรือความเสี่ยงที่สามารถครอบคลุมเรื่องดังกล่าวอยู่แล้ว

ส่วนที่ 2 ข้อพิจารณาเกี่ยวกับผู้ให้บริการคลาวด์ (CSP Considerations)

เนื่องจากประกาศไม่ได้กำหนดข้อกำหนดเฉพาะสำหรับ CSP ในข้อ 5.2.3.1 ส่วนนี้จึงมีวัตถุประสงค์เพื่อช่วยให้ CSC พิจารณาความสามารถของบริการคลาวด์ที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดเท่านั้น

CSC ควรพิจารณาว่าบริการของ CSP มีความสามารถเพียงพอสำหรับการกำหนดและบังคับใช้ข้อกำหนดการเข้าถึงที่หน่วยงานกำหนดหรือไม่ เช่น ความสามารถในการ

- กำหนดผู้ใช้งานหรือกลุ่มผู้ใช้งานที่สามารถเข้าถึงบริการ
- จำกัดการเข้าถึงส่วนบริหารจัดการหรือบริการที่มีความสำคัญ
- รองรับกลไกการพิสูจน์และยืนยันตัวตนตามที่หน่วยงานต้องการ
- กำหนดหรือปรับเปลี่ยนสิทธิและเงื่อนไขการเข้าถึงตามขอบเขตบริการ

หากความสามารถดังกล่าวเกี่ยวข้องกับข้อกำหนดอื่นโดยตรง ให้พิจารณาตามข้อกำหนดนั้น เช่น การจัดสรรสิทธิตามข้อ 5.2.3.3 การควบคุมสิทธิพิเศษตามข้อ 5.2.3.4 และการเข้าสู่ระบบอย่างปลอดภัยตามข้อ 5.2.3.8

ร่างเพื่อรับฟังความคิดเห็นสาธารณะ (Public Hearing) เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดนี้ไปปฏิบัติ ไม่จำเป็นต้องเริ่มจากการกำหนดเทคโนโลยีเครือข่าย แต่ควรเริ่มจากการพิจารณาว่า

ใคร ⟶ ต้องเข้าถึงอะไร ⟶ เพื่อวัตถุประสงค์ใด ⟶ ผ่านช่องทางหรือเงื่อนไขใด

จากนั้นจึงพิจารณาว่าความสามารถของบริการคลาวด์และมาตรการที่หน่วยงานมีอยู่สามารถรองรับข้อกำหนดดังกล่าวได้หรือไม่

ตัวอย่างตารางที่สามารถนำไปใช้ประกอบการกำหนดข้อกำหนดได้ มีดังนี้

บริการ/ทรัพยากร	กลุ่มผู้ใช้งาน	ขอบเขตการเข้าถึง	เงื่อนไขสำคัญ
ระบบงานสำหรับผู้ใช้งาน	ผู้ใช้งานที่ได้รับอนุญาต	เฉพาะส่วนที่เกี่ยวข้องกับหน้าที่	ตามนโยบายของหน่วยงาน
ระบบบริหารจัดการบริการคลาวด์	ผู้ดูแลระบบที่ได้รับมอบหมาย	เฉพาะขอบเขตที่รับผิดชอบ	ใช้การยืนยันตัวตนที่เหมาะสมกับความเสี่ยง
บริการเชื่อมต่อระหว่างระบบ	ระบบหรือบริการที่ได้รับอนุญาต	เฉพาะการเชื่อมต่อที่จำเป็น	ตามข้อกำหนดของระบบและบริการ

ตารางดังกล่าวเป็นเพียงตัวอย่างสำหรับการประยุกต์ใช้ หน่วยงานสามารถใช้เอกสารหรือระบบที่มีอยู่แล้วได้ หากสามารถแสดงสาระสำคัญเกี่ยวกับบริการ ผู้ใช้งาน ขอบเขตการเข้าถึง และเงื่อนไขที่เกี่ยวข้องได้อย่างเพียงพอ

การเชื่อมโยงกับข้อกำหนดอื่น

เพื่อหลีกเลี่ยงการกำหนดมาตรการซ้ำซ้อน การดำเนินการตามข้อ 5.2.3.1 ควรเชื่อมโยงกับข้อกำหนดอื่นที่เกี่ยวข้อง ดังนี้

ประเด็น	พิจารณาตามข้อกำหนด
การลงทะเบียนและยกเลิกผู้ใช้งาน	5.2.3.2
การจัดสรรสิทธิ	5.2.3.3
สิทธิของผู้ดูแลระบบ	5.2.3.4
ข้อมูลที่ใช้พิสูจน์ตัวตน	5.2.3.5
การจำกัดการเข้าถึงข้อมูล	5.2.3.6
การเข้าสู่ระบบอย่างปลอดภัย	5.2.3.8
การบันทึกเหตุการณ์	5.2.6.4–5.2.6.6
การแบ่งแยกเครือข่าย	5.2.7.2

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามนำไปอ้างอิง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานที่ใช้แสดงการดำเนินการตามข้อ 5.2.3.1 อาจแตกต่างกันตามลักษณะของหน่วยงานและบริการคลาวด์ โดยอาจพิจารณาหลักฐาน เช่น

หลักฐาน	ตัวอย่างสาระสำคัญ
นโยบายหรือแนวทางการควบคุมการเข้าถึง	กำหนดหลักเกณฑ์การเข้าถึงบริการคลาวด์
รายการบริการคลาวด์และผู้ได้รับอนุญาต	แสดงบริการ กลุ่มผู้ใช้งาน หรือขอบเขตการเข้าถึง
การกำหนดสิทธิในระบบ	แสดงการตั้งค่าหรือการกำหนดสิทธิที่สอดคล้องกับข้อกำหนด
หลักฐานการอนุมัติ	แสดงการอนุมัติการเข้าถึงตามกระบวนการของหน่วยงาน
หลักฐานการทบทวน	แสดงการทบทวนหรือปรับปรุงเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้อง

หมายเหตุ: รายการข้างต้นเป็นตัวอย่างหลักฐาน มิได้หมายความว่าต้องจัดทำเอกสารแยกต่างหากทุกประเภท หากหลักฐานที่หน่วยงานมีอยู่สามารถแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

5.2.3.2 การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ (User Registration and Deregistration)

การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้เป็นกระบวนการสำคัญในการควบคุมให้บัญชีผู้ใช้งานที่สามารถเข้าถึงบริการคลาวด์มีสถานะและสิทธิที่สอดคล้องกับการได้รับอนุญาตของหน่วยงาน รวมทั้งสามารถระงับหรือยกเลิกการเข้าถึงได้เมื่อหมดความจำเป็น หรือเมื่อข้อมูลที่ใช้ในการเข้าถึงถูกเปิดเผย สูญหาย หรือถูกคุกคาม

ในสภาพแวดล้อมคลาวด์ การดำเนินการดังกล่าวเกี่ยวข้องกับทั้ง CSC ซึ่งรับผิดชอบการกำกับดูแลผู้ใช้งานภายใต้การควบคุมของตน และ CSP ซึ่งต้องจัดเตรียมฟังก์ชันสำหรับการลงทะเบียนและยกเลิกการลงทะเบียนผู้ใช้งาน พร้อมข้อกำหนดสำหรับการใช้งานฟังก์ชันดังกล่าว ตามที่ประกาศกำหนดไว้โดยตรง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ต้องครอบคลุมถึงสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคาม เช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่น ๆ (ยกตัวอย่างเช่น จากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม	ก) เพื่อจัดการการเข้าถึงบริการคลาวด์โดยผู้ใช้งานของผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้แก่ ผู้ใช้บริการคลาวด์

วัตถุประสงค์

เพื่อให้บัญชีผู้ใช้งานที่สามารถเข้าถึงบริการคลาวด์ได้รับการสร้าง เปิดใช้งาน ระงับ หรือยกเลิกอย่างเหมาะสมตามสถานะและความจำเป็นในการใช้งาน รวมทั้งสามารถดำเนินการได้อย่างเหมาะสมเมื่อพบว่าบัญชี รหัสผ่าน หรือข้อมูลที่เกี่ยวข้องกับการเข้าถึงอาจถูกเปิดเผยหรือถูกคุกคาม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การกำหนดกระบวนการลงทะเบียนผู้ใช้งาน

CSC ต้องกำหนดขั้นตอนสำหรับการลงทะเบียนผู้ใช้งานที่ต้องการเข้าถึงบริการคลาวด์ เพื่อให้สามารถระบุได้ว่าผู้ใช้งานได้รับอนุญาตให้ใช้บริการตามกระบวนการของหน่วยงานแล้ว

กระบวนการดังกล่าวควรพิจารณาอย่างน้อยในเรื่อง

- การระบุผู้ใช้งานหรือบัญชีที่ต้องการลงทะเบียน
- การระบุบริการหรือระบบที่ต้องการเข้าถึง
- การตรวจสอบความจำเป็นในการใช้งาน
- การอนุมัติตามหน้าที่หรือกระบวนการของหน่วยงาน
- การดำเนินการลงทะเบียนผ่านฟังก์ชันที่ CSP จัดให้

การลงทะเบียนไม่จำเป็นต้องดำเนินการด้วยวิธีการเดียวกันสำหรับบริการคลาวด์ทั้งหมด โดยสามารถใช้กระบวนการหรือระบบบริหารจัดการบัญชีที่หน่วยงานมีอยู่แล้ว หากสามารถควบคุมการลงทะเบียนผู้ใช้งานบริการคลาวด์ได้อย่างเหมาะสม

2. การยกเลิกหรือระงับบัญชีผู้ใช้งาน

CSC ต้องสามารถดำเนินการยกเลิกการลงทะเบียนหรือระงับการเข้าถึงเมื่อผู้ใช้งานไม่มีความจำเป็นต้องใช้บริการอีกต่อไป หรือเมื่อมีเหตุที่ทำให้การเข้าถึงเดิมไม่เหมาะสม

ตัวอย่างกรณีที่ควรพิจารณา ได้แก่

- ผู้ใช้งานพ้นจากหน้าที่หรือสิ้นสุดความสัมพันธ์กับหน่วยงาน
- มีการเปลี่ยนแปลงหน้าที่จนไม่มีความจำเป็นต้องใช้บริการ
- บัญชีถูกสร้างขึ้นเพื่อวัตถุประสงค์ชั่วคราวและสิ้นสุดความจำเป็น
- พบการใช้งานบัญชีที่อาจไม่ได้รับอนุญาต
- พบว่าข้อมูลที่ใช้สำหรับการเข้าถึงอาจถูกเปิดเผยหรือถูกคุกคาม

การดำเนินการอาจเป็นการระงับบัญชีชั่วคราวหรือการยกเลิกบัญชี ขึ้นอยู่กับเหตุการณ์ ความเสี่ยง และกระบวนการของหน่วยงาน

3. การจัดการกรณีการควบคุมการเข้าถึงถูกคุกคาม

CSC ต้องกำหนดให้ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสามารถรองรับสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคาม เช่น รหัสผ่านหรือข้อมูลการลงทะเบียนของผู้ใช้งานถูกเปิดเผยโดยไม่ได้ตั้งใจ หรือมีเหตุให้เชื่อได้ว่าบุคคลอื่นอาจสามารถนำข้อมูลดังกล่าวไปใช้เข้าถึงบริการได้

เมื่อเกิดสถานการณ์ดังกล่าว หน่วยงานควรสามารถดำเนินการตามความเหมาะสม เช่น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- ระงับการใช้งานบัญชีเป็นการชั่วคราว
- ยกเลิกหรือเพิกถอนข้อมูลที่ใช้ในการเข้าถึงเดิม
- ดำเนินการลงทะเบียนหรือกำหนดข้อมูลสำหรับการเข้าถึงใหม่
- ตรวจสอบว่าบัญชีดังกล่าวยังมีความจำเป็นต้องใช้งานหรือไม่
- ดำเนินการตามกระบวนการจัดการเหตุการณ์ หากเหตุการณ์เข้าข่ายเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

รายละเอียดเกี่ยวกับการตอบสนองและจัดการเหตุการณ์ให้ดำเนินการตามข้อ 5.2.10

4. การเปลี่ยนแปลงสถานะของผู้ใช้งาน

ในกรณีที่สถานะ หน้าที่ หรือความรับผิดชอบของผู้ใช้งานเปลี่ยนแปลง CSC ควรพิจารณาว่าการลงทะเบียนหรือบัญชีที่มีอยู่ยังคงมีความจำเป็นและเหมาะสมหรือไม่

หากผู้ใช้งานยังจำเป็นต้องใช้บริการแต่ต้องเปลี่ยนขอบเขตสิทธิ ควรดำเนินการตามกระบวนการจัดสรรหรือเปลี่ยนแปลงสิทธิที่เกี่ยวข้อง โดยรายละเอียดของการจัดสรรสิทธิให้พิจารณาตามข้อ **5.2.3.3 การจัดสรรการเข้าถึงของผู้ใช้**

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดเตรียมฟังก์ชันการลงทะเบียนผู้ใช้งาน

CSP ต้องจัดเตรียมฟังก์ชันที่ทำให้ CSC สามารถลงทะเบียนผู้ใช้งานสำหรับการเข้าถึงบริการคลาวด์ได้ตามขอบเขตของบริการที่จัดให้

ฟังก์ชันดังกล่าวควรมีความเหมาะสมกับลักษณะของบริการ และสามารถรองรับการบริหารจัดการผู้ใช้งานของ CSC ได้

ประกาศไม่ได้กำหนดว่าฟังก์ชันดังกล่าวต้องใช้เทคโนโลยีหรือสถาปัตยกรรมรูปแบบใด ดังนั้น CSP อาจจัดให้ผ่านระบบบริหารจัดการ ส่วนติดต่อของบริการ หรือกลไกอื่นที่เหมาะสมกับบริการ

2. การจัดเตรียมฟังก์ชันการยกเลิกการลงทะเบียน

CSP ต้องจัดเตรียมความสามารถให้ CSC สามารถยกเลิกการลงทะเบียนผู้ใช้งานที่ไม่ควรหรือไม่จำเป็นต้องเข้าถึงบริการอีกต่อไป

การดำเนินการควรทำให้ CSC สามารถควบคุมสถานะการเข้าถึงของผู้ใช้งานภายใต้ความรับผิดชอบของตนได้อย่างเหมาะสม รวมถึงรองรับกรณีที่จำเป็นต้องระงับหรือยกเลิกการเข้าถึงเนื่องจากความเสี่ยงด้านความมั่นคงปลอดภัย

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

3. การให้ข้อมูลเกี่ยวกับการใช้ฟังก์ชัน

นอกจากการจัดเตรียมฟังก์ชันแล้ว CSP ต้องจัดให้มีข้อกำหนดหรือข้อมูลสำหรับการใช้งานฟังก์ชันการลงทะเบียนและยกเลิกการลงทะเบียนแก่ CSC ตามที่ประกาศกำหนด

ข้อมูลดังกล่าวควรเพียงพอให้ CSC สามารถเข้าใจและใช้ความสามารถของบริการเพื่อบริหารจัดการผู้ใช้งานได้อย่างเหมาะสม เช่น

- วิธีการลงทะเบียนผู้ใช้งาน
- วิธีการระงับหรือยกเลิกผู้ใช้งาน
- เงื่อนไขหรือข้อจำกัดของฟังก์ชัน
- ข้อมูลที่จำเป็นต่อการบริหารจัดการบัญชีตามขอบเขตบริการ

ทั้งนี้ ไม่จำเป็นต้องกำหนดรูปแบบเอกสารเฉพาะ หาก CSP มีเอกสารประกอบบริการ คู่มือ หรือข้อมูลอื่นที่สามารถแสดงสาระดังกล่าวได้เพียงพอ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การดำเนินการตามข้อ 5.2.3.2 ควรมุ่งให้ CSC สามารถควบคุม **สถานะของบัญชีผู้ใช้งาน** ได้ตลอดช่วงที่มีการใช้บริการคลาวด์ โดยอาจพิจารณาตามวงจรพื้นฐานดังนี้

ความจำเป็นในการใช้งาน

↓

ขอและอนุมัติการลงทะเบียน

↓

ลงทะเบียน / เปิดใช้งานบัญชี

↓

ใช้งานบริการ

↓

เปลี่ยนแปลงสถานะเมื่อจำเป็น

↓

ระงับหรือยกเลิกการลงทะเบียน

หากพบว่าบัญชีหรือข้อมูลที่ใช้ในการเข้าถึงถูกคุกคาม ควรสามารถดำเนินการระงับหรือยกเลิกการเข้าถึงได้โดยไม่จำเป็นต้องรอให้ถึงกระบวนการยกเลิกตามปกติ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างแนวทางการพิจารณา

เหตุการณ์	แนวทางที่ควรพิจารณา
ผู้ใช้งานใหม่	ตรวจสอบความจำเป็นและอนุมัติก่อนลงทะเบียน
เปลี่ยนหน้าที่	ตรวจสอบว่าบัญชีและการเข้าถึงเดิมยังจำเป็นหรือไม่
สิ้นสุดการปฏิบัติงาน	ยกเลิกหรือระงับการเข้าถึงตามกระบวนการ
บัญชีชั่วคราวหมดความจำเป็น	ยกเลิกหรือปิดการใช้งาน
รหัสผ่านหรือข้อมูลการเข้าถึงถูกเปิดเผย	ระงับหรือเพิกถอนข้อมูลเดิมและดำเนินการตามความเสี่ยง
สงสัยว่าบัญชีถูกใช้โดยไม่ได้รับอนุญาต	จำกัดหรือระงับการเข้าถึงและพิจารณาดำเนินการตามกระบวนการจัดการเหตุการณ์

ตารางนี้มีวัตถุประสงค์เพื่อช่วยในการประยุกต์ใช้ มิได้กำหนดว่าทุกหน่วยงานต้องจัดทำกระบวนการหรือแบบฟอร์มแยกสำหรับทุกเหตุการณ์

การเชื่อมโยงกับข้อกำหนดอื่น

การลงทะเบียนและยกเลิกผู้ใช้งานมีความสัมพันธ์กับข้อกำหนดอื่นที่เกี่ยวข้อง โดยรายละเอียดของการควบคุมในแต่ละประเด็นให้พิจารณาตามข้อกำหนดที่ระบุไว้ในตารางต่อไปนี้

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การกำหนดสิทธิหลังจากลงทะเบียน	5.2.3.3 การจัดสรรการเข้าถึงของผู้ใช้
บัญชีที่มีสิทธิพิเศษ	5.2.3.4 การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ
รหัสผ่านและข้อมูลพิสูจน์ตัวตน	5.2.3.5 การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ
การเข้าสู่ระบบ	5.2.3.8 ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย
การบันทึกกิจกรรมที่เกี่ยวข้อง	5.2.6.4–5.2.6.6
การจัดการเมื่อเกิดเหตุการณ์	5.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานสำหรับแสดงการดำเนินการตามข้อ 5.2.3.2 อาจประกอบด้วยเอกสาร บันทึก หรือข้อมูลจากระบบตามความเหมาะสม เช่น

หลักฐาน	ตัวอย่างสาระสำคัญ
ขั้นตอนการบริหารบัญชีผู้ใช้งาน	แสดงการลงทะเบียน ระงับ และยกเลิกผู้ใช้งาน
รายการหรือข้อมูลบัญชีผู้ใช้งาน	แสดงสถานะบัญชีที่อยู่ภายใต้การควบคุม
หลักฐานการอนุมัติ	แสดงว่าการลงทะเบียนเป็นไปตามกระบวนการของหน่วยงาน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักฐานการระงับหรือยกเลิก	แสดงการดำเนินการเมื่อหมดความจำเป็นหรือมีการเปลี่ยนแปลง
หลักฐานกรณีบัญชีถูกคุกคาม	แสดงการระงับ เพิกถอน หรือดำเนินการที่เหมาะสม
ข้อมูลจาก CSP	คู่มือหรือข้อมูลเกี่ยวกับฟังก์ชันการลงทะเบียนและยกเลิกผู้ใช้งาน

หมายเหตุ: หลักฐานข้างต้นเป็นตัวอย่าง มิใช่รายการเอกสารบังคับทั้งหมด และสามารถใช้หลักฐานจากกระบวนการหรือระบบที่หน่วยงานมีอยู่แล้วได้ หากสามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

5.2.3.3 การจัดสรรการเข้าถึงของผู้ใช้ (User Access Provisioning)

การจัดสรรการเข้าถึงของผู้ใช้เป็นกระบวนการสำหรับกำหนด เปลี่ยนแปลง และยกเลิกสิทธิในการเข้าถึงข้อมูล ระบบ หรือส่วนการทำงานของบริการคลาวด์ ภายหลังจากที่ผู้ใช้งานได้รับการลงทะเบียนและได้รับอนุญาตให้ใช้บริการแล้ว

ในบริบทของบริการคลาวด์ CSP มีบทบาทสำคัญในการจัดเตรียมความสามารถที่ทำให้ CSC สามารถบริหารจัดการสิทธิของผู้ใช้งานได้ตามความต้องการและขอบเขตของบริการ ขณะที่ CSC เป็นผู้ใช้ความสามารถดังกล่าวเพื่อกำหนดสิทธิให้สอดคล้องกับหน้าที่และความจำเป็นในการใช้งาน

ประเด็นนี้จึงแตกต่างจากข้อ 5.2.3.2 ซึ่งมุ่งเน้นว่า **ผู้ใดควรมีหรือไม่มีบัญชีสำหรับใช้บริการ** ส่วนข้อ 5.2.3.3 มุ่งเน้นว่า **เมื่อมีบัญชีแล้ว ผู้ใช้งานนั้นสามารถเข้าถึงหรือดำเนินการใดได้บ้าง**

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันสำหรับการจัดการสิทธิการเข้าถึงของผู้ใช้บริการคลาวด์ รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้

วัตถุประสงค์ (Objective)

เพื่อให้บริการคลาวด์มีความสามารถที่เหมาะสมสำหรับการกำหนด เปลี่ยนแปลง และยกเลิกสิทธิการเข้าถึงของผู้ใช้งาน และทำให้ CSC สามารถใช้ความสามารถดังกล่าวในการควบคุมการเข้าถึงข้อมูล ระบบ และส่วนการทำงานของบริการให้สอดคล้องกับความจำเป็นในการใช้งาน

ส่วนที่ 1 ข้อพิจารณาสำหรับผู้ใช้บริการคลาวด์ (CSC Considerations)

แม้ประกาศไม่ได้กำหนดข้อกำหนดโดยตรงสำหรับ CSC ในข้อ 5.2.3.3 แต่ CSC ควรใช้ความสามารถด้านการจัดการสิทธิที่ CSP จัดให้ เพื่อสนับสนุนการควบคุมการเข้าถึงตามนโยบายและข้อกำหนดของหน่วยงาน

ร่างเพื่อการรับฟังความคิดเห็น Public Hearing ยังไม่ประกาศใช้บังคับ

1. การกำหนดสิทธิให้เหมาะสมกับหน้าที่

CSC ควรใช้ความสามารถในการจัดการสิทธิที่ CSP จัดให้ เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงเฉพาะข้อมูล บริการ หรือส่วนการทำงานที่จำเป็นต่อหน้าที่และวัตถุประสงค์ในการใช้งาน

การกำหนดสิทธิควรพิจารณาหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) โดยไม่จำเป็นต้องกำหนดรูปแบบการบริหารสิทธิเป็นการเฉพาะ หากวิธีการที่เลือกใช้สามารถจำกัดสิทธิได้อย่างเหมาะสม

ตัวอย่างเช่น หน่วยงานอาจกำหนดสิทธิตามบทบาท กลุ่มผู้ใช้งาน หรือเป็นรายบุคคลตามความสามารถของบริการคลาวด์ โดยไม่จำเป็นต้องใช้รูปแบบเดียวกันกับทุกบริการ

2. การเปลี่ยนแปลงและยกเลิกสิทธิ

เมื่อหน้าที่ ความรับผิดชอบ หรือความจำเป็นในการใช้งานของผู้ใช้เปลี่ยนแปลง CSC ควรพิจารณาปรับเปลี่ยนหรือลดสิทธิให้สอดคล้องกับสถานะปัจจุบัน

ในกรณีที่ผู้ใช้งานไม่มีความจำเป็นต้องเข้าถึงข้อมูลหรือส่วนการทำงานบางส่วนอีกต่อไป ควรยกเลิกสิทธิดังกล่าว แม้ว่าบัญชีของผู้ใช้งานยังคงมีความจำเป็นสำหรับการใช้บริการส่วนอื่น

จึงควรแยกการพิจารณาระหว่าง **การยกเลิกบัญชี** ซึ่งเกี่ยวข้องกับข้อ 5.2.3.2 และ **การยกเลิกสิทธิบางส่วนของบัญชี** ซึ่งเกี่ยวข้องกับข้อ 5.2.3.3

3. การทบทวนความเหมาะสมของสิทธิ

CSC ควรพิจารณาความเหมาะสมของสิทธิเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้อง เช่น การเปลี่ยนหน้าที่ การย้ายหน่วยงาน การเปลี่ยนแปลงบริการ หรือการเปลี่ยนระดับความสำคัญของข้อมูลและระบบ

หากหน่วยงานมีกระบวนการทบทวนสิทธิอยู่แล้ว สามารถใช้กระบวนการดังกล่าวกับบริการคลาวด์ได้ โดยไม่จำเป็นต้องกำหนดกระบวนการทบทวนแยกต่างหากเฉพาะสำหรับข้อ 5.2.3.3

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดเตรียมฟังก์ชันสำหรับจัดการสิทธิ

CSP ต้องจัดเตรียมฟังก์ชันที่ทำให้ CSC สามารถจัดการสิทธิการเข้าถึงของผู้ใช้งานได้ตามขอบเขตและลักษณะของบริการคลาวด์ที่จัดให้

ฟังก์ชันดังกล่าวควรทำให้ CSC สามารถดำเนินการที่จำเป็นต่อการบริหารสิทธิ เช่น

- กำหนดสิทธิการเข้าถึง
- เปลี่ยนแปลงสิทธิ
- ลดหรือยกเลิกสิทธิ

ร่างเอกสารเพื่อรับฟังความคิดเห็น (Public Hearing เท่านั้น - ห้ามใช้อ้างอิง)

- กำหนดขอบเขตการเข้าถึงตามความสามารถของบริการ

ประกาศไม่ได้กำหนดว่าต้องใช้กลไกการจัดการสิทธิรูปแบบใด ดังนั้น CSP สามารถจัดให้ผ่านบทบาท กลุ่ม นโยบายการเข้าถึง หรือกลไกอื่นที่เหมาะสมกับลักษณะบริการ

2. การรองรับระดับสิทธิที่เหมาะสมกับบริการ

ความสามารถในการจัดการสิทธิของ CSP ควรมีรายละเอียดเพียงพอให้ CSC สามารถแยกขอบเขตการใช้งานตามความเหมาะสม

ตัวอย่างเช่น หากบริการประกอบด้วยส่วนสำหรับผู้ใช้งานทั่วไปและส่วนสำหรับบริหารจัดการระบบ CSP ควรมีความสามารถที่ทำให้ CSC สามารถแยกสิทธิของผู้ใช้งานตามขอบเขตดังกล่าวได้

อย่างไรก็ตาม หัวข้อนี้ไม่ได้กำหนดว่าบริการคลาวด์ทุกประเภทต้องมีระดับสิทธิหรือรูปแบบการแบ่งบทบาทเหมือนกัน การพิจารณาควรขึ้นอยู่กับลักษณะและขอบเขตของบริการ

3. การให้ข้อมูลเกี่ยวกับการใช้ฟังก์ชัน

CSP ต้องจัดให้มีข้อกำหนดหรือข้อมูลสำหรับการใช้ฟังก์ชันจัดการสิทธิแก่ CSC ตามที่ประกาศกำหนด

ข้อมูลดังกล่าวควรเพียงพอให้ CSC สามารถเข้าใจวิธีการกำหนด เปลี่ยนแปลง และยกเลิกสิทธิ รวมถึงข้อจำกัดที่สำคัญของบริการ

ข้อมูลอาจจัดทำในรูปแบบคู่มือบริการ เอกสารประกอบระบบ ข้อมูลในส่วนบริหารจัดการ หรือช่องทางอื่นที่เหมาะสม โดยไม่จำเป็นต้องจัดทำเป็นเอกสารเฉพาะสำหรับข้อกำหนดนี้

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดนี้ไปปฏิบัติควรเริ่มจากการพิจารณา **ความจำเป็นในการเข้าถึง** มากกว่าการเริ่มจากเทคโนโลยีที่ใช้จัดการสิทธิ แนวคิดพื้นฐานสามารถพิจารณาได้ดังนี้

ผู้ใช้งานมีหน้าที่อะไร

↓

จำเป็นต้องเข้าถึงข้อมูลหรือบริการใด

↓

ต้องสามารถดำเนินการอะไรได้บ้าง

↓

กำหนดสิทธิเท่าที่จำเป็น

↓

เปลี่ยนแปลงหรือยกเลิกเมื่อความจำเป็นเปลี่ยนแปลง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างการประยุกต์ใช้:

ลักษณะผู้ใช้งาน	ตัวอย่างขอบเขตสิทธิ
ผู้ใช้งานทั่วไป	ใช้เฉพาะส่วนการทำงานที่เกี่ยวข้องกับหน้าที่
ผู้รับผิดชอบระบบงาน	จัดการเฉพาะระบบหรือบริการที่รับผิดชอบ
ผู้ดูแลระบบ	เข้าถึงส่วนบริหารจัดการตามขอบเขตที่ได้รับมอบหมาย
ผู้ใช้งานชั่วคราว	ได้รับสิทธิเฉพาะที่จำเป็นและตามระยะเวลาที่เหมาะสม

ตารางดังกล่าวเป็นเพียงตัวอย่างเพื่อแสดงแนวคิด มิได้กำหนดประเภทผู้ใช้งานหรือระดับสิทธิที่ทุกหน่วยงานต้องนำไปใช้

ความสัมพันธ์ระหว่างการลงทะเบียนและการจัดสรรสิทธิ

ความสัมพันธ์ระหว่างข้อ 5.2.3.2 และ 5.2.3.3 สามารถพิจารณาเป็นกระบวนการต่อเนื่องตั้งแต่การลงทะเบียนบัญชีจนถึงการยกเลิกบัญชีและสิทธิ

1. ระบุความจำเป็นในการใช้งาน

↓

2. ขอและอนุมัติการลงทะเบียน

↓

3. ลงทะเบียนหรือเปิดใช้งานบัญชี

↓

4. จัดสรรสิทธิตามหน้าที่และความจำเป็น

↓

5. ใช้งานบริการ

↓

6. ทบทวนหรือเปลี่ยนแปลงเมื่อมีเหตุที่เกี่ยวข้อง

↓

7. ลดหรือยกเลิกสิทธิ

↓

8. ระงับหรือยกเลิกบัญชีเมื่อหมดความจำเป็น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปที่ 11 วงจรชีวิตบัญชีและสิทธิการเข้าถึง

ร่างสำหรับ Public Hearing

การเชื่อมโยงกับข้อกำหนดอื่น

เพื่อหลีกเลี่ยงความซ้ำซ้อน ควรเชื่อมโยงข้อกำหนดดังนี้

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การลงทะเบียนและยกเลิกบัญชี	5.2.3.2
สิทธิพิเศษหรือบัญชีผู้ดูแลระบบ	5.2.3.4
ข้อมูลที่ใช้ในการพิสูจน์ตัวตน	5.2.3.5
การจำกัดการเข้าถึงข้อมูล	5.2.3.6
การเข้าสู่ระบบอย่างปลอดภัย	5.2.3.8
การบันทึกกิจกรรมผู้ดูแลระบบ	5.2.6.6

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานที่แสดงถึงการดำเนินการตามข้อ 5.2.3.3 อาจพิจารณาตามความเหมาะสม ดังนี้

หลักฐาน	ตัวอย่างสาระสำคัญ
ข้อมูลการกำหนดสิทธิ	แสดงสิทธิของผู้ใช้งาน กลุ่ม หรือบทบาท
หลักฐานการอนุมัติหรือเปลี่ยนแปลงสิทธิ	แสดงที่มาและความเหมาะสมของการให้หรือเปลี่ยนสิทธิ
หลักฐานการยกเลิกสิทธิ	แสดงการถอนสิทธิเมื่อหมดความจำเป็น
หลักฐานการทบทวนสิทธิ	แสดงการตรวจสอบความเหมาะสมของสิทธิเมื่อเกี่ยวข้อง
ข้อมูลจาก CSP	แสดงความสามารถและวิธีใช้ฟังก์ชันจัดการสิทธิ

หมายเหตุ: หลักฐานดังกล่าวเป็นตัวอย่าง มิได้กำหนดให้ต้องจัดทำเอกสารใหม่ทุกประเภท หากข้อมูลจากระบบหรือกระบวนการที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

5.2.3.4 การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights)

สิทธิการเข้าถึงที่ได้รับสิทธิพิเศษเป็นสิทธิที่ทำให้ผู้ใช้งานสามารถดำเนินการที่มีผลกระทบต่อการบริหารจัดการการกำหนดค่า หรือการรักษาความมั่นคงปลอดภัยของระบบและบริการคลาวด์ได้มากกว่าผู้ใช้งานทั่วไป การใช้สิทธิดังกล่าวโดยไม่ได้รับอนุญาตหรือเกินกว่าความจำเป็นอาจส่งผลกระทบต่อข้อมูล ระบบ หรือบริการในวงกว้าง

การบริหารจัดการสิทธิพิเศษจึงควรให้ความสำคัญกับการจำกัดผู้ได้รับสิทธิ การกำหนดขอบเขตสิทธิให้เหมาะสมกับหน้าที่ การใช้กลไกการพิสูจน์และยืนยันตัวตนที่เพียงพอ และการทบทวนความเหมาะสมของสิทธิ โดยพิจารณาตามความเสี่ยงและขอบเขตความรับผิดชอบของ CSC และ CSP

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของ ผู้ใช้บริการคลาวด์ ให้มีความสามารถในการจัดการบริการคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้	ก) ผู้ให้บริการคลาวด์ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

วัตถุประสงค์

เพื่อให้การใช้สิทธิที่สามารถดำเนินการกับส่วนสำคัญของระบบหรือบริการคลาวด์ได้รับการควบคุมอย่างเหมาะสม จำกัดเฉพาะผู้ที่มีความจำเป็นและได้รับอนุญาต และใช้กลไกการยืนยันตัวตนที่เหมาะสมกับระดับความเสี่ยง เพื่อลดโอกาสและผลกระทบจากการใช้สิทธิพิเศษโดยไม่ได้รับอนุญาตหรือเกินกว่าขอบเขตที่กำหนด

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การระบุสิทธิที่มีความสำคัญ

CSC ควรพิจารณาว่าบัญชี บทบาท หรือสิทธิใดภายใต้การควบคุมของตนสามารถดำเนินการที่มีผลกระทบสำคัญต่อบริการคลาวด์ เช่น

- การบริหารจัดการผู้ใช้งานหรือสิทธิ
- การเปลี่ยนแปลงการกำหนดค่าที่สำคัญ
- การเข้าถึงหรือบริหารจัดการทรัพยากรที่มีความสำคัญ
- การดำเนินการที่อาจส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยหรือความพร้อมใช้งานของบริการ

การระบุสิทธิพิเศษควรพิจารณาจากความสามารถและผลกระทบของสิทธินั้น มากกว่าพิจารณาจากชื่อบัญชีหรือตำแหน่งของบุคคลเพียงอย่างเดียว

2. การจำกัดการให้สิทธิพิเศษ

CSC ควรจำกัดการให้สิทธิพิเศษเฉพาะบุคลากรหรือบัญชีที่มีความจำเป็นตามหน้าที่ และกำหนดขอบเขตสิทธิให้เหมาะสมกับความรับผิดชอบ

การมีสถานะเป็นผู้ดูแลระบบไม่ได้หมายความว่าผู้ใช้งานต้องได้รับสิทธิสูงสุดสำหรับทุกบริการ หากสามารถกำหนดสิทธิให้เฉพาะส่วนที่รับผิดชอบได้

แนวทางดังกล่าวสอดคล้องกับหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) และช่วยลดผลกระทบหากบัญชีที่มีสิทธิพิเศษถูกนำไปใช้โดยไม่ได้รับอนุญาต

3. การใช้การยืนยันตัวตนที่เหมาะสม

สำหรับการเข้าถึงที่มีสิทธิพิเศษ CSC **ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอสำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ ให้สอดคล้องกับระดับความเสี่ยงที่ระบุไว้** โดยอาจใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) ตามที่ประกาศยกตัวอย่างไว้

4. การทบทวนสิทธิพิเศษ

CSC ควรทบทวนความเหมาะสมของสิทธิพิเศษเมื่อมีเหตุที่อาจทำให้ความจำเป็นหรือความเหมาะสมของสิทธิเปลี่ยนแปลง เช่น

- การเปลี่ยนแปลงหน้าที่หรือความรับผิดชอบ
- การเปลี่ยนแปลงผู้ดูแลระบบ
- การเปลี่ยนแปลงบริการหรือระบบที่รับผิดชอบ
- การสิ้นสุดความจำเป็นในการใช้สิทธิ
- การพบเหตุการณ์หรือความเสี่ยงที่เกี่ยวข้องกับบัญชีดังกล่าว

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

หากหน่วยงานมีกระบวนการทบทวนสิทธิการเข้าถึงอยู่แล้ว สามารถนำกระบวนการดังกล่าวมาใช้กับสิทธิพิเศษได้ โดยไม่จำเป็นต้องสร้างกระบวนการแยกใหม่

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดให้มีความสามารถในการยืนยันตัวตน

CSP ต้องจัดเตรียมความสามารถในการยืนยันตัวตนที่เพียงพอสำหรับการใช้สิทธิการเข้าถึงที่ได้รับสิทธิพิเศษของ CSC ตามระดับความเสี่ยงที่ระบุไว้ โดยประกาศยกตัวอย่างการยืนยันตัวตนแบบหลายปัจจัย

ความสามารถดังกล่าวควรรองรับการเข้าถึงส่วนของบริการที่มีสิทธิในการบริหารจัดการหรือดำเนินการที่มีผลกระทบสำคัญตามขอบเขตของบริการที่ CSP จัดให้

2. การรองรับการควบคุมสิทธิพิเศษ

ในส่วนที่เกี่ยวข้องกับการบริหารสิทธิ CSP ควรจัดให้มีความสามารถที่ทำให้ CSC สามารถกำหนดขอบเขตของสิทธิพิเศษได้อย่างเหมาะสมกับลักษณะบริการ

ตัวอย่างเช่น บริการอาจรองรับการแยกผู้ดูแลตามขอบเขตของทรัพยากรหรือหน้าที่ แทนการกำหนดให้ผู้ดูแลทุกรายมีสิทธิครอบคลุมบริการทั้งหมด

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การบริหารสิทธิพิเศษควรพิจารณาจาก **ความสามารถของสิทธิและผลกระทบหากสิทธินั้นถูกใช้โดยมิชอบ** มากกว่าการพิจารณาจากชื่อบัญชีเพียงอย่างเดียว

แนวทางพื้นฐานสามารถพิจารณาได้ดังนี้

ระบุบัญชีหรือสิทธิที่มีอำนาจสูง

↓

พิจารณาความจำเป็น

↓

อนุมัติและกำหนดขอบเขตสิทธิ

↓

ใช้การยืนยันตัวตนที่เหมาะสมกับความเสี่ยง

↓

ใช้งานภายในขอบเขตที่ได้รับอนุญาต

↓

ทบทวน / ปรับเปลี่ยน / ยกเลิกเมื่อหมดความจำเป็น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ตัวอย่างการพิจารณาสิทธิพิเศษ

ลักษณะสิทธิ	แนวทางที่ควรพิจารณา
บริหารจัดการผู้ใช้งานและสิทธิ	จำกัดเฉพาะผู้รับผิดชอบและขอบเขตที่จำเป็น
เปลี่ยนแปลงการกำหนดค่าที่สำคัญ	จำกัดเฉพาะผู้ได้รับมอบหมาย
บริหารจัดการทรัพยากรสำคัญ	กำหนดสิทธิตามขอบเขตความรับผิดชอบ
เข้าถึงส่วนบริหารจัดการบริการ	ใช้กลไกการยืนยันตัวตนที่เหมาะสมกับความเสี่ยง
สิทธิพิเศษหมดความจำเป็น	ลดหรือยกเลิกสิทธิ

ตารางดังกล่าวเป็นเพียงตัวอย่างสำหรับการประยุกต์ใช้ มิได้กำหนดว่าทุกบริการต้องมีประเภทบัญชีหรือระดับสิทธิตามรายการดังกล่าว

ห้ามใช้งานอิง



รูปที่ 12 แนวคิดการควบคุมสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ

หลักการ: การใช้สิทธิพิเศษควรจำกัดเฉพาะผู้ที่ได้รับอนุญาต กำหนดขอบเขตเท่าที่จำเป็น และใช้กลไกการยืนยันตัวตนที่เหมาะสมกับระดับความเสี่ยง

การเชื่อมโยงกับข้อกำหนดอื่น

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การลงทะเบียนและยกเลิกบัญชี	5.2.3.2
การจัดสรรและถอนสิทธิ	5.2.3.3
ข้อมูลที่ใช้ในการพิสูจน์ตัวตน	5.2.3.5
โปรแกรมที่สามารถข้ามการควบคุม	5.2.3.7
การเข้าสู่ระบบอย่างปลอดภัย	5.2.3.8
การบันทึกกิจกรรมผู้ดูแลระบบ	5.2.6.6
การจัดการเหตุการณ์ที่เกี่ยวข้อง	5.2.10

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐาน	ตัวอย่างสาระสำคัญ
รายการบัญชีหรือสิทธิพิเศษ	แสดงผู้ใช้งานหรือบัญชีที่มีสิทธิสำคัญ
การอนุมัติสิทธิ	แสดงความจำเป็นและการได้รับอนุญาต
การกำหนดสิทธิในบริการคลาวด์	แสดงขอบเขตสิทธิที่ได้รับ
การตั้งค่าการยืนยันตัวตน	แสดงกลไกที่ใช้กับบัญชีหรือสิทธิพิเศษ
ผลการทบทวนสิทธิ	แสดงการตรวจสอบความเหมาะสมของสิทธิ
ข้อมูลจาก CSP	แสดงความสามารถด้านการยืนยันตัวตนและการจัดการสิทธิ

หมายเหตุ: หลักฐานดังกล่าวเป็นเพียงตัวอย่าง และไม่จำเป็นต้องจัดทำเป็นเอกสารแยกทั้งหมด หากหลักฐานจากระบบ กระบวนการ หรือเอกสารที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

5.2.3.5 การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users)

ข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ หมายถึง ข้อมูลที่ใช้ประกอบการพิสูจน์หรือยืนยันตัวตนของผู้ใช้งานและจำเป็นต้องได้รับการปกป้องจากการเปิดเผยหรือการนำไปใช้โดยไม่ได้รับอนุญาต เช่น รหัสผ่าน หรือข้อมูลลับอื่นที่บริการคลาวด์ใช้ในการยืนยันตัวตน

การจัดการข้อมูลดังกล่าวมีความสำคัญต่อการควบคุมการเข้าถึง เนื่องจากหากข้อมูลถูกเปิดเผย สูญหาย หรือถูกนำไปใช้โดยบุคคลอื่น อาจทำให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูล ระบบ หรือบริการคลาวด์ภายใต้สิทธิของเจ้าของข้อมูลการพิสูจน์ตัวตนนั้นได้

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ในสภาพแวดล้อมคลาวด์ CSC และ CSP มีบทบาทที่สัมพันธ์กัน โดย CSC ต้องพิจารณาว่ากระบวนการของ CSP สำหรับการจัดสรรข้อมูลการพิสูจน์ตัวตนที่เป็นความลับสามารถตอบสนองข้อกำหนดของ CSC ได้หรือไม่ ขณะที่ CSP ต้องให้ข้อมูลเกี่ยวกับกระบวนการดังกล่าวแก่ CSC ตามที่ประกาศกำหนดไว้

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับ (Secret Authentication Information) เช่น รหัสผ่าน เป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) ของผู้ใช้บริการคลาวด์ รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าวสำหรับการตรวจสอบสิทธิผู้ใช้งาน

วัตถุประสงค์

เพื่อให้ข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้งานได้รับการจัดสรรและจัดการอย่างเหมาะสม และให้ CSC สามารถตรวจสอบได้ว่ากระบวนการที่ CSP จัดให้สามารถตอบสนองข้อกำหนดด้านการควบคุมการเข้าถึงและความมั่นคงปลอดภัยของ CSC ได้

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การกำหนดความต้องการด้านข้อมูลการพิสูจน์ตัวตน

CSC ควรทราบข้อกำหนดของหน่วยงานเกี่ยวกับข้อมูลที่ใช้ในการพิสูจน์และยืนยันตัวตน เพื่อใช้เป็นเกณฑ์ในการพิจารณาความสามารถและกระบวนการของ CSP

ข้อกำหนดดังกล่าวอาจเป็นส่วนหนึ่งของนโยบายการควบคุมการเข้าถึง นโยบายความมั่นคงปลอดภัยสารสนเทศ หรือข้อกำหนดอื่นที่หน่วยงานมีอยู่แล้ว โดยไม่จำเป็นต้องจัดทำเป็นนโยบายใหม่เฉพาะสำหรับบริการคลาวด์

การกำหนดความต้องการควรคำนึงถึงลักษณะของบริการ ประเภทผู้ใช้งาน ความสำคัญของข้อมูลหรือระบบ และความเสี่ยงที่เกี่ยวข้อง

2. การตรวจสอบกระบวนการของ CSP

CSC ต้องตรวจสอบกระบวนการของ CSP ที่เกี่ยวข้องกับการจัดสรรข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ เพื่อพิจารณาว่าสามารถตอบสนองข้อกำหนดของ CSC ได้หรือไม่

การตรวจสอบอาจพิจารณาจากข้อมูลที่ CSP จัดให้ เช่น

- วิธีการจัดสรรหรือกำหนดข้อมูลการพิสูจน์ตัวตน
- วิธีการที่ผู้ใช้งานได้รับหรือกำหนดข้อมูลดังกล่าว

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- ความสามารถในการเปลี่ยนหรือกำหนดข้อมูลใหม่
- แนวทางที่เกี่ยวข้องกับการปกป้องข้อมูลระหว่างกระบวนการจัดสรร
- ข้อจำกัดหรือเงื่อนไขที่ CSC ควรทราบ

ระดับของการตรวจสอบควรเหมาะสมกับลักษณะบริการและความเสี่ยง ไม่จำเป็นต้องตรวจสอบรายละเอียดภายในของ CSP ที่อยู่นอกเหนือข้อมูลหรือขอบเขตที่ CSP เปิดเผยให้ CSC

3. การดำเนินการเมื่อกระบวนการไม่ตอบสนองข้อกำหนด

หาก CSC พบว่ากระบวนการหรือความสามารถที่ CSP จัดให้ไม่สามารถตอบสนองข้อกำหนดของหน่วยงานได้อย่างเพียงพอ CSC ควรพิจารณาความเสี่ยงและแนวทางดำเนินการที่เหมาะสม

แนวทางอาจรวมถึงการใช้ความสามารถเพิ่มเติมที่ CSP รองรับ การกำหนดมาตรการภายใต้การควบคุมของ CSC หรือการพิจารณาความเหมาะสมของบริการกับข้อมูลและระบบที่จะนำไปใช้งาน

ทั้งนี้ การกำหนดมาตรการเพิ่มเติมควรเป็นไปตามผลการประเมินความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง มิใช่การกำหนดมาตรการทางเทคนิคเดียวกันสำหรับบริการคลาวด์ทุกประเภท

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ

CSP ต้องมีกระบวนการสำหรับการจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้งานภายใต้การใช้บริการของ CSC ตามขอบเขตบริการที่จัดให้

กระบวนการดังกล่าวควรรองรับการจัดการข้อมูลที่จำเป็นสำหรับการพิสูจน์หรือยืนยันตัวตนของผู้ใช้งาน และสอดคล้องกับความสามารถของบริการที่ CSP จัดให้

อย่างไรก็ตาม ข้อกำหนดนี้ไม่ควรตีความว่า CSP ต้องใช้กลไกหรือเทคโนโลยีสำหรับจัดการข้อมูลลับรูปแบบใดรูปแบบหนึ่งโดยเฉพาะ เว้นแต่มีข้อกำหนดอื่นที่เกี่ยวข้องกำหนดไว้

2. การจัดสรรข้อมูลการพิสูจน์ตัวตน

CSP ต้องมีกระบวนการที่เหมาะสมสำหรับการจัดสรรข้อมูลการพิสูจน์ตัวตนที่เป็นความลับให้แก่ผู้ใช้งานของ CSC ตามลักษณะของบริการ

กระบวนการดังกล่าวควรลดความเสี่ยงที่ข้อมูลการพิสูจน์ตัวตนจะถูกเปิดเผยหรือได้รับโดยบุคคลที่ไม่ได้รับอนุญาตในระหว่างการจัดสรรหรือการเริ่มใช้งาน

ทั้งนี้ รูปแบบของกระบวนการอาจแตกต่างกันตามบริการ เช่น การให้ผู้ใช้งานกำหนดข้อมูลด้วยตนเอง หรือการใช้กระบวนการอื่นที่ CSP จัดให้ โดยไม่จำเป็นต้องกำหนดวิธีการเดียวสำหรับทุกบริการ

3. การให้ข้อมูลแก่ CSC

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

CSP ต้องให้ข้อมูลเกี่ยวกับกระบวนการจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ รวมถึงกระบวนการจัดสรรข้อมูลดังกล่าวแก่ CSC เพื่อให้ CSC สามารถพิจารณาความสอดคล้องกับข้อกำหนดของตนได้

ข้อมูลอาจอยู่ในรูปของเอกสารประกอบบริการ คู่มือ ข้อกำหนดการใช้งาน หรือข้อมูลอื่นที่ CSP จัดให้ โดยไม่จำเป็นต้องจัดทำเอกสารใหม่เฉพาะสำหรับข้อ 5.2.3.5 หากข้อมูลที่มีอยู่สามารถแสดงสาระสำคัญได้เพียงพอ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การดำเนินการตามข้อ 5.2.3.5 ควรมุ่งที่การตอบคำถามสำคัญว่า “กระบวนการที่ CSP ใช้ในการจัดสรรและจัดการข้อมูลการพิสูจน์ตัวตน สามารถตอบสนองความต้องการด้านความมั่นคงปลอดภัยของ CSC ได้หรือไม่”

แนวทางพื้นฐานสามารถพิจารณาได้ดังนี้

CSC กำหนดความต้องการ

↓

CSP ให้ข้อมูลเกี่ยวกับกระบวนการและความสามารถ

↓

CSC ตรวจสอบความสอดคล้อง

↓

นำความสามารถของบริการไปใช้

↓

พิจารณามาตรการเพิ่มเติมเมื่อจำเป็น

ตัวอย่างการพิจารณา

ประเด็น	แนวทางที่ควรพิจารณา
การจัดสรรข้อมูล	มีกระบวนการที่ลดความเสี่ยงจากการเปิดเผยแก่ผู้ไม่ได้รับอนุญาต
การกำหนดข้อมูลใหม่	สามารถเปลี่ยนหรือกำหนดข้อมูลใหม่เมื่อมีความจำเป็น
การถูกเปิดเผยหรือถูกคุกคาม	สามารถดำเนินการเพื่อป้องกันการใช้ข้อมูลเดิมต่อไป
ข้อกำหนดของ CSC	ความสามารถของบริการสามารถรองรับข้อกำหนดที่เกี่ยวข้องของหน่วยงาน
ข้อมูลจาก CSP	มีข้อมูลเพียงพอให้ CSC เข้าใจกระบวนการและข้อจำกัดที่สำคัญ

ตารางนี้เป็นแนวทางประกอบการพิจารณา มิได้กำหนดรายการตรวจสอบทางเทคนิคที่ CSP ทุกแห่งต้องปฏิบัติเหมือนกัน

การเชื่อมโยงกับข้อกำหนดอื่น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การลงทะเบียนและยกเลิกผู้ใช้งาน	5.2.3.2
การจัดสรรสิทธิ	5.2.3.3
สิทธิพิเศษ	5.2.3.4
การเข้าสู่ระบบอย่างปลอดภัย	5.2.3.8
การเข้ารหัสและการจัดการกุญแจ	5.2.4
การจัดการเมื่อข้อมูลการเข้าถึงถูกคุกคามจนเกิดเหตุการณ์	5.2.10

การเชื่อมโยงดังกล่าวมีความสำคัญ โดยเฉพาะกรณีข้อมูลการพิสูจน์ตัวตนถูกเปิดเผย หากจำเป็นต้องระงับหรือยกเลิกบัญชีให้เชื่อมโยงกับข้อ 5.2.3.2 และหากเหตุการณ์เข้าข่ายเหตุการณ์ด้านความมั่นคงปลอดภัย ให้ดำเนินการตามข้อ 5.2.10 การจัดการเหตุการณ์ โดยการดำเนินการในข้อ 5.2.3.5 ให้มุ่งเฉพาะการจัดการข้อมูลการพิสูจน์ตัวตนที่เกี่ยวข้อง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐาน	ตัวอย่างสาระสำคัญ
ข้อกำหนดของ CSC	นโยบายหรือข้อกำหนดเกี่ยวกับข้อมูลการพิสูจน์ตัวตน
ข้อมูลหรือเอกสารจาก CSP	อธิบายกระบวนการจัดสรรและจัดการข้อมูลการพิสูจน์ตัวตน
ผลการพิจารณาความสามารถของบริการ	แสดงว่า CSC ได้พิจารณาความสอดคล้องกับข้อกำหนดของตน
การตั้งค่าที่เกี่ยวข้อง	แสดงการใช้ความสามารถของบริการตามที่หน่วยงานกำหนด
หลักฐานการดำเนินการเมื่อข้อมูลถูกคุกคาม	แสดงการเปลี่ยน เพิกถอน หรือดำเนินการอื่นตามความเหมาะสม

หมายเหตุ: รายการดังกล่าวเป็นตัวอย่างหลักฐาน มิได้กำหนดให้ต้องจัดทำเอกสารใหม่ทุกประเภท หากเอกสารข้อมูลจากระบบ หรือหลักฐานที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

ร่างสำหรับ Public Hearing ขั้นที่ 1 - ห้ามใช้อ้างอิง

5.2.3.6 การจำกัดการเข้าถึงข้อมูล (Information Access Restriction)

การจำกัดการเข้าถึงข้อมูลมีวัตถุประสงค์เพื่อให้ข้อมูลและบริการคลาวด์สามารถเข้าถึงได้เฉพาะผู้ใช้งานหรือระบบที่ได้รับอนุญาต และเฉพาะภายในขอบเขตที่กำหนดตามนโยบายการควบคุมการเข้าถึงของ CSC

ข้อกำหนดนี้ครอบคลุมทั้ง **การเข้าถึงบริการต่าง ๆ บนระบบคลาวด์** และ **ข้อมูลของ CSC ที่จัดเก็บอยู่ในบริการคลาวด์** โดย CSC มีหน้าที่กำหนดและนำข้อจำกัดการเข้าถึงไปใช้ ขณะที่ CSP ต้องจัดให้มีกลไกการควบคุมที่ทำให้ CSC สามารถกำหนดข้อจำกัดดังกล่าวได้ตามขอบเขตของบริการ

หัวข้อนี้จึงมุ่งเน้นที่ **การบังคับใช้ข้อจำกัดการเข้าถึงตามนโยบาย** ไม่ใช่การกำหนดรายละเอียดเกี่ยวกับการจัดชั้นข้อมูล การเข้ารหัส การป้องกันข้อมูลรั่วไหล หรือการแบ่งแยกเครือข่าย ซึ่งควรพิจารณาตามข้อกำหนดที่เกี่ยวข้องแยกต่างหาก

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบายการควบคุมการเข้าถึงและปฏิบัติตามข้อจำกัดดังกล่าว ซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูลผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ	ก) ผู้ให้บริการคลาวด์ต้องให้การควบคุมการเข้าถึงที่อนุญาตให้กับผู้ใช้บริการคลาวด์ เพื่อจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูลผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ

วัตถุประสงค์

เพื่อให้การเข้าถึงบริการคลาวด์และข้อมูลที่จัดเก็บหรือประมวลผลภายในบริการถูกจำกัดตามนโยบายการควบคุมการเข้าถึง โดยผู้ใช้งานหรือระบบสามารถเข้าถึงได้เฉพาะข้อมูล บริการ หรือส่วนการทำงานที่ได้รับอนุญาตและมีความจำเป็นต่อการปฏิบัติงาน

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การกำหนดขอบเขตการเข้าถึง

CSC ต้องตรวจสอบให้แน่ใจว่าสามารถกำหนดข้อจำกัดการเข้าถึงบริการและข้อมูลที่อยู่ในบริการคลาวด์ให้สอดคล้องกับนโยบายการควบคุมการเข้าถึงของหน่วยงาน

การกำหนดขอบเขตควรพิจารณาว่า

- ผู้ใช้งานหรือระบบใดมีความจำเป็นต้องเข้าถึง
- สามารถเข้าถึงบริการหรือข้อมูลใด
- สามารถดำเนินการกับข้อมูลหรือบริการได้ในขอบเขตใด
- มีเงื่อนไขหรือข้อจำกัดเพิ่มเติมตามความสำคัญของข้อมูลหรือบริการหรือไม่

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานอื่น

หลักสำคัญคือ การมีบัญชีหรือสามารถเข้าสู่บริการคลาวด์ได้ **ไม่ควรหมายความว่าผู้ใช้งานสามารถเข้าถึงข้อมูลและส่วนการทำงานทั้งหมดของบริการได้โดยอัตโนมัติ**

2. การจำกัดการเข้าถึงบริการคลาวด์

CSC ควรกำหนดให้ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการหรือส่วนการทำงานที่จำเป็นตามหน้าที่และวัตถุประสงค์ในการใช้งาน

ตัวอย่างเช่น ผู้ใช้งานที่มีหน้าที่ใช้งานระบบงานอาจไม่จำเป็นต้องเข้าถึงส่วนบริหารจัดการบริการ ขณะที่ผู้รับผิดชอบระบบอาจได้รับสิทธิเพิ่มเติมเฉพาะบริการหรือทรัพยากรที่อยู่ภายใต้ความรับผิดชอบของตน

3. การจำกัดการเข้าถึงข้อมูล

CSC ต้องสามารถจำกัดการเข้าถึงข้อมูลที่จัดเก็บไว้ในบริการคลาวด์ให้สอดคล้องกับนโยบายการควบคุมการเข้าถึงของหน่วยงาน ตามที่ประกาศกำหนดไว้โดยตรง

การกำหนดข้อจำกัดควรพิจารณาตามความจำเป็นในการใช้งานและความสำคัญของข้อมูล ตัวอย่างเช่น

ลักษณะการใช้งาน	แนวทางการจำกัดการเข้าถึง
ข้อมูลสำหรับผู้ใช้งานทั่วไป	จำกัดเฉพาะผู้ใช้งานหรือกลุ่มที่เกี่ยวข้อง
ข้อมูลของหน่วยงานหรือระบบงาน	จำกัดตามหน้าที่และความจำเป็นในการปฏิบัติงาน
ข้อมูลที่มีความสำคัญ	จำกัดเฉพาะผู้ได้รับอนุญาตและมีความจำเป็น
ข้อมูลสำหรับการบริหารระบบ	จำกัดเฉพาะผู้รับผิดชอบตามขอบเขตหน้าที่

ตารางดังกล่าวเป็นเพียงตัวอย่างแนวคิด ไม่ได้กำหนดระดับชั้นข้อมูลหรือรูปแบบสิทธิที่หน่วยงานทุกแห่งต้องนำไปใช้

4. การนำข้อจำกัดไปบังคับใช้

การกำหนดนโยบายหรือระบุผู้มีสิทธิเพียงอย่างเดียวไม่เพียงพอ CSC ต้องนำข้อจำกัดดังกล่าวไปใช้กับบริการคลาวด์ตามที่ประกาศกำหนด

CSC จึงควรตรวจสอบว่าการกำหนดค่าหรือสิทธิที่ใช้งานจริงสอดคล้องกับข้อจำกัดที่หน่วยงานกำหนดไว้

ตัวอย่างเช่น หากนโยบายกำหนดว่าข้อมูลชุดหนึ่งสามารถเข้าถึงได้เฉพาะผู้ปฏิบัติงานที่เกี่ยวข้อง การกำหนดสิทธิในบริการคลาวด์ก็ควรสะท้อนข้อกำหนดดังกล่าว ไม่ควรกำหนดให้ผู้ใช้งานทั้งหมดสามารถเข้าถึงข้อมูลนั้นได้โดยไม่มีความจำเป็น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5. การทบทวนเมื่อมีการเปลี่ยนแปลง

CSC ควรพิจารณาทบทวนข้อจำกัดการเข้าถึงเมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อความเหมาะสมของการเข้าถึง เช่น

- หน้าที่หรือความรับผิดชอบของผู้ใช้งานเปลี่ยนแปลง
- มีการเพิ่มหรือเปลี่ยนแปลงบริการคลาวด์
- มีการเปลี่ยนแปลงลักษณะหรือความสำคัญของข้อมูล
- มีการเปลี่ยนแปลงรูปแบบการใช้งานหรือการแบ่งปันข้อมูล
- พบว่าการกำหนดสิทธิเดิมเปิดให้เข้าถึงกว้างเกินความจำเป็น

หากหน่วยงานมีกระบวนการทบทวนสิทธิหรือการเปลี่ยนแปลงระบบอยู่แล้ว สามารถใช้กระบวนการดังกล่าวได้ โดยไม่จำเป็นต้องสร้างกระบวนการใหม่เฉพาะสำหรับข้อ 5.2.3.6

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดให้มีความสามารถในการจำกัดการเข้าถึง

CSP ต้องจัดให้มีการควบคุมการเข้าถึงที่ทำให้ CSC สามารถจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์และข้อมูลของ CSC ที่จัดเก็บไว้ในบริการได้

ความสามารถดังกล่าวควรสอดคล้องกับลักษณะและขอบเขตของบริการที่ CSP จัดให้ และทำให้ CSC สามารถนำข้อกำหนดการควบคุมการเข้าถึงของตนไปบังคับใช้ได้อย่างเหมาะสม

2. การรองรับการจำกัดสิทธิตามขอบเขตบริการ

กลไกที่ CSP จัดให้ควรมีความละเอียดเพียงพอกับลักษณะของบริการ เพื่อให้ CSC สามารถจำกัดการเข้าถึงตามขอบเขตที่เหมาะสม เช่น ตามผู้ใช้งาน กลุ่ม บทบาท ทรัพยากร หรือส่วนการทำงานของบริการ ในกรณีที่บริการรองรับความสามารถดังกล่าว

อย่างไรก็ตาม ไม่ควรตีความข้อกำหนดนี้ว่า CSP ทุกแห่งต้องใช้รูปแบบการควบคุมสิทธิเหมือนกัน เนื่องจากความสามารถและระดับการควบคุมอาจแตกต่างกันตามรูปแบบและขอบเขตของบริการคลาวด์

3. การสนับสนุนการนำข้อจำกัดไปใช้

CSP ควรจัดให้มีข้อมูลหรือวิธีการที่เพียงพอสำหรับให้ CSC สามารถเข้าใจและใช้ความสามารถด้านการจำกัดการเข้าถึงของบริการได้อย่างเหมาะสม

ในกรณีที่บริการมีข้อจำกัดเกี่ยวกับระดับหรือรูปแบบการกำหนดสิทธิ CSC ควรสามารถทราบข้อจำกัดดังกล่าวเพื่อใช้ประกอบการพิจารณาความเหมาะสมของบริการกับข้อมูลและระบบที่จะนำมาใช้งาน

ทั้งนี้ ประเด็นดังกล่าวเป็นแนวทางประกอบการประยุกต์ใช้ โดยข้อกำหนดหลักของประกาศคือ CSP ต้องจัดให้มี **การควบคุมการเข้าถึงที่ทำให้ CSC สามารถจำกัดการเข้าถึงบริการและข้อมูลได้**

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อ 5.2.3.6 ไปปฏิบัติสามารถพิจารณาตามหลักการพื้นฐานว่า

ข้อมูลหรือบริการใด

↓

ใครมีความจำเป็นต้องเข้าถึง

↓

ต้องสามารถดำเนินการอะไรได้บ้าง

↓

กำหนดข้อจำกัดการเข้าถึง

↓

นำข้อจำกัดไปบังคับใช้ในบริการคลาวด์

↓

ทบทวนเมื่อมีการเปลี่ยนแปลง

ตัวอย่างการประยุกต์ใช้สามารถแสดงได้ดังนี้

สถานการณ์	แนวทางที่ควรพิจารณา
ผู้ใช้งานต้องดูข้อมูลเพื่อปฏิบัติงาน	ให้เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง
ผู้ใช้งานต้องแก้ไขข้อมูล	กำหนดสิทธิแก้ไขเฉพาะผู้ที่มีหน้าที่
ผู้ใช้งานไม่จำเป็นต้องเข้าถึงส่วนบริหารระบบ	ไม่ให้สิทธิส่วนบริหารจัดการ
มีการเปลี่ยนหน้าที่	ปรับขอบเขตการเข้าถึงให้สอดคล้องกับหน้าที่ใหม่
ข้อมูลมีความสำคัญเพิ่มขึ้น	ทบทวนว่าข้อจำกัดเดิมยังเหมาะสมหรือไม่

หัวใจสำคัญคือ **สิทธิที่กำหนดในระบบต้องสอดคล้องกับข้อจำกัดที่กำหนดไว้ในนโยบาย** มิใช่เพียงมีนโยบายแต่การตั้งค่าจริงเปิดกว้างกว่าที่กำหนด

การเชื่อมโยงกับข้อกำหนดอื่น

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การเข้าถึงเครือข่ายและบริการ	5.2.3.1
การจัดสรรและเปลี่ยนแปลงสิทธิ	5.2.3.3
สิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ	5.2.3.4
การเข้าสู่ระบบอย่างปลอดภัย	5.2.3.8

ร่างเอกสารเพื่อรับฟังความคิดเห็นสาธารณะ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การเข้ารหัสข้อมูล	5.2.4
การบันทึกและปกป้องข้อมูลบันทึกเหตุการณ์	5.2.6.4–5.2.6.6
การแบ่งแยกเครือข่าย	5.2.7.2

รายละเอียดเกี่ยวกับการแบ่งแยกเครือข่ายและสถาปัตยกรรมเครือข่ายให้พิจารณาตามข้อ 5.2.7.2 โดยข้อ 5.2.3.6 ให้มุ่งที่การกำหนดและบังคับใช้ข้อจำกัดการเข้าถึงข้อมูลและบริการ

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐาน	ตัวอย่างสาระสำคัญ
นโยบายการควบคุมการเข้าถึง	แสดงหลักเกณฑ์หรือข้อจำกัดในการเข้าถึงข้อมูลและบริการ
การกำหนดสิทธิในบริการคลาวด์	แสดงว่ามีการนำข้อจำกัดไปบังคับใช้
รายการสิทธิหรือกลุ่มผู้ใช้งาน	แสดงขอบเขตการเข้าถึงข้อมูลหรือบริการ
หลักฐานการอนุมัติ	แสดงที่มาของการได้รับสิทธิในกรณีที่เกี่ยวข้อง
ผลการทบทวนสิทธิ	แสดงการตรวจสอบหรือปรับเปลี่ยนข้อจำกัดเมื่อมีความจำเป็น
ข้อมูลความสามารถของ CSP	แสดงความสามารถในการจำกัดการเข้าถึงบริการและข้อมูล

หลักฐานดังกล่าวเป็น **ตัวอย่างหลักฐาน (Examples of Evidence)** มิใช่รายการเอกสารบังคับทั้งหมด และ CSC หรือ CSP สามารถใช้เอกสาร การตั้งค่าระบบ หรือหลักฐานที่มีอยู่เดิมได้ หากสามารถแสดงการดำเนินงานตามข้อกำหนดได้อย่างเพียงพอ

5.2.3.7 การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privileged Utility Programs)

โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิพิเศษ หมายถึง โปรแกรม เครื่องมือ หรือความสามารถที่สามารถดำเนินการในระดับที่อาจข้าม หลีกเลี่ยง หรือมีผลต่อการควบคุมตามปกติของระบบหรือมาตรการด้านความมั่นคงปลอดภัย การใช้เครื่องมือดังกล่าวจึงอาจก่อให้เกิดผลกระทบต่อข้อมูล ระบบ หรือบริการคลาวด์ หากถูกใช้งานโดยบุคคลที่ไม่ได้รับอนุญาตหรือใช้เกินกว่าขอบเขตที่กำหนด

ในสภาพแวดล้อมคลาวด์ โปรแกรมอรรถประโยชน์อาจอยู่ภายใต้การควบคุมของ CSC หรือ CSP ขึ้นอยู่กับรูปแบบและขอบเขตของบริการ ดังนั้น การควบคุมควรพิจารณาตามความรับผิดชอบของแต่ละฝ่าย โดยมุ่งให้เครื่องมือที่มีความสามารถดังกล่าวถูกใช้เฉพาะเมื่อมีความจำเป็นและอยู่ภายใต้การควบคุมที่เหมาะสม

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ ผู้ใช้บริการคลาวด์ต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์ และตรวจสอบให้มั่นใจว่าโปรแกรมเหล่านั้น ไม่รบกวนการควบคุมของบริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ใด ๆ ที่ใช้ในบริการคลาวด์ ผู้ให้บริการคลาวด์ต้องตรวจสอบให้มั่นใจว่าการใช้โปรแกรมอรรถประโยชน์ใด ๆ ที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการรักษาความปลอดภัยนั้น จำกัดเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น และต้อง

ร่างสำหรับ Public Hearing ห้ามนำไปใช้งาน

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	มีการทบทวนและตรวจสอบการใช้โปรแกรมดังกล่าวอย่างสม่ำเสมอ

วัตถุประสงค์

เพื่อควบคุมการใช้โปรแกรมอรรถประโยชน์ที่มีความสามารถในการข้าม หลีกเลี่ยง หรือมีผลต่อการควบคุมของระบบและบริการคลาวด์ ให้จำกัดเฉพาะการใช้งานที่ได้รับอนุญาตและมีความจำเป็น รวมทั้งลดความเสี่ยงที่เครื่องมือดังกล่าวจะถูกนำไปใช้ในลักษณะที่กระทบต่อความมั่นคงปลอดภัยของบริการคลาวด์

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การระบุโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้

ในกรณีที่ CSC อนุญาตให้ใช้โปรแกรมอรรถประโยชน์ในสภาพแวดล้อมคลาวด์ CSC ต้องสามารถระบุได้ว่าโปรแกรมหรือเครื่องมือใดได้รับอนุญาตให้ใช้งาน ตามที่ประกาศกำหนด

การระบุอาจดำเนินการในรูปแบบที่เหมาะสมกับหน่วยงาน เช่น รายการเครื่องมือที่ได้รับอนุญาต เอกสารการกำหนดค่าระบบ หรือเอกสารประกอบกระบวนการปฏิบัติงาน โดยไม่จำเป็นต้องจัดทำทะเบียนใหม่เฉพาะสำหรับข้อ 5.2.3.7 หากข้อมูลที่มีอยู่สามารถแสดงเครื่องมือที่ได้รับอนุญาตได้อย่างเพียงพอ

2. การพิจารณาผลกระทบต่อการควบคุมของบริการคลาวด์

CSC ต้องตรวจสอบให้แน่ใจว่าโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้ไม่รบกวนหรือทำให้การควบคุมของระบบคลาวด์ไม่สามารถทำงานได้ตามที่กำหนด

การพิจารณาควรคำนึงถึงความสามารถของเครื่องมือ เช่น เครื่องมือสามารถเปลี่ยนแปลงการกำหนดค่าที่สำคัญ เข้าถึงข้อมูลนอกเหนือสิทธิของผู้ใช้งานทั่วไป หรือหลีกเลี่ยงมาตรการควบคุมที่มีอยู่ได้หรือไม่

หากเครื่องมือมีความสามารถดังกล่าว ควรพิจารณาความจำเป็นและกำหนดการควบคุมให้เหมาะสมกับระดับความเสี่ยง

3. การจำกัดการใช้งานตามความจำเป็น

CSC ควรจำกัดการใช้โปรแกรมอรรถประโยชน์ที่มีความสามารถสูงเฉพาะบุคลากรหรือบัญชีที่ได้รับมอบหมายและมีความจำเป็นต่อการปฏิบัติงาน

การอนุญาตให้บุคลากรเป็นผู้ดูแลระบบไม่ควรหมายความว่าบุคลากรนั้นสามารถใช้เครื่องมือทุกประเภทได้โดยอัตโนมัติ หากเครื่องมือดังกล่าวไม่เกี่ยวข้องกับหน้าที่หรือมีความสามารถเกินกว่าที่จำเป็น

ทั้งนี้ การกำหนดสิทธิสำหรับบัญชีที่ใช้เครื่องมือดังกล่าวควรพิจารณาร่วมกับข้อ 5.2.3.4 การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การกำหนดข้อกำหนดสำหรับการใช้โปรแกรมอรรถประโยชน์

CSP ต้องกำหนดข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ที่ใช้ในการให้บริการคลาวด์ โดยเฉพาะเครื่องมือที่มีความสามารถในการข้ามขั้นตอนการทำงานตามปกติหรือการควบคุมด้านความมั่นคงปลอดภัย

ข้อกำหนดดังกล่าวควรเหมาะสมกับความสามารถและความเสี่ยงของเครื่องมือ รวมถึงขอบเขตหน้าที่ของบุคลากรที่จำเป็นต้องใช้งาน

2. การจำกัดผู้ได้รับอนุญาต

โปรแกรมอรรถประโยชน์ที่สามารถข้ามขั้นตอนการทำงานปกติหรือการควบคุมด้านความมั่นคงปลอดภัยต้องจำกัดการใช้งานเฉพาะบุคลากรที่ได้รับอนุญาต

การกำหนดผู้ได้รับอนุญาตควรสัมพันธ์กับหน้าที่ ความรับผิดชอบ และความจำเป็นในการปฏิบัติงาน โดยหลีกเลี่ยงการให้สิทธิใช้งานเครื่องมือที่มีความสามารถสูงแก่บุคลากรที่ไม่มีความจำเป็น

3. การทบทวนและตรวจสอบการใช้งาน

CSP ต้องมีการทบทวนและตรวจสอบการใช้โปรแกรมอรรถประโยชน์ที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการควบคุมด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ ตามที่ประกาศกำหนด

การดำเนินการควรมุ่งให้สามารถตรวจพบการใช้งานที่ไม่เหมาะสมหรือไม่สอดคล้องกับวัตถุประสงค์ที่ได้รับอนุญาต

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การพิจารณาว่าเครื่องมือใดควรอยู่ภายใต้การควบคุมของข้อ 5.2.3.7 ไม่ควรพิจารณาจากชื่อหรือประเภทของโปรแกรมเพียงอย่างเดียว แต่ควรพิจารณาจาก ความสามารถของเครื่องมือและผลกระทบที่อาจเกิดขึ้นจากการใช้งาน

แนวคิดพื้นฐานสามารถพิจารณาได้ดังนี้

ระบุเครื่องมือที่ใช้งาน

↓

พิจารณาความสามารถและผลกระทบ

↓

พิจารณาความจำเป็นในการใช้งาน

↓

กำหนดผู้ได้รับอนุญาต

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

↓

ควบคุมการใช้งาน

↓

ทบทวนและตรวจสอบการใช้งานอย่างสม่ำเสมอ

ตัวอย่างการพิจารณา:

ลักษณะของเครื่องมือ	แนวทางที่ควรพิจารณา
เครื่องมือทั่วไปที่ไม่มีความสามารถข้ามการควบคุม	บริหารจัดการตามกระบวนการปกติของหน่วยงาน
เครื่องมือที่สามารถเปลี่ยนการกำหนดค่าที่สำคัญ	จำกัดเฉพาะผู้ที่มีหน้าที่และได้รับอนุญาต
เครื่องมือที่สามารถเข้าถึงข้อมูลหรือทรัพยากรในระดับสูง	พิจารณาความจำเป็นและขอบเขตการใช้งาน
เครื่องมือที่สามารถข้ามการควบคุมด้านความมั่นคงปลอดภัย	จำกัดการใช้งานเฉพาะผู้ได้รับอนุญาต พร้อมทั้งทบทวนและตรวจสอบการใช้งานตามข้อกำหนด
เครื่องมือหมดความจำเป็น	พิจารณายกเลิกการอนุญาตหรือการเข้าถึง

ตัวอย่างดังกล่าวใช้เพื่ออธิบายหลักการ ไม่ได้กำหนดว่าเครื่องมือทุกประเภทต้องได้รับการควบคุมในระดับเดียวกัน

การเชื่อมโยงกับข้อกำหนดอื่น

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การจัดสรรสิทธิการเข้าถึง	5.2.3.3
การจัดการสิทธิพิเศษ	5.2.3.4
การจำกัดการเข้าถึงข้อมูลและบริการ	5.2.3.6
การเข้าสู่ระบบอย่างปลอดภัย	5.2.3.8
การบันทึกเหตุการณ์	5.2.6.4
การปกป้องข้อมูลบันทึกเหตุการณ์	5.2.6.5
การบันทึกกิจกรรมผู้ดูแลระบบ	5.2.6.6

การทบทวนและตรวจสอบการใช้โปรแกรมอรรถประโยชน์ควรเชื่อมโยงกับข้อมูลจากกระบวนการบันทึกเหตุการณ์ตามข้อ 5.2.6.4–5.2.6.6 ตามความเหมาะสม

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐาน	ตัวอย่างสาระสำคัญ
รายการโปรแกรมอรรถประโยชน์ที่ได้รับอนุญาต	แสดงเครื่องมือที่อนุญาตให้ใช้ในสภาพแวดล้อมคลาวด์
ข้อกำหนดหรือแนวทางการใช้งาน	แสดงเงื่อนไขหรือข้อจำกัดสำหรับการใช้เครื่องมือ
รายการผู้ได้รับอนุญาต	แสดงผู้ที่มีสิทธิใช้เครื่องมือที่มีความสามารถสูง
การกำหนดสิทธิในระบบ	แสดงการจำกัดการใช้งานเฉพาะผู้ได้รับอนุญาต
หลักฐานการทบทวนและตรวจสอบการใช้งาน	แสดงการทบทวนและตรวจสอบการใช้โปรแกรมอรรถประโยชน์ตามข้อกำหนด
ข้อมูลการประเมินเครื่องมือ	แสดงการพิจารณาว่าเครื่องมืออาจรบกวนหรือข้ามการควบคุมหรือไม่

หลักฐานดังกล่าวเป็นตัวอย่าง มิได้กำหนดให้ต้องจัดทำเอกสารใหม่ทุกประเภท หากสามารถใช้ข้อมูลจากระบบเอกสาร หรือกระบวนการที่มีอยู่เพื่อแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

5.2.3.8 ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures)

การเข้าสู่ระบบเป็นจุดเริ่มต้นสำคัญของการเข้าถึงข้อมูล ระบบ และบริการคลาวด์ หากกระบวนการเข้าสู่ระบบไม่มีการควบคุมที่เหมาะสม อาจทำให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงบริการโดยใช้บัญชีหรือข้อมูลการพิสูจน์ตัวตนของผู้อื่นได้

การเข้าสู่ระบบอย่างปลอดภัยจึงควรมีกระบวนการที่สามารถพิสูจน์และยืนยันตัวตนของผู้ใช้งานได้อย่างเหมาะสมก่อนอนุญาตให้เข้าถึงบริการ โดยระดับของการควบคุมควรสอดคล้องกับลักษณะของบัญชี ความสำคัญของบริการ และความเสี่ยงที่เกี่ยวข้อง

ในสภาพแวดล้อมคลาวด์ CSC มีหน้าที่กำหนดให้ผู้ใช้งานภายใต้การควบคุมของตนปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย ขณะที่ CSP ต้องจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีของผู้ใช้งานภายใต้การควบคุมของ CSC ในกรณีที่มีความจำเป็นตามที่ประกาศกำหนด

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ	ก) ในกรณีที่จำเป็น ผู้ให้บริการคลาวด์ต้องจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ ที่ผู้ใช้บริการคลาวด์ร้องขอสำหรับผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์

ร่างเพื่อรับฟังความคิดเห็น (Public Hearing) เท่านั้น - ห้ามใช้อ้างอิง

วัตถุประสงค์ (Objective)

เพื่อให้การเข้าสู่ระบบคลาวด์ของผู้ใช้งานดำเนินการผ่านกระบวนการพิสูจน์และยืนยันตัวตนที่เหมาะสม ลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต และสนับสนุนให้การเข้าสู่ระบบมีระดับการควบคุมสอดคล้องกับความสำคัญของบัญชี บริการ และความเสี่ยงที่เกี่ยวข้อง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

1. การกำหนดขั้นตอนการเข้าสู่ระบบ

CSC ต้องกำหนดให้ผู้ใช้งานภายใต้การควบคุมของตนปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีที่ใช้เข้าถึงบริการคลาวด์

ขั้นตอนดังกล่าวอาจกำหนดเป็นส่วนหนึ่งของนโยบายการควบคุมการเข้าถึง แนวปฏิบัติสำหรับผู้ใช้งาน หรือการกำหนดค่าของระบบที่บังคับใช้กับผู้ใช้งาน โดยไม่จำเป็นต้องจัดทำเอกสารแยกเฉพาะสำหรับข้อ 5.2.3.8 หากกระบวนการที่มีอยู่สามารถครอบคลุมการใช้บริการคลาวด์ได้อย่างเพียงพอ

2. การใช้กลไกการยืนยันตัวตนที่เหมาะสม

CSC ควรพิจารณาใช้กลไกการยืนยันตัวตนที่เหมาะสมกับความเสี่ยงของการเข้าถึง โดยคำนึงถึงประเภทของบัญชี ความสำคัญของบริการ ข้อมูลที่สามารถเข้าถึง และผลกระทบหากบัญชีถูกนำไปใช้โดยไม่ได้รับอนุญาต

บัญชีหรือการเข้าถึงที่มีความเสี่ยงสูงอาจต้องใช้มาตรการที่เข้มงวดกว่าการเข้าถึงทั่วไป ทั้งนี้ ในกรณีของบัญชีที่มีสิทธิพิเศษ ควรพิจารณาร่วมกับข้อ 5.2.3.4 ซึ่งประกาศระบุการยืนยันตัวตนแบบหลายปัจจัย (MFA) เป็นตัวอย่างของการยืนยันตัวตนที่เพียงพอตามระดับความเสี่ยง

3. การปกป้องข้อมูลระหว่างการเข้าสู่ระบบ

CSC ควรกำหนดให้ผู้ใช้งานปฏิบัติต่อข้อมูลที่ใช้ในการเข้าสู่ระบบในลักษณะที่ไม่ทำให้ข้อมูลดังกล่าวถูกเปิดเผยหรือถูกนำไปใช้โดยไม่ได้รับอนุญาต

ในกรณีที่พบหรือสงสัยว่าข้อมูลการพิสูจน์ตัวตนถูกเปิดเผยหรือถูกคุกคาม ควรดำเนินการตามกระบวนการที่เกี่ยวข้อง เช่น การเปลี่ยนหรือเพิกถอนข้อมูลการพิสูจน์ตัวตน การระงับบัญชี หรือการจัดการเหตุการณ์ตามความเหมาะสม

รายละเอียดเกี่ยวกับการบริหารข้อมูลการพิสูจน์ตัวตนให้พิจารณาตามข้อ 5.2.3.5 และการจัดการกรณีบัญชีถูกคุกคามให้เชื่อมโยงกับข้อ 5.2.3.2

4. การใช้ขั้นตอนการเข้าสู่ระบบตามที่กำหนด

CSC ควรทำให้มั่นใจว่าผู้ใช้งานใช้ช่องทางและขั้นตอนการเข้าสู่ระบบที่หน่วยงานหรือ CSP กำหนด และไม่ใช้วิธีการที่หลีกเลี่ยงการควบคุมโดยไม่มีการอนุมัติ

ร่างคำสั่ง Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ในกรณีที่บริการรองรับช่องทางการเข้าสู่ระบบหลายรูปแบบ CSC ควรพิจารณาว่าช่องทางใดเหมาะสมกับผู้ใช้งานแต่ละประเภทและความเสี่ยงของบริการ

อย่างไรก็ตาม ไม่ควรกำหนดเทคโนโลยีสำหรับการเข้าสู่ระบบเป็นรูปแบบเดียวสำหรับบริการคลาวด์ทุกประเภท เนื่องจากความสามารถและรูปแบบการให้บริการอาจแตกต่างกัน

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย

ในกรณีที่มีความจำเป็น CSP ต้องจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีที่ CSC ร้องขอสำหรับผู้ใช้งานภายใต้การควบคุมของ CSC ตามที่ประกาศกำหนด

ขั้นตอนดังกล่าวควรเหมาะสมกับลักษณะและขอบเขตของบริการ และสนับสนุนให้ CSC สามารถควบคุมการเข้าสู่บริการของผู้ใช้งานได้ตามความต้องการด้านความมั่นคงปลอดภัย

2. การรองรับกลไกการพิสูจน์และยืนยันตัวตน

CSP ควรจัดให้มีความสามารถในการพิสูจน์และยืนยันตัวตนที่เหมาะสมกับบริการ โดยเฉพาะกรณีที่ลักษณะบัญชีหรือการเข้าถึงมีความเสี่ยงสูง

ความสามารถดังกล่าวอาจแตกต่างกันตามประเภทและขอบเขตบริการ จึงไม่ควรกำหนดว่าบริการคลาวด์ทุกประเภทต้องรองรับกลไกหรือเทคโนโลยีแบบเดียวกัน

ในกรณีที่เกี่ยวข้องกับสิทธิพิเศษ ให้พิจารณาร่วมกับข้อ 5.2.3.4 ซึ่งมีข้อกำหนดเฉพาะเกี่ยวกับการยืนยันตัวตนตามระดับความเสี่ยง

3. การให้ข้อมูลที่จำเป็นต่อ CSC

CSP ควรจัดให้มีข้อมูลที่จำเป็นเกี่ยวกับวิธีการหรือเงื่อนไขในการเข้าสู่ระบบ เพื่อให้ CSC สามารถกำหนดและสื่อสารขั้นตอนการเข้าสู่ระบบแก่ผู้ใช้งานภายใต้การควบคุมของตนได้อย่างเหมาะสม

ข้อมูลดังกล่าวอาจอยู่ในคู่มือบริการ เอกสารประกอบระบบ หรือช่องทางอื่นที่ CSP จัดให้ โดยไม่จำเป็นต้องจัดทำเอกสารใหม่เฉพาะสำหรับข้อกำหนดนี้

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

แนวทางพื้นฐานสามารถพิจารณาได้ดังนี้

ระบุบัญชีและบริการที่ต้องเข้าสู่ระบบ

↓

พิจารณาความสำคัญและความเสี่ยง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

↓

กำหนดวิธีการพิสูจน์และยืนยันตัวตนที่เหมาะสม

↓

กำหนดขั้นตอนสำหรับผู้ใช้งาน

↓

นำมาตรการไปใช้กับบริการ

↓

ทบทวนเมื่อความเสี่ยงหรือบริการเปลี่ยนแปลง

ตัวอย่างการพิจารณา:

สถานการณ์	**แนวทางที่ควรพิจารณา**
บัญชีผู้ใช้งานทั่วไป	ใช้กระบวนการเข้าสู่ระบบตามข้อกำหนดของ CSC และความสามารถของบริการ
บัญชีที่เข้าถึงข้อมูลหรือบริการสำคัญ	พิจารณามาตรการยืนยันตัวตนให้เหมาะสมกับความเสี่ยง
บัญชีที่มีสิทธิพิเศษ	พิจารณาการยืนยันตัวตนที่เข้มงวดขึ้นตามข้อ 5.2.3.4
ข้อมูลการพิสูจน์ตัวตนถูกคุกคาม	ระงับ เปลี่ยน หรือเพิกถอนตามกระบวนการที่เกี่ยวข้อง
มีการเปลี่ยนแปลงบริการหรือระดับความเสี่ยง	ทบทวนความเหมาะสมของขั้นตอนการเข้าสู่ระบบ

ตารางดังกล่าวเป็นแนวทางประกอบการประยุกต์ใช้ มิได้กำหนดวิธีการยืนยันตัวตนตายตัวสำหรับแต่ละประเภทบัญชี

การเชื่อมโยงกับข้อกำหนดอื่น

ประเด็น	**ข้อกำหนดที่เกี่ยวข้อง**
การเข้าถึงเครือข่ายและบริการ	5.2.3.1
การลงทะเบียนและยกเลิกบัญชี	5.2.3.2
การจัดสรรสิทธิ	5.2.3.3
การจัดการสิทธิพิเศษ	5.2.3.4
ข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ	5.2.3.5
การจำกัดการเข้าถึงข้อมูล	5.2.3.6
การบันทึกเหตุการณ์ที่เกี่ยวข้อง	5.2.6.4–5.2.6.6
การจัดการเหตุการณ์	5.2.10

ร่างเพื่อรับฟังความคิดเห็นสาธารณะ Public Hearing ไม่ควรนำไปใช้อ้างอิง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐาน	ตัวอย่างสาระสำคัญ
นโยบายหรือแนวทางการเข้าสู่ระบบ	แสดงข้อกำหนดที่ผู้ใช้งานต้องปฏิบัติ
การกำหนดค่าการยืนยันตัวตน	แสดงกลไกที่ใช้กับบัญชีหรือบริการตามความเหมาะสม
การตั้งค่าสำหรับบัญชีสิทธิพิเศษ	แสดงมาตรการยืนยันตัวตนที่เหมาะสมกับความเสี่ยง
คู่มือหรือข้อมูลจาก CSP	แสดงขั้นตอนและความสามารถสำหรับการเข้าสู่ระบบ
หลักฐานการสื่อสารแก่ผู้ใช้งาน	แสดงว่าผู้ใช้งานได้รับทราบขั้นตอนที่เกี่ยวข้อง
หลักฐานการทบทวน	แสดงการปรับปรุงเมื่อบริการหรือความเสี่ยงเปลี่ยนแปลง

หมายเหตุ: รายการข้างต้นเป็นตัวอย่างหลักฐาน มิได้หมายความว่าต้องจัดทำเอกสารแยกต่างหากทุกประเภท หากเอกสาร การตั้งค่าระบบ หรือหลักฐานที่มีอยู่สามารถแสดงการดำเนินการตามข้อกำหนดได้อย่างเพียงพอ

แนวทางการดำเนินงานร่วมสำหรับการควบคุมการเข้าถึง

การดำเนินการตามข้อ 5.2.3 การควบคุมการเข้าถึง ควรพิจารณาข้อกำหนดตามข้อ 5.2.3.1–5.2.3.8 ร่วมกัน เนื่องจากการควบคุมการเข้าถึงบริการคลาวด์เป็นกระบวนการที่เชื่อมโยงตั้งแต่การกำหนดผู้ที่ได้รับอนุญาต การลงทะเบียนผู้ใช้งาน การจัดสรรสิทธิ การควบคุมสิทธิพิเศษ การจัดการข้อมูลการพิสูจน์ตัวตน การจำกัดการเข้าถึง การควบคุมโปรแกรมอรรถประโยชน์พิเศษ ตลอดจนการเข้าสู่ระบบอย่างปลอดภัย

การดำเนินงานควรคำนึงถึงขอบเขตความรับผิดชอบของผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) ตามข้อกำหนดที่เกี่ยวข้อง ลักษณะของบริการ และความสามารถในการควบคุมของแต่ละฝ่าย โดยไม่ควรตีความว่าทั้ง 2 ฝ่ายมีหน้าที่เหมือนกันในทุกข้อ

1. การกำหนดความรับผิดชอบระหว่าง CSC และ CSP

การควบคุมการเข้าถึงในบริการคลาวด์ควรเริ่มจากการระบุว่า กิจกรรมใดอยู่ภายใต้การควบคุมของ CSC และกิจกรรมใดเป็นความสามารถหรือกระบวนการที่ CSP ต้องจัดให้ตามข้อกำหนด

โดยทั่วไป CSC เป็นผู้กำหนดความต้องการด้านการเข้าถึงของผู้ใช้งานภายใต้การควบคุมของตน เช่น ผู้ใดมีความจำเป็นต้องใช้บริการ ผู้ใช้งานควรได้รับสิทธิในระดับใด และเมื่อใดควรเปลี่ยนแปลง ระงับ หรือยกเลิกการเข้าถึง

ส่วน CSP มีหน้าที่จัดให้มีความสามารถหรือกระบวนการตามข้อกำหนดที่เกี่ยวข้อง เช่น การลงทะเบียนและยกเลิกผู้ใช้งาน การจัดการสิทธิ การยืนยันตัวตน การจำกัดการเข้าถึง และการเข้าสู่ระบบอย่างปลอดภัย ตามขอบเขตของบริการที่จัดให้

อย่างไรก็ตาม ขอบเขตความรับผิดชอบอาจแตกต่างกันตามประเภทและรูปแบบของบริการคลาวด์ จึงควรพิจารณาจากบริการที่ใช้งานจริง ไม่ควรกำหนดรูปแบบความรับผิดชอบเดียวกันสำหรับบริการทุกประเภท

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักสำคัญคือ

CSC รับผิดชอบการกำหนดและใช้การควบคุมในขอบเขตที่ตนสามารถบริหารจัดการได้ ขณะที่ CSP รับผิดชอบการจัดให้มีความสามารถและกระบวนการตามที่ข้อกำหนดกำหนด ภายในขอบเขตของบริการที่ให้แก่ CSC

2. การใช้กระบวนการควบคุมการเข้าถึงที่องค์กรมีอยู่

CSC ไม่จำเป็นต้องจัดทำระบบ นโยบาย หรือกระบวนการใหม่ขึ้นเฉพาะสำหรับบริการคลาวด์ หากกระบวนการที่องค์กรมีอยู่สามารถนำมาใช้ครอบคลุมบริการคลาวด์ได้อย่างเพียงพอ

กระบวนการที่สามารถนำมาใช้ร่วมกันอาจประกอบด้วย

- การขอและอนุมัติบัญชีผู้ใช้งาน
- การอนุมัติสิทธิการเข้าถึง
- การเปลี่ยนแปลงสิทธิเมื่อหน้าที่หรือความรับผิดชอบเปลี่ยนแปลง
- การระงับหรือยกเลิกบัญชีเมื่อหมดความจำเป็น
- การทบทวนบัญชีและสิทธิ
- การดำเนินการเมื่อบัญชีหรือข้อมูลการพิสูจน์ตัวตนถูกคุกคาม

CSC ควรเพิ่มเติมเฉพาะประเด็นที่เกิดจากลักษณะเฉพาะของบริการคลาวด์ เช่น ความสามารถที่ CSP จัดให้ ข้อจำกัดของบริการ หรือขอบเขตความรับผิดชอบระหว่าง CSC และ CSP

แนวทางนี้ช่วยลดการจัดทำเอกสารหรือกระบวนการที่ซ้ำซ้อน และทำให้การควบคุมบริการคลาวด์สามารถบูรณาการกับกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่องค์กรมีอยู่ได้

3. การควบคุมตามความจำเป็นและระดับความเสี่ยง

การควบคุมการเข้าถึงควรกำหนดให้เหมาะสมกับความจำเป็นในการใช้งานและระดับความเสี่ยง โดยอาจพิจารณาปัจจัย เช่น

- ความสำคัญของข้อมูลหรือบริการ
- ลักษณะและขอบเขตของสิทธิ
- ผลกระทบหากบัญชีถูกนำไปใช้โดยไม่ได้รับอนุญาต
- ความสามารถของบัญชีหรือสิทธิในการเปลี่ยนแปลงหรือบริหารจัดการระบบ
- ช่องทางและลักษณะการเข้าถึง
- ข้อกำหนดทางกฎหมาย ระเบียบ หรือนโยบายขององค์กรที่เกี่ยวข้อง

บัญชีหรือการเข้าถึงที่มีความเสี่ยงสูงควรได้รับการควบคุมในระดับที่เหมาะสม โดยเฉพาะการใช้สิทธิพิเศษ ซึ่งข้อ 5.2.3.4 กำหนดให้ใช้เทคนิคการยืนยันตัวตนที่เพียงพอตามระดับความเสี่ยง และยกตัวอย่างการยืนยันตัวตนแบบหลายปัจจัย (MFA) ไว้โดยตรง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ทั้งนี้ การพิจารณาตามความเสี่ยงไม่หมายความว่าต้องกำหนดมาตรการเฉพาะแตกต่างกันสำหรับทุกบัญชี แต่หมายถึงการหลีกเลี่ยงการใช้มาตรการเดียวกันโดยไม่คำนึงถึงความสำคัญและผลกระทบของการเข้าถึง

4. การบริหารบัญชีและสิทธิการเข้าถึงตลอดวงจร

การควบคุมการเข้าถึงควรครอบคลุมตลอดช่วงเวลาที่ผู้ใช้งานมีความจำเป็นต้องใช้บริการ ตั้งแต่การระบุความจำเป็น การลงทะเบียน การจัดสรรสิทธิ การใช้งาน การทบทวนหรือเปลี่ยนแปลง จนถึงการลดหรือยกเลิกสิทธิและบัญชี โดยให้พิจารณาตามวงจรชีวิตบัญชีและสิทธิการเข้าถึงที่แสดงไว้ในรูปที่ 2

กระบวนการนี้สอดคล้องกับความสัมพันธ์ระหว่างข้อ 5.2.3.2 และข้อ 5.2.3.3 ที่ได้อธิบายไว้ก่อนหน้า กล่าวคือ ข้อ 5.2.3.2 มุ่งที่สถานะของบัญชี ส่วนข้อ 5.2.3.3 มุ่งที่ขอบเขตของสิทธิภายใต้บัญชีนั้น

ดังนั้น เมื่อผู้ใช้งานยังจำเป็นต้องใช้บริการแต่ไม่จำเป็นต้องใช้สิทธิบางส่วน ควรลดหรือยกเลิกเฉพาะสิทธิที่ไม่จำเป็น โดยไม่จำเป็นต้องยกเลิกบัญชีทั้งหมด

5. การให้สิทธิเท่าที่จำเป็นและการควบคุมสิทธิพิเศษ

การจัดสรรสิทธิควรยึดหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) โดยให้ผู้ใช้งานได้รับสิทธิเพียงพอต่อหน้าที่หรือวัตถุประสงค์ที่ได้รับอนุญาต

การกำหนดสิทธิอาจดำเนินการตามผู้ใช้งาน กลุ่ม บทบาท หรือกลไกอื่นที่บริการรองรับ โดยไม่จำเป็นต้องใช้รูปแบบเดียวกันสำหรับบริการคลาวด์ทุกประเภท

หลักสำคัญคือ

การมีบัญชีสำหรับใช้บริการ ไม่ได้หมายความว่าผู้ใช้งานควรสามารถเข้าถึงข้อมูล ทรัพยากร หรือส่วนการทำงานทั้งหมดของบริการ

สำหรับบัญชีหรือสิทธิที่สามารถบริหารจัดการ เปลี่ยนแปลงการกำหนดค่าที่สำคัญ หรือดำเนินการที่อาจส่งผลกระทบในวงกว้าง ควรพิจารณาตามข้อ 5.2.3.4 และใช้การควบคุมที่เหมาะสมกับระดับความเสี่ยง

ในกรณีที่เหมาะสม อาจพิจารณาแยกการใช้งานทั่วไปออกจากการดำเนินการที่ต้องใช้สิทธิพิเศษ เพื่อลดการใช้สิทธิที่มีอำนาจสูงโดยไม่จำเป็น อย่างไรก็ตาม ไม่ควรตีความเป็นข้อบังคับว่าต้องใช้บัญชีแยกหรือเทคโนโลยีบริหารบัญชีสิทธิพิเศษในทุกกรณี หากไม่มีข้อกำหนดหรือความเสี่ยงรองรับ

6. การทบทวนและจัดการเมื่อมีการเปลี่ยนแปลงหรือความเสี่ยง

CSC ควรพิจารณาทบทวนบัญชีและสิทธิเมื่อมีเหตุที่อาจส่งผลต่อความเหมาะสมของการเข้าถึง เช่น

- การเปลี่ยนหน้าที่หรือความรับผิดชอบ
- การย้ายหน่วยงาน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- การสิ้นสุดการปฏิบัติงาน
- การเปลี่ยนแปลงบริการหรือระบบ
- การเปลี่ยนแปลงความสำคัญของข้อมูล
- การพบสิทธิที่กว้างเกินความจำเป็น
- การพบเหตุการณ์ที่เกี่ยวข้องกับบัญชีหรือการเข้าถึง

หากพบว่าบัญชี รหัสผ่าน หรือข้อมูลการพิสูจน์ตัวตนอาจถูกเปิดเผยหรือถูกนำไปใช้โดยไม่ได้รับอนุญาต ควรดำเนินการตามความเหมาะสม เช่น ระงับบัญชี เปลี่ยนหรือเพิกถอนข้อมูลการพิสูจน์ตัวตน หรือลดหรือยกเลิกสิทธิ

หากเหตุการณ์ดังกล่าวเข้าข่ายเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามกระบวนการจัดการเหตุการณ์ตามข้อ 5.2.10

ตารางสรุปความรับผิดชอบในการควบคุมการเข้าถึง

ตารางต่อไปนี้ใช้เป็นข้อมูลอ้างอิงโดยสรุปสำหรับข้อ 5.2.3.1–5.2.3.8 เพื่อช่วยให้เห็นความแตกต่างระหว่างหน้าที่ของ CSC และ CSP โดยไม่ใช้แทนรายละเอียดของข้อกำหนดตามประกาศ

ข้อ	การควบคุม	CSC	CSP
5.2.3.1	การเข้าถึงเครือข่ายและบริการเครือข่าย	กำหนดข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์แต่ละบริการ	ไม่มีข้อกำหนดเฉพาะในข้อนี้
5.2.3.2	การลงทะเบียนและยกเลิกผู้ใช้งาน	กำหนดกระบวนการลงทะเบียนและยกเลิก รวมถึงกรณีการควบคุมการเข้าถึงถูกคุกคาม	จัดให้มีฟังก์ชันลงทะเบียนและยกเลิก พร้อมข้อกำหนดการใช้งาน
5.2.3.3	การจัดสรรการเข้าถึง	พิจารณาใช้ความสามารถของบริการเพื่อกำหนด เปลี่ยนแปลง และยกเลิกสิทธิตามความเหมาะสม	จัดให้มีฟังก์ชันบริหารสิทธิและข้อกำหนดสำหรับการใช้งาน
5.2.3.4	การจัดการสิทธิพิเศษ	ใช้เทคนิคการยืนยันตัวตนที่เพียงพอตามระดับความเสี่ยง	จัดให้มีเทคนิคการยืนยันตัวตนที่เพียงพอตามระดับความเสี่ยง
5.2.3.5	ข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ	ตรวจสอบว่ากระบวนการของ CSP สามารถตอบสนองข้อกำหนดของ CSC	ให้ข้อมูลเกี่ยวกับกระบวนการจัดการและการจัดสรรข้อมูลดังกล่าว
5.2.3.6	การจำกัดการเข้าถึงข้อมูล	กำหนดและนำข้อจำกัดการเข้าถึงบริการและข้อมูลไปใช้ตามนโยบาย	จัดให้มีการควบคุมที่ทำให้ CSC สามารถจำกัดการเข้าถึงได้
5.2.3.7	โปรแกรมอรรถประโยชน์พิเศษ	ระบุเครื่องมือที่ใช้และตรวจสอบว่าไม่รบกวนการควบคุมของบริการคลาวด์	กำหนดข้อกำหนด จำกัดการใช้งานเฉพาะผู้ได้รับอนุญาต และมีการทบทวนและตรวจสอบการใช้งานอย่างสม่ำเสมอ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

5.2.3.8	การเข้าสู่ระบบอย่างปลอดภัย	กำหนดให้ผู้ใช้งานภายใต้การควบคุมปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย	จัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยตามความจำเป็น

หมายเหตุ: ตารางนี้เป็นการสรุปเพื่อช่วยในการประยุกต์ใช้เท่านั้น การพิจารณาความสอดคล้องต้องอ้างอิงข้อกำหนดตามประกาศเป็นหลัก

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานสำหรับการควบคุมการเข้าถึงอาจอยู่ในรูปของเอกสาร การตั้งค่าระบบ บันทึกจากระบบ หรือข้อมูลที่ CSP จัดให้ โดยควรเลือกใช้ให้เหมาะสมกับบทบาทของ CSC และ CSP และลักษณะของบริการคลาวด์

ไม่จำเป็นต้องจัดทำเอกสารแยกใหม่ทุกประเภท หากหลักฐานที่มีอยู่สามารถแสดงการดำเนินงานตามข้อกำหนดได้อย่างเพียงพอ

ตารางเชื่อมโยงข้อกำหนดกับหลักฐานที่ควรพิจารณา

ข้อ	ประเด็น	หลักฐาน CSC ที่ควรพิจารณา	หลักฐาน CSP ที่ควรพิจารณา
5.2.3.1	การเข้าถึงเครือข่ายและบริการ	นโยบายหรือข้อกำหนดการเข้าถึงรายการบริการและผู้ได้รับอนุญาต	ไม่มีข้อกำหนดเฉพาะสำหรับ CSP ในข้อนี้
5.2.3.2	การลงทะเบียนและยกเลิกผู้ใช้งาน	ขั้นตอนการลงทะเบียน/ยกเลิก ข้อมูลบัญชี หลักฐานการระงับหรือยกเลิก และกรณีข้อมูลการเข้าถึงถูกคุกคาม	หลักฐานความสามารถสำหรับลงทะเบียนและยกเลิกผู้ใช้งาน และข้อมูลเกี่ยวกับการใช้ฟังก์ชัน
5.2.3.3	การจัดสรรการเข้าถึง	ข้อมูลการกำหนด เปลี่ยนแปลง และยกเลิกสิทธิ	หลักฐานความสามารถสำหรับจัดการสิทธิ และข้อมูลการใช้งานฟังก์ชัน
5.2.3.4	การจัดการสิทธิพิเศษ	รายการบัญชีหรือสิทธิพิเศษ การอนุมัติการกำหนดสิทธิ และการตั้งค่าการยืนยันตัวตน	หลักฐานความสามารถในการยืนยันตัวตนสำหรับการใช้สิทธิพิเศษ
5.2.3.5	ข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ	ข้อกำหนดของ CSC และหลักฐานการพิจารณากระบวนการของ CSP	ข้อมูลเกี่ยวกับกระบวนการจัดการและการจัดสรรข้อมูลการพิสูจน์ตัวตน
5.2.3.6	การจำกัดการเข้าถึงข้อมูล	นโยบาย ขอบเขตสิทธิ และหลักฐานการนำข้อจำกัดไปใช้กับบริการ	หลักฐานความสามารถที่ทำให้ CSC สามารถจำกัดการเข้าถึงบริการและข้อมูล
5.2.3.7	โปรแกรมอรรถประโยชน์พิเศษ	รายการเครื่องมือที่อนุญาตและหลักฐานการพิจารณาผลกระทบต่อการควบคุม	ข้อกำหนดการใช้งาน รายการผู้ได้รับอนุญาต และหลักฐานการทบทวนและตรวจสอบการใช้งาน

ร่างสำหรับ Public Hearing ขั้นต้น - ห้ามใช้งาน

5.2.3.8	การเข้าสู่ระบบอย่างปลอดภัย	นโยบายหรือแนวทางการเข้าสู่ระบบและการตั้งค่าที่เกี่ยวข้อง	คู่มือ การตั้งค่า หรือข้อมูลเกี่ยวกับขั้นตอนและกลไกการเข้าสู่ระบบอย่างปลอดภัย

แนวทางการพิจารณาความเพียงพอของหลักฐาน

การพิจารณาความเพียงพอของหลักฐานควรมุ่งที่ความสามารถในการแสดงว่า การควบคุมที่กำหนดไว้ถูกนำไปปฏิบัติจริง มากกว่าการตรวจสอบว่ามีเอกสารครบตามรายการหรือไม่

โดยทั่วไปควรสามารถเชื่อมโยงได้ว่า

ข้อกำหนดหรือความจำเป็น

⟶ การอนุมัติ

⟶ การกำหนดบัญชีหรือสิทธิ

⟶ การใช้งานจริง

⟶ การทบทวนหรือเปลี่ยนแปลง

ตัวอย่างเช่น หากนโยบายกำหนดให้ผู้ใช้งานได้รับสิทธิตามหน้าที่ หลักฐานจากบริการคลาวด์ควรสามารถแสดงได้ว่าสิทธิที่กำหนดให้กับผู้ใช้งานหรือกลุ่มผู้ใช้งานสอดคล้องกับหลักการดังกล่าว

สำหรับบัญชีหรือสิทธิที่มีความสำคัญสูง อาจพิจารณาหลักฐานในรายละเอียดมากขึ้นตามระดับความเสี่ยง

ทั้งนี้ หลักฐานไม่จำเป็นต้องอยู่ในรูปเอกสารอย่างเป็นทางการเสมอไป หากข้อมูลจากระบบ การตั้งค่า หรือบันทึกที่มีอยู่สามารถตรวจสอบย้อนกลับได้อย่างเพียงพอ

ข้อพิจารณาในการประยุกต์ใช้ (Application Considerations)

การนำข้อ 5.2.3 ไปประยุกต์ใช้ควรคำนึงถึงบริบทของบริการคลาวด์และความเสี่ยงขององค์กร โดยอย่างน้อยควรพิจารณาประเด็นต่อไปนี้

1. รูปแบบและขอบเขตบริการคลาวด์

ความสามารถในการบริหารบัญชี สิทธิ การยืนยันตัวตน และการจำกัดการเข้าถึงอาจแตกต่างกันตามรูปแบบและขอบเขตของบริการ

ดังนั้น CSC ควรทำความเข้าใจความสามารถและข้อจำกัดของบริการที่ใช้งาน และพิจารณาว่าสามารถรองรับข้อกำหนดด้านการควบคุมการเข้าถึงขององค์กรได้หรือไม่

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ไม่ควรสมมติว่าบริการคลาวด์ทุกประเภทต้องมีรูปแบบการบริหารบัญชี สิทธิ หรือกลไกการยืนยันตัวตนเหมือนกัน

2. ความสำคัญของข้อมูล ระบบ และสิทธิการเข้าถึง

ระดับการควบคุมควรสัมพันธ์กับความสำคัญของข้อมูล ระบบ และผลกระทบที่อาจเกิดขึ้นหากการเข้าถึงถูกใช้โดยไม่ได้รับอนุญาต

โดยเฉพาะบัญชีหรือสิทธิที่สามารถบริหารจัดการระบบ เปลี่ยนแปลงการกำหนดค่าที่สำคัญ หรือเข้าถึงข้อมูลสำคัญ ควรได้รับการพิจารณาในระดับที่เหมาะสมกับความเสี่ยง

3. ขอบเขตความรับผิดชอบของ CSC และ CSP

การประยุกต์ใช้ควรพิจารณาว่า การควบคุมใดอยู่ภายใต้การบริหารจัดการของ CSC และการควบคุมใดเป็นความสามารถหรือกระบวนการที่ CSP จัดให้

การใช้บริการคลาวด์ไม่ทำให้ความรับผิดชอบของ CSC ในส่วนที่ตนควบคุมได้ถูกโอนไปยัง CSP โดยอัตโนมัติ และในทางกลับกัน CSC ไม่ควรกำหนดให้ CSP รับผิดชอบกิจกรรมที่อยู่นอกขอบเขตของบริการหรือข้อกำหนดที่เกี่ยวข้อง

4. การใช้มาตรการตามความเหมาะสม

แนวทางในเอกสารนี้ไม่ควรตีความเป็นการกำหนดเทคโนโลยี ผลิตภัณฑ์ สถาปัตยกรรม หรือค่าทางเทคนิคเฉพาะที่ต้องใช้ในทุกกรณี

องค์กรสามารถเลือกใช้วิธีการที่เหมาะสมกับลักษณะบริการ ความเสี่ยง และความสามารถของระบบ หากสามารถบรรลุวัตถุประสงค์ของข้อกำหนดได้

5. การใช้กระบวนการและหลักฐานที่มีอยู่

ไม่จำเป็นต้องจัดทำกระบวนการ แบบฟอร์ม หรือหลักฐานใหม่เฉพาะสำหรับข้อ 5.2.3 หากกระบวนการเดิมขององค์กรหรือข้อมูลจากบริการคลาวด์สามารถแสดงการดำเนินงานตามข้อกำหนดได้อย่างเพียงพอ

หลักการนี้มีความสำคัญเพื่อหลีกเลี่ยงการสร้างภาระด้านเอกสารที่ไม่จำเป็น และทำให้การควบคุมบริการคลาวด์สามารถรวมอยู่ในระบบบริหารจัดการที่องค์กรมีอยู่แล้ว

6. การเชื่อมโยงกับข้อกำหนดด้านอื่น

การควบคุมการเข้าถึงมีความสัมพันธ์กับการควบคุมด้านอื่น แต่ไม่ควรนำรายละเอียดของข้อกำหนดเหล่านั้นมาเขียนซ้ำภายใต้ข้อ 5.2.3

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ประเด็น	ข้อกำหนดที่เกี่ยวข้อง
การเข้ารหัสและการจัดการกุญแจ	5.2.4
การบันทึกเหตุการณ์	5.2.6.4
การปกป้องข้อมูลบันทึกเหตุการณ์	5.2.6.5
การบันทึกกิจกรรมผู้ดูแลระบบ	5.2.6.6
การแบ่งแยกเครือข่าย	5.2.7.2
การจัดการเหตุการณ์	5.2.10

รายละเอียดของมาตรการดังกล่าวควรพิจารณาตามข้อกำหนดที่เกี่ยวข้องโดยตรง

บทสรุป

การควบคุมการเข้าถึงตามข้อ 5.2.3 ควรมุ่งให้การเข้าถึงบริการคลาวด์และข้อมูลถูกจำกัดเฉพาะผู้ที่ได้รับอนุญาต ภายในขอบเขตสิทธิที่เหมาะสม และสามารถบริหารจัดการบัญชีและสิทธิได้ตลอดช่วงเวลาที่มีความจำเป็นในการใช้งาน

การนำไปปฏิบัติควรพิจารณาความรับผิดชอบของ CSC และ CSP ตามข้อกำหนดแต่ละข้อ ลักษณะของบริการและระดับความเสี่ยง โดยสามารถใช้กระบวนการ ระบบ และหลักฐานที่องค์กรมีอยู่แล้วได้ หากสามารถแสดงการดำเนินงานตามข้อกำหนดได้อย่างเพียงพอ

สาระสำคัญสามารถสรุปได้ว่า

ผู้ใดควรเข้าถึงบริการหรือข้อมูลใด ได้รับสิทธิในระดับใด ใช้วิธีการเข้าสู่ระบบและการยืนยันตัวตนที่เหมาะสมหรือไม่ และเมื่อความจำเป็นหรือความเสี่ยงเปลี่ยนแปลง สามารถปรับเปลี่ยน ระงับ หรือยกเลิกการเข้าถึงได้อย่างเหมาะสมหรือไม่

แนวทางดังกล่าวช่วยให้ข้อ 5.2.3 สามารถประยุกต์ใช้กับบริการคลาวด์ที่มีรูปแบบและความสามารถแตกต่างกันได้ โดยไม่สร้างข้อกำหนดทางเทคนิคหรือภาระด้านเอกสารเพิ่มเติมเกินกว่าที่จำเป็น

5.2.4 การเข้ารหัส (Cryptography)

การเข้ารหัส (Cryptography) เป็นมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่มีความสำคัญในการปกป้องข้อมูลและระบบสารสนเทศ โดยช่วยลดความเสี่ยงจากการเข้าถึง การเปิดเผย การแก้ไข หรือการใช้งานข้อมูลโดยไม่ได้รับอนุญาต ผ่านการใช้กลไกทางคณิตศาสตร์และการบริหารจัดการกุญแจเข้ารหัสที่เหมาะสม ทั้งนี้ การเข้ารหัสสามารถนำมาใช้เพื่อสนับสนุนการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) การพิสูจน์ตัวตน (Authentication) และการปฏิเสธความรับผิด (Non-repudiation) ของข้อมูลและธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานสถิติแห่งชาติ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

สำหรับสภาพแวดล้อมระบบคลาวด์ การเข้ารหัสมีบทบาทสำคัญในการปกป้องข้อมูลทั้งขณะจัดเก็บ (Data at Rest) และขณะรับส่งข้อมูล (Data in Transit) รวมถึงช่วยสนับสนุนการกำกับดูแลข้อมูลและลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างไรก็ตาม ประสิทธิผลของมาตรการเข้ารหัสยังขึ้นอยู่กับการบริหารจัดการกุญแจเข้ารหัส การกำหนดสิทธิ์การเข้าถึง และการกำกับดูแลที่เหมาะสมตลอดวงจรชีวิตการใช้งาน

หมายเหตุ

การเข้ารหัสและการบริหารจัดการกุญแจในบริการคลาวด์อาจเป็นความรับผิดชอบร่วมระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ ทั้งนี้ ขอบเขตความรับผิดชอบอาจแตกต่างกันตามรูปแบบบริการคลาวด์และสถาปัตยกรรมของผู้ให้บริการ หน่วยงานควรพิจารณาหลักการแบ่งความรับผิดชอบ (Shared Responsibility Model) ประกอบการกำหนดมาตรการควบคุมที่เหมาะสม

5.2.4.1 นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม ข) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใด ๆ ผู้ใช้บริการคลาวด์ต้องตรวจสอบข้อมูลที่ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่ – ปฏิบัติตามข้อกำหนดด้านนโยบายของ ผู้ใช้บริการคลาวด์ – เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่น ๆ ที่ใช้โดยผู้ใช้บริการคลาวด์ – ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคล ที่ผู้ให้บริการคลาวด์ประมวลผล นอกจากนี้ ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถใด ๆ ที่ผู้ให้บริการคลาวด์มอบให้ซึ่งสามารถช่วยผู้ใช้บริการคลาวด์ในการใช้การเข้ารหัสดังกล่าว

วัตถุประสงค์

เพื่อกำหนดแนวทางและหลักเกณฑ์ในการใช้มาตรการควบคุมการเข้ารหัสสำหรับระบบคลาวด์ให้เหมาะสมกับประเภทข้อมูล ระดับความสำคัญของข้อมูล และผลการประเมินความเสี่ยงของหน่วยงาน เพื่อสนับสนุนการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และการปกป้องข้อมูลตลอดวงจรชีวิตการใช้งาน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ก) ผู้ใช้บริการคลาวด์ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มี ความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม

ข) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใด ๆ ผู้ใช้บริการคลาวด์ต้องตรวจสอบข้อมูลที่ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่

- ปฏิบัติตามข้อกำหนดด้านนโยบายของ ผู้ใช้บริการคลาวด์
- เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่น ๆ ที่ใช้โดยผู้ใช้บริการคลาวด์
- ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์

โดยควรดำเนินการดังต่อไปนี้

1. การกำหนดนโยบายการเข้ารหัส (Cryptographic Policy Definition)

หน่วยงานควรกำหนดนโยบายการเข้ารหัสสำหรับข้อมูลและระบบสารสนเทศบนระบบคลาวด์อย่างชัดเจน โดยพิจารณาตามระดับชั้นข้อมูล (Data Classification) ระดับผลกระทบของระบบสารสนเทศ และผลการประเมินความเสี่ยง

อย่างน้อยควรครอบคลุมรายละเอียดดังต่อไปนี้

1. ข้อมูลประเภทใดต้องได้รับการเข้ารหัส
2. ช่วงเวลาที่ต้องใช้การเข้ารหัส
3. มาตรฐานอัลกอริทึมที่อนุญาต
4. ความยาวกุญแจขั้นต่ำ
5. แนวทางการจัดการกุญแจเข้ารหัส
6. บทบาทและผู้รับผิดชอบ

ตัวอย่าง

ระดับข้อมูล	**แนวทาง**
Public	พิจารณาตามความเหมาะสม
Internal	เข้ารหัสระหว่างรับส่ง
Confidential	เข้ารหัสขณะจัดเก็บและรับส่ง
Restricted	เข้ารหัสร่วมกับ Customer Managed Key

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

การใช้มาตรการเข้ารหัสกับข้อมูลทุกประเภทในระดับเดียวกันอาจส่งผลต่อประสิทธิภาพและต้นทุนโดยไม่จำเป็น การกำหนดนโยบายตามระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถเลือกใช้มาตรการป้องกันได้เหมาะสมและสอดคล้องกับบริบทของข้อมูล

2. การเข้ารหัสข้อมูลขณะจัดเก็บ (Encryption at Rest)

หน่วยงานควรเปิดใช้งานการเข้ารหัสสำหรับข้อมูลที่จัดเก็บอยู่บนบริการคลาวด์ เช่น

- ฐานข้อมูล (Database)
- พื้นที่จัดเก็บวัตถุ (Object Storage)
- ดิสก์เสมือน (Virtual Disk)
- ระบบสำรองข้อมูล (Backup Storage)
- Snapshot และ Replica

โดยควรใช้อัลกอริทึมมาตรฐานที่ได้รับการยอมรับในระดับสากล และหลีกเลี่ยงอัลกอริทึมที่ล้าสมัยหรือยุติการใช้งานแล้ว

สำหรับข้อมูลที่มีผลกระทบระดับสูง อาจพิจารณาใช้กุญแจเข้ารหัสที่ผู้ใช้บริการเป็นผู้บริหารจัดการเอง (Customer Managed Key)

เหตุผลและความจำเป็น (Rationale)

การเปิดใช้มาตรการเข้ารหัสข้อมูลขณะจัดเก็บจะช่วยลดความเสี่ยงกรณีเกิดการเข้าถึงสื่อบันทึกข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลจากผู้ปฏิบัติงานภายใน หรือการสูญหายของสื่อบันทึกข้อมูล

3. การเข้ารหัสข้อมูลขณะรับส่ง (Encryption in Transit)

1. ใช้โพรโทคอล TLS เวอร์ชันที่ยังได้รับการสนับสนุนและเป็นไปตามมาตรฐานปัจจุบันของหน่วยงาน (เช่น TLS 1.3 หรือใหม่กว่า)
2. ใช้ใบรับรองอิเล็กทรอนิกส์จากหน่วยงานออกใบรับรองที่เชื่อถือได้
3. ปิดใช้งาน Cipher Suite ที่ล้าสมัยหรือมีความเสี่ยง
4. ป้องกันการใช้โพรโทคอลหรือวิธีการเข้ารหัสที่ไม่มั่นคงปลอดภัย

เหตุผลและความจำเป็น (Rationale)

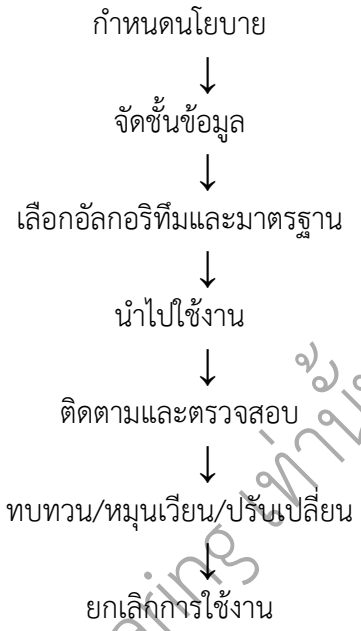
การรับส่งข้อมูลผ่านเครือข่ายโดยไม่มีการเข้ารหัสอาจทำให้ข้อมูลถูกดักรับ แก้ไข หรือปลอมแปลงระหว่างทางได้ ส่งผลกระทบต่อทั้งความลับและความถูกต้องครบถ้วนของข้อมูล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. การบริหารจัดการมาตรการเข้ารหัสตลอดวงจรชีวิต (Cryptographic Control Lifecycle)

หน่วยงานควรบริหารจัดการมาตรการเข้ารหัสตลอดวงจรชีวิต ตั้งแต่การกำหนดนโยบาย การเลือกเทคโนโลยี การนำไปใช้งาน การติดตามตรวจสอบ และการยกเลิกหรือเปลี่ยนอัลกอริทึมเมื่อหมดความเหมาะสม

ตัวอย่างวงจรชีวิตสามารถแสดงได้ดังนี้



คำอธิบายวงจรชีวิต

ขั้นตอน	**คำอธิบาย**
กำหนดนโยบาย	ระบุข้อกำหนดและความรับผิดชอบ
จัดชั้นข้อมูล	พิจารณาความสำคัญของข้อมูล
เลือกเทคโนโลยี	กำหนดมาตรฐานและอัลกอริทึม
นำไปใช้งาน	เปิดใช้มาตรการบนระบบจริง
ติดตามตรวจสอบ	ตรวจสอบการตั้งค่าและการใช้งาน
ทบทวน/ปรับเปลี่ยน	ประเมินความเหมาะสมและเปลี่ยนอัลกอริทึมหรือมาตรการเมื่อจำเป็น
ยกเลิก	ถอนระบบที่หมดความมั่นคงปลอดภัย

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคล ที่ผู้ให้บริการคลาวด์ประมวลผล นอกจากนี้ ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถใด ๆ ที่ผู้ให้บริการคลาวด์มอบให้ซึ่งสามารถช่วยผู้ใช้บริการคลาวด์ในการใช้การเข้ารหัสดังกล่าว

โดยควรดำเนินการดังต่อไปนี้

1. การเปิดเผยข้อมูลความสามารถด้านการเข้ารหัส (Cryptographic Capability Disclosure)

ผู้ให้บริการคลาวด์ควรจัดทำเอกสารหรือช่องทางเผยแพร่ข้อมูลเกี่ยวกับความสามารถด้านการเข้ารหัสของบริการอย่างชัดเจน เพื่อให้ผู้ใช้บริการสามารถประเมินความเหมาะสมและความสอดคล้องกับข้อกำหนดของหน่วยงานผู้ใช้บริการได้

อย่างน้อยควรครอบคลุมข้อมูลดังต่อไปนี้

1. อัลกอริทึมที่ระบบรองรับ
2. ความยาวกุญแจที่รองรับ
3. โพรโทคอลที่ใช้สำหรับการรับส่งข้อมูล
4. วิธีการจัดเก็บกุญแจเข้ารหัส
5. กลไกการบริหารจัดการกุญแจ
6. ข้อจำกัดของบริการ
7. ความสามารถในการทำงานร่วมกับระบบของผู้ใช้บริการ

ตัวอย่างข้อมูลที่ควรเปิดเผย

รายการ	**ตัวอย่าง**
Encryption Algorithm	AES-256
Key Management	Customer Managed Key
Transport Encryption	TLS
Certificate Support	Managed Certificate
HSM Support	Supported
Rotation Capability	Automatic

ร่างเอกสาร Public Hearing เท่านั้น - ห้ามอ้างอิง

เหตุผลและความจำเป็น (Rationale)

ผู้ใช้บริการไม่สามารถประเมินความเสี่ยงหรือกำหนดมาตรการควบคุมเพิ่มเติมได้ หากไม่ทราบว่าบริการคลาวด์ใช้กลไกการเข้ารหัสใด การเปิดเผยข้อมูลอย่างโปร่งใสจึงเป็นพื้นฐานสำคัญของการบริหารความเสี่ยงและการกำกับดูแล

2. การสนับสนุนมาตรฐานการเข้ารหัสที่เป็นปัจจุบัน (Current Cryptographic Standard Support)

ผู้ให้บริการคลาวด์ควรสนับสนุนมาตรฐานการเข้ารหัสที่ได้รับการยอมรับในระดับสากล และควรมีแผนบริหารจัดการการเลิกใช้งานอัลกอริทึมหรือโพรโทคอลที่มีความเสี่ยงหรือหมดความเหมาะสม ดังต่อไปนี้

- ทบทวนมาตรฐานการเข้ารหัสเป็นระยะ
- ยกเลิกการใช้โพรโทคอลล้าสมัย
- แจ้งเตือนลูกค้าล่วงหน้าเมื่อมีการเปลี่ยนแปลง
- จัดเตรียมระยะเวลาเปลี่ยนผ่านอย่างเหมาะสม

ควรหลีกเลี่ยงอัลกอริทึม ฟังก์ชันเข้ารหัส หรือโพรโทคอลที่ล้าสมัยหรือไม่เป็นไปตามมาตรฐานที่ได้รับการยอมรับในปัจจุบัน

ตัวอย่างอัลกอริทึม ฟังก์ชันเข้ารหัส หรือโพรโทคอลที่ควรยุติหรือหลีกเลี่ยง

อัลกอริทึม	**สถานะ**
DES	ห้ามใช้งาน
3DES	ควรยุติ (ห้ามใช้งานในการเข้ารหัส)
RC4	ห้ามใช้งาน
SHA-1	ห้ามใช้งาน (ยกเว้นใช้งานเพื่อตรวจสอบลายมือชื่อดิจิทัล)
SSL	ไม่ควรใช้งาน

เหตุผลและความจำเป็น (Rationale)

มาตรฐานการเข้ารหัสมีการเปลี่ยนแปลงอย่างต่อเนื่อง อัลกอริทึมที่เคยมีความมั่นคงปลอดภัยอาจไม่เพียงพอต่อภัยคุกคามในปัจจุบัน หากไม่มีการปรับปรุงอย่างต่อเนื่อง อาจเกิดความเสี่ยงต่อการถูกถอดรหัสหรือโจมตีได้

3. การสนับสนุนการทำงานร่วมกับมาตรการเข้ารหัสของผู้ใช้บริการ (Interoperability Support)

ผู้ให้บริการคลาวด์ควรสนับสนุนการทำงานร่วมกับมาตรการเข้ารหัสของผู้ใช้บริการ เพื่อหลีกเลี่ยงการผูกติดกับเทคโนโลยีของผู้ให้บริการรายเดียว (Vendor Lock-in)

ตัวอย่างแนวทาง

- รองรับการนำกุญแจเข้ารหัสของผู้ใช้บริการมาใช้งาน (Bring Your Own Key: BYOK)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- รองรับ Customer Managed Key
- รองรับมาตรฐาน API แบบเปิด
- รองรับการนำกุญแจออกเมื่อย้ายบริการ

เหตุผลและความจำเป็น (Rationale)

หากระบบเข้ารหัสผูกติดกับเทคโนโลยีเฉพาะของผู้ให้บริการ ผู้ใช้บริการอาจประสบข้อจำกัดในการย้ายระบบหรือเปลี่ยนผู้ให้บริการในอนาคต ส่งผลต่อความต่อเนื่องในการดำเนินงานและการกำกับดูแลข้อมูล

4. ความสามารถในการติดตามและตรวจสอบการใช้งานด้านการเข้ารหัส (Cryptographic Monitoring and Audit Capability)

ผู้ให้บริการคลาวด์ควรจัดเตรียมความสามารถในการบันทึกและติดตามกิจกรรมที่เกี่ยวข้องกับการใช้งานมาตรการเข้ารหัส

อย่างน้อยควรครอบคลุม

1. การสร้างกุญแจ
2. การใช้งานกุญแจ
3. การเปลี่ยนกุญแจ
4. การลบกุญแจ
5. การเปลี่ยนแปลงการตั้งค่า
6. การร้องขอสิทธิ์เข้าถึง

เหตุผลและความจำเป็น (Rationale)

บันทึกเหตุการณ์ด้านการเข้ารหัสมีความสำคัญต่อการตรวจสอบย้อนหลัง การสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และการพิสูจน์การปฏิบัติตามข้อกำหนดทางกฎหมาย

ตัวอย่างแนวทางการดำเนินการของผู้ให้บริการคลาวด์

ประเด็น	แนวทางการดำเนินการ
Cryptographic Disclosure	เปิดเผยอัลกอริทึมและมาตรฐาน
Algorithm Lifecycle	มีแผนเลิกใช้งานอัลกอริทึมล้าสมัย
BYOK Support	รองรับการนำกุญแจของลูกค้า
Audit Capability	มี Log และ Dashboard
Certificate Service	รองรับบริการจัดการใบรับรอง

ร่างเพื่อรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

โดยควรดำเนินการดังต่อไปนี้

1. การจัดการวงจรชีวิตใบรับรองอิเล็กทรอนิกส์ (Certificate Lifecycle Management)

หน่วยงานควรกำหนดมาตรการบริหารจัดการใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) อย่างเหมาะสม เพื่อสนับสนุนความมั่นคงปลอดภัยในการรับส่งข้อมูล

หน่วยงานควรบริหารจัดการวงจรชีวิตใบรับรองตั้งแต่การร้องขอ การติดตั้ง การใช้งาน การติดตามอายุ และการยกเลิกใช้งาน



คำอธิบายวงจรชีวิต

ขั้นตอน	คำอธิบาย
Request	ร้องขอใบรับรอง
Validation	ตรวจสอบความถูกต้อง
Issuance	ออกใบรับรอง
Deployment	ติดตั้งเข้าสู่ระบบ
Monitoring	ติดตามอายุ การหมดอายุ และสถานะของใบรับรอง
Renewal	ต่ออายุ
Revocation	ยกเลิกหรือเพิกถอน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

แนวทางการดำเนินการ

- ใช้ระบบติดตามวันหมดอายุแบบอัตโนมัติ
- ตั้งค่าการแจ้งเตือนล่วงหน้า
- ใช้ระบบต่ออายุอัตโนมัติเมื่อเหมาะสม
- จัดทำทะเบียนใบรับรองกลางของหน่วยงาน

เหตุผลและความจำเป็น (Rationale)

ปัญหาใบรับรองหมดอายุเป็นสาเหตุที่พบได้บ่อยและอาจทำให้ระบบสำคัญหยุดชะงักโดยไม่จำเป็น

2. การเตรียมความพร้อมด้านความคล่องตัวทางรหัสลับ (Crypto-Agility)

หน่วยงานควรออกแบบระบบให้สามารถเปลี่ยนอัลกอริทึมหรือกลไกเข้ารหัสได้ในอนาคตโดยไม่ต้องปรับเปลี่ยนระบบทั้งหมด

ควรดำเนินการดังต่อไปนี้

- แยกชั้นการทำงานของระบบเข้ารหัสออกจากระบบงาน
- หลีกเลี่ยงการฝังอัลกอริทึมไว้ใน Source Code โดยตรง
- ใช้มาตรฐานเปิด
- รองรับการอัปเดตอัลกอริทึม

เหตุผลและความจำเป็น (Rationale)

อัลกอริทึมที่มั่นคงปลอดภัยในปัจจุบันอาจไม่เพียงพอในอนาคต โดยเฉพาะเมื่อเทคโนโลยีการประมวลผลแบบควอนตัมพัฒนามากขึ้น

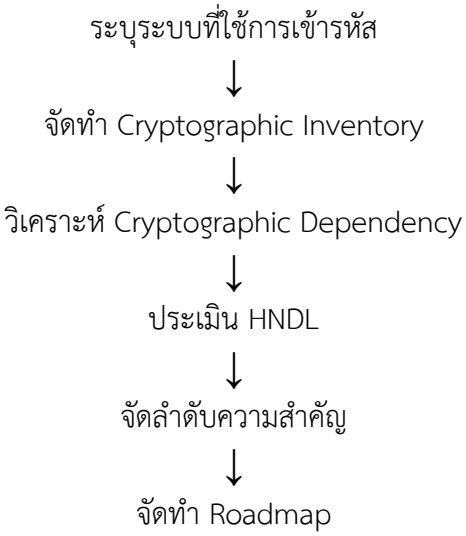
นอกจากนี้ หน่วยงานควรเตรียมความพร้อมสำหรับผลกระทบจากเทคโนโลยีการประมวลผลแบบควอนตัมที่อาจส่งผลต่ออัลกอริทึมการเข้ารหัสแบบดั้งเดิม โดยเฉพาะอัลกอริทึมกุญแจสาธารณะ (Public Key Cryptography) เพื่อให้สามารถวางแผนและบริหารความเสี่ยงได้ล่วงหน้า

ควรดำเนินการดังต่อไปนี้

1. อ้างอิงบัญชีรายการการใช้งานการเข้ารหัส (Cryptographic Inventory) ที่หน่วยงานจัดทำไว้ เพื่อใช้ในการประเมินผลกระทบ
2. ระบุระบบ ข้อมูล หรือบริการที่ต้องการการปกป้องระยะยาว
3. ประเมินผลกระทบจากภัยคุกคามแบบ Harvest Now, Decrypt Later (HNDL)
4. ประเมินการพึ่งพาองค์ประกอบด้านการเข้ารหัส (Cryptographic Dependency)
5. จัดลำดับความสำคัญของระบบตามผลกระทบและระยะเวลาการคุ้มครองข้อมูล
6. จัดทำ Roadmap สำหรับการเปลี่ยนผ่านในอนาคต

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างกระบวนการเตรียมความพร้อม



คำอธิบาย

ขั้นตอน	**รายละเอียด**
System Identification	ระบุระบบและองค์ประกอบที่ใช้การเข้ารหัส
Inventory	จัดทำบัญชีรายการการใช้งานการเข้ารหัส
Dependency Analysis	ระบุการพึ่งพาระบบเข้ารหัส
Risk Assessment	ประเมินความเสี่ยง HNDL
Prioritization	จัดลำดับความสำคัญ
Roadmap	จัดทำแผนเปลี่ยนผ่าน

เหตุผลและความจำเป็น (Rationale)

การเตรียมความพร้อมล่วงหน้าช่วยให้หน่วยงานเข้าใจผลกระทบของการเปลี่ยนแปลงมาตรฐานการเข้ารหัส ลดความซับซ้อนและต้นทุนในการเปลี่ยนผ่านในอนาคต

3. แนวปฏิบัติที่เหมาะสมและไม่เหมาะสมด้านการเข้ารหัส

แนวปฏิบัติที่เหมาะสม	**แนวปฏิบัติที่ไม่เหมาะสม**
เปิดใช้การเข้ารหัสข้อมูลขณะจัดเก็บ	จัดเก็บข้อมูลสำคัญแบบไม่เข้ารหัส
ใช้ TLS ที่เป็นมาตรฐานปัจจุบัน	ใช้ SSL/TLS ที่ล้าสมัย
ใช้ใบรับรองที่เชื่อถือได้	ใช้ Self-Signed ในระบบสำคัญ
ทบทวนมาตรฐานการเข้ารหัสเป็นระยะ	ใช้อัลกอริทึมหมดความเหมาะสม
ประเมินค่าตั้งต้นของผู้ให้บริการ	ใช้งานค่า Default โดยไม่ทบทวน

เอกสารสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. เกณฑ์การคัดเลือกผู้ให้บริการ (Selection Criteria)

ในการจัดซื้อจัดจ้างหรือคัดเลือกบริการคลาวด์ หน่วยงานควรพิจารณาความสามารถด้านการเข้ารหัสของผู้ให้บริการให้สอดคล้องกับประเภทข้อมูล ระดับผลกระทบ ผลการประเมินความเสี่ยง และข้อกำหนดของหน่วยงาน โดยสามารถพิจารณาแนวทางเพิ่มเติมตามภาคผนวก ก

เหตุผลและความจำเป็น (Rationale)

การเลือกผู้ให้บริการคลาวด์โดยพิจารณาเฉพาะคุณลักษณะการให้บริการหรือค่าใช้จ่าย อาจไม่เพียงพอต่อการปกป้องข้อมูลและการบริหารความเสี่ยงด้านการเข้ารหัส การกำหนดเกณฑ์การประเมินที่ชัดเจนจะช่วยให้หน่วยงานสามารถเปรียบเทียบและคัดเลือกผู้ให้บริการที่สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยและการกำกับดูแลได้อย่างเหมาะสม

5. กระบวนการยกเว้นการใช้มาตรการเข้ารหัส (Cryptographic Exception Process)

ในบางกรณี หน่วยงานอาจมีความจำเป็นต้องใช้งานอัลกอริทึม โพรโทคอล หรือมาตรการเข้ารหัสที่ไม่เป็นไปตามมาตรฐานปัจจุบัน เช่น ระบบเดิม (Legacy System) หรือข้อจำกัดด้านความเข้ากันได้

การดำเนินการดังกล่าวควรอยู่ภายใต้กระบวนการควบคุมอย่างเป็นทางการ ดังต่อไปนี้

1. จัดทำการประเมินความเสี่ยง
2. ระบุเหตุผลและความจำเป็น
3. กำหนดมาตรการควบคุมชดเชย (Compensating Controls)
4. กำหนดระยะเวลาการใช้งาน
5. ได้รับอนุมัติจากผู้มีอำนาจ
6. ทบทวนเป็นระยะ

ตัวอย่างการยกเว้นการใช้มาตรการเข้ารหัส

รายการ	**ตัวอย่าง**
Exception	ใช้ TLS รุ่นเก่า
เหตุผล	ระบบเดิมไม่รองรับ
มาตรการชดเชย	Network Segmentation
ผู้อนุมัติ	CISO
วันหมดอายุ	31 ธันวาคม 2570

เหตุผลและความจำเป็น (Rationale)

หลายหน่วยงานยังมีระบบเดิมที่ไม่สามารถเปลี่ยนแปลงได้ทันที การกำหนดกระบวนการยกเว้นอย่างเป็นระบบช่วยลดความเสี่ยงและเพิ่มความสามารถในการกำกับดูแล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

6. ข้อผิดพลาดและความเสี่ยงด้านการเข้ารหัสที่พบบ่อย (Common Cryptographic Misconfigurations and Risks)

หน่วยงานควรตระหนักถึงข้อผิดพลาดและความเสี่ยงที่อาจเกิดขึ้นจากการกำหนดค่า การเลือกใช้งาน และการบริหารจัดการมาตรการเข้ารหัสบนระบบคลาวด์ ซึ่งอาจส่งผลกระทบต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) รวมถึงการปฏิบัติตามข้อกำหนดด้านกฎหมายและการกำกับดูแลที่เกี่ยวข้อง

ตัวอย่างความเสี่ยงที่พบบ่อย มีดังนี้

6.1 ไม่เปิดใช้การเข้ารหัสข้อมูลขณะจัดเก็บ (Missing Encryption at Rest)

ข้อมูลสำคัญถูกจัดเก็บโดยไม่มีการเปิดใช้มาตรการเข้ารหัส ส่งผลให้ข้อมูลอาจถูกเข้าถึง เปิดเผย หรือถูกนำไปใช้งานได้ หากเกิดเหตุการณ์ข้อมูลรั่วไหลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

ผลกระทบ

- การเปิดเผยข้อมูลสำคัญ
- ความเสี่ยงต่อข้อมูลส่วนบุคคล
- ไม่สอดคล้องตามข้อกำหนดหรือกฎหมายที่เกี่ยวข้อง

6.2 ใช้โพรโทคอลหรืออัลกอริทึมที่ล้าสมัย (Use of Weak or Deprecated Algorithms)

มีการใช้งานอัลกอริทึมหรือโพรโทคอลที่มีความเสี่ยงหรือหมดความเหมาะสม เช่น SSL, DES, RC4, SHA-1 หรือ Cipher Suite ที่ไม่เป็นไปตามมาตรฐานปัจจุบัน

ผลกระทบ

- เพิ่มโอกาสการถูกโจมตีหรือถอดรหัส
- ลดระดับความมั่นคงปลอดภัยของระบบ
- อาจไม่ผ่านข้อกำหนดการตรวจประเมิน

6.3 ใช้ใบรับรองอิเล็กทรอนิกส์อย่างไม่เหมาะสม (Improper Certificate Usage)

มีการใช้ใบรับรองอิเล็กทรอนิกส์ที่หมดอายุ ไม่น่าเชื่อถือ หรือใช้ใบรับรองแบบ Self-Signed กับระบบสำคัญโดยไม่มีเหตุผลรองรับและมาตรการควบคุมเพิ่มเติม

ผลกระทบ

- ระบบอาจไม่สามารถให้บริการได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- ผู้ใช้อาจไม่สามารถตรวจสอบความน่าเชื่อถือของระบบ
- เพิ่มความเสี่ยงต่อการปลอมแปลงตัวตน

6.4 ใช้ค่าตั้งต้นของผู้ให้บริการโดยไม่ประเมินความเหมาะสม (Unreviewed Default Security Settings)

มีการใช้งานค่าตั้งต้นด้านการเข้ารหัสของผู้ให้บริการคลาวด์โดยไม่ประเมินความเหมาะสมกับประเภทข้อมูล ความเสี่ยง หรือข้อกำหนดของหน่วยงาน

ผลกระทบ

- มาตรการป้องกันอาจไม่สอดคล้องกับระดับความเสี่ยง
- เพิ่มโอกาสการกำหนดค่าที่ไม่เหมาะสม
- อาจเกิดช่องว่างด้านการกำกับดูแล

6.5 เปิดเผยข้อมูลลับหรือข้อมูลกำหนดค่าในระบบควบคุมเวอร์ชัน (Exposure of Secrets in Source Code Repository)

มีการจัดเก็บข้อมูลลับ เช่น API Key, Access Token, Encryption Key หรือ Private Key ไว้ใน Source Code หรือระบบควบคุมเวอร์ชันโดยตรง

ผลกระทบ

- ข้อมูลลับอาจรั่วไหลสู่บุคคลที่ไม่ได้รับอนุญาต
- เพิ่มความเสี่ยงต่อการเข้าถึงระบบโดยมิชอบ
- อาจส่งผลกระทบต่อหลายระบบพร้อมกัน

6.6 ไม่มีการทบทวนความเหมาะสมของมาตรฐานการเข้ารหัสเป็นระยะ (Lack of Cryptographic Review)

ไม่มีการประเมินหรือทบทวนอัลกอริทึม โพรโทคอล หรือมาตรฐานการเข้ารหัสที่ใช้งานอยู่เป็นระยะ

ผลกระทบ

- ใช้งานมาตรการที่หมดความเหมาะสมโดยไม่ทราบ
- เพิ่มความเสี่ยงจากช่องโหว่ใหม่
- อาจไม่สอดคล้องกับมาตรฐานปัจจุบัน

6.7 ไม่เตรียมความพร้อมต่อการเปลี่ยนแปลงมาตรฐานการเข้ารหัสในอนาคต (Insufficient Cryptographic Transition Readiness)

ไม่มีการเตรียมความพร้อมสำหรับการเปลี่ยนผ่านมาตรฐานการเข้ารหัสในอนาคต หรือไม่มีการประเมินผลกระทบจากภัยคุกคามใหม่ เช่น การประมวลผลแบบควอนตัม

ร่างหลักเกณฑ์สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผลกระทบ

- ข้อมูลที่ต้องปกป้องระยะยาวอาจมีความเสี่ยง
- เพิ่มความเสี่ยงจากภัยคุกคามแบบ Harvest Now, Decrypt Later (HNDL)
- เพิ่มต้นทุนและผลกระทบในการเปลี่ยนผ่านในอนาคต

ตัวอย่างสรุปความเสี่ยง

ประเด็น	**ผลกระทบ**
Encryption Disabled	ข้อมูลรั่วไหล
Weak Algorithm	ถูกโจมตี
Improper Certificate Usage	ระบบหยุดชะงัก
Default Settings	การกำหนดค่าไม่เหมาะสม
Secret Exposure	เปิดเผยข้อมูลลับ
Lack of Review	ใช้มาตรฐานล้าสมัย
No PQC Readiness	ความเสี่ยงระยะยาว

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.2.4.2 การจัดการกุญแจ (Key Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์ – ประเภทของกุญแจ – ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัส เช่น การสร้าง เปลี่ยนแปลง หรือปรับปรุง จัดเก็บ หมดอายุการใช้งาน เรียกคืน เก็บรักษา และทำลาย – ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์	

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ค) ผู้ใช้บริการคลาวด์ต้องไม่อนุญาตให้ ผู้ให้บริการคลาวด์ จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัสเมื่อผู้ใช้บริการคลาวด์ ใช้กุญแจเข้ารหัสของตนเอง	

วัตถุประสงค์ (Objective)

เพื่อกำหนดแนวทางในการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key) ตลอดวงจรชีวิตอย่างเหมาะสม ตั้งแต่การสร้าง การจัดเก็บ การสำรองและกู้คืน การแจกจ่าย การใช้งาน การติดตามตรวจสอบ การหมุนเวียน การเพิกถอน และการทำลาย เพื่อป้องกันการเข้าถึงหรือการใช้งานกุญแจโดยไม่ได้รับอนุญาต และลดความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ก) ผู้ใช้บริการคลาวด์ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ

ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์

- ประเภทของกุญแจ
- ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัส เช่น การสร้าง เปลี่ยนแปลง หรือปรับปรุง จัดเก็บ หมดอายุการใช้งาน เรียกคืน เก็บรักษา และทำลาย
- ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์

ค) ผู้ใช้บริการคลาวด์ต้องไม่อนุญาตให้ ผู้ให้บริการคลาวด์ จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัสเมื่อผู้ใช้บริการคลาวด์ ใช้กุญแจเข้ารหัสของตนเอง

คำอธิบายเพิ่มเติมข้อ ค)

ข้อกำหนดนี้มีวัตถุประสงค์เพื่อให้ผู้ใช้บริการคลาวด์ยังคงสามารถรักษาการควบคุมกุญแจเข้ารหัสของตนเองได้อย่างเหมาะสม ทั้งนี้ หน่วยงานควรพิจารณารูปแบบการจัดการกุญแจของผู้ให้บริการ เช่น Bring Your Own Key (BYOK), Customer Managed Key (CMK) หรือ Hold Your Own Key (HYOK) รวมถึงขอบเขตการมีส่วนเกี่ยวข้องของผู้ให้บริการ เพื่อให้สอดคล้องกับข้อกำหนดด้านกฎหมาย ระดับความเสี่ยง และความต้องการด้านการกำกับดูแลข้อมูลของหน่วยงาน

เอกสารสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานอื่น

โดยควรดำเนินการดังต่อไปนี้

1. การบริหารจัดการกุญแจตลอดวงจรชีวิต (Cryptographic Key Lifecycle Management)

หน่วยงานควรบริหารจัดการกุญแจเข้ารหัสตลอดวงจรชีวิต ตั้งแต่การสร้าง การจัดเก็บ การสำรองและกู้คืน การแจกจ่าย การใช้งาน การติดตามตรวจสอบ การหมุนเวียน การเพิกถอน และการทำลาย เพื่อให้สามารถควบคุมการเข้าถึงและลดความเสี่ยงจากการรั่วไหลของกุญแจได้อย่างเหมาะสม



ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

คำอธิบายวงจรชีวิต

ขั้นตอน	คำอธิบาย
Generation	สร้างกุญแจโดยใช้แหล่งสุ่มที่มั่นคงปลอดภัย
Secure Storage	จัดเก็บในระบบที่มีการป้องกัน
Backup/Recovery	สำรองและกู้คืนกุญแจอย่างมั่นคงปลอดภัย
Distribution	ควบคุมการกระจายกุญแจ
Usage	ใช้งานตามวัตถุประสงค์
Monitoring	ติดตาม ตรวจสอบ และบันทึกกิจกรรมที่เกี่ยวข้องกับการใช้งานกุญแจ
Rotation	เปลี่ยนกุญแจตามระยะเวลา
Revocation	ยกเลิกสิทธิ์
Destruction	ทำลายอย่างมั่นคงปลอดภัย

2. การแยกกุญแจออกจากข้อมูล (Key Separation)

หน่วยงานควรแยกกุญแจเข้ารหัสออกจากข้อมูลที่ถูกเข้ารหัสอย่างชัดเจน และไม่ควรจัดเก็บไว้ในพื้นที่เดียวกัน

ตัวอย่างแนวทางที่เหมาะสม

องค์ประกอบ	ตำแหน่ง
ข้อมูล	Storage Service
กุญแจ	Key Management Service
Secret	Secret Vault

เหตุผลและความจำเป็น (Rationale)

หากผู้ไม่หวังดีเข้าถึงข้อมูลและกุญแจได้จากแหล่งเดียวกัน มาตรการเข้ารหัสอาจไม่สามารถปกป้องข้อมูลได้อย่างมีประสิทธิภาพ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การกำหนดกระบวนการจัดการกุญแจ (Key Management Procedures)

หน่วยงานควรกำหนดกระบวนการบริหารจัดการกุญแจอย่างเป็นทางการ และกำหนดผู้รับผิดชอบอย่างชัดเจน อย่างน้อยควรครอบคลุม

1. การสร้างกุญแจ
2. การอนุมัติการใช้งาน
3. การแจกจ่าย
4. การสำรองข้อมูลกุญแจ
5. การกู้คืนกุญแจ
6. การหมุนเวียน
7. การเพิกถอน
8. การทำลาย

เหตุผลและความจำเป็น (Rationale)

การจัดการกุญแจที่ไม่มีขั้นตอนหรือไม่มีผู้รับผิดชอบชัดเจน อาจทำให้เกิดความเสี่ยงจากการสูญหาย การใช้งานผิดวัตถุประสงค์ หรือการเข้าถึงโดยไม่ได้รับอนุญาต

4. การใช้กุญแจที่ผู้ใช้บริการบริหารจัดการเอง (Customer Managed Key / BYOK)

สำหรับข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือระบบที่มีผลกระทบระดับสูง หน่วยงานอาจพิจารณาใช้ Customer Managed Key (CMK), BYOK หรือ HYOK ตามระดับความต้องการด้านการควบคุม

ภายใต้แนวทางดังกล่าว หน่วยงานอาจเป็นผู้สร้างหรือควบคุมกุญแจเข้ารหัสด้วยตนเอง และนำกุญแจหรือองค์ประกอบของกุญแจไปใช้ร่วมกับบริการของผู้ให้บริการคลาวด์ ทั้งนี้รูปแบบการควบคุมอาจแตกต่างกันตามสถาปัตยกรรมของผู้ให้บริการ

เหตุผลและความจำเป็น (Rationale)

การใช้ Customer Managed Key ช่วยให้หน่วยงานมีสิทธิ์ควบคุมการเข้าถึงข้อมูลได้มากขึ้น ลดความเสี่ยงด้านการกำกับดูแลข้อมูล และช่วยสนับสนุนหลักการอธิปไตยของข้อมูล (Data Sovereignty)

5. การจัดทำบัญชีรายการการใช้งานการเข้ารหัสและกุญแจ (Cryptographic Inventory)

หน่วยงานควรจัดทำบัญชีรายการการใช้งานการเข้ารหัสและกุญแจ (Cryptographic Inventory) เพื่อให้สามารถระบุ ติดตาม และประเมินผลกระทบจากการใช้งานอัลกอริทึม กุญแจ ระบบ และองค์ประกอบด้านการเข้ารหัสที่เกี่ยวข้อง รวมถึงรองรับการเปลี่ยนแปลงมาตรฐานหรือการเปลี่ยนผ่านสู่ Post-Quantum Cryptography ในอนาคต อย่างน้อยควรระบุ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

รายการ	ตัวอย่าง
ระบบ	Citizen Portal
Algorithm	AES-256
Storage Location	KMS
Rotation Period	พิจารณาตามความเสี่ยง ลักษณะการใช้งาน และข้อกำหนดของหน่วยงาน
Impact Level	สูง
Data Type	Personal Data
Cryptographic Dependency	TLS / PKI / HSM
Key Type	Symmetric / Asymmetric
System Owner	เจ้าของระบบ
Key Custodian	ผู้ดูแลกุญแจ
Retention Requirement	10 ปี

เหตุผลและความจำเป็น (Rationale)

หลายหน่วยงานไม่สามารถระบุได้ว่ามีการใช้งานอัลกอริทึม กุญแจ หรือองค์ประกอบด้านการเข้ารหัสอยู่ในระบบใดบ้าง ส่งผลให้การปรับปรุงมาตรฐาน การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย และการเปลี่ยนผ่านสู่เทคโนโลยีการเข้ารหัสในอนาคตทำได้ยาก

ตัวอย่างแนวปฏิบัติที่เหมาะสมและไม่เหมาะสม

แนวปฏิบัติที่เหมาะสม	แนวปฏิบัติที่ไม่เหมาะสม
ใช้ KMS หรือ HSM	เก็บกุญแจไว้ใน Source Code
หมุนเวียนกุญแจอัตโนมัติ	ใช้กุญแจเดิมหลายปี
แยกกุญแจออกจากข้อมูล	เก็บทุกอย่างไว้ระบบเดียว
จำกัดสิทธิ์เข้าถึง	ให้สิทธิ์ผู้ใช้ทั่วไปเข้าถึงกุญแจ

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

สำหรับหัวข้อนี้ แม้ไม่ได้กำหนดข้อกำหนดเฉพาะสำหรับผู้ให้บริการคลาวด์ไว้โดยตรง อย่างไรก็ตาม ผู้ให้บริการคลาวด์ควรพิจารณาดำเนินการดังต่อไปนี้

1. มาตรฐานความมั่นคงปลอดภัยของระบบจัดการกุญแจ (Secure Key Management Infrastructure)

ผู้ให้บริการคลาวด์ควรจัดให้มีระบบบริหารจัดการกุญแจ (Key Management Service: KMS) ที่มีมาตรการป้องกันด้านเทคนิคและกายภาพอย่างเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

สำหรับระบบหรือบริการที่เกี่ยวข้องกับกุญแจหลัก (Master Key) ควรพิจารณาใช้อุปกรณ์ความมั่นคงปลอดภัยฮาร์ดแวร์ (Hardware Security Module: HSM)

อย่างน้อยควรมีความสามารถดังต่อไปนี้

1. การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
2. การแยกส่วนกุญแจระหว่างผู้ใช้บริการ
3. การควบคุมสิทธิ์เข้าถึง
4. การตรวจสอบกิจกรรมย้อนหลัง
5. การป้องกันการแก้ไขหรือดึงกุญแจออกโดยมิชอบ

เหตุผลและความจำเป็น (Rationale)

การจัดเก็บกุญแจเข้ารหัสโดยไม่มีมาตรการป้องกันที่เหมาะสมอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล

2. ความโปร่งใสของวงจรชีวิตกุญแจ (Key Lifecycle Transparency)

ผู้ให้บริการควรเปิดเผยข้อมูลเกี่ยวกับกระบวนการจัดการกุญแจตลอดวงจรชีวิต เพื่อให้ผู้ใช้บริการสามารถประเมินความเสี่ยงและความสอดคล้องตามข้อกำหนดของหน่วยงานผู้ใช้บริการ

อย่างน้อยควรเปิดเผยข้อมูลต่อไปนี้

หัวข้อ	**รายละเอียด**
Key Generation	วิธีการสร้างกุญแจ
Storage	วิธีการจัดเก็บ
Rotation	การหมุนเวียน
Backup	การสำรอง
Revocation	การเพิกถอน
Destruction	การทำลาย

เหตุผลและความจำเป็น (Rationale)

ผู้ใช้บริการควรทราบว่ากุญแจที่ใช้ปกป้องข้อมูลถูกจัดการอย่างไร เพื่อใช้ในการบริหารความเสี่ยงและการตรวจสอบด้านการกำกับดูแล

3. การสนับสนุนรูปแบบการจัดการกุญแจของผู้ใช้บริการ (Customer Key Management Support)

ผู้ให้บริการควรสนับสนุนรูปแบบการจัดการกุญแจที่หลากหลาย เพื่อให้เหมาะสมกับข้อกำหนดด้านความมั่นคงปลอดภัยและการกำกับดูแลข้อมูล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างรูปแบบ

รูปแบบ	รายละเอียด
Provider Managed Key	ผู้ให้บริการบริหารจัดการ
Customer Managed Key	ลูกค้าควบคุมการใช้งาน
BYOK	นำกุญแจเข้ามาใช้งาน
HYOK	กุญแจอยู่ภายนอกระบบผู้ให้บริการ

เหตุผลและความจำเป็น (Rationale)

แต่ละหน่วยงานมีข้อกำหนดด้านกฎหมาย ความเสี่ยง และระดับการควบคุมข้อมูลแตกต่างกัน การรองรับหลายรูปแบบช่วยเพิ่มความยืดหยุ่นในการกำกับดูแล

4. ความสามารถด้านการติดตามและตรวจสอบ (Audit and Monitoring Capability)

ผู้ให้บริการควรจัดเตรียมบันทึกเหตุการณ์และความสามารถในการตรวจสอบกิจกรรมที่เกี่ยวข้องกับกุญแจ

อย่างน้อยควรบันทึก

- การสร้างกุญแจ
- การเรียกใช้งานกุญแจ
- การเปลี่ยนแปลงสิทธิ์
- การหมุนเวียน
- การลบ
- การเพิกถอน
- ความพยายามเข้าถึงที่ผิดปกติ

ตัวอย่างรายการบันทึก

เวลา	กิจกรรม	ผู้ดำเนินการ
10:01	Generate Key	Security Admin
10:15	Rotate Key	System
11:00	Delete Key	Key Custodian

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

การตรวจสอบย้อนหลังเป็นองค์ประกอบสำคัญของการสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัย การตรวจประเมิน และการพิสูจน์การปฏิบัติตามข้อกำหนด

5. การบริหารจัดการข้อมูลลับ (Secret Management)

หน่วยงานควรกำหนดมาตรการสำหรับการบริหารจัดการข้อมูลลับ (Secret) ที่ใช้ในการยืนยันตัวตน การเชื่อมต่อระบบ หรือการปกป้องระบบงาน เพื่อป้องกันการเปิดเผย การรั่วไหล หรือการนำไปใช้งานโดยไม่ได้รับอนุญาต

ตัวอย่างข้อมูลลับ เช่น

- API Key
- Access Token
- Password
- Private Key
- Database Credential
- Certificate Secret
- Encryption Key

ควรดำเนินการดังต่อไปนี้

1. จัดเก็บข้อมูลลับไว้ในระบบบริหารจัดการข้อมูลลับ (Secret Vault) หรือระบบที่มีการควบคุมการเข้าถึงอย่างเหมาะสม
2. หลีกเลี่ยงการจัดเก็บข้อมูลลับใน Source Code โปรแกรม ไฟล์กำหนดค่า หรือระบบควบคุมเวอร์ชัน
3. กำหนดสิทธิ์เข้าถึงตามหลักสิทธิ์เท่าที่จำเป็น (Least Privilege)
4. กำหนดอายุการใช้งานและการหมุนเวียนข้อมูลลับ
5. บันทึกและติดตามกิจกรรมที่เกี่ยวข้องกับข้อมูลลับ
6. จัดให้มีกระบวนการเพิกถอนหรือเปลี่ยนข้อมูลลับเมื่อสงสัยว่ามีการรั่วไหล

ตัวอย่างแนวทาง

แนวปฏิบัติที่เหมาะสม	แนวปฏิบัติที่ไม่เหมาะสม
ใช้ Secret Vault	เก็บ Password ใน Source Code
ใช้ Token อายุสั้น	ใช้ API Key แบบถาวร
หมุนเวียน Secret	ใช้ Credential เดิมหลายปี

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

การรั่วไหลของข้อมูลลับมักเป็นสาเหตุสำคัญของการเข้าถึงระบบโดยไม่ได้รับอนุญาต และอาจส่งผลกระทบต่อหลายระบบพร้อมกัน หากไม่มีมาตรการบริหารจัดการที่เหมาะสม

6. การสนับสนุนความคล่องตัวทางรหัสลับและการเปลี่ยนผ่านสู่ Post-Quantum Cryptography (Crypto-Agility and Post-Quantum Transition Support)

ผู้ให้บริการควรออกแบบระบบจัดการกุญแจให้สามารถรองรับการเปลี่ยนแปลงมาตรฐานการเข้ารหัสในอนาคต รวมถึงรองรับการเปลี่ยนผ่านสู่เทคโนโลยีหลังยุคควอนตัม (Post-Quantum Cryptography)

ควรพิจารณาดำเนินการดังต่อไปนี้

- รองรับการปรับเปลี่ยนหรือเปลี่ยนผ่านมาตรฐานและอัลกอริทึมการเข้ารหัสโดยไม่กระทบระบบทั้งหมด
- สนับสนุนความสามารถด้านความคล่องตัวทางรหัสลับ (Crypto-Agility) และรองรับการเปลี่ยนผ่านสู่เทคโนโลยีการเข้ารหัสยุคหลังควอนตัม (Post-Quantum Cryptography: PQC) รวมถึงแนวทาง Hybrid Cryptography ซึ่งหมายถึงการใช้อัลกอริทึมเดิมร่วมกับ Post-Quantum Cryptography ในช่วงเปลี่ยนผ่านเพื่อลดผลกระทบด้านความเข้ากันได้
- ลดการผูกติดกับกลไกเฉพาะของผู้ให้บริการ

เหตุผลและความจำเป็น (Rationale)

มาตรฐานด้านการเข้ารหัสมีการเปลี่ยนแปลงอย่างต่อเนื่อง การออกแบบระบบที่รองรับการปรับเปลี่ยนได้จะช่วยลดความเสี่ยงและต้นทุนในระยะยาว

ตัวอย่างแนวทางการดำเนินการของผู้ให้บริการคลาวด์

ประเด็น	แนวทางการดำเนินการ
HSM	มีระบบป้องกันกุญแจระดับฮาร์ดแวร์
BYOK	รองรับการนำกุญแจเข้ามาใช้งาน
HYOK	รองรับการควบคุมกุญแจภายนอก
Audit Logging	มีการติดตามกิจกรรม
Lifecycle Transparency	เปิดเผยวงจรชีวิตกุญแจ
PQC Readiness	มีแผนรองรับการเปลี่ยนผ่าน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้อ้างอิง

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines) โดยควรดำเนินการดังต่อไปนี้

1. การหมุนเวียนกุญแจอัตโนมัติ (Automated Key Rotation)

หน่วยงานควรกำหนดนโยบายและระยะเวลาการหมุนเวียนกุญแจเข้ารหัสอย่างเหมาะสมตามประเภทข้อมูล ระดับผลกระทบ และข้อกำหนดของหน่วยงาน

แนวทางการดำเนินการ

- ใช้ระบบ Key Management Service (KMS) เพื่อดำเนินการหมุนเวียนอัตโนมัติ
- กำหนดรอบการหมุนเวียนตามความเสี่ยง
- บันทึกและตรวจสอบประวัติการหมุนเวียน
- ทดสอบผลกระทบก่อนใช้งานจริง

ตัวอย่างระยะเวลาที่อาจพิจารณา

ประเภท	ตัวอย่าง
ข้อมูลทั่วไป	ทบทวนเป็นระยะ
กุญแจสำหรับข้อมูลสำคัญ	พิจารณาหมุนเวียนเป็นระยะตามความเสี่ยง หรือเมื่อเกิดเหตุการณ์สำคัญ เช่น บุคลากรเปลี่ยน สิทธิ์เปลี่ยน หรือสงสัยการรั่วไหล
กุญแจฉุกเฉิน	เปลี่ยนทันทีหลังใช้งาน
กุญแจชั่วคราว	อายุสั้น

เหตุผลและความจำเป็น (Rationale)

การใช้กุญแจเดิมเป็นเวลานานเกินไปอาจเพิ่มผลกระทบหากกุญแจรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

2. การทำลายข้อมูลด้วยการเข้ารหัส (Crypto-Shredding)

เมื่อหน่วยงานต้องการยกเลิกการใช้งานข้อมูลจำนวนมากบนระบบคลาวด์ หรือจำเป็นต้องทำลายข้อมูลอย่างรวดเร็ว หน่วยงานควรพิจารณาใช้วิธีทำลายกุญแจเข้ารหัสแทนการลบข้อมูลแบบปกติ

หลักการดำเนินงาน

ข้อมูลเข้ารหัส
+
กุญแจเข้ารหัส
↓
ลบกุญแจ
↓
ข้อมูลไม่สามารถอ่านได้

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

ในระบบคลาวด์ ข้อมูลอาจมีสำเนาหลายชุดหรืออยู่ในหลายตำแหน่ง การลบกุญแจเข้ารหัสอาจช่วยลดความเสี่ยงที่ข้อมูลคงเหลือจะถูกนำกลับมาใช้งานได้

ข้อพิจารณาเพิ่มเติม

- ตรวจสอบผลกระทบก่อนดำเนินการ
- มีขั้นตอนอนุมัติอย่างเป็นทางการ
- จัดเก็บหลักฐานการดำเนินการ
- พิจารณาข้อกำหนดทางกฎหมายเกี่ยวกับการเก็บรักษาข้อมูล
- ควรประเมินผลกระทบต่อข้อมูลสำรอง (Backup) ข้อมูลที่จำเป็นต้องเก็บรักษาตามกฎหมาย และระบบที่ใช้กุญแจร่วมกันก่อนดำเนินการ
- ควรตรวจสอบข้อกำหนดการเก็บรักษาพยานหลักฐานดิจิทัลหรือข้อมูลตามกฎหมายก่อนทำลายกุญแจ
- ไม่ควรใช้กับระบบที่ใช้กุญแจร่วมกันหลายระบบโดยไม่ประเมินผลกระทบ

3. แนวปฏิบัติที่เหมาะสมและไม่เหมาะสมในการจัดการกุญแจ

แนวปฏิบัติที่เหมาะสม	แนวปฏิบัติที่ไม่เหมาะสม
ใช้ระบบ KMS หรือ HSM	เก็บกุญแจไว้ใน Source Code
หมุนเวียนกุญแจตามนโยบาย	ใช้กุญแจเดิมหลายปี
จำกัดสิทธิ์เข้าถึงกุญแจ	ให้ผู้ใช้ทั่วไปเข้าถึงกุญแจ
แยกกุญแจออกจากข้อมูล	เก็บกุญแจกับข้อมูลไว้ที่เดียวกัน
ติดตามกิจกรรมการใช้งาน	ไม่มีการเก็บบันทึกเหตุการณ์

4. การเปลี่ยนผ่านสู่การเข้ารหัสยุคหลังควอนตัม (Post-Quantum Cryptography Transition)

หน่วยงานควรดำเนินการเปลี่ยนผ่านมาตรฐานการเข้ารหัสอย่างเป็นลำดับ โดยอ้างอิงข้อมูลจากบัญชีรายการการใช้งานการเข้ารหัส (Cryptographic Inventory) และผลการประเมินความเสี่ยง

ควรดำเนินการดังต่อไปนี้

1. ระบุระบบที่ได้รับผลกระทบจากการเปลี่ยนผ่าน
2. จัดลำดับความสำคัญของระบบที่ต้องเปลี่ยนผ่านก่อน
3. ทดสอบแนวทาง Hybrid Cryptography ระหว่างอัลกอริทึมแบบเดิมและ Post-Quantum Cryptography
4. ประเมินผลกระทบด้าน Performance และ Compatibility
5. จัดทำ Rollback Plan
6. ทดสอบ Interoperability ระหว่างระบบ
7. ดำเนินการเปลี่ยนผ่านแบบค่อยเป็นค่อยไป

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

8. ติดตามและประเมินผลหลังการเปลี่ยนผ่าน

ตัวอย่างกระบวนการเปลี่ยนผ่าน

อ้างอิง Cryptographic Inventory

↓

ระบุระบบที่ได้รับผลกระทบ

↓

จัดลำดับความสำคัญ

↓

ทดสอบ Hybrid Cryptography

↓

ประเมินผลกระทบ

↓

ดำเนินการเปลี่ยนผ่าน

↓

ติดตามผล

คำอธิบาย

ขั้นตอน	รายละเอียด
Inventory Reference	อ้างอิงรายการการใช้งาน
Impact Analysis	ระบุระบบที่ได้รับผลกระทบ
Prioritization	จัดลำดับความสำคัญ
Hybrid Testing	ทดสอบการทำงานร่วมกัน
Impact Evaluation	ประเมิน Performance
Migration	ดำเนินการเปลี่ยนผ่าน
Monitoring	ติดตามผล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

การเปลี่ยนผ่านด้านการเข้ารหัสอาจกระทบระบบจำนวนมาก หากไม่มีแผนดำเนินการและการทดสอบที่เหมาะสม อาจส่งผลต่อความต่อเนื่องในการให้บริการและความเข้ากันได้ของระบบ

5. เกณฑ์การคัดเลือกผู้ให้บริการ (Selection Criteria)

ในการจัดซื้อจัดจ้างหรือคัดเลือกบริการคลาวด์ หน่วยงานควรพิจารณาความสามารถด้านการเข้ารหัสและการบริหารจัดการกุญแจของผู้ให้บริการให้สอดคล้องกับประเภทข้อมูล ระดับผลกระทบของระบบสารสนเทศ ผลการประเมินความเสี่ยง ข้อกำหนดด้านกฎหมาย และบริบทของหน่วยงาน

รายละเอียดเกณฑ์การประเมินเพิ่มเติมสามารถพิจารณาได้ตาม **ภาคผนวก ก แนวทางการคัดเลือกผู้ให้บริการคลาวด์ด้านการเข้ารหัสและการจัดการกุญแจ**

เหตุผลและความจำเป็น (Rationale)

การเลือกผู้ให้บริการคลาวด์โดยพิจารณาเฉพาะคุณลักษณะการให้บริการหรือค่าใช้จ่าย อาจไม่เพียงพอต่อการปกป้องข้อมูลและการบริหารความเสี่ยงด้านการเข้ารหัส การกำหนดเกณฑ์การประเมินที่ชัดเจนจะช่วยให้หน่วยงานสามารถคัดเลือกผู้ให้บริการที่เหมาะสมกับระดับความเสี่ยงและข้อกำหนดของหน่วยงานได้

6. ข้อผิดพลาดและความเสี่ยงด้านการเข้ารหัสที่พบบ่อย (Common Cryptographic Misconfigurations and Risks)

หน่วยงานควรตระหนักถึงข้อผิดพลาดและความเสี่ยงที่อาจเกิดขึ้นจากการออกแบบ การกำหนดค่า และการใช้งานมาตรการเข้ารหัสบนระบบคลาวด์ ซึ่งอาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) รวมถึงการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ความเสี่ยงที่พบได้บ่อย มีดังนี้

6.1 ไม่เปิดใช้การเข้ารหัสข้อมูลขณะจัดเก็บ (Missing Encryption at Rest)

ข้อมูลสำคัญถูกจัดเก็บโดยไม่มีการเปิดใช้มาตรการเข้ารหัส ส่งผลให้ข้อมูลอาจถูกเข้าถึง เปิดเผย หรือถูกนำออกไปใช้งานได้ หากเกิดเหตุการณ์ข้อมูลรั่วไหลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

ผลกระทบ

- การเปิดเผยข้อมูลสำคัญ
- ความเสี่ยงต่อข้อมูลส่วนบุคคล
- ไม่สอดคล้องตามข้อกำหนดหรือกฎหมายที่เกี่ยวข้อง

6.2 ใช้โพรโทคอลหรืออัลกอริทึมที่ล้าสมัย (Use of Weak or Deprecated Algorithms)

มีการใช้งานอัลกอริทึมหรือโพรโทคอลที่มีความเสี่ยงหรือหมดความเหมาะสม เช่น SSL, DES, RC4, SHA-1 หรือ Cipher Suite ที่ไม่เป็นไปตามมาตรฐานปัจจุบัน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผลกระทบ

- เพิ่มโอกาสการถูกโจมตีหรือถอดรหัส
- ลดระดับความมั่นคงปลอดภัยของระบบ
- อาจไม่ผ่านข้อกำหนดการตรวจประเมิน

6.3 การจัดเก็บหรือเปิดเผยข้อมูลลับอย่างไม่เหมาะสม (Improper Secret Handling)

มีการจัดเก็บข้อมูลลับไว้ใน Source Code โปรแกรม สคริปต์ ไฟล์กำหนดค่า หรือระบบควบคุมเวอร์ชันโดยตรง เช่น

- API Key
- Access Token
- Password
- Encryption Key
- Private Key

ผลกระทบ

- ข้อมูลลับอาจรั่วไหลผ่านระบบควบคุมเวอร์ชัน
- เพิ่มความเสี่ยงต่อการเข้าถึงโดยไม่ได้รับอนุญาต
- ส่งผลกระทบต่อหลายระบบพร้อมกัน

6.4 ใช้ใบรับรองอิเล็กทรอนิกส์ที่หมดอายุหรือไม่เหมาะสม (Improper Certificate Usage)

มีการใช้ใบรับรองที่หมดอายุ ใช้ใบรับรองแบบ Self-Signed ในระบบสำคัญ หรือไม่มีการติดตามวงจรชีวิตของใบรับรองอย่างเหมาะสม

ผลกระทบ

- ระบบอาจไม่สามารถให้บริการได้
- ผู้ใช้อาจไม่สามารถตรวจสอบความน่าเชื่อถือของระบบ
- เพิ่มความเสี่ยงต่อการโจมตีแบบปลอมแปลงตัวตน

6.5 ไม่มีการบันทึกเหตุการณ์ด้านการเข้ารหัส (Missing Cryptographic Audit Logging)

ไม่มีการจัดเก็บบันทึกเหตุการณ์ที่เกี่ยวข้องกับการสร้าง การใช้งาน การเปลี่ยนแปลง หรือการเข้าถึงองค์ประกอบด้านการเข้ารหัส

ผลกระทบ

- ไม่สามารถตรวจสอบย้อนหลังได้
- เพิ่มข้อจำกัดในการสืบสวนเหตุการณ์
- ไม่สามารถพิสูจน์การปฏิบัติตามข้อกำหนดได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

6.6 ใช้ค่าตั้งต้นของผู้ให้บริการโดยไม่ประเมินความเหมาะสม (Unreviewed Default Security Settings)

มีการใช้งานค่าตั้งต้นด้านการเข้ารหัสของผู้ให้บริการคลาวด์โดยไม่ประเมินความเหมาะสมกับประเภทข้อมูล ความเสี่ยง หรือข้อกำหนดของหน่วยงาน

ผลกระทบ

- มาตรการป้องกันอาจไม่สอดคล้องกับระดับความเสี่ยง
- เพิ่มโอกาสการกำหนดค่าที่ไม่เหมาะสม
- อาจเกิดช่องว่างด้านการกำกับดูแล

6.7 ไม่เตรียมความพร้อมต่อการเปลี่ยนแปลงมาตรฐานการเข้ารหัสในอนาคต (Insufficient Cryptographic Transition Readiness)

ไม่มีการเตรียมความพร้อมสำหรับการเปลี่ยนผ่านมาตรฐานการเข้ารหัสในอนาคต หรือไม่มีการประเมินผลกระทบจากภัยคุกคามใหม่ เช่น การประมวลผลแบบควอนตัม

ผลกระทบ

- ข้อมูลที่ต้องปกป้องระยะยาวอาจมีความเสี่ยง
- เพิ่มความเสี่ยงจากภัยคุกคามแบบ Harvest Now, Decrypt Later (HNDL)
- เพิ่มต้นทุนและผลกระทบจากการเปลี่ยนผ่านในอนาคต

ตัวอย่างสรุปความเสี่ยง

ประเด็น	ผลกระทบ
Encryption Disabled	ข้อมูลรั่วไหล
Weak Algorithm	ถูกโจมตี
Hard-coded Secrets	เปิดเผยข้อมูลลับ
Improper Certificate Usage	ระบบหยุดชะงัก
Missing Logging	ตรวจสอบย้อนหลังไม่ได้
Default Settings	การกำหนดค่าไม่เหมาะสม
No PQC Readiness	ความเสี่ยงระยะยาว

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อมสำหรับบริการคลาวด์ มีวัตถุประสงค์เพื่อให้สถานที่ โครงสร้างพื้นฐาน อุปกรณ์ และทรัพยากรทางกายภาพที่ใช้ในการประมวลผล จัดเก็บ หรือสนับสนุนการให้บริการคลาวด์ ได้รับการบริหารจัดการให้สอดคล้องกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ความสำคัญของบริการ และความเสี่ยงที่เกี่ยวข้อง

สำหรับบริการคลาวด์สาธารณะ ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) โดยทั่วไปไม่สามารถควบคุมหรือเข้าถึงศูนย์ข้อมูลและโครงสร้างพื้นฐานทางกายภาพของผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ได้โดยตรง การกำกับดูแลจึงต้องอาศัยการกำหนดข้อกำหนด การขอและประเมินข้อมูลหรือหลักฐานที่เหมาะสม การพิจารณาความสามารถและข้อจำกัดของบริการ ตลอดจนการกำหนดความรับผิดชอบระหว่าง CSC และ CSP ตามหลักความรับผิดชอบร่วม (Shared Responsibility)

การดำเนินการตามข้อ 5.2.5 ควรเชื่อมโยงกับการกำกับดูแลตามข้อ 5.1 โดยเฉพาะนโยบายและหลักการใช้บริการคลาวด์ตามข้อ 5.1.1 การกำหนดบทบาท ผู้มีอำนาจตัดสินใจ และเจ้าของความเสี่ยงที่เหลืออยู่ตามข้อ 5.1.2 รวมถึงการพิจารณากฎหมาย เขตอำนาจทางกฎหมาย ข้อกำหนดตามสัญญา และหลักฐานการปฏิบัติตามข้อกำหนดตามข้อ 5.1.3 โดยไม่จำเป็นต้องจัดทำการประเมินซ้ำ หากผลการประเมินเดิมยังมีความเหมาะสม เป็นปัจจุบัน และครอบคลุมขอบเขตบริการที่เกี่ยวข้อง

การประยุกต์ใช้ตามระดับผลกระทบ

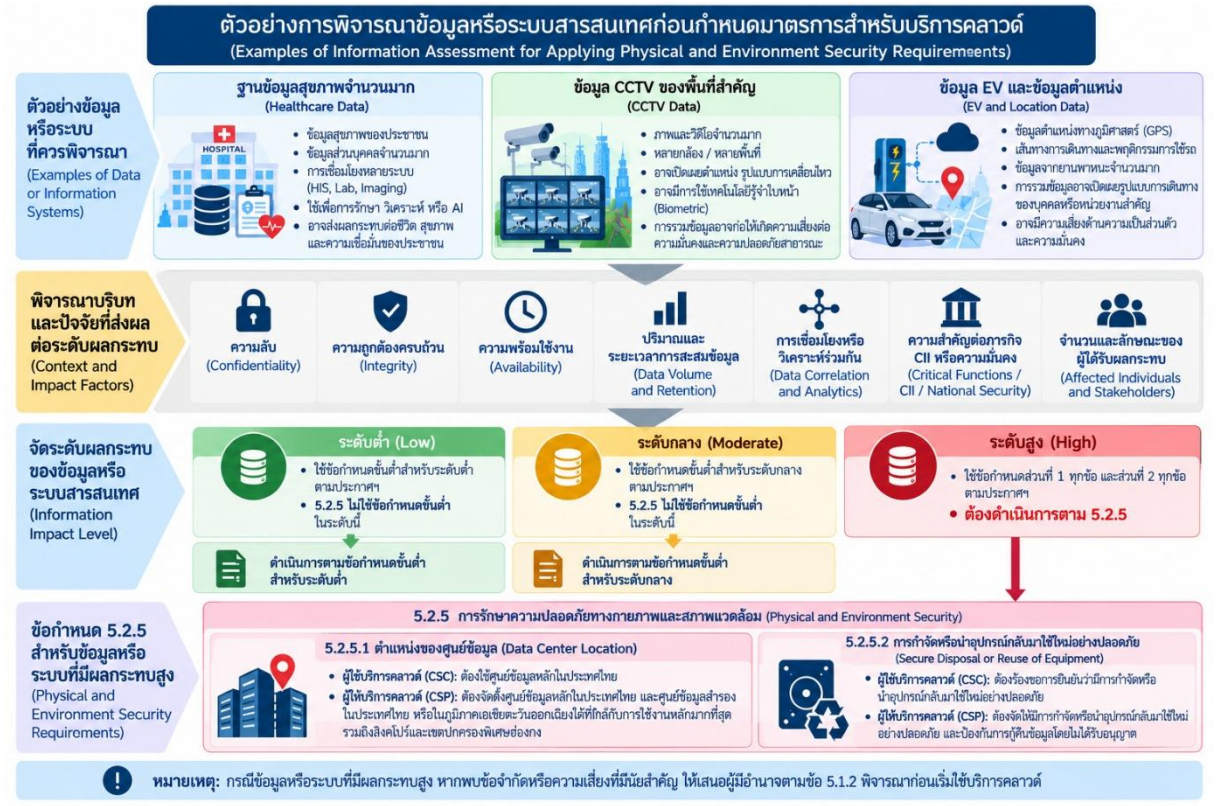
ตามตารางข้อกำหนดขั้นต่ำของประกาศ ข้อ 5.2.5 เป็นข้อกำหนดขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง ซึ่งต้องดำเนินการตามข้อกำหนดส่วนที่ 1 และส่วนที่ 2 ทุกข้อ ส่วนข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับต่ำและระดับปานกลาง มิได้ถูกกำหนดให้ต้องดำเนินการตามข้อ 5.2.5 ในฐานะข้อกำหนดขั้นต่ำของมาตรฐานฉบับนี้ ทั้งนี้ องค์กรยังคงต้องพิจารณากฎหมาย ประกาศ ข้อกำหนดตามสัญญา และข้อกำหนดอื่นที่มีผลใช้บังคับกับบริการนั้น

ดังนั้น การนำข้อ 5.2.5 ไปใช้ควรเริ่มจากผลการจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ แล้วจึงพิจารณาข้อกำหนดที่ใช้บังคับ ความสามารถและหลักฐานของ CSP ช่องว่างหรือข้อจำกัด ความเสี่ยงที่เหลืออยู่ และการตัดสินใจตามระดับอำนาจที่กำหนด

ข้อมูลหรือระบบสารสนเทศ ⟶ ระดับผลกระทบ ⟶ ข้อกำหนดที่ใช้บังคับ ⟶ ความสามารถและหลักฐานของ CSP ⟶ ช่องว่างหรือข้อจำกัด ⟶ ความเสี่ยง ⟶ การตัดสินใจ ⟶ การติดตามและทบทวน

แนวทางดังกล่าวทำให้ข้อ 5.2.5 เป็นการนำผลจากการกำกับดูแลตามข้อ 5.1 มาสู่การควบคุมในทางปฏิบัติ มิใช่การจัดทำกระบวนการบริหารความเสี่ยงหรือการตัดสินใจขึ้นใหม่อีกชุดหนึ่ง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง



รูปที่ 13 แนวทางการพิจารณาระดับผลกระทบก่อนนำ ข้อกำหนดด้านการรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อมไปใช้

ร่างประกาศ Public Hearing

5.2.5.1 ตำแหน่งของศูนย์ข้อมูล (Data Center Location)

ตำแหน่งของศูนย์ข้อมูลเป็นปัจจัยสำคัญต่อการกำกับดูแลบริการคลาวด์ โดยเฉพาะสำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง ซึ่งต้องดำเนินการตามข้อกำหนดส่วนที่ 2 ของประกาศ การพิจารณาตำแหน่งของศูนย์ข้อมูลจึงมิได้จำกัดเฉพาะสถานที่ตั้งทางกายภาพ แต่ควรพิจารณาร่วมกับพื้นที่ให้บริการ สถานที่จัดเก็บหรือประมวลผลข้อมูล การกู้คืนบริการ เขตอำนาจทางกฎหมาย และความเสี่ยงด้านอธิปไตยข้อมูลตามความเกี่ยวข้อง

ข้อ 5.2.5.1 กำหนดข้อกำหนดเฉพาะเกี่ยวกับศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองสำหรับบริการที่อยู่ภายใต้ข้อกำหนดดังกล่าว โดย CSC ต้องพิจารณาว่าบริการที่เลือกใช้จริงเป็นไปตามข้อกำหนดหรือไม่ ขณะที่ CSP ต้องจัดให้มีศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองตามเงื่อนไขที่ประกาศกำหนด

การพิจารณาตามข้อนี้ควรใช้ผลจากการประเมินตามข้อ 5.1.1–5.1.3 เป็นข้อมูลประกอบ โดยไม่ควรตีความว่าการปฏิบัติตามข้อกำหนดด้านตำแหน่งศูนย์ข้อมูลเพียงอย่างเดียวทำให้ความเสี่ยงด้านเขตอำนาจทางกฎหมาย ความต่อเนื่องของบริการ หรืออธิปไตยข้อมูลหมดไปทั้งหมด

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)	ก) ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization) ข) ต้องจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย (Data Localization) หรือ อยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของผู้ใช้บริการคลาวด์ให้มากที่สุด รวมถึงสิงคโปร์และเขตปกครองพิเศษฮ่องกง

วัตถุประสงค์

1. เพื่อให้ตำแหน่งของศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองที่ใช้ในการให้บริการคลาวด์เป็นไปตามข้อกำหนดของประกาศและข้อกำหนดอื่นที่เกี่ยวข้อง
2. เพื่อให้ CSC สามารถตรวจสอบและประเมินได้ว่า บริการและพื้นที่ให้บริการที่เลือกใช้มีความเหมาะสมกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และมีหลักฐานสนับสนุนการปฏิบัติตามข้อกำหนดอย่างเพียงพอ
3. เพื่อให้การพิจารณาตำแหน่งของศูนย์ข้อมูลเชื่อมโยงกับความต่อเนื่องของบริการ เขตอำนาจทางกฎหมายอธิปไตยข้อมูล และกระบวนการตัดสินใจเกี่ยวกับความเสี่ยงตามข้อ 5.1.1–5.1.3

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

สำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูงและต้องดำเนินการตามข้อ 5.2.5 ผู้ใช้บริการคลาวด์ (CSC) ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทยตามข้อกำหนดของข้อ 5.2.5.1 และควรตรวจสอบว่าบริการและพื้นที่ให้บริการที่เลือกใช้จริงมีตำแหน่งของศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองเป็นไปตามข้อกำหนดที่เกี่ยวข้อง

การพิจารณาไม่ควรจำกัดเฉพาะการตรวจสอบว่าผู้ให้บริการคลาวด์มีศูนย์ข้อมูลอยู่ในประเทศไทยหรือไม่ แต่ควรพิจารณาบริการ พื้นที่ให้บริการ สถานที่จัดเก็บหรือประมวลผลข้อมูล และรูปแบบการกู้คืนบริการที่ CSC เลือกใช้จริง รวมถึงข้อมูลหรือหลักฐานที่เพียงพอต่อการยืนยันการปฏิบัติตามข้อกำหนด

1. การตรวจสอบตำแหน่งของศูนย์ข้อมูล

CSC ควรตรวจสอบข้อมูลอย่างน้อยในประเด็นต่อไปนี้ตามความเกี่ยวข้อง

- ประเทศหรือพื้นที่ที่ตั้งของศูนย์ข้อมูลหลัก
- ประเทศหรือพื้นที่ที่ตั้งของศูนย์ข้อมูลสำรอง
- พื้นที่ให้บริการ (Region) ที่ CSC เลือกใช้
- ข้อมูลของ CSC อาจถูกจัดเก็บ สำรอง หรือประมวลผลในสถานที่อื่นนอกเหนือจากพื้นที่ที่เลือกหรือไม่

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- มีข้อจำกัดหรือเงื่อนไขในการกำหนดตำแหน่งของข้อมูลหรือบริการหรือไม่
- มีองค์ประกอบสำคัญใดของบริการที่อาจต้องพึ่งพาโครงสร้างพื้นฐานในประเทศหรือเขตอำนาจทางกฎหมายอื่นหรือไม่

CSC ไม่จำเป็นต้องได้รับรายละเอียดตำแหน่งทางกายภาพของศูนย์ข้อมูลในระดับที่อาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัยของ CSP หากข้อมูลระดับประเทศ ภูมิภาค หรือพื้นที่ให้บริการสามารถใช้ยืนยันการปฏิบัติตามข้อกำหนดและประเมินความเสี่ยงได้อย่างเพียงพอ

2. การตรวจสอบการปฏิบัติตามข้อกำหนดด้านตำแหน่งศูนย์ข้อมูล

สำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง CSC ต้องตรวจสอบว่าบริการที่เลือกใช้เป็นไปตามข้อกำหนดของข้อ 5.2.5.1 โดยเฉพาะตำแหน่งของศูนย์ข้อมูลหลัก

การตรวจสอบไม่ควรพิจารณาเพียงข้อความทางการตลาดหรือการระบุว่าผู้ให้บริการมีศูนย์ข้อมูลอยู่ในประเทศไทย แต่ควรพิจารณาว่า **บริการและพื้นที่ให้บริการที่ CSC เลือกใช้จริง** เป็นไปตามข้อกำหนดหรือไม่

ตัวอย่างหลักฐานที่อาจใช้ประกอบการตรวจสอบ ได้แก่

- เอกสารคำอธิบายบริการของ CSP
- ข้อมูลพื้นที่ให้บริการ (Region) หรือตำแหน่งของศูนย์ข้อมูล
- ข้อตกลงการให้บริการหรือข้อกำหนดตามสัญญา
- เอกสารเกี่ยวกับสถานที่จัดเก็บหรือประมวลผลข้อมูล (Data Residency / Data Location)
- รายงานการตรวจประเมินหรือการรับรองที่เกี่ยวข้อง
- หนังสือหรือข้อมูลยืนยันจาก CSP

หลักฐานที่ใช้ควรมีความเพียงพอและเหมาะสมกับความสำคัญของข้อมูลหรือระบบสารสนเทศ โดยไม่จำเป็นต้องกำหนดหลักฐานประเภทเดียวกันสำหรับ CSP ทุกราย

3. การพิจารณาศูนย์ข้อมูลสำรองและความต่อเนื่องของบริการ

CSC ควรพิจารณาตำแหน่งของศูนย์ข้อมูลสำรองร่วมกับรูปแบบการสำรองและกู้คืนบริการ เพื่อให้ทราบว่าหากศูนย์ข้อมูลหลักไม่สามารถให้บริการได้ บริการจะถูกกู้คืนหรือย้ายไปดำเนินงาน ณ สถานที่ใด และสถานที่ดังกล่าวเป็นไปตามข้อกำหนดที่เกี่ยวข้องหรือไม่

การพิจารณาควรเชื่อมโยงกับกระบวนการบริหารความต่อเนื่องและการกู้คืนบริการของหน่วยงาน โดยไม่จำเป็นต้องกำหนดรายละเอียดด้านการสำรองหรือการกู้คืนซ้ำในหัวข้อนี้

4. การพิจารณาเขตอำนาจทางกฎหมายและอธิปไตยข้อมูล

การที่ศูนย์ข้อมูลตั้งอยู่ในประเทศไทยมิได้หมายความว่าความเสี่ยงด้านเขตอำนาจทางกฎหมายหรืออธิปไตยข้อมูลจะหมดไปทั้งหมด เนื่องจากการให้บริการอาจเกี่ยวข้องกับผู้ให้บริการ บริษัทในเครือ ผู้รับจ้างช่วง บุคลากร ระบบบริหารจัดการ หรือองค์ประกอบทางเทคนิคที่อยู่ภายใต้เขตอำนาจทางกฎหมายอื่น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

CSC จึงควรนำผลการพิจารณากฎหมาย เขตอำนาจทางกฎหมาย และข้อกำหนดตามสัญญาจากข้อ 5.1.3 รวมถึงหลักการด้านอธิปไตยข้อมูลจากข้อ 5.1.1 มาใช้ประกอบการประเมิน โดยไม่จำเป็นต้องจัดทำการประเมินชุดใหม่เฉพาะสำหรับข้อ 5.2.5

ประเด็นที่อาจพิจารณาเพิ่มเติม ได้แก่

- ประเทศหรือเขตอำนาจทางกฎหมายที่เกี่ยวข้องกับ CSP
- การเข้าถึงหรือบริหารจัดการบริการจากต่างประเทศ
- การใช้ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง
- การสำรองหรือจำลองข้อมูลไปยังพื้นที่อื่น
- ข้อจำกัดในการเคลื่อนย้ายหรือส่งออกข้อมูล
- ความสามารถของ CSC ในการเข้าถึง นำออก กู้คืน หรือลบข้อมูลของตน

หากผลการประเมินพบความเสี่ยงที่มีนัยสำคัญ ให้ดำเนินการตามกระบวนการบริหารความเสี่ยงและระดับอำนาจการตัดสินใจที่กำหนดไว้ในข้อ 5.1.2

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. ศูนย์ข้อมูลหลัก

CSP ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทยตามข้อกำหนดของประกาศ สำหรับการให้บริการที่อยู่ภายใต้ข้อกำหนดดังกล่าว

CSP ควรจัดให้มีข้อมูลหรือหลักฐานที่เพียงพอเพื่อให้ CSC สามารถยืนยันได้ว่าบริการและพื้นที่ให้บริการที่เลือกใช้เป็นไปตามข้อกำหนด โดยข้อมูลดังกล่าวอาจอยู่ในเอกสารคำอธิบายบริการ ข้อตกลง เอกสารหรือข้อมูลเกี่ยวกับตำแหน่งของข้อมูลและศูนย์ข้อมูล หรือหลักฐานอื่นที่เหมาะสม

2. ศูนย์ข้อมูลสำรอง

CSP ต้องจัดตั้งศูนย์ข้อมูลสำรองตามเงื่อนไขที่ประกาศกำหนด และควรให้ข้อมูลแก่ CSC อย่างเพียงพอเพื่อให้สามารถพิจารณาตำแหน่งของศูนย์ข้อมูลสำรองและรูปแบบการกู้คืนบริการที่เกี่ยวข้องได้

ข้อมูลที่ให้ไม่จำเป็นต้องเปิดเผยรายละเอียดทางกายภาพหรือข้อมูลที่อาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัยของศูนย์ข้อมูล หากข้อมูลในระดับประเทศ ภูมิภาค หรือพื้นที่ให้บริการเพียงพอสำหรับการยืนยันการปฏิบัติตามข้อกำหนด

3. ข้อมูลเกี่ยวกับตำแหน่งและเขตอำนาจทางกฎหมาย

CSP ควรให้ข้อมูลที่จำเป็นแก่ CSC เพื่อสนับสนุนการประเมินตำแหน่งของข้อมูลและเขตอำนาจทางกฎหมายที่เกี่ยวข้องกับบริการ โดยเชื่อมโยงกับข้อมูลที่ CSP ต้องจัดให้ตามข้อ 5.1.2 และข้อ 5.1.3

หากบริการมีการใช้ผู้ให้บริการภายนอก ผู้รับจ้างช่วง หรือองค์ประกอบของบริการในต่างประเทศ ข้อมูลดังกล่าวควรมีความเพียงพอให้ CSC สามารถประเมินข้อกำหนดและความเสี่ยงที่เกี่ยวข้องได้

ภาคสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. การเปลี่ยนแปลงตำแหน่งการให้บริการ

หาก CSP มีการเปลี่ยนแปลงตำแหน่งของศูนย์ข้อมูล พื้นที่ให้บริการ หรือองค์ประกอบสำคัญที่อาจทำให้การปฏิบัติตามข้อกำหนดหรือความเสี่ยงของ CSC เปลี่ยนแปลง CSP ควรแจ้งข้อมูลแก่ CSC ตามข้อตกลงหรือเงื่อนไขบริการที่เกี่ยวข้อง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดเรื่องตำแหน่งศูนย์ข้อมูลไปปฏิบัติไม่ควรเริ่มจากการพิจารณาเพียงว่า “CSP มีศูนย์ข้อมูลในประเทศไทยหรือไม่” แต่ควรเริ่มจากข้อมูลหรือระบบสารสนเทศที่หน่วยงานจะนำไปใช้บริการคลาวด์ ระดับผลกระทบ และข้อกำหนดที่ใช้บังคับกับข้อมูลหรือระบบนั้น

ขั้นตอน	ประเด็นพิจารณา	ผลลัพธ์ที่ควรได้
1. ระบุข้อมูลหรือระบบ	ข้อมูล ระบบ และบริการใดจะนำไปใช้บนคลาวด์	ขอบเขตของข้อมูล ระบบ และบริการ
2. จัดระดับผลกระทบ	ข้อมูลหรือระบบมีผลกระทบระดับต่ำ ปานกลาง หรือสูง	ผลการจัดระดับผลกระทบ
3. ระบุข้อกำหนดที่ใช้บังคับ	ข้อ 5.2.5 ใช้บังคับหรือไม่ และมีข้อกำหนดอื่นใดเกี่ยวข้อง	รายการข้อกำหนดที่ใช้บังคับ
4. ตรวจสอบตำแหน่งของบริการ	ศูนย์ข้อมูลหลัก ศูนย์ข้อมูลสำรอง และพื้นที่ให้บริการอยู่ที่ใด	ข้อมูลตำแหน่งของศูนย์ข้อมูลและพื้นที่ให้บริการ
5. ตรวจสอบหลักฐาน	CSP สามารถแสดงหลักฐานสนับสนุนการปฏิบัติตามข้อกำหนดได้หรือไม่	หลักฐานที่เกี่ยวข้อง
6. ประเมินช่องว่างและความเสี่ยง	พิจารณาความต่อเนื่อง เขตอำนาจทางกฎหมาย อธิปไตยข้อมูล และการพึ่งพาบริการ	ช่องว่าง ข้อจำกัด และผลการประเมินความเสี่ยง
7. พิจารณาตัดสินใจ	ใช้บริการ กำหนดมาตรการเพิ่มเติม เปลี่ยนบริการ หรือยกระดับการตัดสินใจ	ผลการตัดสินใจและผู้รับผิดชอบ
8. ติดตามและทบทวน	ตำแหน่ง พื้นที่ให้บริการ เขตอำนาจทางกฎหมาย หรือองค์ประกอบสำคัญมีการเปลี่ยนแปลงหรือไม่	ผลการติดตามและการทบทวน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. ตัวอย่างการนำไปใช้

ตัวอย่างที่ 1 ระบบที่มีผลกระทบระดับต่ำหรือระดับปานกลาง

หน่วยงานประเมินระบบและพบว่าไม่อยู่ในระดับผลกระทบสูง ดังนั้น ข้อ 5.2.5 มิใช่ข้อกำหนดขั้นต่ำที่ใช้บังคับกับระบบดังกล่าวตามตารางท้ายประกาศ

อย่างไรก็ตาม หน่วยงานยังคงพิจารณาตำแหน่งของข้อมูลตามนโยบายในข้อ 5.1.1 และตรวจสอบว่ามีกฎหมาย สัญญา หรือข้อกำหนดอื่นที่เกี่ยวข้องหรือไม่

ตัวอย่างที่ 2 ระบบผลกระทบสูงที่ศูนย์ข้อมูลหลักอยู่ประเทศไทย

หน่วยงานประเมินระบบบริการประชาชนเป็นผลกระทบระดับสูง และตรวจสอบพบว่าพื้นที่ให้บริการที่เลือกใช้มีศูนย์ข้อมูลหลักในประเทศไทย

CSC ตรวจสอบหลักฐานของ CSP และตำแหน่งศูนย์ข้อมูลสำรองตามข้อกำหนด พร้อมพิจารณาว่าการกู้คืนบริการ การบริหารจัดการ หรือองค์ประกอบสำคัญอื่นมีการพึ่งพาบริการจากต่างประเทศหรือไม่

หากไม่พบช่องว่างที่มีนัยสำคัญและมีหลักฐานเพียงพอ หน่วยงานสามารถบันทึกผลการประเมินและดำเนินการตามกระบวนการอนุมัติขององค์กร

ตัวอย่างที่ 3 ระบบผลกระทบสูงที่เป็นไปตามข้อกำหนดด้านสถานที่จัดเก็บข้อมูล แต่ยังมีความเสี่ยงด้านอธิปไตยข้อมูล

CSC ตรวจสอบพบว่าศูนย์ข้อมูลหลักเป็นไปตามข้อกำหนดด้านสถานที่จัดเก็บข้อมูล แต่การกู้คืนบริการหรือองค์ประกอบสำคัญบางส่วนยังต้องพึ่งพาโครงสร้างพื้นฐาน การบริหารจัดการ หรือการสนับสนุนจากต่างประเทศ

กรณีดังกล่าวไม่ควรสรุปเพียงว่า “เป็นไปตามข้อกำหนดด้านสถานที่จัดเก็บข้อมูลแล้ว จึงไม่มีความเสี่ยงเพิ่มเติม” เนื่องจากตำแหน่งทางกายภาพของศูนย์ข้อมูลเป็นเพียงองค์ประกอบหนึ่งของการประเมินความเสี่ยงด้านอธิปไตยข้อมูล (Data Sovereignty)

CSC ควรนำข้อจำกัดดังกล่าวมาพิจารณาร่วมกับผลการประเมินตามข้อ 5.1.1–5.1.3 และหากพบว่าความเสี่ยงที่เหลืออยู่เกินระดับอำนาจของผู้ปฏิบัติงาน ให้ยกระดับไปยังผู้มีอำนาจตามข้อ 5.1.2

เส้นทางการตรวจสอบย้อนกลับควรสามารถแสดงได้ดังนี้

ระดับผลกระทบ ⟶ ข้อกำหนดที่ใช้บังคับ ⟶ หลักฐาน ⟶ ช่องว่างหรือข้อจำกัด ⟶ ความเสี่ยง ⟶ การตัดสินใจ ⟶ ผู้มีอำนาจตัดสินใจ ⟶ เจ้าของความเสี่ยงที่เหลืออยู่ ⟶ การติดตามและทบทวน

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

2. หลักฐานที่ควรพิจารณา (Recommended Evidence)

CSC ไม่จำเป็นต้องสร้างเอกสารใหม่ทุกประเภท หากสามารถใช้หลักฐานจากกระบวนการที่มีอยู่เพื่อแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

ประเด็นที่ต้องสามารถยืนยันได้	ตัวอย่างหลักฐาน
ระดับผลกระทบของข้อมูลหรือระบบ	ผลการจัดระดับผลกระทบ
ข้อกำหนดที่ใช้บังคับ	รายการข้อกำหนดขั้นต่ำ กฎหมาย ประกาศ หรือข้อกำหนดอื่น
พื้นที่ให้บริการและตำแหน่งของบริการ	ข้อมูลพื้นที่ให้บริการ ศูนย์ข้อมูลหลัก และศูนย์ข้อมูลสำรอง
ตำแหน่งศูนย์ข้อมูล	เอกสารหรือข้อมูลยืนยันจาก CSP
เงื่อนไขตามสัญญา	สัญญา ข้อตกลงการให้บริการ หรือเงื่อนไขด้านสถานที่จัดเก็บข้อมูล
การปฏิบัติตามข้อกำหนด	หลักฐานหรือรายงานสนับสนุนจาก CSP
ความเสี่ยง	ผลการประเมินหรือทะเบียนความเสี่ยง
การตัดสินใจ	บันทึกการพิจารณาหรือการอนุมัติ
การติดตามการเปลี่ยนแปลง	ผลการทบทวนหรือบันทึกการเปลี่ยนแปลงบริการ

5.2.5.2 การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure Disposal or Reuse of Equipment)

บริการคลาวด์อาศัยโครงสร้างพื้นฐาน ทรัพยากรทางกายภาพ และสื่อบันทึกข้อมูลที่ CSP บริหารจัดการและอาจนำกลับมาใช้ใหม่ตามวงจรชีวิตของบริการ โดยทรัพยากรดังกล่าวอาจถูกนำกลับมาใช้ใหม่ เปลี่ยนวัตถุประสงค์การใช้งาน หรือกำจัดเมื่อสิ้นสุดอายุการใช้งาน หากข้อมูลที่เคยจัดเก็บหรือประมวลผลยังสามารถถูกเข้าถึงหรือกู้คืนได้ อาจก่อให้เกิดความเสี่ยงต่อการเปิดเผยข้อมูลของ CSC โดยไม่ได้รับอนุญาต

ข้อ 5.2.5.2 จึงกำหนดให้ CSC ต้องร้องขอการยืนยันว่า CSP มีนโยบายและขั้นตอนในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย ขณะที่ CSP ต้องจัดให้มีการดำเนินการดังกล่าวอย่างปลอดภัยและทันท่วงที และต้องปฏิบัติต่ออุปกรณ์หรือสื่อที่อาจมีข้อมูลส่วนบุคคลเสมือนว่ามีข้อมูลส่วนบุคคลอยู่จริง เพื่อป้องกันการกู้คืนข้อมูลโดยไม่ได้รับอนุญาต

การนำข้อกำหนดนี้ไปปฏิบัติควรคำนึงถึงลักษณะของบริการและขอบเขตความรับผิดชอบร่วม โดย CSC ไม่จำเป็นต้องควบคุมกระบวนการทางกายภาพของ CSP โดยตรง แต่ต้องสามารถได้รับและประเมินข้อมูลหรือหลักฐานที่เหมาะสมเพื่อยืนยันการปฏิบัติตามข้อกำหนด

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องร้องขอการยืนยันว่าผู้ให้บริการคลาวด์มีนโยบายและขั้นตอนในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย	ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่ามีการเตรียมการสำหรับการกำจัดหรือนำทรัพยากร

ร่างมาตรฐาน Public Hearing ห้ามนำไปใช้อ้างอิง

	(เช่น อุปกรณ์ ที่เก็บข้อมูล ไฟล์ หน่วยความจำ) กลับมาใช้ใหม่อย่างปลอดภัยและทันท่วงที ข) เพื่อวัตถุประสงค์ในการกำจัดหรือนำกลับมาใช้ใหม่อย่างมั่นคงปลอดภัย และไม่สามารถกู้คืนข้อมูลกลับมาได้ อุปกรณ์ที่มีสื่อจัดเก็บข้อมูลที่อาจมีข้อมูลส่วนบุคคลต้องได้รับการปฏิบัติเสมือนว่ามีข้อมูลส่วนบุคคลจริง

วัตถุประสงค์

1. เพื่อให้ข้อมูลของ CSC ที่จัดเก็บหรือประมวลผลบนอุปกรณ์หรือสื่อบันทึกข้อมูลภายใต้การควบคุมของ CSP ได้รับการลบหรือทำลายอย่างเหมาะสมก่อนการกำจัด การเปลี่ยนวัตถุประสงค์การใช้งาน หรือการนำอุปกรณ์กลับมาใช้ใหม่ เพื่อป้องกันการเข้าถึง การกู้คืน หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
2. เพื่อให้ CSC สามารถได้รับและประเมินการยืนยันจาก CSP ว่ากระบวนการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่ได้รับการควบคุมอย่างเหมาะสม และสามารถใช้ข้อมูลหรือหลักฐานดังกล่าวประกอบการกำกับดูแล การประเมินความเสี่ยง และการตรวจสอบการปฏิบัติตามข้อกำหนด

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

สำหรับข้อมูลหรือระบบสารสนเทศที่ข้อ 5.2.5 ใช้บังคับ ผู้ใช้บริการคลาวด์ (CSC) ต้องร้องขอการยืนยันจากผู้ให้บริการคลาวด์ (CSP) เกี่ยวกับการกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัยตามข้อกำหนดของประกาศ

การดำเนินการดังกล่าวมิได้หมายความว่า CSC ต้องเข้าไปควบคุมกระบวนการทางกายภาพภายในศูนย์ข้อมูลของ CSP โดยตรง แต่ CSC ต้องสามารถแสดงให้เห็นว่าได้พิจารณาและได้รับข้อมูลหรือหลักฐานที่เหมาะสมเพียงพอสำหรับการยืนยันว่าข้อมูลของตนได้รับการคุ้มครองเมื่ออุปกรณ์หรือสื่อบันทึกข้อมูลถูกนำกลับมาใช้ใหม่หรือกำจัด

การกำหนดข้อกำหนดเกี่ยวกับการลบหรือทำลายข้อมูล

CSC ควรกำหนดความต้องการด้านการลบหรือทำลายข้อมูลให้เหมาะสมกับลักษณะของข้อมูล ระดับผลกระทบ รูปแบบบริการ และขอบเขตความรับผิดชอบของ CSC และ CSP

ประเด็นที่ควรพิจารณา ได้แก่

1. ข้อมูลประเภทใดอยู่ภายใต้บริการและอาจถูกจัดเก็บบนอุปกรณ์หรือสื่อของ CSP
2. CSP มีหลักการหรือกระบวนการสำหรับการลบข้อมูลก่อนนำอุปกรณ์หรือสื่อกลับมาใช้ใหม่หรือกำจัดหรือไม่

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้อ้างอิง

3. กระบวนการดังกล่าวครอบคลุมอุปกรณ์หรือสื่อที่เกี่ยวข้องกับบริการของ CSC ตามขอบเขตที่เหมาะสมหรือไม่
4. มีการใช้ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วงในการกำจัดอุปกรณ์หรือสื่อหรือไม่
5. CSC สามารถได้รับข้อมูลหรือหลักฐานยืนยันการดำเนินการจาก CSP ในระดับที่เหมาะสมหรือไม่

ข้อกำหนดดังกล่าวอาจกำหนดไว้ในสัญญา ข้อตกลงการให้บริการ ข้อกำหนดด้านความมั่นคงปลอดภัย หรือเอกสารอื่นที่เกี่ยวข้อง โดยไม่จำเป็นต้องจัดทำเอกสารแยกต่างหาก หากข้อกำหนดที่มีอยู่สามารถครอบคลุมประเด็นดังกล่าวได้อย่างเพียงพอ

การร้องขอและพิจารณาการยืนยันจาก CSP

CSC ต้องร้องขอการยืนยันจาก CSP ตามข้อกำหนด โดยรูปแบบของการยืนยันอาจแตกต่างกันตามลักษณะของบริการและวิธีการที่ CSP ใช้ในการแสดงการปฏิบัติตามข้อกำหนด

ตัวอย่างข้อมูลหรือหลักฐานที่อาจใช้ประกอบการยืนยัน ได้แก่

- นโยบายหรือแนวทางการกำจัดสื่อและอุปกรณ์
- คำอธิบายกระบวนการลบหรือทำลายข้อมูล
- ข้อกำหนดหรือคำรับรองในสัญญาหรือข้อตกลงการให้บริการ
- รายงานการตรวจประเมินโดยหน่วยงานอิสระ
- ใบรับรองหรือรายงานการประเมินที่มีขอบเขตครอบคลุมกระบวนการดังกล่าว
- หนังสือหรือข้อมูลยืนยันจาก CSP
- หลักฐานการทำลายหรือการกำจัดในกรณีที่ CSP สามารถจัดให้ได้

CSC ไม่จำเป็นต้องกำหนดให้ CSP เปิดเผยรายละเอียดทางเทคนิคหรือกระบวนการภายในทั้งหมด หากหลักฐานที่ได้รับมีความน่าเชื่อถือและเพียงพอต่อการยืนยันการปฏิบัติตามข้อกำหนด

การพิจารณาความเพียงพอของหลักฐาน

CSC ควรพิจารณาความเพียงพอของหลักฐานโดยคำนึงถึงระดับผลกระทบ ความสำคัญและความอ่อนไหวของข้อมูล ขอบเขตของบริการ และความเสี่ยงที่เกี่ยวข้อง

การมีข้อความทั่วไปว่า CSP “มีการลบข้อมูลอย่างปลอดภัย” เพียงอย่างเดียวอาจไม่เพียงพอสำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง หากไม่สามารถระบุได้ว่ากระบวนการดังกล่าวครอบคลุมข้อมูล อุปกรณ์หรือสื่อ และบริการที่ CSC ใช้งานอยู่หรือไม่

ในกรณีที่หลักฐานมีข้อจำกัด CSC ควรบันทึกข้อจำกัดดังกล่าวและประเมินว่าก่อให้เกิดช่องว่างหรือความเสี่ยงที่ต้องได้รับการจัดการเพิ่มเติมหรือไม่

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่า เมื่ออุปกรณ์หรือสื่อที่อาจมีข้อมูลของ CSC ถูกกำจัด นำกลับมาใช้ใหม่ หรือเปลี่ยนวัตถุประสงค์การใช้งาน ข้อมูลที่เกี่ยวข้องได้รับการลบหรือทำลายอย่างเหมาะสมตามข้อกำหนดของประกาศ

1. การกำหนดกระบวนการกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่

CSP ควรกำหนดและดำเนินกระบวนการสำหรับการจัดการอุปกรณ์และสื่อบันทึกข้อมูลตลอดวงจรชีวิต เพื่อป้องกันไม่ให้ข้อมูลของ CSC ยังคงอยู่ในรูปแบบที่สามารถเข้าถึงหรือกู้คืนได้โดยไม่ได้รับอนุญาตเมื่ออุปกรณ์หรือสื่อดังกล่าวถูกนำกลับมาใช้ใหม่หรือกำจัด

กระบวนการควรครอบคลุมตามความเหมาะสม เช่น

1. การระบุอุปกรณ์หรือสื่อที่ต้องนำกลับมาใช้ใหม่หรือกำจัด
2. การกำหนดวิธีการลบข้อมูลหรือทำลายสื่อให้เหมาะสมกับประเภทของอุปกรณ์และข้อมูล
3. การตรวจสอบหรือยืนยันผลการดำเนินการ
4. การควบคุมอุปกรณ์หรือสื่อระหว่างรอการดำเนินการ
5. การบันทึกผลการดำเนินการตามความเหมาะสม
6. การควบคุมผู้ให้บริการภายนอกหรือผู้รับจ้างช่วงที่เกี่ยวข้อง

รายละเอียดของวิธีการทางเทคนิคอาจแตกต่างกันตามประเภทของสื่อ เทคโนโลยี และสถาปัตยกรรมของบริการ โดยควรเลือกวิธีการที่ทำให้ข้อมูลไม่สามารถเข้าถึงหรือกู้คืนได้โดยไม่ได้รับอนุญาต และมีความเหมาะสมกับประเภทของสื่อ ระดับผลกระทบ และความเสี่ยงที่เกี่ยวข้อง

2. การนำอุปกรณ์หรือสื่อกลับมาใช้ใหม่

ก่อนนำอุปกรณ์หรือสื่อที่เคยใช้จัดเก็บหรือประมวลผลข้อมูลของ CSC กลับมาใช้ใหม่ CSP ต้องตรวจสอบให้แน่ใจว่าข้อมูลเดิมได้รับการลบอย่างเหมาะสม เพื่อป้องกันไม่ให้ผู้ใช้บริการรายอื่น บุคลากร หรือบุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลที่หลงเหลืออยู่ได้

ประเด็นนี้มีความสำคัญเป็นพิเศษในสภาพแวดล้อมคลาวด์ที่มีการใช้ทรัพยากรร่วมกันระหว่างผู้ใช้บริการหลายราย โดยควรเชื่อมโยงกับหลักการแยกผู้ใช้บริการและการปกป้องข้อมูลที่กำหนดไว้ในข้ออื่นที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดมาตรการดังกล่าวซ้ำในหัวข้อนี้

3. การกำจัดอุปกรณ์หรือสื่อ

เมื่ออุปกรณ์หรือสื่อไม่สามารถนำกลับมาใช้ใหม่ หรือถึงกำหนดสิ้นสุดอายุการใช้งาน CSP ต้องตรวจสอบให้แน่ใจว่าข้อมูลที่เกี่ยวข้องได้รับการลบหรือทำลายอย่างปลอดภัยก่อนหรือระหว่างกระบวนการกำจัดตามความเหมาะสม

วิธีการอาจประกอบด้วยการลบข้อมูลอย่างปลอดภัย การทำให้ข้อมูลไม่สามารถกู้คืนได้ หรือการทำลายสื่อทางกายภาพ โดยเลือกใช้ให้เหมาะสมกับประเภทของสื่อ เทคโนโลยี ความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. การใช้ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง

หาก CSP ใช้ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วงสำหรับการขนย้าย การเก็บรักษา การลบข้อมูล การทำลาย หรือการกำจัดอุปกรณ์และสื่อ CSP ควรกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยที่เหมาะสม และกำกับดูแลให้กระบวนการดังกล่าวเป็นไปตามข้อกำหนดของ CSP และข้อผูกพันที่มีต่อ CSC

การใช้ผู้รับจ้างช่วงไม่ควรทำให้ความรับผิดชอบของ CSP ตามข้อกำหนดนี้ลดลง

5. การจัดให้มีข้อมูลหรือหลักฐานแก่ CSC

CSP ควรสามารถให้ข้อมูลหรือหลักฐานที่เหมาะสมแก่ CSC เพื่อสนับสนุนการยืนยันตามข้อกำหนด โดยไม่จำเป็นต้องเปิดเผยข้อมูลที่อาจเพิ่มความเสี่ยงต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานหรือผู้ใช้บริการรายอื่น

หลักฐานอาจอยู่ในรูปของนโยบาย คำอธิบายกระบวนการ ข้อกำหนดตามสัญญา รายงานการตรวจประเมินโดยหน่วยงานอิสระ หรือหลักฐานอื่นที่สามารถแสดงว่ากระบวนการกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่ได้รับการควบคุมอย่างเหมาะสม

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อ 5.2.5.2 ไปปฏิบัติควรใช้แนวทางที่อิงระดับผลกระทบและความเสี่ยง โดย CSC ไม่จำเป็นต้องเข้าไปควบคุมหรือสั่งการกระบวนการกำจัดอุปกรณ์ภายในศูนย์ข้อมูลของ CSP แต่ต้องสามารถได้รับและประเมินการยืนยันจาก CSP ตามที่ข้อกำหนดกำหนด

สามารถสรุปกระบวนการได้ดังนี้

ข้อมูลหรือระบบสารสนเทศ

⟶ ระดับผลกระทบ

⟶ ระบุข้อกำหนดที่ใช้บังคับ

⟶ ระบุความต้องการด้านการลบหรือทำลายข้อมูล

⟶ ขอข้อมูลหรือการยืนยันจาก CSP

⟶ ประเมินความเพียงพอของหลักฐาน

⟶ ระบุช่องว่างหรือข้อจำกัด

⟶ ประเมินความเสี่ยง

⟶ ตัดสินใจและกำหนดผู้รับผิดชอบ

⟶ ติดตามและทบทวน

ร่างเพื่อรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. การใช้หลักฐานตามระดับความเสี่ยง

ไม่จำเป็นต้องกำหนดหลักฐานรูปแบบเดียวกันสำหรับบริการคลาวด์ทุกประเภท การพิจารณาความเพียงพอควรสัมพันธ์กับระดับผลกระทบ ความอ่อนไหวของข้อมูล และลักษณะของบริการ

สำหรับบริการที่มีผลกระทบระดับสูง CSC ควรให้ความสำคัญกับหลักฐานที่สามารถตรวจสอบขอบเขตและความน่าเชื่อถือได้ เช่น ข้อกำหนดตามสัญญา รายงานการตรวจประเมินโดยหน่วยงานอิสระ หรือหลักฐานอื่นที่ครอบคลุมกระบวนการจัดการอุปกรณ์และสื่อที่เกี่ยวข้อง

2. การเชื่อมโยงกับการสิ้นสุดบริการและการลบข้อมูล

เมื่อสิ้นสุดบริการ CSC อาจร้องขอให้ CSP ลบข้อมูลออกจากระบบบริการ อย่างไรก็ตาม สำเนาของข้อมูลบางส่วนอาจยังคงอยู่ในระบบสำรองหรือสื่อบันทึกข้อมูลตามระยะเวลาการเก็บรักษาและวงจรชีวิตของโครงสร้างพื้นฐาน จนกว่าจะเข้าสู่กระบวนการลบข้อมูล การทำให้ข้อมูลไม่สามารถกู้คืนได้ หรือการนำอุปกรณ์หรือสื่อกลับมาใช้ใหม่ตามกระบวนการของ CSP

ดังนั้น CSC ควรทำความเข้าใจทั้งเงื่อนไขการลบข้อมูลเมื่อยุติบริการ ระยะเวลาการเก็บรักษาหรือการลบข้อมูล การจัดการสำเนาสำรอง และกระบวนการจัดการอุปกรณ์หรือสื่อเมื่อมีการนำกลับมาใช้ใหม่หรือกำจัด

ทั้งนี้ ไม่ควรตีความว่า **การลบบัญชีผู้ใช้หรือการยุติบริการมีความหมายเท่ากับการทำลายสื่อบันทึกข้อมูลทางกายภาพในทันที**

3. การพิจารณากรณีใช้การเข้ารหัส

การเข้ารหัสข้อมูลสามารถช่วยลดความเสี่ยงจากข้อมูลที่อาจหลงเหลืออยู่บนอุปกรณ์หรือสื่อ แต่ไม่ควรถือว่าการเข้ารหัสเพียงอย่างเดียวทดแทนข้อกำหนดด้านการกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัยในทุกกรณี

หาก CSP ใช้การจัดการกุญแจเข้ารหัสเพื่อทำให้ข้อมูลไม่สามารถเข้าถึงหรือกู้คืนได้ (Cryptographic Erasure) ควรมีกระบวนการบริหารจัดการกุญแจและการยืนยันผลที่เหมาะสมกับเทคโนโลยีและความเสี่ยงที่เกี่ยวข้อง

รายละเอียดเกี่ยวกับการเข้ารหัสและการบริหารจัดการกุญแจควรเชื่อมโยงไปยังข้อกำหนดเฉพาะที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดซ้ำในข้อ 5.2.5.2

4. ตัวอย่างการนำไปใช้

ตัวอย่างที่ 1 การใช้บริการโครงสร้างพื้นฐานเป็นบริการ

หน่วยงานใช้บริการโครงสร้างพื้นฐานเป็นบริการ (Infrastructure as a Service: IaaS) สำหรับระบบที่ได้รับการจัดระดับผลกระทบเป็นระดับสูง

CSC ตรวจสอบข้อกำหนดของ CSP และได้รับหลักฐานว่ามีกระบวนการทำให้ข้อมูลบนสื่อไม่สามารถเข้าถึงได้ก่อนนำทรัพยากรกลับไปจัดสรรให้ผู้ใช้บริการรายอื่น และมีกระบวนการจัดการสื่อเมื่อสิ้นสุดอายุการใช้งาน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

CSC บันทึกหลักฐานดังกล่าวประกอบผลการประเมินบริการ โดยไม่จำเป็นต้องร้องขอหมายเลขประจำตัวของดิสก์หรือใบรับรองการทำลายสื่อเป็นรายอุปกรณ์ หาก CSP ไม่สามารถเชื่อมโยงสื่อทางกายภาพกับ CSC รายใดรายหนึ่งได้เนื่องจากสถาปัตยกรรมของบริการ และมีหลักฐานอื่นที่เพียงพอต่อการยืนยันการควบคุม

ตัวอย่างที่ 2 การใช้บริการซอฟต์แวร์เป็นบริการ

หน่วยงานใช้บริการซอฟต์แวร์เป็นบริการ (Software as a Service: SaaS) ซึ่ง CSC ไม่มีสิทธิเข้าถึงหรือควบคุมสื่อบันทึกข้อมูลทางกายภาพ

CSC จึงใช้ข้อกำหนดตามสัญญา เอกสารอธิบายกระบวนการลบข้อมูล และรายงานการตรวจประเมินของ CSP เป็นหลักฐานประกอบการยืนยันว่ามีกระบวนการจัดการสื่อและข้อมูลอย่างเหมาะสม

กรณีนี้ **ไม่ควรกำหนดให้ CSC ต้องได้รับใบรับรองการทำลายดิสก์ของตนเองทุกครั้ง** เพราะอาจไม่สอดคล้องกับลักษณะสถาปัตยกรรมแบบใช้ทรัพยากรร่วมกันของบริการคลาวด์

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างที่ 3 หลักฐานของ CSP ยังไม่เพียงพอ

CSC ร้องขอการยืนยันตามข้อ 5.2.5.2 แต่ CSP ให้เพียงข้อความทั่วไปว่า “ดำเนินการตามมาตรฐานอุตสาหกรรม” โดยไม่มีข้อมูลเพิ่มเติมที่สามารถใช้ประเมินขอบเขตหรือความน่าเชื่อถือของกระบวนการได้

CSC ควรขอข้อมูลหรือหลักฐานเพิ่มเติมตามความเหมาะสม หากยังไม่สามารถได้รับหลักฐานที่เพียงพอ ให้บันทึกช่องว่างดังกล่าวและประเมินความเสี่ยง

หากความเสี่ยงที่เหลืออยู่มีนัยสำคัญ การดำเนินการควรเชื่อมโยงไปยังกระบวนการตัดสินใจตามข้อ 5.1.2 โดยสามารถพิจารณาทางเลือก เช่น ขอเงื่อนไขเพิ่มเติม เลือกบริการหรือ CSP อื่น ใช้มาตรการลดความเสี่ยงเพิ่มเติม หรือยกระดับการตัดสินใจไปยังผู้มีอำนาจที่เหมาะสม

การที่ CSP ไม่สามารถจัดให้มีหลักฐานประเภทใดประเภทหนึ่ง ไม่ควรถูกใช้เป็นเหตุให้สรุปโดยอัตโนมัติว่าไม่เป็นไปตามข้อกำหนด หากประกาศมิได้กำหนดรูปแบบหลักฐานนั้นไว้โดยเฉพาะ อย่างไรก็ตาม CSC ต้องสามารถแสดงได้ว่า ข้อจำกัดของหลักฐานได้รับการประเมิน ผลกระทบและความเสี่ยงได้รับการพิจารณา และมีการตัดสินใจโดยผู้มีอำนาจตามความเหมาะสม

5. หลักฐานที่ควรพิจารณา

เพื่อสนับสนุนการตรวจสอบการปฏิบัติตามข้อ 5.2.5.2 CSC และ CSP ควรเก็บรักษาหรือสามารถเข้าถึงหลักฐานที่เหมาะสมกับบทบาท ขอบเขตบริการ และระดับความเสี่ยง โดยไม่จำเป็นต้องจัดทำเอกสารแยกต่างหากสำหรับทุกประเด็น

ลำดับ	ประเด็นที่ต้องสามารถยืนยันได้	ตัวอย่างหลักฐาน
1	ข้อกำหนดด้านการลบหรือทำลายข้อมูล	สัญญา ข้อตกลงการให้บริการ ข้อกำหนดด้านความมั่นคงปลอดภัย หรือนโยบายที่เกี่ยวข้อง
2	กระบวนการกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่	นโยบายหรือคำอธิบายกระบวนการจัดการอุปกรณ์และสื่อของ CSP
3	การลบข้อมูลก่อนนำสื่อกลับมาใช้ใหม่	คำอธิบายวิธีการควบคุม รายงานการประเมิน หรือหลักฐานการตรวจสอบที่เกี่ยวข้อง
4	การกำจัดหรือทำลายสื่อ	บันทึกการกำจัด รายงานการทำลาย หนังสือรับรอง หรือหลักฐานจากผู้ให้บริการที่เกี่ยวข้อง ตามความเหมาะสม
5	การใช้ผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง	ข้อกำหนดตามสัญญา รายชื่อผู้ให้บริการ ขอบเขตความรับผิดชอบ หรือหลักฐานการกำกับดูแล
6	การยืนยันจาก CSP	หนังสือยืนยัน ข้อกำหนดบริการ รายงานการตรวจประเมินโดยหน่วยงานอิสระ หรือหลักฐานอื่นที่สามารถใช้ยืนยันการปฏิบัติตามข้อกำหนด

ร่างสำหรับ Public Research เท่านั้น ห้ามใช้อ้างอิง

7	การประเมินโดย CSC	ผลการประเมิน CSP แบบประเมินความมั่นคงปลอดภัย บันทึกการตรวจสอบ หรือผลการพิจารณาความเพียงพอของหลักฐาน
8	ช่องว่างและความเสี่ยงที่เหลืออยู่	ผลการประเมินความเสี่ยง ทะเบียนความเสี่ยง หรือบันทึกข้อจำกัดที่เกี่ยวข้อง
9	การตัดสินใจและการอนุมัติ	บันทึกการตัดสินใจ การยอมรับความเสี่ยง หรือหลักฐานการอนุมัติของผู้มีอำนาจตามความเหมาะสม
10	การติดตามและทบทวน	ผลการทบทวน CSP การเปลี่ยนแปลงกระบวนการหรือบริการ และบันทึกการประเมินซ้ำเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

หมายเหตุ: หลักฐานข้างต้นเป็นตัวอย่างสำหรับประกอบการนำข้อกำหนดไปปฏิบัติ มิได้หมายความว่า CSC หรือ CSP ต้องจัดทำหลักฐานครบทุกประเภทในทุกกรณี และไม่จำเป็นต้องจัดทำเอกสารใหม่ หากเอกสาร ระบบรายงานการตรวจประเมิน ข้อกำหนดตามสัญญา หรือหลักฐานที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอและตรวจสอบย้อนกลับได้

สรุปข้อกำหนดและความรับผิดชอบด้านการรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security Requirements and Responsibility Summary)

การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อมสำหรับบริการคลาวด์ควรดำเนินการโดยเชื่อมโยงผลการประเมินระดับผลกระทบของข้อมูลหรือระบบสารสนเทศกับข้อกำหนดด้านตำแหน่งของศูนย์ข้อมูล และการกำจัดหรือนำอุปกรณ์หรือทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย ตามขอบเขตที่ข้อ 5.2.5 กำหนด

ตามตารางข้อกำหนดขั้นต่ำของประกาศ ข้อ 5.2.5 เป็นข้อกำหนดขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศที่มี **ผลกระทบระดับสูง** ซึ่งต้องดำเนินการตามข้อกำหนดส่วนที่ 1 และส่วนที่ 2 ทุกข้อ ดังนั้น การใช้ข้อ 5.2.5 ควรเริ่มจากผลการจัดระดับผลกระทบก่อน แล้วจึงพิจารณาข้อกำหนดและมาตรการที่เกี่ยวข้อง ไม่ควรเริ่มจากตำแหน่งของศูนย์ข้อมูลหรือความสามารถของ CSP แล้วจึงย้อนกลับไปกำหนดระดับผลกระทบภายหลัง

สาระสำคัญของข้อ 5.2.5 สามารถแบ่งออกเป็น 2 ประเด็น ได้แก่

1. **ตำแหน่งของศูนย์ข้อมูล** ตามข้อ 5.2.5.1 เพื่อให้การใช้ศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองเป็นไปตามข้อกำหนดของประกาศ และสามารถพิจารณาความเสี่ยงที่เกี่ยวข้องกับสถานที่จัดเก็บหรือประมวลผลข้อมูล เขตอำนาจทางกฎหมาย ความต่อเนื่องของบริการ และอธิปไตยข้อมูล
2. **การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย** ตามข้อ 5.2.5.2 เพื่อป้องกันไม่ให้ข้อมูลของ CSC สามารถถูกเข้าถึงหรือกู้คืนโดยไม่ได้รับอนุญาตเมื่ออุปกรณ์หรือสื่อถูกนำกลับมาใช้ใหม่ เปลี่ยนวัตถุประสงค์การใช้งาน หรือกำจัด

ร่างสำหรับ Public Hearing ไม่ใช่ - ห้ามอ้างอิง

หลักการสำคัญ

การนำข้อ 5.2.5 ไปปฏิบัติควรยึดหลักสำคัญ ดังนี้

1. **เริ่มจากระดับผลกระทบ**

   CSC ต้องพิจารณาระดับผลกระทบของข้อมูลหรือระบบสารสนเทศก่อน เพื่อกำหนดว่าข้อ 5.2.5 เป็นข้อกำหนดขั้นต่ำที่ใช้บังคับหรือไม่

2. **แยกการปฏิบัติตามข้อกำหนดออกจากการประเมินความเสี่ยง**

   การที่บริการเป็นไปตามข้อกำหนดด้านตำแหน่งศูนย์ข้อมูลมิได้หมายความว่าความเสี่ยงที่เกี่ยวข้องหมดไปทั้งหมด CSC ยังคงต้องพิจารณาความต่อเนื่อง เขตอำนาจทางกฎหมาย การพึ่งพาบริการ และอธิปไตยข้อมูลตามความเหมาะสม

3. **ใช้หลักความรับผิดชอบร่วม**

   CSC และ CSP มีบทบาทต่างกันตามขอบเขตที่แต่ละฝ่ายควบคุมได้ โดย CSC มีหน้าที่กำหนดความต้องการ ประเมินความเหมาะสม และขอข้อมูลหรือหลักฐาน ส่วน CSP มีหน้าที่จัดให้มีบริการและมาตรการที่เป็นไปตามข้อกำหนดในส่วนที่ตนรับผิดชอบ

4. **ใช้หลักฐานที่เหมาะสมกับความเสี่ยง**

   CSC ไม่จำเป็นต้องเข้าตรวจสอบศูนย์ข้อมูลหรืออุปกรณ์ทางกายภาพทุกกรณี หากสามารถใช้ข้อมูลจาก CSP ข้อกำหนดตามสัญญา รายงานการตรวจประเมิน หรือหลักฐานอื่นที่มีความน่าเชื่อถือและเพียงพอได้

5. **เชื่อมโยงช่องว่างกับการตัดสินใจ**

   หากพบข้อจำกัดหรือความเสี่ยงที่มีนัยสำคัญ ควรเชื่อมโยงผลการประเมินไปยังผู้มีอำนาจตัดสินใจและเจ้าของความเสี่ยงที่เหลืออยู่ตามข้อ 5.1.2 ไม่ควรหยุดเพียงการระบุว่า “ผ่าน” หรือ “ไม่ผ่าน” ทางเทคนิค

แนวทางดังกล่าวสามารถสรุปได้ดังนี้

ข้อมูลหรือระบบสารสนเทศ

⟶ ระดับผลกระทบ

⟶ ข้อกำหนดที่ใช้บังคับ

⟶ ความสามารถและหลักฐานของ CSP

⟶ ช่องว่างหรือข้อจำกัด

⟶ ความเสี่ยง

⟶ การตัดสินใจ

⟶ เจ้าของความเสี่ยงที่เหลืออยู่

⟶ การติดตามและทบทวน

ร่างสำหรับ Public Hearing ห้ามนำไปใช้งานจริง

1. สรุปความรับผิดชอบของ CSC และ CSP

ประเด็น	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
ระดับผลกระทบ	ประเมินและจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และกำหนดข้อกำหนดที่ใช้บังคับ	ให้ข้อมูลเกี่ยวกับความสามารถและข้อจำกัดของบริการเพื่อสนับสนุนการประเมิน
ศูนย์ข้อมูลหลัก	ตรวจสอบว่าบริการที่เลือกใช้เป็นไปตามข้อกำหนดด้านตำแหน่งศูนย์ข้อมูล	จัดตั้งศูนย์ข้อมูลหลักตามข้อกำหนดของประกาศ
ศูนย์ข้อมูลสำรอง	พิจารณาตำแหน่งของศูนย์ข้อมูลสำรองร่วมกับความต่อเนื่องและการกู้คืนบริการ	จัดตั้งศูนย์ข้อมูลสำรองตามเงื่อนไขที่ประกาศกำหนด และให้ข้อมูลที่เกี่ยวข้องแก่ CSC
สถานที่จัดเก็บและประมวลผลข้อมูล	พิจารณาตำแหน่ง ประเทศ พื้นที่ให้บริการ และข้อจำกัดที่เกี่ยวข้อง	ให้ข้อมูลในระดับที่เพียงพอให้ CSC สามารถยืนยันการปฏิบัติตามข้อกำหนด
เขตอำนาจทางกฎหมายและอธิปไตยข้อมูล	นำผลการประเมินจากข้อ 5.1.1 และ 5.1.3 มาประกอบการพิจารณา	ให้ข้อมูลเกี่ยวกับบริการ สถานที่ และองค์ประกอบที่เกี่ยวข้องตามขอบเขตความรับผิดชอบ
การเปลี่ยนแปลงตำแหน่งบริการ	ประเมินผลกระทบเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	แจ้งข้อมูลการเปลี่ยนแปลงตามข้อตกลงหรือเงื่อนไขบริการที่เกี่ยวข้อง
การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่	ร้องขอการยืนยันว่า CSP มีกระบวนการที่เหมาะสม	ตรวจสอบให้แน่ใจว่าการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่ดำเนินการอย่างปลอดภัยและทันท่วงที
อุปกรณ์หรือสื่อที่อาจมีข้อมูลส่วนบุคคล	พิจารณาความเพียงพอของการควบคุมตามความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง	ปฏิบัติต่ออุปกรณ์หรือสื่อที่อาจมีข้อมูลส่วนบุคคลเสมือนว่ามีข้อมูลส่วนบุคคลอยู่จริงตามข้อกำหนดของประกาศ
หลักฐาน	ขอ ประเมิน และเก็บรักษาหลักฐานที่เพียงพอต่อการตรวจสอบย้อนกลับ	จัดให้มีข้อมูลหรือหลักฐานที่เหมาะสมตามขอบเขตบริการ
ความเสี่ยงที่เหลืออยู่	ยกระดับประเด็นที่มีนัยสำคัญไปยังผู้มีอำนาจตามข้อ 5.1.2	สนับสนุนข้อมูลและการดำเนินการตามขอบเขตที่ CSP รับผิดชอบ

สาระในตารางข้างต้นเป็นการสรุปหน้าที่จากข้อ 5.2.5.1 และ 5.2.5.2 เพื่อให้เห็นความสัมพันธ์ของ CSC และ CSP โดยรายละเอียดข้อบังคับให้ยึดตามข้อความของประกาศแต่ละข้อเป็นหลัก

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

2. ความสัมพันธ์กับข้อกำหนดอื่น

ข้อ 5.2.5 ไม่ควรดำเนินการแยกจากข้อกำหนดด้านการกำกับดูแลในข้อ 5.1 แต่ควรใช้ผลการประเมินและการตัดสินใจที่ดำเนินการไว้แล้วเป็นข้อมูลนำเข้า โดยมีความสัมพันธ์โดยสรุป ดังนี้

ข้อ	บทบาทในการเชื่อมโยง
5.1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ	กำหนดหลักการตามระดับผลกระทบ ความเสี่ยง สถานที่จัดเก็บ และประมวลผล และอธิปไตยข้อมูล
5.1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ	กำหนดบทบาท ผู้มีอำนาจตัดสินใจ และเจ้าของความเสี่ยงที่เหลืออยู่
5.1.3 การปฏิบัติตามกฎ ระเบียบข้อบังคับ	พิจารณากฎหมาย เขตอำนาจทางกฎหมาย ข้อกำหนดตามสัญญา และหลักฐานการปฏิบัติตามข้อกำหนด
5.2.5.1 ตำแหน่งของศูนย์ข้อมูล	นำผลการประเมินมาใช้กับข้อกำหนดด้านตำแหน่งศูนย์ข้อมูลและพื้นที่ให้บริการ
5.2.5.2 การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย	ควบคุมความเสี่ยงจากข้อมูลที่อาจหลงเหลือเมื่ออุปกรณ์หรือสื่อถูกนำกลับมาใช้ใหม่หรือกำจัด
5.2.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน	รองรับรายละเอียดด้านการเปลี่ยนแปลง การสำรองข้อมูล บันทึกเหตุการณ์ และการดำเนินงานที่เกี่ยวข้อง
5.2.9 การจัดการผู้ให้บริการภายนอก	รองรับการกำกับดูแล CSP ผู้ให้บริการภายนอก และผู้รับจ้างช่วงที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

3. หลักฐานที่ควรพิจารณา

องค์กรไม่จำเป็นต้องจัดทำเอกสารใหม่สำหรับข้อ 5.2.5 ทุกประเภท หากหลักฐานจากกระบวนการที่มีอยู่สามารถใช้ยืนยันการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

ลำดับ	ประเด็นที่ต้องสามารถยืนยันได้	ตัวอย่างหลักฐาน
1	ระดับผลกระทบของข้อมูลหรือระบบ	ผลการจัดระดับผลกระทบ หรือผลการประเมินที่เกี่ยวข้อง
2	ข้อกำหนดที่ใช้บังคับ	รายการข้อกำหนดขั้นต่ำ กฎหมาย ประกาศ สัญญา หรือข้อกำหนดอื่นที่เกี่ยวข้อง
3	ตำแหน่งศูนย์ข้อมูลหลัก	ข้อมูลจาก CSP ข้อกำหนดบริการ หรือหลักฐานด้านพื้นที่ให้บริการ
4	ตำแหน่งศูนย์ข้อมูลสำรอง	ข้อมูลตำแหน่งศูนย์ข้อมูลสำรองและรูปแบบการกู้คืนบริการ
5	เขตอำนาจทางกฎหมาย	ผลการพิจารณากฎหมาย ประเทศ และเขตอำนาจทางกฎหมายที่เกี่ยวข้อง
6	อธิปไตยข้อมูล	ผลการประเมินความสามารถในการควบคุม เข้าถึง เคลื่อนย้าย กู้คืน หรือลบข้อมูล
7	การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่	นโยบาย ขั้นตอน คำรับรอง รายงานการตรวจประเมิน หรือหลักฐานอื่นจาก CSP
8	การใช้ผู้รับจ้างช่วง	ข้อมูลผู้ให้บริการภายนอกหรือผู้รับจ้างช่วง และข้อกำหนดการกำกับดูแลที่เกี่ยวข้อง
9	ช่องว่างและความเสี่ยง	ผลการประเมินความเสี่ยง ทะเบียนความเสี่ยง หรือบันทึกข้อจำกัด
10	การตัดสินใจและการติดตาม	บันทึกการอนุมัติ บันทึกการยอมรับความเสี่ยง ผลการทบทวน หรือหลักฐานการประเมินซ้ำ

หมายเหตุ: รายการดังกล่าวเป็นตัวอย่างหลักฐานสำหรับสนับสนุนการนำข้อกำหนดไปปฏิบัติ มิได้หมายความว่าองค์กรต้องจัดทำเอกสารแยกต่างหากหรือมีหลักฐานครบทุกประเภทในทุกกรณี หากหลักฐานที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอและตรวจสอบย้อนกลับได้

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้งานจริง

4. ข้อพิจารณาในการนำไปใช้

การดำเนินการตามข้อ 5.2.5 ควรมุ่งให้สามารถตอบคำถามสำคัญได้ว่า

ข้อมูลหรือระบบมีระดับผลกระทบใด ⟶ ข้อ 5.2.5 ใช้บังคับหรือไม่ ⟶ ตำแหน่งศูนย์ข้อมูลและกระบวนการจัดการอุปกรณ์เป็นไปตามข้อกำหนดหรือไม่ ⟶ มีหลักฐานใดยืนยัน ⟶ มีช่องว่างหรือความเสี่ยงใดเหลืออยู่ ⟶ ใครเป็นผู้ตัดสินใจ ⟶ ใครเป็นเจ้าของความเสี่ยงที่เหลืออยู่ ⟶ จะติดตามและทบทวนอย่างไร

สำหรับบริการคลาวด์สาธารณะ CSC ไม่ควรถูกกำหนดให้ต้องเข้าถึงหรือควบคุมโครงสร้างพื้นฐานทางกายภาพของ CSP ในระดับที่ไม่สอดคล้องกับลักษณะของบริการ แต่ควรกำหนดความต้องการและใช้ข้อมูลหรือหลักฐานที่มีความเหมาะสมกับระดับผลกระทบและความเสี่ยง

ในทางกลับกัน การที่ CSP มีศูนย์ข้อมูลอยู่ในประเทศไทยหรือมีนโยบายกำจัดอุปกรณ์เพียงอย่างเดียวไม่ควรถูกใช้เป็นข้อสรุปว่าการปฏิบัติตามข้อกำหนดครบถ้วนโดยอัตโนมัติ CSC ยังต้องพิจารณาว่าข้อมูลและหลักฐานดังกล่าวครอบคลุมบริการที่เลือกใช้จริง มีความเป็นปัจจุบัน และเพียงพอต่อข้อกำหนดที่มีผลใช้บังคับหรือไม่

โดยสรุป ข้อ 5.2.5 ทำหน้าที่นำผลจากการกำกับดูแลและการประเมินตามข้อ 5.1 มาสู่การควบคุมด้านกายภาพและสภาพแวดล้อมสำหรับข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูง โดย CSC และ CSP ต้องสามารถแสดงความเชื่อมโยงระหว่างข้อกำหนดที่ใช้บังคับ ข้อมูลหรือหลักฐาน ช่องว่างหรือข้อจำกัด ความเสี่ยง การตัดสินใจ ความรับผิดชอบ และการติดตามผลได้อย่างเหมาะสมและตรวจสอบย้อนกลับได้

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security) เป็นมาตรการสำคัญในการทำให้ระบบสารสนเทศและบริการคลาวด์สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย มีประสิทธิภาพ และต่อเนื่อง โดยมุ่งลดความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงระบบ การใช้ทรัพยากรที่ไม่เพียงพอ การสูญหายของข้อมูล ช่องโหว่ทางเทคนิค ตลอดจนการดำเนินงานหรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต

สำหรับสภาพแวดล้อมระบบคลาวด์ การรักษาความมั่นคงปลอดภัยการปฏิบัติการควรครอบคลุมการจัดการการเปลี่ยนแปลง (Change Management) การบริหารจัดการความจุ (Capacity Management) การสำรองข้อมูล (Information Backup) การบันทึกและการปกป้องข้อมูลในบันทึกเหตุการณ์ (Event Logging and Protection of Log Information) การบันทึกกิจกรรมของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs) การซิงโครไนซ์นาฬิกา (Clock Synchronization) การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities) และการแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน (Separation of Development, Testing and Operational Environments) ซึ่งสอดคล้องกับขอบเขตข้อกำหนด 5.2.6 ของมาตรฐาน

การดำเนินการดังกล่าวควรพิจารณาตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ลักษณะและประเภทของบริการคลาวด์ ตลอดจนผลการประเมินความเสี่ยง เพื่อให้มาตรการควบคุมมีความเหมาะสมกับบริบทของ

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามนำไปใช้อ้างอิง

หน่วยงาน และสามารถสนับสนุนการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศได้อย่างเหมาะสม

หมายเหตุ

การรักษาความมั่นคงปลอดภัยการปฏิบัติการในสภาพแวดล้อมระบบคลาวด์อาจเป็นความรับผิดชอบร่วมระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยขอบเขตความรับผิดชอบอาจแตกต่างกันตามประเภทบริการคลาวด์ เช่น การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) และการให้บริการซอฟต์แวร์ (Software as a Service: SaaS)

หน่วยงานจึงควรพิจารณาหลักการแบ่งความรับผิดชอบ (Shared Responsibility Model) ประกอบการกำหนดมาตรการควบคุม รวมถึงทำความเข้าใจความสามารถ ข้อจำกัด และขอบเขตความรับผิดชอบด้านการปฏิบัติการที่ผู้ให้บริการคลาวด์จัดให้ เพื่อให้สามารถกำหนดมาตรการเพิ่มเติมในส่วนที่อยู่ภายใต้ความรับผิดชอบของหน่วยงานได้อย่างเหมาะสม

5.2.6.1 การจัดการการเปลี่ยนแปลง (Change Management)

การเปลี่ยนแปลงระบบ บริการ หรือองค์ประกอบของบริการคลาวด์อาจส่งผลต่อความมั่นคงปลอดภัย ความพร้อมใช้งาน ประสิทธิภาพ และความต่อเนื่องของบริการ โดยการเปลี่ยนแปลงอาจเกิดขึ้นจากทั้งผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ตามขอบเขตการควบคุมของแต่ละฝ่าย

ในกรณีที่การเปลี่ยนแปลงอยู่ภายใต้การควบคุมของ CSC หน่วยงานควรดำเนินการตามกระบวนการจัดการการเปลี่ยนแปลงของตน ส่วนการเปลี่ยนแปลงที่อยู่ภายใต้การควบคุมของ CSP ควรมีการแจ้งข้อมูลที่เพียงพอให้ CSC สามารถประเมินผลกระทบและดำเนินมาตรการที่เกี่ยวข้องได้ ทั้งนี้ ขอบเขตความรับผิดชอบควรพิจารณาร่วมกับรูปแบบบริการคลาวด์ ข้อตกลงการให้บริการ และหลักความรับผิดชอบร่วม

การควบคุมการเปลี่ยนแปลงจึงไม่ควรตีความว่า CSC ต้องร้องขอให้ CSP ดำเนินการทุกกรณี แต่ควรมุ่งให้การเปลี่ยนแปลงที่อาจส่งผลกระทบต่อบริการได้รับการระบุ ประเมิน อนุมัติ ดำเนินการ และตรวจสอบอย่างเหมาะสมตามขอบเขตความรับผิดชอบ

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) กระบวนการจัดการการเปลี่ยนแปลงของผู้ใช้บริการคลาวด์ ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นจาก ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลแก่ ผู้ใช้บริการคลาวด์ เกี่ยวกับการเปลี่ยนแปลงในบริการคลาวด์ที่อาจส่งผลเสียต่อบริการคลาวด์ ข้อมูลต่อไปนี้จะช่วยให้ ผู้ใช้บริการคลาวด์ ระบุถึงผลกระทบของการเปลี่ยนแปลงที่อาจมีผลต่อความมั่นคงปลอดภัยสารสนเทศ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	– ประเภทของการเปลี่ยนแปลง – วันที่และเวลาที่วางแผนไว้ของการเปลี่ยนแปลง – คำอธิบายทางเทคนิคเกี่ยวกับการเปลี่ยนแปลงของบริการคลาวด์และระบบที่เกี่ยวข้อง (Underlying Systems) – การแจ้งเตือนการเริ่มต้นและการเปลี่ยนแปลงที่เสร็จสมบูรณ์ ข) เมื่อ ผู้ให้บริการคลาวด์ ให้บริการคลาวด์ที่ขึ้นอยู่กับผู้ให้บริการรายย่อยของ ผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ อาจจำเป็นต้องแจ้งการเปลี่ยนแปลงที่เกิดขึ้นให้ ผู้ใช้บริการคลาวด์ ทราบ

วัตถุประสงค์ (Objective)

1. เพื่อให้การเปลี่ยนแปลงที่เกี่ยวข้องกับบริการคลาวด์ได้รับการระบุ ประเมินผลกระทบ อนุมัติ ดำเนินการ และตรวจสอบอย่างเป็นระบบตามระดับความเสี่ยง
2. เพื่อให้ CSC สามารถพิจารณาและตอบสนองต่อการเปลี่ยนแปลงของ CSP ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย ความพร้อมใช้งาน หรือการดำเนินงานของระบบ
3. เพื่อให้ขอบเขตความรับผิดชอบและหลักฐานของการเปลี่ยนแปลงสามารถตรวจสอบย้อนกลับได้ตามรูปแบบบริการคลาวด์และข้อตกลงที่เกี่ยวข้อง
4.

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรดำเนินการจัดการการเปลี่ยนแปลงที่เกี่ยวข้องกับการใช้บริการคลาวด์ โดยอย่างน้อยควรครอบคลุมดังต่อไปนี้

1. การกำหนดกระบวนการจัดการการเปลี่ยนแปลง (Change Management Process)

ผู้ใช้บริการคลาวด์ควรกำหนดกระบวนการจัดการการเปลี่ยนแปลงอย่างเป็นทางการ (Formal Change Management Process) เพื่อให้มั่นใจว่าการเปลี่ยนแปลงที่เกิดขึ้นกับระบบคลาวด์ได้รับการควบคุมอย่างเหมาะสม

กระบวนการดังกล่าวควรครอบคลุมอย่างน้อย

1. การร้องขอการเปลี่ยนแปลง (Change Request)
2. การจำแนกประเภทของการเปลี่ยนแปลง (Change Classification)
3. การประเมินผลกระทบ (Impact Assessment)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

4. การประเมินความเสี่ยง (Risk Assessment)
5. การอนุมัติการเปลี่ยนแปลง (Change Approval)
6. การทดสอบก่อนนำไปใช้งาน (Testing Before Deployment)
7. การนำการเปลี่ยนแปลงไปใช้งาน (Change Implementation)
8. การตรวจสอบผลหลังการเปลี่ยนแปลง (Post-Change Review)

2. การประเมินผลกระทบจากการเปลี่ยนแปลง (Change Impact Assessment)

ผู้ใช้บริการคลาวด์ควรประเมินผลกระทบของการเปลี่ยนแปลงที่อาจส่งผลต่อ

- ความมั่นคงปลอดภัยสารสนเทศ (Information Security)
- ความพร้อมใช้งานของบริการ (Service Availability)
- ประสิทธิภาพของระบบ (System Performance)
- ความถูกต้องครบถ้วนของข้อมูล (Data Integrity)
- ข้อกำหนดทางกฎหมายและข้อกำหนดด้านการกำกับดูแล (Legal and Regulatory Requirements)

โดยควรพิจารณาผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงของผู้ให้บริการคลาวด์ด้วย

3. การติดตามและสื่อสารการเปลี่ยนแปลงจากผู้ให้บริการคลาวด์ (Cloud Provider Change Notification)

ในกรณีที่ผู้ให้บริการคลาวด์มีการเปลี่ยนแปลงบริการ (Cloud Service Change) ที่อาจส่งผลกระทบต่อระบบของผู้ใช้บริการ ผู้ใช้บริการควรมีช่องทางและกระบวนการในการรับทราบ วิเคราะห์ และดำเนินการตอบสนองต่อการเปลี่ยนแปลงดังกล่าว

ข้อมูลที่ควรได้รับจากผู้ให้บริการคลาวด์อาจประกอบด้วย

- ประเภทของการเปลี่ยนแปลง (Type of Change)
- วันที่และเวลาที่ดำเนินการ (Scheduled Date and Time)
- รายละเอียดทางเทคนิคของการเปลี่ยนแปลง (Technical Description)
- ผลกระทบที่คาดว่าจะเกิดขึ้น (Expected Impact)
- แนวทางการลดผลกระทบ (Mitigation Approach)
- สถานะการดำเนินการ (Implementation Status)

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถและข้อมูลที่เหมาะสม เพื่อสนับสนุนให้ผู้ใช้บริการสามารถบริหารจัดการผลกระทบจากการเปลี่ยนแปลงของบริการคลาวด์ได้

โดยควรดำเนินการดังต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. การแจ้งการเปลี่ยนแปลงของบริการคลาวด์ (Cloud Service Change Notification)

ผู้ให้บริการคลาวด์ควรมีกระบวนการแจ้งการเปลี่ยนแปลง (Change Notification Process) สำหรับการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย ความพร้อมใช้งาน หรือการทำงานของบริการคลาวด์

ข้อมูลที่ควรเปิดเผยแก่ผู้ใช้บริการ ได้แก่

รายการ	**ตัวอย่างข้อมูล**
ประเภทการเปลี่ยนแปลง (Change Type)	Software Update, Infrastructure Upgrade
ขอบเขตบริการ (Service Scope)	Compute, Storage, Network
ช่วงเวลาดำเนินการ (Maintenance Window)	วันที่และเวลาที่กำหนด
ผลกระทบที่คาดการณ์ (Expected Impact)	ไม่มีผลกระทบ / มีผลกระทบบางส่วน
แนวทางลดผลกระทบ (Mitigation)	Backup, Rollback Plan

2. การสนับสนุนการตรวจสอบย้อนกลับ (Change Traceability)

ผู้ให้บริการคลาวด์ควรมีความสามารถในการบันทึกข้อมูลการเปลี่ยนแปลง (Change Record) เพื่อสนับสนุนการตรวจสอบย้อนหลัง รวมถึงการวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Investigation)

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. ขอบเขตและที่มาของการเปลี่ยนแปลงในบริการคลาวด์ (Cloud Change Scope and Initiation)

การเปลี่ยนแปลงที่เกี่ยวข้องกับบริการคลาวด์อาจเกิดขึ้นจากผู้ใช้บริการคลาวด์ (CSC) หรือผู้ให้บริการคลาวด์ (CSP) โดยไม่จำเป็นต้องเป็นการร้องขอจาก CSC ไปยัง CSP ในทุกกรณี การพิจารณากระบวนการจัดการการเปลี่ยนแปลงควรพิจารณาตามขอบเขตการควบคุม (Control Boundary) รูปแบบบริการคลาวด์ และข้อตกลงการให้บริการที่เกี่ยวข้อง

ในกรณีที่การเปลี่ยนแปลงอยู่ภายใต้ขอบเขตการควบคุมของ CSC ผู้ใช้บริการคลาวด์อาจดำเนินการเปลี่ยนแปลงได้โดยตรงตามกระบวนการจัดการการเปลี่ยนแปลงของหน่วยงาน ส่วนการเปลี่ยนแปลงที่อยู่นอกขอบเขตการควบคุมของ CSC และต้องดำเนินการโดย CSP อาจต้องดำเนินการผ่านกระบวนการร้องขอบริการหรือการเปลี่ยนแปลงที่ CSP กำหนด

ในทางกลับกัน CSP อาจเป็นผู้ริเริ่มการเปลี่ยนแปลงต่อโครงสร้างพื้นฐาน แพลตฟอร์ม หรือบริการที่อยู่ภายใต้ความรับผิดชอบของตน โดย CSP ควรแจ้งข้อมูลเกี่ยวกับการเปลี่ยนแปลงที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อ CSC ตามเงื่อนไขของบริการ เพื่อให้ CSC สามารถประเมินผลกระทบและดำเนินมาตรการที่เกี่ยวข้องได้อย่างเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

จากขอบเขตดังกล่าว การเปลี่ยนแปลงในบริการคลาวด์สามารถเกิดขึ้นได้ทั้งจาก CSC และ CSP โดยกระบวนการที่ใช้ดำเนินการและการตอบสนองต่อการเปลี่ยนแปลงจะแตกต่างกันตามขอบเขตการควบคุม รูปแบบบริการคลาวด์ และข้อตกลงที่เกี่ยวข้อง ดังแสดงในรูปต่อไปนี้



รูปที่ 1 ขอบเขตและที่มาของการเปลี่ยนแปลงในบริการคลาวด์

ร่างสำหรับ Public

2. วงจรชีวิตการจัดการการเปลี่ยนแปลง (Change Management Lifecycle)

การเปลี่ยนแปลงที่อยู่ภายใต้ความรับผิดชอบของ CSC หรือ CSP ควรได้รับการบริหารจัดการอย่างเป็นระบบ โดยขอบเขตและรายละเอียดของกระบวนการขึ้นอยู่กับระดับความเสี่ยง ลักษณะของการเปลี่ยนแปลง และขอบเขตการควบคุมของแต่ละฝ่าย ดังแสดงในรูปต่อไปนี้



รูปที่ 2 วงจรชีวิตการจัดการการเปลี่ยนแปลงบนระบบคลาวด์

เหตุผลและความจำเป็น (Rationale)

การเปลี่ยนแปลงระบบโดยไม่มีการควบคุมที่เหมาะสมอาจทำให้เกิดความผิดพลาด การกำหนดกระบวนการจัดการการเปลี่ยนแปลงช่วยให้องค์กรสามารถควบคุมความเสี่ยง รักษาความต่อเนื่องของบริการ และลดผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศบนระบบคลาวด์

สำหรับผู้ให้บริการคลาวด์ การมีความสามารถในการแจ้งเตือนและให้ข้อมูลเกี่ยวกับการเปลี่ยนแปลงอย่างโปร่งใส ช่วยสร้างความเชื่อมั่นแก่ผู้ใช้บริการ และสนับสนุนหลักการความร่วมรับผิดชอบ (Shared Responsibility Model) ระหว่าง CSC และ CSP

ร่างสำหรับ Public

3. การจำแนกประเภทการเปลี่ยนแปลง (Change Classification)

หน่วยงานอาจกำหนดระดับการเปลี่ยนแปลงตามระดับความเสี่ยง เช่น

ประเภท	คำอธิบาย
การเปลี่ยนแปลงมาตรฐาน (Standard Change)	การเปลี่ยนแปลงที่มีขั้นตอนและความเสี่ยงต่ำ
การเปลี่ยนแปลงปกติ (Normal Change)	ต้องผ่านการประเมินและอนุมัติ
การเปลี่ยนแปลงฉุกเฉิน (Emergency Change)	ดำเนินการเมื่อจำเป็นเพื่อแก้ไขเหตุการณ์เร่งด่วน

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานที่ใช้ยืนยันการดำเนินการอาจอยู่ในรูปแบบข้อมูลจากระบบ เอกสาร รายงาน หรือบันทึกการปฏิบัติงานที่องค์กรมีอยู่แล้ว โดยไม่จำเป็นต้องจัดทำแบบฟอร์มใหม่ หากสามารถแสดงข้อมูลที่จำเป็นและตรวจสอบย้อนกลับได้อย่างเพียงพอ

ตัวอย่างหลักฐานสำหรับการจัดการการเปลี่ยนแปลง ได้แก่ แบบคำร้องขอเปลี่ยนแปลง บันทึกการประเมินผลกระทบ บันทึกการอนุมัติ ผลการทดสอบ แผนย้อนกลับ และบันทึกผลหลังการเปลี่ยนแปลง

ในกรณีที่องค์กรใช้แบบคำร้องขอเปลี่ยนแปลงและประเมินผลกระทบ (Change Request and Impact Assessment Form) ข้อมูลอาจประกอบด้วย

รายการ	รายละเอียด
Change ID	หมายเลขอ้างอิง
Description	รายละเอียดการเปลี่ยนแปลง
Business Impact	ผลกระทบทางธุรกิจ
Security Impact	ผลกระทบด้านความมั่นคงปลอดภัย
Risk Level	ระดับความเสี่ยง
Approval	ผู้อนุมัติ
Rollback Plan	แผนย้อนกลับ

ร่างเพื่อการประชาพิจารณ์ Public Hearing ไม่ใช้อ้างอิง

5.2.6.2 การบริหารจัดการความจุ (Capacity Management)

การใช้บริการคลาวด์ช่วยให้องค์กรสามารถเพิ่มหรือลดทรัพยากรตามความต้องการได้ แต่ความยืดหยุ่นดังกล่าวมิได้หมายความว่าทรัพยากรจะมีความเพียงพอโดยอัตโนมัติ องค์กรยังคงต้องติดตามการใช้งาน วิเคราะห์แนวโน้ม และพิจารณาข้อจำกัดของบริการ เช่น Quota, Service Limits และความสามารถในการขยายทรัพยากร

การบริหารจัดการความจุในสภาพแวดล้อมคลาวด์จึงเป็นความรับผิดชอบที่เกี่ยวข้องทั้ง CSC และ CSP โดย CSC มีหน้าที่กำหนดความต้องการและติดตามการใช้ทรัพยากรในส่วนที่ตนควบคุม ขณะที่ CSP ต้องบริหารความสามารถของโครงสร้างพื้นฐานและบริการภายใต้ขอบเขตที่ตนรับผิดชอบ เพื่อป้องกันผลกระทบจากการขาดแคลนทรัพยากร

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบให้แน่ใจว่าขีดความสามารถของทรัพยากรที่ตกลงกันไว้ในบริการคลาวด์นั้นตรงตามข้อกำหนดของ ผู้ใช้บริการคลาวด์ ข) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากรของบริการคลาวด์เพื่อให้มั่นใจในประสิทธิภาพของบริการคลาวด์เมื่อเวลาผ่านไป	ก) ผู้ให้บริการคลาวด์ ต้องตรวจสอบขีดความสามารถของทรัพยากรทั้งหมดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการขาดแคลนทรัพยากร

วัตถุประสงค์ (Objective)

1. เพื่อให้ทรัพยากรของบริการคลาวด์มีความเพียงพอและเหมาะสมกับปริมาณงาน ความสำคัญของระบบและระดับการให้บริการที่กำหนด
2. เพื่อให้สามารถตรวจพบแนวโน้ม ข้อจำกัด หรือภาวะที่อาจทำให้ทรัพยากรไม่เพียงพอ และดำเนินการปรับเพิ่มหรือลดทรัพยากรได้อย่างเหมาะสม
3. เพื่อให้ CSC และ CSP สามารถประสานข้อมูลด้านการใช้ทรัพยากร ข้อจำกัด และความสามารถในการขยายบริการตามขอบเขตความรับผิดชอบ

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรดำเนินการบริหารจัดการความจุของบริการคลาวด์ให้เหมาะสมกับความต้องการทางธุรกิจ (Business Requirements) และระดับความสำคัญของระบบสารสนเทศ (Information System Criticality) โดยควรดำเนินการอย่างน้อยดังต่อไปนี้

ร่างฯ เพื่อรับ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

1. การกำหนดความต้องการด้านทรัพยากร (Resource Requirement Definition)

ผู้ใช้บริการคลาวด์ควรกำหนดความต้องการด้านทรัพยากรของระบบสารสนเทศที่ใช้งานบนระบบคลาวด์ โดยพิจารณาจาก

- ลักษณะการใช้งานของระบบ (System Usage Pattern)
- ปริมาณข้อมูล (Data Volume)
- จำนวนผู้ใช้งาน (Number of Users)
- ระดับการให้บริการที่ต้องการ (Service Level Requirement)
- ความต้องการด้านการขยายระบบในอนาคต (Future Scalability Requirement)

ทั้งนี้ ควรมีการกำหนดค่าพื้นฐานด้านทรัพยากร (Resource Baseline) เพื่อใช้เป็นข้อมูลอ้างอิงในการติดตามและประเมินประสิทธิภาพของบริการ

2. การติดตามการใช้ทรัพยากร (Resource Utilization Monitoring)

ผู้ใช้บริการคลาวด์ควรมีการติดตามการใช้ทรัพยากรของบริการคลาวด์อย่างเหมาะสม เพื่อให้สามารถตรวจสอบแนวโน้มการใช้งาน (Usage Trend) และระบุความต้องการปรับเพิ่มหรือลดทรัพยากรได้อย่างเหมาะสม

ตัวอย่างข้อมูลที่ควรติดตาม ได้แก่

ประเภททรัพยากร	ตัวอย่างตัวชี้วัด
หน่วยประมวลผล (CPU)	CPU Utilization
หน่วยความจำ (Memory)	Memory Usage
พื้นที่จัดเก็บข้อมูล (Storage)	Storage Capacity / Growth Rate
เครือข่าย (Network)	Bandwidth Utilization
ระบบฐานข้อมูล (Database)	Connection Usage / Transaction Volume

3. การวิเคราะห์แนวโน้มและการวางแผนความจุ (Capacity Planning)

ผู้ใช้บริการคลาวด์ควรมีการวิเคราะห์แนวโน้มการใช้งานทรัพยากร (Capacity Trend Analysis) เพื่อวางแผนการเพิ่ม ลด หรือปรับเปลี่ยนทรัพยากรให้เหมาะสมกับความต้องการในอนาคต

การวางแผนความจุควรพิจารณา

- การเติบโตของปริมาณข้อมูล (Data Growth)
- การเพิ่มขึ้นของจำนวนผู้ใช้งาน (User Growth)
- การเปลี่ยนแปลงของกระบวนการทางธุรกิจ (Business Process Change)
- ช่วงเวลาที่มีการใช้งานสูง (Peak Usage Period)

สงวนสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

4. การกำหนดขีดจำกัดและการแจ้งเตือน (Threshold and Alert Management)

ผู้ใช้บริการคลาวด์ควรกำหนดค่าขีดจำกัด (Threshold) สำหรับทรัพยากรที่สำคัญ เพื่อให้สามารถตรวจพบสถานการณ์ที่อาจส่งผลกระทบต่อบริการได้ล่วงหน้า

ตัวอย่างเช่น

- การใช้งาน CPU สูงกว่าค่าที่กำหนด
- พื้นที่จัดเก็บข้อมูลใกล้เต็ม
- ปริมาณการใช้งานเครือข่ายเกินระดับที่กำหนด
- จำนวน Transaction สูงกว่าความสามารถรองรับ

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถในการบริหารจัดการทรัพยากรของระบบคลาวด์ เพื่อสนับสนุนความมั่นคงปลอดภัย ความพร้อมใช้งาน และประสิทธิภาพของบริการ

1. การตรวจสอบและบริหารทรัพยากรของระบบคลาวด์ (Cloud Resource Monitoring and Management)

ผู้ให้บริการคลาวด์ควรมีมาตรการในการติดตามการใช้ทรัพยากรของระบบคลาวด์ (Cloud Resource Monitoring) เพื่อป้องกันสถานการณ์ที่ทรัพยากรไม่เพียงพอ ซึ่งอาจส่งผลกระทบต่อบริการของผู้ใช้บริการคลาวด์

ผู้ให้บริการควรมีความสามารถ เช่น

- การตรวจสอบสถานะทรัพยากร (Resource Status Monitoring)
- การวิเคราะห์แนวโน้มการใช้งาน (Usage Trend Analysis)
- การแจ้งเตือนเหตุการณ์ผิดปกติ (Abnormal Condition Alerting)
- การเพิ่มหรือลดทรัพยากรตามความเหมาะสม (Resource Scaling)

2. การสนับสนุนการขยายทรัพยากร (Resource Scalability Support)

ผู้ให้บริการคลาวด์ควรมีความสามารถในการสนับสนุนการขยายทรัพยากร (Scalability) ตามความต้องการของผู้ใช้บริการ เช่น

- การเพิ่มทรัพยากรแบบอัตโนมัติ (Auto Scaling)
- การเพิ่มทรัพยากรตามคำร้องขอ (On-demand Scaling)
- การจัดสรรทรัพยากรเพิ่มเติมตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การให้ข้อมูลด้านความสามารถของบริการ (Service Capacity Transparency)

ผู้ให้บริการคลาวด์ควรให้ข้อมูลที่เหมาะสมเกี่ยวกับความสามารถของบริการ (Service Capability Information) เพื่อให้ผู้ใช้บริการสามารถประเมินความเหมาะสมของบริการกับความต้องการของตนเองได้

ข้อมูลอาจประกอบด้วย

- ข้อจำกัดของบริการ (Service Limitation)
- ความสามารถในการรองรับการขยายระบบ (Scaling Capability)
- ข้อกำหนดด้านประสิทธิภาพ (Performance Specification)
- เงื่อนไขการให้บริการ (Service Condition)

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. วงจรการบริหารจัดการความจุ (Capacity Management Lifecycle)

กระบวนการบริหารจัดการความจุควรดำเนินการอย่างต่อเนื่องตั้งแต่การวิเคราะห์ความต้องการ การติดตามการใช้ทรัพยากร การวางแผนความจุ การปรับขนาดทรัพยากร ตลอดจนการทบทวนและปรับปรุงตามผลการใช้งานจริง ดังแสดงในรูปต่อไปนี้



รูปที่ 3 วงจรการบริหารจัดการความจุ (Capacity Management Lifecycle)

เอกสาร - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

การบริหารจัดการความจุเป็นองค์ประกอบสำคัญของการรักษาความต่อเนื่องและความมั่นคงปลอดภัยของบริการคลาวด์ เนื่องจากทรัพยากรที่ไม่เพียงพออาจทำให้เกิดผลกระทบต่อประสิทธิภาพของระบบ ความพร้อมใช้งานของบริการ และประสบการณ์ของผู้ใช้งาน

การกำหนดกระบวนการติดตาม วิเคราะห์ และวางแผนความจุอย่างเหมาะสม ช่วยให้องค์กรสามารถใช้ทรัพยากรคลาวด์ได้อย่างมีประสิทธิภาพ ลดความเสี่ยงจากการขาดแคลนทรัพยากร และสนับสนุนการเติบโตของบริการดิจิทัลในระยะยาว

2. แนวทางการบริหารทรัพยากรอย่างมีประสิทธิภาพ (Resource Optimization)

หน่วยงานควรพิจารณาการใช้ทรัพยากรอย่างเหมาะสม เช่น

- การปรับขนาดทรัพยากรให้เหมาะสม (Right-sizing)
- การยกเลิกทรัพยากรที่ไม่ได้ใช้งาน (Resource Decommissioning)
- การกำหนดนโยบายการใช้งานทรัพยากร (Resource Usage Policy)
- การทบทวนทรัพยากรตามรอบระยะเวลา (Periodic Resource Review)

หลักฐานที่ควรพิจารณา (Recommended Evidence) การติดตามและบริหารจัดการความจุอาจใช้ข้อมูลจากเครื่องมือบริหารจัดการทรัพยากรของ CSC หรือ CSP รวมถึงรายงานจากระบบที่เกี่ยวข้องเป็นหลักฐานประกอบ โดยไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มใหม่ หากข้อมูลที่มีอยู่สามารถแสดงการติดตาม การวิเคราะห์แนวโน้ม การกำหนดค่าขีดจำกัด และการดำเนินการเมื่อทรัพยากรมีแนวโน้มไม่เพียงพอได้อย่างเหมาะสม

ตัวอย่างหลักฐานที่อาจใช้ประกอบการพิจารณา ได้แก่ รายงานการใช้ทรัพยากรจากระบบ Monitoring หรือ Management Console การแจ้งเตือนเมื่อถึงค่าขีดจำกัด ผลการวิเคราะห์แนวโน้ม แผนการปรับเพิ่มหรือลดทรัพยากร และบันทึกการทบทวนความจุ

ในกรณีที่องค์กรจัดทำ**รายงานการติดตามการใช้ทรัพยากรคลาวด์ (Cloud Resource Utilization Report)** ข้อมูลอาจประกอบด้วยรายการต่อไปนี้

รายการ	**รายละเอียด**
Service Name	ชื่อบริการ
Resource Type	ประเภททรัพยากร
Current Usage	ปริมาณใช้งานปัจจุบัน
Trend	แนวโน้มการใช้งาน
Threshold	ค่าควบคุม
Action Plan	แผนดำเนินการ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.2.6.3 การสำรองข้อมูล (Information Backup)

การสำรองข้อมูลบนระบบคลาวด์อาจดำเนินการโดย CSC, CSP หรือทั้งสองฝ่าย ขึ้นอยู่กับรูปแบบบริการและความสามารถที่ CSP จัดให้ ดังนั้น การใช้บริการที่มีคุณสมบัติด้านการสำรองข้อมูลมิได้ทำให้ความรับผิดชอบของ CSC สิ้นสุดลงโดยอัตโนมัติ CSC ยังคงต้องพิจารณาว่าความสามารถดังกล่าวสอดคล้องกับข้อกำหนดด้านขอบเขต ความถี่ ระยะเวลาเก็บรักษา และการกู้คืนขององค์กรหรือไม่

ในกรณีที่ CSP ไม่ได้จัดให้มีบริการสำรองข้อมูลในขอบเขตที่องค์กรต้องการ CSC ต้องพิจารณาจัดให้มีมาตรการเพิ่มเติมตามความเหมาะสม โดยควรเชื่อมโยงกับความสำคัญของข้อมูล RPO, RTO ข้อกำหนดทางกฎหมาย และความต้องการด้านความต่อเนื่องของบริการ

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ ผู้ให้บริการคลาวด์ มีความสามารถในการสำรองข้อมูลซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลจากผู้ให้บริการคลาวด์ นอกจากนี้ ผู้ใช้บริการคลาวด์ต้องทำการตรวจสอบเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดในการสำรองข้อมูลหรือไม่ ข) ผู้ใช้บริการคลาวด์ มีหน้าที่รับผิดชอบในการดำเนินการสำรองข้อมูลเมื่อ ผู้ให้บริการคลาวด์ ไม่ได้ให้บริการนี้	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลแก่ ผู้ใช้บริการคลาวด์ ข้อมูลจำเพาะควรมีข้อมูลต่อไปนี้ตามความเหมาะสม – ขอบเขตและกำหนดการของการสำรองข้อมูล – วิธีการสำรองข้อมูลและรูปแบบข้อมูล รวมถึงวิธีการเข้ารหัส หากมีความเกี่ยวข้อง – ระยะเวลาเก็บรักษาข้อมูลสำรอง – ขั้นตอนการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง – ขั้นตอนและระยะเวลาที่เกี่ยวข้องกับการกู้คืนข้อมูลจากการสำรองข้อมูล – ขั้นตอนในการทดสอบความสามารถในการสำรองข้อมูล – สถานที่จัดเก็บข้อมูลสำรอง ข) ผู้ให้บริการคลาวด์ ต้องให้บริการการเข้าถึงข้อมูลสำรองที่ปลอดภัยและแยกออกจากกัน หากบริการดังกล่าวมีการนำเสนอให้ ผู้ใช้บริการคลาวด์

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

วัตถุประสงค์ (Objective)

1. เพื่อให้ข้อมูลและองค์ประกอบสำคัญของระบบสามารถกู้คืนได้เมื่อเกิดการสูญหาย ความเสียหาย หรือเหตุการณ์ที่กระทบต่อความพร้อมใช้งาน
2. เพื่อให้ความสามารถด้านการสำรองและกู้คืนของ CSC และ CSP สอดคล้องกับความสำคัญของข้อมูล RPO, RTO และข้อกำหนดที่เกี่ยวข้อง

3. เพื่อให้มีการตรวจสอบและทดสอบความสามารถในการกู้คืนอย่างเหมาะสม และสามารถใช้ผลการทดสอบในการปรับปรุงมาตรการสำรองข้อมูลอย่างต่อเนื่อง

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดและดำเนินการบริหารจัดการการสำรองข้อมูลให้เหมาะสมกับลักษณะการใช้งานและระดับความสำคัญของข้อมูล โดยควรครอบคลุมประเด็นดังต่อไปนี้

1. การกำหนดขอบเขตข้อมูลที่ต้องสำรอง (Backup Scope Definition)

ผู้ใช้บริการคลาวด์ควรกำหนดประเภทข้อมูล ระบบสารสนเทศ และองค์ประกอบที่จำเป็นต้องได้รับการสำรองข้อมูล (Backup Target) โดยพิจารณาจาก

- ความสำคัญของข้อมูล (Information Classification)
- ผลกระทบต่อธุรกิจ (Business Impact)
- ความต้องการด้านการกู้คืน (Recovery Requirement)
- ข้อกำหนดทางกฎหมายและข้อกำหนดด้านการกำกับดูแล (Legal and Regulatory Requirement)

ตัวอย่างข้อมูลที่อาจต้องพิจารณาสำรอง ได้แก่

- ข้อมูลสำคัญขององค์กร (Critical Business Data)
- ฐานข้อมูล (Database)
- ไฟล์ระบบและข้อมูลการตั้งค่า (System Configuration)
- ข้อมูลสำหรับการให้บริการ (Service Data)
- ข้อมูลที่ใช้สำหรับการกู้คืนระบบ (Recovery Data)

2. การกำหนดนโยบายและรอบเวลาการสำรองข้อมูล (Backup Policy and Schedule)

ผู้ใช้บริการคลาวด์ควรกำหนดนโยบายการสำรองข้อมูล (Backup Policy) และรอบเวลาการสำรองข้อมูล (Backup Schedule) ให้เหมาะสมกับความต้องการของระบบ

ปัจจัยที่ควรพิจารณา ได้แก่

- ความถี่ในการสำรองข้อมูล (Backup Frequency)
- ระยะเวลาการเก็บรักษาข้อมูลสำรอง (Backup Retention Period)
- จุดเวลาที่สามารถกู้คืนได้ (Recovery Point Objective: RPO)
- ระยะเวลาที่ต้องใช้ในการกู้คืนระบบ (Recovery Time Objective: RTO)

ตัวอย่างเช่น

ระดับข้อมูล	แนวทางพิจารณา
ข้อมูลสำคัญมาก (High Criticality Data)	สำรองข้อมูลบ่อยและทดสอบการกู้คืนอย่างสม่ำเสมอ
ข้อมูลทั่วไป (General Data)	กำหนดรอบเวลาตามความเหมาะสมของธุรกิจ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การปกป้องข้อมูลสำรอง (Backup Protection)

ผู้ใช้บริการคลาวด์ควรจัดให้มีมาตรการป้องกันข้อมูลสำรอง เพื่อป้องกันการเข้าถึง การแก้ไข หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต

มาตรการที่ควรพิจารณา ได้แก่

- การควบคุมการเข้าถึงข้อมูลสำรอง (Backup Access Control)
- การเข้ารหัสข้อมูลสำรอง (Backup Encryption)
- การกำหนดสิทธิผู้ดูแลระบบสำรอง (Backup Administrator Privilege Management)
- การป้องกันข้อมูลสำรองจากมัลแวร์หรือแรนซัมแวร์ (Malware and Ransomware Protection)

4. การทดสอบการกู้คืนข้อมูล (Backup Restoration Testing)

ผู้ใช้บริการคลาวด์ควรดำเนินการทดสอบการกู้คืนข้อมูล (Restore Testing) อย่างสม่ำเสมอ เพื่อยืนยันว่าข้อมูลสำรองสามารถนำกลับมาใช้งานได้จริงเมื่อเกิดเหตุการณ์ผิดปกติ

การทดสอบควรครอบคลุม

- ความครบถ้วนของข้อมูล (Data Completeness)
- ความถูกต้องของข้อมูล (Data Integrity)
- ระยะเวลาการกู้คืน (Recovery Time)
- ขั้นตอนการกู้คืน (Recovery Procedure)

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถด้านการสำรองและกู้คืนข้อมูล (Backup and Recovery Capability) เพื่อสนับสนุนให้ผู้ใช้บริการสามารถบริหารจัดการข้อมูลได้อย่างเหมาะสม

1. การจัดให้มีความสามารถในการสำรองข้อมูล (Backup Capability)

ผู้ให้บริการคลาวด์ควรมีบริการหรือความสามารถที่สนับสนุนการสำรองข้อมูลตามประเภทบริการคลาวด์ (Cloud Service Model) ที่ให้บริการ

ความสามารถดังกล่าวอาจประกอบด้วย

- การกำหนดรอบเวลาการสำรองข้อมูล (Backup Scheduling)
- การกำหนดระยะเวลาเก็บรักษาข้อมูล (Retention Management)
- การกู้คืนข้อมูลตามความต้องการ (On-demand Restore)
- การตรวจสอบสถานะการสำรองข้อมูล (Backup Status Monitoring)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2. การให้ข้อมูลเกี่ยวกับบริการสำรองข้อมูล (Backup Service Transparency)

ผู้ให้บริการคลาวด์ควรเปิดเผยข้อมูลที่จำเป็นเกี่ยวกับความสามารถและข้อจำกัดของบริการสำรองข้อมูล เพื่อให้ผู้ใช้บริการสามารถประเมินความเหมาะสมกับความต้องการของตนเอง

ข้อมูลที่ควรมี ได้แก่

รายการ	**รายละเอียด**
ขอบเขตการสำรอง (Backup Scope)	ข้อมูลหรือบริการที่รองรับ
วิธีการสำรอง (Backup Method)	Full / Incremental / Snapshot
ระยะเวลาเก็บรักษา (Retention Period)	ระยะเวลาการจัดเก็บ
วิธีการกู้คืน (Restore Method)	ขั้นตอนและเงื่อนไข
ข้อจำกัดบริการ (Service Limitation)	เงื่อนไขที่เกี่ยวข้อง

3. การสนับสนุนการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง (Backup Integrity Verification)

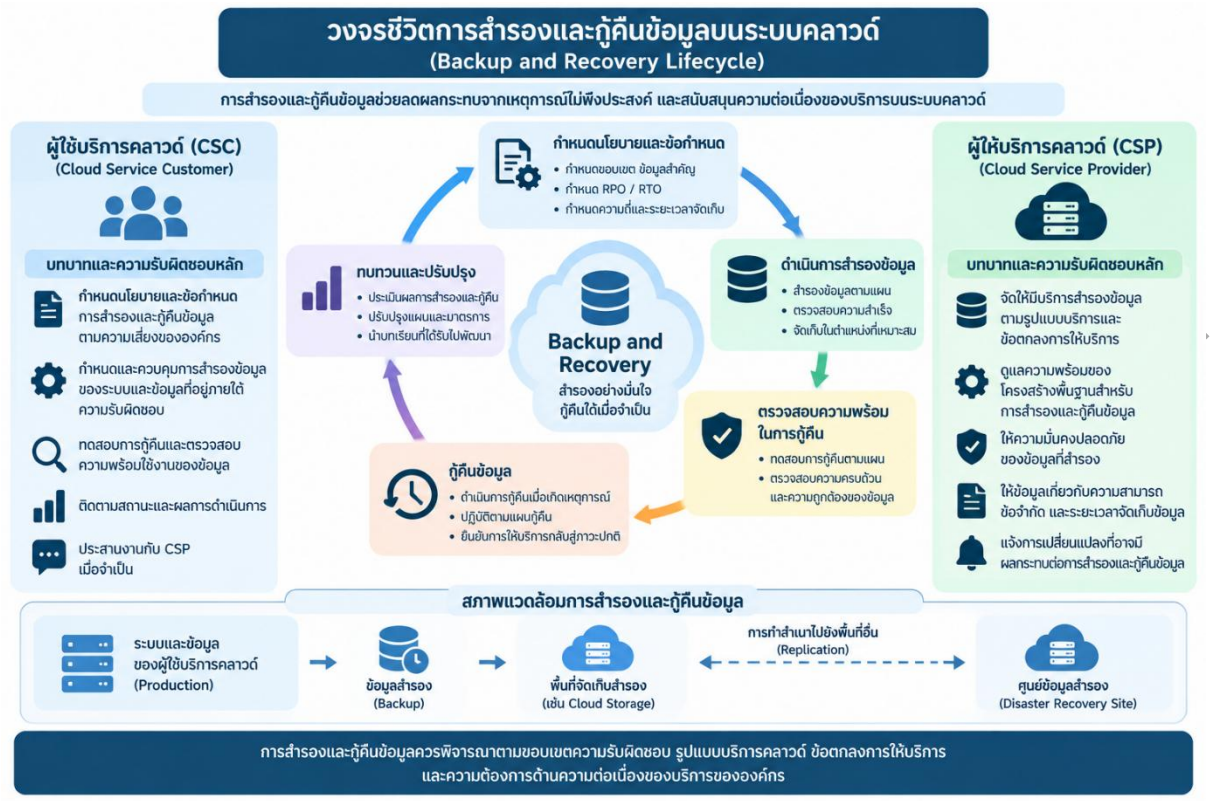
ผู้ให้บริการคลาวด์ควรมีความสามารถในการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง (Backup Integrity Verification) เพื่อช่วยลดความเสี่ยงจากข้อมูลสำรองที่ไม่สามารถใช้งานได้เมื่อเกิดเหตุการณ์จำเป็น

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. วงจรชีวิตการสำรองและกู้คืนข้อมูล (Backup and Recovery Lifecycle)

การสำรองข้อมูลที่มีประสิทธิผลไม่สิ้นสุดเพียงการสร้างสำเนาข้อมูล แต่ควรครอบคลุมตั้งแต่การกำหนดความต้องการ การสำรองและปกป้องข้อมูล การติดตามผล การทดสอบการกู้คืน ตลอดจนการทบทวนและปรับปรุงให้สอดคล้องกับความต้องการของระบบ ดังแสดงในรูปต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง



รูปที่ 4 วงจรชีวิตการสำรองและกู้คืนข้อมูล (Backup and Recovery Lifecycle)

เหตุผลและความจำเป็น (Rationale)

การสำรองข้อมูลเป็นมาตรการพื้นฐานในการลดผลกระทบจากเหตุการณ์ที่อาจทำให้ข้อมูลสูญหายหรือไม่สามารถเข้าถึงได้ การมีนโยบาย กระบวนการ และการทดสอบการกู้คืนที่เหมาะสม ช่วยให้องค์กรสามารถรักษาความต่อเนื่องของบริการ (Service Continuity) และลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

สำหรับบริการคลาวด์ ความรับผิดชอบด้านการสำรองข้อมูลอาจแตกต่างกันตามรูปแบบบริการ (Cloud Service Model) ดังนั้นผู้ใช้บริการและผู้ให้บริการคลาวด์ควรกำหนดขอบเขตความรับผิดชอบ (Responsibility Boundary) ให้ชัดเจน เพื่อป้องกันความเข้าใจคลาดเคลื่อนและเพิ่มความเชื่อมั่นในการใช้บริการคลาวด์

2. แนวทางการสำรองข้อมูลตามหลักการบริหารความเสี่ยง (Risk-based Backup Strategy)

องค์กรควรกำหนดกลยุทธ์การสำรองข้อมูล (Backup Strategy) บนพื้นฐานของการบริหารความเสี่ยง (Risk-based Approach) โดยพิจารณาระดับความสำคัญของข้อมูล (Information Classification and Criticality) ความเสี่ยงทางธุรกิจ (Business Risk) ผลกระทบจากการหยุดชะงักของบริการ (Business Impact) ข้อกำหนดด้านกฎหมาย ระเบียบ และพันธกรณีตามสัญญา ตลอดจนสถาปัตยกรรมบริการคลาวด์ (Cloud Service Architecture) และรูปแบบความรับผิดชอบร่วม (Shared Responsibility Model) ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service

ร่างสำหรับ Public Hearing

Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) เพื่อให้สามารถกู้คืนข้อมูลและบริการได้ภายในระดับที่องค์กรยอมรับได้

การกำหนดกลยุทธ์การสำรองข้อมูลควรพิจารณาประเด็นสำคัญ ดังต่อไปนี้

- พิจารณาเลือกใช้แนวทาง 3-2-1 Backup Principle หรือแนวทางที่มีประสิทธิผลเทียบเท่าหรือดีกว่า โดยคำนึงถึงความเหมาะสมของระบบสารสนเทศและระดับความเสี่ยงขององค์กร
- สำหรับข้อมูลที่มีความสำคัญสูงหรือมีความเสี่ยงต่อการถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) หรือการทำลายข้อมูลโดยเจตนา ควรพิจารณาใช้แนวทาง 3-2-1-1 Backup หรือ 3-2-1-1-0 Backup ซึ่งมีการจัดเก็บข้อมูลสำรองแบบไม่สามารถแก้ไขหรือลบได้ (Immutable Backup) หรือจัดเก็บแบบแยกขาดจากระบบ (Air-gapped Backup) พร้อมมีการตรวจสอบความถูกต้องของข้อมูลสำรองหลังการสำรองหรือหลังการกู้คืน (Zero Backup Errors)
- พิจารณาตำแหน่งที่จัดเก็บข้อมูลสำรอง (Backup Location) ให้สอดคล้องกับข้อกำหนดด้านกฎหมาย ข้อกำหนดของหน่วยงานกำกับดูแล นโยบายขององค์กร และข้อกำหนดเรื่องตำแหน่งของศูนย์ข้อมูล (Data Center Location) ตามข้อ 5.2.5.1 โดยเฉพาะกรณีที่มีการจัดเก็บหรือประมวลผลข้อมูลในต่างประเทศ ซึ่งต้องพิจารณาความเสี่ยงจากกฎหมายต่างประเทศ (Extraterritorial Laws) เขตอำนาจศาล (Jurisdiction) การโอนข้อมูลข้ามพรมแดน (Cross-border Data Transfer) และอำนาจในการเข้าถึงข้อมูลของหน่วยงานภาครัฐในต่างประเทศ
- พิจารณาเลือกรูปแบบการจัดเก็บข้อมูลสำรองให้เหมาะสมกับระดับความเสี่ยงและความต่อเนื่องทางธุรกิจ เช่น การจัดเก็บภายในองค์กร (On-premises Backup) การจัดเก็บบนระบบคลาวด์ (Cloud Backup) การจัดเก็บแบบหลายผู้ให้บริการคลาวด์ (Multi-Cloud Backup) หรือการใช้รูปแบบผสมผสาน (Hybrid Backup) ทั้งนี้ควรคำนึงถึงความพร้อมใช้งาน ความยืดหยุ่น ความสามารถในการกู้คืน ความเสี่ยงจากการพึ่งพาผู้ให้บริการรายเดียว (Vendor Lock-in) และต้นทุนรวมในการดำเนินงาน (Total Cost of Ownership)
- พิจารณาเลือกประเภทของพื้นที่จัดเก็บข้อมูลสำรอง (Storage Tier) ให้เหมาะสมกับความถี่ในการกู้คืนข้อมูล ระยะเวลาการเก็บรักษา (Retention Period) ระยะเวลาในการกู้คืน (Recovery Time Objective: RTO) จุดกู้คืนข้อมูล (Recovery Point Objective: RPO) และค่าใช้จ่ายของพื้นที่จัดเก็บแต่ละประเภท เช่น Hot Storage, Cool Storage, Cold Storage หรือ Archive Storage
- กำหนดให้ข้อมูลสำรองได้รับการปกป้องด้วยมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล (Encryption) การควบคุมสิทธิ์ในการเข้าถึง (Access Control) การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-factor Authentication: MFA) การบันทึกเหตุการณ์ (Logging) และการติดตามตรวจสอบ (Monitoring)
- ทดสอบการกู้คืนข้อมูล (Backup Restoration Testing) เป็นระยะ เพื่อยืนยันว่าข้อมูลสำรองสามารถกู้คืนได้จริงภายในระยะเวลาที่องค์กรกำหนด และผลการทดสอบควรถูกนำไปใช้ในการปรับปรุงแผนการสำรองและการกู้คืนข้อมูลอย่างต่อเนื่อง (Continual Improvement)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานเกี่ยวกับการสำรองและกู้คืนข้อมูลควรสามารถแสดงให้เห็นว่า ขอบเขตและความถี่ในการสำรองข้อมูล ระยะเวลาเก็บรักษา สถานะการสำรอง ตลอดจนการทดสอบความสามารถในการกู้คืนได้รับการกำหนดและดำเนินการอย่างเหมาะสมกับความสำคัญของข้อมูลและความต้องการของระบบ

หลักฐานอาจอยู่ในรูปของรายงานจากระบบสำรองข้อมูล การตั้งค่า Backup Policy หรือ Schedule สถานะการสำรองข้อมูล ผลการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง รายงานการทดสอบการกู้คืน หรือข้อมูลจาก CSP ตามขอบเขตความรับผิดชอบ โดยไม่จำเป็นต้องจัดทำแบบฟอร์มแยกเพิ่มเติม หากหลักฐานที่มีอยู่สามารถตรวจสอบได้อย่างเพียงพอ

ในกรณีที่องค์กรใช้**แบบตรวจสอบการสำรองและกู้คืนข้อมูลบนระบบคลาวด์ (Cloud Backup and Restore Verification Checklist)** ข้อมูลอาจประกอบด้วยรายการต่อไปนี้

รายการ	**รายละเอียด**
System / Service Name	ระบบหรือบริการ
Backup Scope	ขอบเขตข้อมูลสำรอง
Backup Frequency	ความถี่การสำรอง
Retention Period	ระยะเวลาเก็บรักษา
Last Backup Status	สถานะล่าสุด
Restore Test Date	วันที่ทดสอบกู้คืน
Test Result	ผลการทดสอบ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.2.6.4 การบันทึกเหตุการณ์ (Event Logging)

การบันทึกเหตุการณ์เป็นพื้นฐานสำคัญของการตรวจสอบย้อนกลับ การวิเคราะห์เหตุการณ์ และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย โดยแหล่งข้อมูลและความสามารถในการเข้าถึงบันทึกเหตุการณ์อาจแตกต่างกันตามรูปแบบบริการคลาวด์และขอบเขตที่ CSC และ CSP ควบคุม

CSC จึงควรกำหนดว่าระบบหรือบริการใดต้องบันทึกเหตุการณ์ เหตุการณ์ประเภทใดต้องถูกบันทึก ข้อมูลใดต้องมีในบันทึก และต้องเก็บรักษาเป็นระยะเวลาเท่าใด ขณะที่ CSP ควรจัดให้มีความสามารถในการบันทึก เข้าถึง ส่งออก หรือเชื่อมต่อข้อมูลบันทึกตามขอบเขตของบริการที่ให้

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องจัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์และตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนดเหล่านั้นหรือไม่	ก) ผู้ให้บริการคลาวด์ ต้องให้ผู้ใช้บริการสามารถบันทึกเหตุการณ์ ข) ในกรณีที่เป็นไปได้ บันทึกเหตุการณ์ควรบันทึกว่าข้อมูลส่วนบุคคลได้รับการเปลี่ยนแปลงหรือไม่ (เพิ่ม แก้ไข หรือลบ) จากเหตุการณ์นั้น และโดยใคร (Audit Log) ในกรณีที่มีผู้ให้บริการหลายรายเข้ามาเกี่ยวข้องในการให้บริการจากหลากหลายประเภทบริการของสถาปัตยกรรมอ้างอิงประมวลผลคลาวด์ อาจมีบทบาทที่แตกต่างหรือแบ่งปันกันในการปฏิบัติตามข้อนี้

วัตถุประสงค์ (Objective)

1. เพื่อให้มีข้อมูลบันทึกเหตุการณ์ที่เพียงพอสำหรับการตรวจสอบ ติดตาม วิเคราะห์ และสืบสวนเหตุการณ์ที่เกี่ยวข้องกับบริการคลาวด์
2. เพื่อให้ข้อกำหนดด้านประเภทเหตุการณ์ เนื้อหาของบันทึก ระยะเวลาเก็บรักษา และการทบทวนมีความเหมาะสมกับความสำคัญและความเสี่ยงของระบบ
3. เพื่อให้ CSC สามารถใช้ประโยชน์จากความสามารถด้าน Logging ของ CSP และเชื่อมโยงข้อมูลกับระบบติดตามหรือวิเคราะห์เหตุการณ์ตามความเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดแนวทางการจัดการบันทึกเหตุการณ์ (Logging Management) ให้เหมาะสมกับประเภทของระบบสารสนเทศและระดับความเสี่ยง โดยควรดำเนินการดังต่อไปนี้

1. การกำหนดประเภทเหตุการณ์ที่ต้องบันทึก (Logging Requirements Definition)

ผู้ใช้บริการคลาวด์ควรกำหนดประเภทเหตุการณ์ (Event Types) ที่จำเป็นต้องมีการบันทึก เพื่อให้สามารถตรวจสอบและวิเคราะห์กิจกรรมที่เกิดขึ้นกับระบบได้อย่างเหมาะสม

ตัวอย่างเหตุการณ์ที่ควรพิจารณาบันทึก ได้แก่

ประเภทเหตุการณ์	ตัวอย่าง
การเข้าสู่ระบบ (Authentication Events)	Login, Logout, Failed Login
การใช้งานสิทธิพิเศษ (Privileged Activities)	การใช้สิทธิ Administrator
การเปลี่ยนแปลงระบบ (System Changes)	Configuration Change
การเข้าถึงข้อมูล (Data Access Events)	Data Access, Data Export
เหตุการณ์ด้านความปลอดภัย (Security Events)	Malware Detection, Policy Violation

2. การกำหนดข้อมูลที่ต้องบันทึก (Log Content Definition)

ผู้ใช้บริการคลาวด์ควรกำหนดข้อมูลขั้นต่ำที่ต้องจัดเก็บในบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบย้อนหลังได้อย่างมีประสิทธิภาพ

ข้อมูลที่ควรมี ได้แก่

- วันที่และเวลา (Timestamp)
- แหล่งที่มาของเหตุการณ์ (Event Source)
- ผู้ดำเนินการ (User Identity)
- ประเภทกิจกรรม (Activity Type)
- ผลลัพธ์ของกิจกรรม (Event Outcome)
- ระบบหรือทรัพยากรที่เกี่ยวข้อง (Affected System or Resource)

3. การกำหนดระยะเวลาการเก็บรักษาบันทึกเหตุการณ์ (Log Retention)

ผู้ใช้บริการคลาวด์ควรกำหนดระยะเวลาการเก็บรักษาบันทึกเหตุการณ์ (Log Retention Period) ให้สอดคล้องกับ

- ความสำคัญของระบบ (System Criticality)

ร่างสำหรับรับฟังความคิดเห็น (Public Hearing Draft) ห้ามนำไปใช้อ้างอิง

- ข้อกำหนดทางกฎหมาย (Legal Requirement)
- ข้อกำหนดด้านการตรวจสอบ (Audit Requirement)
- ความต้องการด้านการวิเคราะห์เหตุการณ์ (Investigation Requirement)

4. การทบทวนและตรวจสอบบันทึกเหตุการณ์ (Log Review and Monitoring)

ผู้ใช้บริการคลาวด์ควรมีการตรวจสอบและทบทวนบันทึกเหตุการณ์อย่างเหมาะสม เพื่อค้นหากิจกรรมผิดปกติหรือเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบ

แนวทางการตรวจสอบอาจประกอบด้วย

- การตรวจสอบแบบตามรอบเวลา (Periodic Review)
- การแจ้งเตือนเหตุการณ์สำคัญ (Security Alert)
- การวิเคราะห์รูปแบบพฤติกรรม (Behavior Analysis)

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถในการบันทึกเหตุการณ์ของบริการคลาวด์ (Cloud Service Logging Capability) เพื่อสนับสนุนการตรวจสอบและการบริหารจัดการความมั่นคงปลอดภัย

1. การจัดให้มีความสามารถในการบันทึกเหตุการณ์ (Logging Capability)

ผู้ให้บริการคลาวด์ควรสนับสนุนการบันทึกเหตุการณ์ที่เกี่ยวข้องกับบริการที่ให้บริการแก่ผู้ใช้บริการ โดยพิจารณาตามรูปแบบบริการคลาวด์ (Cloud Service Model)

ตัวอย่างข้อมูลที่ควรสนับสนุน ได้แก่

- การเข้าถึงระบบ (Access Logs)
- การใช้งานทรัพยากร (Resource Activity Logs)
- การเปลี่ยนแปลงการตั้งค่า (Configuration Change Logs)
- เหตุการณ์ด้านความมั่นคงปลอดภัย (Security Event Logs)
-

2. การให้บริการเข้าถึงข้อมูลบันทึกเหตุการณ์ (Log Access Capability)

ผู้ให้บริการคลาวด์ควรมีช่องทางที่เหมาะสมสำหรับให้ผู้ใช้บริการสามารถเข้าถึงหรือรับข้อมูลบันทึกเหตุการณ์ตามขอบเขตความรับผิดชอบ

รูปแบบการให้บริการอาจประกอบด้วย

- Portal สำหรับตรวจสอบบันทึก (Management Portal)

เอกสารสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- API สำหรับเรียกข้อมูล (Log API)
- การส่งข้อมูลไปยังระบบภายนอก (Log Forwarding)

3. การสนับสนุนการตรวจสอบด้านความมั่นคงปลอดภัย (Security Monitoring Support)

ผู้ให้บริการคลาวด์ควรมีความสามารถสนับสนุนการเชื่อมต่อกับระบบตรวจสอบด้านความมั่นคงปลอดภัย เช่น

- ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM)
- ระบบตรวจจับภัยคุกคาม (Threat Detection System)
- ศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย (Security Operations Center: SOC)

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. แนวทางสถาปัตยกรรมการจัดการบันทึกเหตุการณ์ (Logging Architecture)

องค์กรควรพิจารณาการจัดเก็บและบริหารจัดการบันทึกเหตุการณ์ในลักษณะรวมศูนย์ (Centralized Logging) เพื่อเพิ่มประสิทธิภาพในการตรวจสอบและวิเคราะห์ข้อมูล

การจัดการบันทึกเหตุการณ์บนระบบคลาวด์ควรพิจารณาตลอดเส้นทางของข้อมูล ตั้งแต่แหล่งกำเนิดบันทึกเหตุการณ์ การรวบรวม การจัดเก็บ การวิเคราะห์ และการนำข้อมูลไปใช้ในการติดตามและตอบสนองต่อเหตุการณ์ โดยคำนึงถึงขอบเขตความรับผิดชอบของ CSC และ CSP ดังแสดงในรูปต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปที่ 5 สถาปัตยกรรมการจัดการบันทึกเหตุการณ์บนระบบคลาวด์

เหตุผลและความจำเป็น (Rationale)

การบันทึกเหตุการณ์เป็นกลไกสำคัญในการสร้างความสามารถด้านการตรวจสอบย้อนกลับ (Traceability) และสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยของบริการคลาวด์ การมีข้อมูลบันทึกที่เพียงพอและเหมาะสมช่วยให้องค์กรสามารถตรวจพบกิจกรรมผิดปกติ วิเคราะห์สาเหตุของเหตุการณ์ และสนับสนุนกระบวนการตรวจสอบตามข้อกำหนดด้านการกำกับดูแล

อย่างไรก็ตาม การกำหนดข้อกำหนดด้าน Logging ควรพิจารณาตามรูปแบบบริการคลาวด์และหลักความรับผิดชอบร่วม (Shared Responsibility Model) เนื่องจากขอบเขตการเข้าถึงและการควบคุม Log อาจแตกต่างกันระหว่าง CSC และ CSP

2. หลักการกำหนดระดับความสำคัญของเหตุการณ์ (Event Prioritization)

ควรกำหนดระดับความสำคัญของเหตุการณ์ (Event Severity Level) เพื่อช่วยจัดลำดับความสำคัญในการตรวจสอบ เช่น

ร่างสำหรับ Public Hearing

ระดับ	คำอธิบาย
Critical	เหตุการณ์ที่อาจส่งผลกระทบรุนแรงต่อระบบ
High	เหตุการณ์ที่ต้องตรวจสอบโดยเร็ว
Medium	เหตุการณ์ที่ควรติดตาม
Low	เหตุการณ์ทั่วไป

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานด้านการบันทึกเหตุการณ์อาจอยู่ในรูปของการตั้งค่าระบบ รายงานจาก Logging Platform หรือ SIEM ข้อมูล Log ที่สามารถเรียกดูได้ หลักฐานการกำหนดระยะเวลาเก็บรักษา และผลการทบทวนหรือติดตามเหตุการณ์ตามความเหมาะสม

องค์กรอาจใช้ **ตารางข้อกำหนดการบันทึกเหตุการณ์ (Log Requirement Matrix)** เพื่อเชื่อมโยงระบบ แหล่งข้อมูล ประเภทเหตุการณ์ ระยะเวลาเก็บรักษา รอบการทบทวน และผู้รับผิดชอบ โดยข้อมูลอาจประกอบด้วยรายการต่อไปนี้

รายการ	รายละเอียด
System/Application	ระบบที่เกี่ยวข้อง
Log Source	แหล่งข้อมูล
Event Type	ประเภทเหตุการณ์
Retention Period	ระยะเวลาจัดเก็บ
Review Frequency	รอบการตรวจสอบ
Responsible Party	ผู้รับผิดชอบ

5.2.6.5 การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log Information)

ข้อมูลบันทึกเหตุการณ์อาจประกอบด้วยข้อมูลเกี่ยวกับผู้ใช้งาน พฤติกรรมการใช้งาน การเข้าถึงข้อมูล การตั้งค่าระบบ และข้อมูลอื่นที่มีความสำคัญต่อการตรวจสอบ จึงต้องได้รับการปกป้องจากการเข้าถึง การแก้ไข การลบ หรือการเปิดเผยโดยไม่ได้รับอนุญาต

การปกป้องข้อมูลบันทึกเหตุการณ์ควรครอบคลุมตลอดวงจรชีวิต ตั้งแต่การสร้าง การส่ง การจัดเก็บ การเข้าถึง การทบทวน การเก็บรักษา จนถึงการลบหรือทำลาย โดยพิจารณาขอบเขตความรับผิดชอบของ CSC และ CSP รวมถึงข้อกำหนดเกี่ยวกับข้อมูลส่วนบุคคลและระยะเวลาเก็บรักษาที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้	ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้

วัตถุประสงค์ (Objective)

1. เพื่อรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลบันทึกเหตุการณ์ตลอดระยะเวลาที่จำเป็น
2. เพื่อป้องกันการเข้าถึง การแก้ไข การลบ หรือการใช้ข้อมูลบันทึกเหตุการณ์นอกเหนือจากวัตถุประสงค์ที่กำหนด
3. เพื่อให้การเก็บรักษาและการลบข้อมูลบันทึกเหตุการณ์เป็นไปตามข้อกำหนดทางกฎหมาย นโยบาย และข้อตกลงที่เกี่ยวข้อง

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดมาตรการป้องกันข้อมูลบันทึกเหตุการณ์ให้เหมาะสมกับระดับความสำคัญของระบบและข้อมูล โดยควรดำเนินการดังต่อไปนี้

1. การควบคุมการเข้าถึงข้อมูลบันทึกเหตุการณ์ (Log Access Control)

ผู้ใช้บริการคลาวด์ควรกำหนดสิทธิการเข้าถึงข้อมูลบันทึกเหตุการณ์ (Log Access Permission) ตามหลักสิทธิเท่าที่จำเป็น (Principle of Least Privilege)

โดยควรพิจารณา

- การกำหนดบทบาทผู้ใช้งาน (Role-Based Access Control: RBAC)
- การจำกัดสิทธิการแก้ไขหรือลบข้อมูลบันทึก (Modification and Deletion Restriction)
- การแยกหน้าที่ผู้ดูแลระบบ (Segregation of Duties)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามเผยแพร่

- การตรวจสอบการเข้าถึงข้อมูลบันทึก (Log Access Monitoring)

บุคคลหรือระบบที่สามารถเข้าถึงข้อมูลบันทึกเหตุการณ์ควรได้รับอนุญาตตามหน้าที่ความรับผิดชอบ และควรมีการบันทึกกิจกรรมการเข้าถึงดังกล่าวเพื่อรองรับการตรวจสอบย้อนหลัง

2. การรักษาความถูกต้องครบถ้วนของข้อมูลบันทึกเหตุการณ์ (Log Integrity Protection)

ผู้ใช้บริการคลาวด์ควรมีมาตรการป้องกันการเปลี่ยนแปลงข้อมูลบันทึกเหตุการณ์โดยไม่ได้รับอนุญาต เพื่อให้ข้อมูลบันทึกสามารถใช้เป็นหลักฐานในการตรวจสอบได้อย่างน่าเชื่อถือ

แนวทางที่ควรพิจารณา ได้แก่

- การกำหนดสิทธิแบบอ่านอย่างเดียว (Read-only Access)
- การใช้กลไกตรวจสอบความถูกต้องของข้อมูล (Integrity Verification)
- การจัดเก็บข้อมูลบันทึกในพื้นที่ที่มีการควบคุมความมั่นคงปลอดภัย (Secure Storage)
- การป้องกันการแก้ไขหรือลบข้อมูลย้อนหลัง (Tamper Protection)

3. การป้องกันการลบหรือสูญหายของข้อมูลบันทึกเหตุการณ์ (Log Preservation)

ผู้ใช้บริการคลาวด์ควรมีมาตรการรักษาข้อมูลบันทึกเหตุการณ์ตามระยะเวลาที่กำหนด (Retention Period) เพื่อให้สามารถนำมาใช้ในการตรวจสอบหรือวิเคราะห์เหตุการณ์ได้เมื่อมีความจำเป็น

มาตรการอาจประกอบด้วย

- การกำหนดระยะเวลาการเก็บรักษา (Retention Policy)
- การสำรองข้อมูลบันทึกที่สำคัญ (Log Backup)
- การกำหนดกระบวนการทำลายข้อมูลบันทึก (Secure Log Disposal)

4. การป้องกันข้อมูลบันทึกที่มีข้อมูลอ่อนไหว (Sensitive Information Protection)

ผู้ใช้บริการคลาวด์ควรพิจารณาว่าข้อมูลบันทึกเหตุการณ์อาจมีข้อมูลที่มีความละเอียดอ่อน (Sensitive Information) เช่น

- ข้อมูลผู้ใช้งาน (User Identity Information)
- ข้อมูลที่อยู่เครือข่าย (IP Address)
- ข้อมูลกิจกรรมของผู้ใช้งาน (User Activity Information)
- ข้อมูลเกี่ยวกับระบบภายใน (System Information)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ดังนั้นควรกำหนดมาตรการป้องกัน เช่น

- การจำกัดการเข้าถึง (Access Restriction)
- การปกปิดข้อมูลบางส่วน (Data Masking)
- การเข้ารหัสข้อมูล (Encryption)

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีมาตรการป้องกันข้อมูลบันทึกเหตุการณ์ของบริการคลาวด์ เพื่อสนับสนุนความน่าเชื่อถือและความสามารถในการตรวจสอบของบริการ

1. การรักษาความมั่นคงปลอดภัยของระบบจัดเก็บ Log (Secure Log Storage)

ผู้ให้บริการคลาวด์ควรจัดให้มีระบบจัดเก็บข้อมูลบันทึกเหตุการณ์ที่มีมาตรการควบคุมความมั่นคงปลอดภัย เช่น

- การควบคุมสิทธิการเข้าถึง (Access Control)
- การป้องกันการแก้ไขข้อมูล (Tamper Protection)
- การติดตามกิจกรรมของผู้ดูแลระบบ (Administrator Activity Monitoring)

2. การแยกข้อมูลบันทึกของผู้ใช้บริการ (Customer Log Isolation)

ในกรณีบริการคลาวด์แบบหลายผู้ใช้งานร่วมกัน (Multi-Tenant Environment) ผู้ให้บริการคลาวด์ควรมีมาตรการแยกข้อมูลบันทึกเหตุการณ์ของผู้ใช้บริการแต่ละราย (Tenant Log Isolation) เพื่อป้องกันการเข้าถึงข้อมูลระหว่างผู้ใช้บริการ

3. การสนับสนุนการเก็บรักษาข้อมูลบันทึก (Log Retention Support)

ผู้ให้บริการคลาวด์ควรมีความสามารถสนับสนุนการเก็บรักษาข้อมูลบันทึกตามข้อตกลงการให้บริการ (Service Agreement) และข้อกำหนดของผู้ใช้บริการ

โดยอาจประกอบด้วย

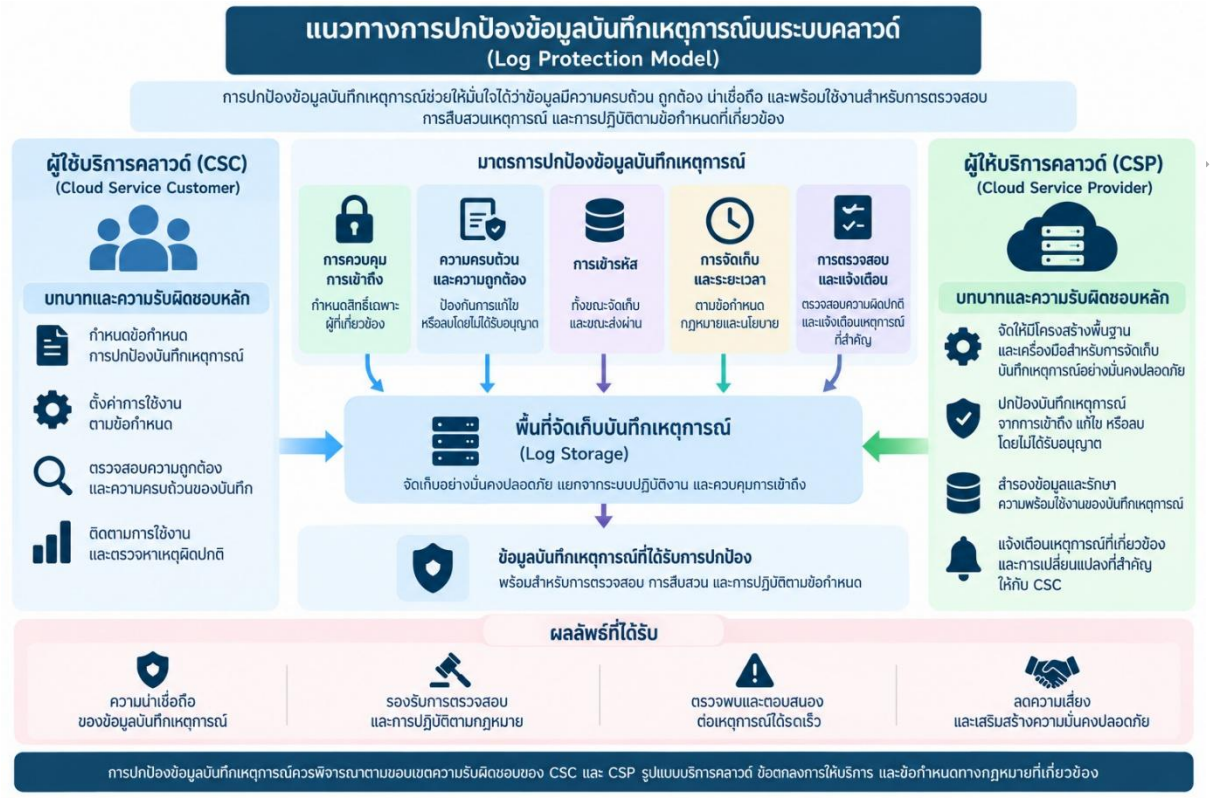
- ระยะเวลาการเก็บรักษา (Retention Period)
- รูปแบบการส่งออกข้อมูล (Log Export Format)
- วิธีการเรียกใช้ข้อมูล (Log Retrieval Method)

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. แนวทางการปกป้องข้อมูลบันทึกเหตุการณ์ (Log Protection Approach)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

นอกจากการจัดให้มีข้อมูลบันทึกเหตุการณ์ที่เพียงพอแล้ว ข้อมูลดังกล่าวควรได้รับการปกป้องตลอดวงจรชีวิต เพื่อป้องกันการเข้าถึง การแก้ไข การลบ หรือการเปิดเผยโดยไม่ได้รับอนุญาต โดยแนวทางการปกป้องข้อมูลบันทึกเหตุการณ์สามารถพิจารณาได้ดังแสดงในรูปต่อไปนี้



รูปที่ 6 แนวทางการปกป้องข้อมูลบันทึกเหตุการณ์

เหตุผลและความจำเป็น (Rationale)

ข้อมูลบันทึกเหตุการณ์เป็นหลักฐานสำคัญที่ช่วยให้องค์กรสามารถตรวจสอบกิจกรรม วิเคราะห์สาเหตุของเหตุการณ์ และสนับสนุนกระบวนการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ดังนั้น หากข้อมูลบันทึกถูกแก้ไข สูญหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต อาจส่งผลกระทบต่อความน่าเชื่อถือของกระบวนการตรวจสอบและการตอบสนองต่อเหตุการณ์

การกำหนดมาตรการปกป้องข้อมูลบันทึกเหตุการณ์ที่เหมาะสม ช่วยเสริมสร้างความโปร่งใส (Transparency) ความสามารถในการตรวจสอบย้อนหลัง (Traceability) และความเชื่อมั่นในการใช้บริการคลาวด์ โดยเฉพาะอย่างยิ่งในสภาพแวดล้อมที่มีการแบ่งปันทรัพยากรร่วมกันระหว่างผู้ใช้บริการหลายราย (Multi-Tenant Cloud Environment)

ร่างสำหรับ Public H

2. การกำหนดสิทธิการเข้าถึงตามบทบาท (Role-Based Access Control)

ตัวอย่างการกำหนดสิทธิ

บทบาท (Role)	สิทธิที่เหมาะสม
Security Analyst	อ่านและวิเคราะห์ Log
System Administrator	บริหารจัดการระบบ Log ตามหน้าที่
Auditor	ตรวจสอบข้อมูลแบบ Read-only
General User	ไม่มีสิทธิเข้าถึง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานด้านการปกป้องข้อมูลบันทึกเหตุการณ์อาจประกอบด้วยการกำหนดสิทธิการเข้าถึง การตั้งค่าการเก็บรักษา การป้องกันการแก้ไขหรือลบข้อมูล การเข้ารหัสหรือมาตรการปกป้องข้อมูลที่เกี่ยวข้อง ตลอดจนบันทึกการทบทวนสิทธิและการเข้าถึงตามความเหมาะสม

องค์กรอาจใช้ **ตารางควบคุมสิทธิการเข้าถึงข้อมูลบันทึกเหตุการณ์ (Log Access Control Matrix)** เป็นเครื่องมือสนับสนุนการบริหารจัดการ โดยข้อมูลอาจประกอบด้วยรายการต่อไปนี้

รายการ	รายละเอียด
System/Log Source	แหล่งข้อมูลบันทึก
User/Role	ผู้ใช้งานหรือบทบาท
Access Level	ระดับสิทธิ
Approval	ผู้อนุมัติ
Review Date	วันที่ทบทวน

5.2.6.6 บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)

ผู้ดูแลระบบและผู้ปฏิบัติงานที่มีสิทธิระดับสูงสามารถดำเนินการที่ส่งผลกระทบต่อการตั้งค่า ทรัพยากร ข้อมูล และความมั่นคงปลอดภัยของบริการคลาวด์ได้อย่างมีนัยสำคัญ การดำเนินการของบัญชีดังกล่าวจึงควรสามารถระบุผู้กระทำ เวลา กิจกรรม ทรัพยากรที่เกี่ยวข้อง และผลของการดำเนินการได้

ขอบเขตการบันทึกและทบทวนกิจกรรมควรพิจารณาตามสิทธิที่ผู้ใช้งานมีจริง และตามขอบเขตการควบคุมของ CSC และ CSP โดยอาจใช้กลไก เช่น Individual Accountability, Privileged Activity Logging, Session Recording หรือ Privileged Access Management ตามระดับความเสี่ยงและความเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น-ห้ามใช้อ้างอิง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากมีการให้สิทธิพิเศษให้แก่ ผู้ใช้บริการคลาวด์ การใช้สิทธิพิเศษนั้นต้องมีการบันทึกเหตุการณ์และประสิทธิภาพของการดำเนินการเหล่านั้น ผู้ใช้บริการคลาวด์ ต้องพิจารณาว่าความสามารถในการบันทึกเหตุการณ์ที่ ผู้ให้บริการคลาวด์ จัดหาให้นั้นเหมาะสมหรือไม่ หรือ ผู้ใช้บริการคลาวด์ ต้องใช้ความสามารถในการบันทึกเหตุการณ์เพิ่มเติมหรือไม่	

วัตถุประสงค์ (Objective)

1. เพื่อให้กิจกรรมของผู้ดูแลระบบ ผู้ปฏิบัติงาน และบัญชีที่มีสิทธิพิเศษสามารถตรวจสอบย้อนกลับและเชื่อมโยงกับผู้ดำเนินการได้
2. เพื่อให้มีการทบทวนกิจกรรมที่มีความเสี่ยงหรือผิดปกติ และสามารถตรวจพบการใช้สิทธิที่ไม่เหมาะสมได้อย่างเหมาะสม
3. เพื่อสนับสนุนความรับผิดชอบต่อการกระทำ การตรวจสอบ และการสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัย

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรจัดให้มีมาตรการควบคุมและบันทึกกิจกรรมของผู้ดูแลระบบและผู้ปฏิบัติงานที่มีสิทธิสูง โดยควรดำเนินการดังต่อไปนี้

1. การกำหนดบัญชีผู้ใช้งานที่มีสิทธิพิเศษ (Privileged Account Identification)

ผู้ใช้บริการคลาวด์ควรกำหนดและจัดทำทะเบียนบัญชีผู้ใช้งานที่มีสิทธิพิเศษ (Privileged Account Register) เพื่อให้สามารถระบุและควบคุมบัญชีที่มีความเสี่ยงสูงได้อย่างเหมาะสม

ตัวอย่างบัญชีที่ควรพิจารณา ได้แก่

- บัญชีผู้ดูแลระบบ (Administrator Account)
- บัญชีผู้บริหารระบบคลาวด์ (Cloud Administrator Account)
- บัญชีผู้ดูแลฐานข้อมูล (Database Administrator Account)
- บัญชีผู้ดูแลระบบเครือข่าย (Network Administrator Account)
- บัญชีบริการของระบบ (Service Account) ที่มีสิทธิสูง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2. การบันทึกกิจกรรมของผู้ใช้งานที่มีสิทธิพิเศษ (Privileged Activity Logging)

ผู้ใช้บริการคลาวด์ควรจัดให้มีการบันทึกกิจกรรมสำคัญของผู้ดูแลระบบและผู้ปฏิบัติงาน เพื่อให้สามารถตรวจสอบได้ว่า

- ใครเป็นผู้ดำเนินการ (Who)
- ดำเนินการเมื่อใด (When)
- ดำเนินการกับระบบหรือทรัพยากรใด (What)
- ดำเนินการจากแหล่งใด (Where)
- ผลลัพธ์ของการดำเนินการเป็นอย่างไร (Outcome)

ตัวอย่างกิจกรรมที่ควรบันทึก ได้แก่

ประเภทกิจกรรม	ตัวอย่าง
การเข้าสู่ระบบ (Authentication)	Login, Failed Login
การเปลี่ยนแปลงสิทธิ (Privilege Change)	เพิ่ม/ลดสิทธิผู้ใช้งาน
การเปลี่ยนแปลงค่าระบบ (Configuration Change)	Firewall Rule, System Parameter
การจัดการทรัพยากร (Resource Management)	Create, Modify, Delete Resource
การเข้าถึงข้อมูลสำคัญ (Sensitive Data Access)	Export, Download Data

3. การใช้บัญชีเฉพาะบุคคล (Individual Accountability)

ผู้ใช้บริการคลาวด์ควรหลีกเลี่ยงการใช้บัญชีร่วมกัน (Shared Account) สำหรับกิจกรรมที่มีความสำคัญหรือมีความเสี่ยงสูง เพื่อให้สามารถระบุผู้รับผิดชอบได้อย่างชัดเจน

หากมีความจำเป็นต้องใช้บัญชีร่วม (Shared Privileged Account) ควรมีกลไกเพิ่มเติม เช่น

- การบันทึกผู้ร้องขอใช้งาน (Request Record)
- การอนุมัติการใช้งาน (Approval)
- การบันทึกช่วงเวลาการใช้งาน (Usage Period)
- การติดตามกิจกรรมที่ดำเนินการ (Activity Tracking)

4. การทบทวนกิจกรรมของบัญชีสิทธิพิเศษ (Privileged Activity Review)

ผู้ใช้บริการคลาวด์ควรกำหนดกระบวนการทบทวนบันทึกกิจกรรมของผู้ดูแลระบบตามความเหมาะสม เพื่อค้นหาการดำเนินการที่ผิดปกติ (Suspicious Activity) หรือการใช้งานสิทธิที่ไม่สอดคล้องกับหน้าที่

การทบทวนควรพิจารณา

- การเปลี่ยนแปลงระบบที่สำคัญ (Critical System Changes)
- การเข้าถึงข้อมูลสำคัญ (Critical Data Access)

ร่างเอกสารเพื่อรับฟังความคิดเห็น (Public Hearing) - ห้ามนำไปใช้อ้างอิง

- การใช้งานนอกเวลาปกติ (Unusual Access Time)
- การดำเนินการที่ผิดจากรูปแบบปกติ (Abnormal Behavior)
-

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถในการบันทึกและตรวจสอบกิจกรรมของบัญชีผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้องกับการให้บริการคลาวด์

1. การบันทึกกิจกรรมของผู้ดูแลระบบบริการคลาวด์ (Cloud Administrator Activity Logging)

ผู้ให้บริการคลาวด์ควรมีความสามารถในการบันทึกกิจกรรมของผู้ดูแลระบบที่เกี่ยวข้องกับการบริหารจัดการโครงสร้างพื้นฐานหรือบริการคลาวด์

ตัวอย่างกิจกรรม ได้แก่

- การเข้าสู่ระบบบริหารจัดการ (Management Console Access)
- การเปลี่ยนแปลงการตั้งค่าบริการ (Service Configuration Change)
- การจัดการสิทธิผู้ใช้งาน (Identity and Access Management Change)
- การดำเนินการกับทรัพยากรคลาวด์ (Cloud Resource Operation)

2. การรักษาความสามารถในการตรวจสอบย้อนหลัง (Auditability)

ผู้ให้บริการคลาวด์ควรจัดให้มีข้อมูลที่เพียงพอสำหรับการตรวจสอบย้อนหลัง โดยข้อมูลบันทึกควรสามารถระบุได้อย่างน้อย

- ตัวตนของผู้ดำเนินการ (User Identity)
- เวลาที่ดำเนินการ (Timestamp)
- รายละเอียดการดำเนินการ (Action Details)
- ทรัพยากรที่เกี่ยวข้อง (Affected Resource)
- ผลการดำเนินการ (Execution Result)

3. การสนับสนุนการตรวจสอบด้านความมั่นคงปลอดภัย (Security Investigation Support)

ผู้ให้บริการคลาวด์ควรมีแนวทางสนับสนุนผู้ใช้บริการในการตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมของผู้ดูแลระบบ เช่น

- การจัดเตรียมข้อมูล Log ตามขอบเขตบริการ
- การสนับสนุนการวิเคราะห์เหตุการณ์
- การประสานงานเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

ทั้งนี้ต้องเป็นไปตามข้อตกลงการให้บริการ (Service Agreement) และข้อกำหนดด้านการรักษาความลับของข้อมูล (Confidentiality Requirement)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. แนวทางการควบคุมบัญชีสิทธิพิเศษ (Privileged Access Control Lifecycle)

สำหรับบัญชีผู้ดูแลระบบ ผู้ปฏิบัติงาน และบัญชีที่มีสิทธิพิเศษ การควบคุมควรครอบคลุมตั้งแต่การระบุและอนุมัติบัญชี การกำหนดและใช้งานสิทธิ การบันทึกและทบทวนกิจกรรม ตลอดจนการลดหรือเพิกถอนสิทธิเมื่อหมดความจำเป็น ดังแสดงในรูปต่อไปนี้



รูปที่ 7 วงจรการบริหารจัดการบัญชีสิทธิพิเศษ

เหตุผลและความจำเป็น (Rationale)

บัญชีผู้ดูแลระบบและผู้ปฏิบัติงานเป็นบัญชีที่มีผลกระทบสูงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การบันทึกและตรวจสอบกิจกรรมของบัญชีเหล่านี้ช่วยให้องค์กรสามารถระบุความรับผิดชอบ ตรวจสอบการดำเนินงาน และลดความเสี่ยงจากการใช้สิทธิที่ไม่เหมาะสม

การจัดให้มี Privileged Activity Logging ที่เหมาะสมยังช่วยสนับสนุนหลักการสำคัญด้านความมั่นคงปลอดภัย ได้แก่ ความรับผิดชอบต่อการกระทำ (Accountability) ความสามารถในการตรวจสอบย้อนหลัง (Traceability) และการควบคุมสิทธิการเข้าถึง (Access Governance)

2. การเชื่อมโยงกับระบบบริหารจัดการสิทธิพิเศษ (Privileged Access Management: PAM)

สำหรับระบบที่มีความสำคัญสูง องค์กรอาจพิจารณาใช้ระบบบริหารจัดการบัญชีสิทธิพิเศษ (Privileged Access Management: PAM) เพื่อสนับสนุนความสามารถ เช่น

- การควบคุมการเข้าถึงแบบรวมศูนย์ (Centralized Access Control)
- การบันทึก Session ของผู้ดูแลระบบ (Privileged Session Recording)
- การบริหารจัดการรหัสผ่านสิทธิพิเศษ (Privileged Credential Management)
- การอนุมัติการเข้าถึงแบบชั่วคราว (Just-in-Time Access)

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานควรสามารถแสดงให้เห็นถึงการระบุบัญชีที่มีสิทธิพิเศษ การอนุมัติและกำหนดขอบเขตสิทธิ การบันทึกกิจกรรม และการทบทวนการใช้งานตามความเหมาะสม

ตัวอย่างหลักฐานที่อาจใช้ประกอบการพิจารณา ได้แก่ ทะเบียนบัญชีสิทธิพิเศษ (Privileged Account Register) บันทึกหรือ Log ของกิจกรรมที่ใช้สิทธิพิเศษ หลักฐานการอนุมัติ และ รายงานทบทวนกิจกรรมผู้ดูแลระบบ (Administrator Activity Review Report)

ในกรณีที่องค์กรจัดทำทะเบียนบัญชีสิทธิพิเศษ ข้อมูลอาจประกอบด้วยรายการต่อไปนี้

รายการ	**รายละเอียด**
Account Name	ชื่อบัญชี
Owner	เจ้าของบัญชี
Privilege Level	ระดับสิทธิ
System Scope	ระบบที่เข้าถึง
Approval Reference	เอกสารอนุมัติ
Review Date	วันที่ทบทวน

นอกจากนี้ องค์กรอาจเก็บรักษารายงานการทบทวนกิจกรรมของผู้ดูแลระบบหรือหลักฐานอื่นที่สามารถแสดงผลการทบทวนกิจกรรมที่มีความเสี่ยงหรือผิดปกติได้

5.2.6.7 การซิงโครไนซ์นาฬิกา (Clock Synchronization)

การมีเวลาของระบบที่ถูกต้องและสอดคล้องกันเป็นองค์ประกอบสำคัญของการตรวจสอบเหตุการณ์ โดยเฉพาะเมื่อองค์กรต้องวิเคราะห์ข้อมูลจากหลายระบบ หลายบริการ หรือหลายแหล่งบันทึก หากเวลาของระบบไม่สอดคล้องกัน อาจทำให้การจัดลำดับเหตุการณ์ การวิเคราะห์สาเหตุ และการเชื่อมโยงข้อมูลเกิดความคลาดเคลื่อน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ระบบและบริการคลาวด์จึงควรใช้แหล่งเวลาอ้างอิงที่เชื่อถือได้ และควรมีการตรวจสอบความถูกต้องของ Timestamp ในระดับที่เหมาะสมกับการใช้งาน โดยขอบเขตการกำหนดค่าและการควบคุมอาจแตกต่างกันตามรูปแบบบริการและความรับผิดชอบของ CSC และ CSP

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ใช้ในระบบของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับนาฬิกาที่ระบบของผู้ให้บริการคลาวด์ใช้และข้อมูลเกี่ยวกับวิธีที่ผู้ใช้บริการคลาวด์สามารถซิงโครไนซ์นาฬิกาภายในกับนาฬิกาในบริการคลาวด์

วัตถุประสงค์ (Objective)

1. เพื่อให้เวลาของระบบและ Timestamp ที่เกี่ยวข้องมีความถูกต้องและสอดคล้องเพียงพอต่อการตรวจสอบและวิเคราะห์เหตุการณ์
2. เพื่อให้ระบบที่สำคัญใช้แหล่งเวลาอ้างอิงที่เชื่อถือได้และได้รับการควบคุมตามความเหมาะสม
3. เพื่อสนับสนุนการเชื่อมโยงข้อมูลจาก Logging, SIEM และระบบอื่นที่ใช้ข้อมูลเวลาสำหรับการตรวจสอบย้อนกลับ

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดแนวทางการบริหารจัดการเวลาของระบบสารสนเทศที่ใช้งานบนระบบคลาวด์ โดยควรดำเนินการดังต่อไปนี้

1. การกำหนดแหล่งอ้างอิงเวลา (Authoritative Time Source)

ผู้ใช้บริการคลาวด์ควรกำหนดแหล่งอ้างอิงเวลามาตรฐาน (Trusted Time Source) สำหรับระบบสารสนเทศที่เกี่ยวข้อง เพื่อให้มั่นใจว่าระบบต่าง ๆ สามารถใช้เวลาเดียวกันในการบันทึกและวิเคราะห์เหตุการณ์

แหล่งอ้างอิงเวลาอาจมาจาก

- ระบบเวลาองค์กร (Enterprise Time Server)
- ระบบ Network Time Protocol (NTP Server)
- แหล่งเวลาอ้างอิงมาตรฐานสากล (External Time Reference)
-

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

2. การกำหนดมาตรฐานเวลา (Time Standard Definition)

องค์กรควรกำหนดมาตรฐานเวลาให้ชัดเจน เช่น

- รูปแบบการแสดงเวลา (Time Format)
- เขตเวลา (Time Zone)
- การใช้เวลามาตรฐานสากล (Coordinated Universal Time: UTC)
- รูปแบบการบันทึกเวลาใน Log (Timestamp Format)

เพื่อให้สามารถเปรียบเทียบและวิเคราะห์เหตุการณ์จากหลายระบบได้อย่างถูกต้อง

3. การตรวจสอบความถูกต้องของเวลา (Time Accuracy Verification)

ผู้ใช้บริการคลาวด์ควรมีการตรวจสอบความถูกต้องของเวลาระบบ (System Time Accuracy) อย่างเหมาะสม โดยเฉพาะระบบที่เกี่ยวข้องกับ

- ระบบรักษาความมั่นคงปลอดภัย (Security Systems)
- ระบบบันทึกเหตุการณ์ (Logging Systems)
- ระบบบริหารจัดการเหตุการณ์ (Incident Management Systems)
- ระบบควบคุมสิทธิการเข้าถึง (Access Control Systems)
-

4. การกำหนดความรับผิดชอบด้านเวลาในระบบคลาวด์ (Cloud Time Responsibility)

ผู้ใช้บริการคลาวด์ควรทำความเข้าใจขอบเขตความรับผิดชอบด้านเวลาระหว่างตนเองและผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)

ตัวอย่างเช่น

- ระบบปฏิบัติการของ Virtual Machine (VM) อาจอยู่ภายใต้ความรับผิดชอบของ CSC
- เวลาของโครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure Time) อาจอยู่ภายใต้ความรับผิดชอบของ CSP

ทั้งนี้ควรกำหนดความรับผิดชอบให้ชัดเจนตามรูปแบบบริการคลาวด์ (Cloud Service Model)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถในการบริหารจัดการเวลาของระบบที่สนับสนุนการให้บริการคลาวด์อย่างเหมาะสม

1. การจัดให้มีระบบเวลาที่มีความน่าเชื่อถือ (Reliable Time Synchronization Service)

ผู้ให้บริการคลาวด์ควรจัดให้มีระบบประสานเวลาที่มีความน่าเชื่อถือ เพื่อสนับสนุนการทำงานของบริการคลาวด์และระบบที่เกี่ยวข้อง

ความสามารถดังกล่าวอาจประกอบด้วย

- การใช้แหล่งเวลาอ้างอิงที่น่าเชื่อถือ (Trusted Time Reference)
- การปรับเทียบเวลาอัตโนมัติ (Automatic Time Synchronization)
- การตรวจสอบสถานะการประสานเวลา (Synchronization Status Monitoring)

2. การสนับสนุนความสอดคล้องของเวลาสำหรับ Log (Log Timestamp Consistency)

ผู้ให้บริการคลาวด์ควรสนับสนุนให้ข้อมูลบันทึกเหตุการณ์ (Log) มีข้อมูลเวลาที่ถูกต้องและสอดคล้องกัน เพื่อให้สามารถนำไปใช้ในการ

- วิเคราะห์เหตุการณ์ (Event Analysis)
- ตรวจสอบลำดับเหตุการณ์ (Event Sequence Analysis)
- เชื่อมโยงเหตุการณ์จากหลายระบบ (Event Correlation)

3. การให้ข้อมูลเกี่ยวกับการตั้งค่าเวลา (Time Configuration Transparency)

ผู้ให้บริการคลาวด์ควรให้ข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเวลา เพื่อให้ผู้ใช้บริการสามารถกำหนดค่าระบบของตนเองได้อย่างเหมาะสม

ข้อมูลอาจประกอบด้วย

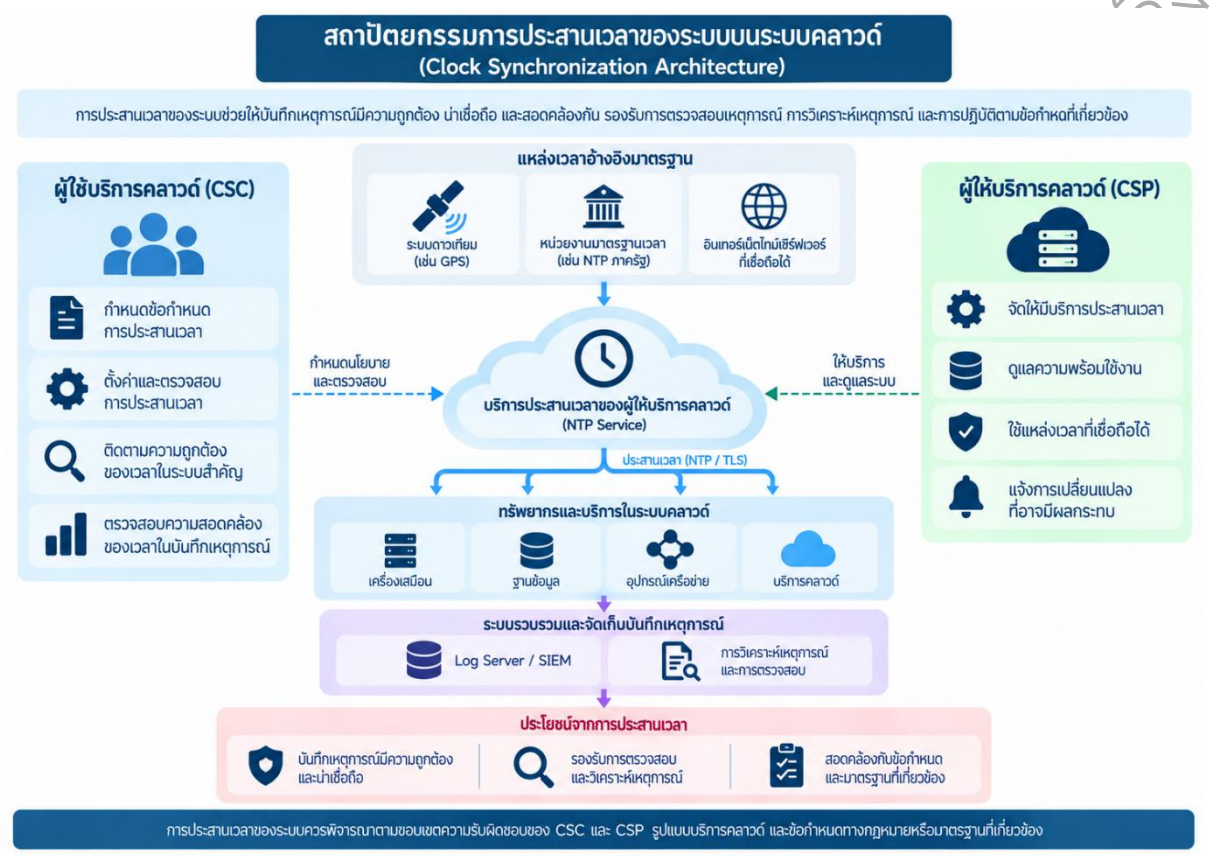
- แนวทางการตั้งค่าเวลา (Time Configuration Guidance)
- ข้อกำหนดของบริการ (Service Requirement)
- ข้อจำกัดที่เกี่ยวข้อง (Service Limitation)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. แนวทางสถาปัตยกรรมการประสานเวลา (Time Synchronization Architecture)

การประสานเวลาควรทำให้ระบบและบริการที่เกี่ยวข้องสามารถอ้างอิงเวลาจากแหล่งที่เชื่อถือได้ และทำให้ Timestamp จากหลายแหล่งสามารถนำมาเชื่อมโยงและวิเคราะห์ร่วมกันได้ โดยความสัมพันธ์ระหว่างแหล่งเวลา ระบบคลาวด์ และระบบ Logging/SIEM แสดงในรูปต่อไปนี้



รูปที่ 8 สถาปัตยกรรมการประสานเวลาของระบบ (Clock Synchronization Architecture)

ร่างสำหรับ

เหตุผลและความจำเป็น (Rationale)

การประสานเวลาของระบบเป็นองค์ประกอบพื้นฐานที่สนับสนุนความถูกต้องของข้อมูลบันทึกเหตุการณ์และความสามารถในการตรวจสอบย้อนหลัง หากระบบต่าง ๆ ใช้เวลาที่ไม่ตรงกัน อาจทำให้การวิเคราะห์เหตุการณ์ผิดพลาดหรือไม่สามารถระบุลำดับเหตุการณ์ที่แท้จริงได้

สำหรับระบบคลาวด์ การกำหนดแนวทางการประสานเวลาที่เหมาะสมช่วยเพิ่มความน่าเชื่อถือของระบบตรวจสอบด้านความมั่นคงปลอดภัย (Security Monitoring) สนับสนุนการบริหารจัดการเหตุการณ์ (Incident Management) และเพิ่มความเชื่อมั่นในการให้บริการคลาวด์

2. การใช้ Network Time Protocol (NTP)

องค์กรควรพิจารณาใช้โปรโตคอลมาตรฐานสำหรับการประสานเวลา เช่น Network Time Protocol (NTP) เพื่อให้ระบบสามารถปรับเวลาให้ตรงกันอย่างอัตโนมัติ

การใช้งานควรพิจารณา

- ความน่าเชื่อถือของแหล่งเวลา
- ความถูกต้องของเวลา
- ความพร้อมใช้งานของระบบเวลา
- การป้องกันการปรับเปลี่ยนเวลาที่ไม่ได้รับอนุญาต

3. ผลกระทบต่อการตรวจสอบ Log และ SIEM

การประสานเวลาที่ถูกต้องมีความสำคัญต่อระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) เนื่องจากระบบดังกล่าวต้องอาศัย Timestamp เพื่อ

- จัดเรียงเหตุการณ์ตามลำดับเวลา (Event Timeline)
- วิเคราะห์รูปแบบการโจมตี (Attack Pattern Analysis)
- เชื่อมโยงเหตุการณ์จากหลายแหล่งข้อมูล (Multi-source Correlation)

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานด้านการประสานเวลาควรสามารถแสดงแหล่งเวลาอ้างอิง การตั้งค่าการซิงโครไนซ์ สถานะการทำงาน และความผิดปกติที่อาจส่งผลต่อความถูกต้องของ Timestamp ตามความเหมาะสม

หลักฐานอาจอยู่ในรูปของการตั้งค่าระบบ NTP รายงานสถานะจากระบบ Monitoring บันทึกการตรวจสอบ หรือข้อมูลจาก CSP โดยไม่จำเป็นต้องจัดทำรายงานแยก หากข้อมูลจากระบบสามารถยืนยันการดำเนินการได้อย่างเพียงพอ

ในกรณีที่องค์กรจัดทำ**รายงานตรวจสอบการประสานเวลาระบบ (System Time Synchronization Report)** ข้อมูลอาจประกอบด้วยรายการต่อไปนี้

รายการ	**รายละเอียด**
System Name	ชื่อระบบ
Time Source	แหล่งเวลา
Synchronization Status	สถานะ
Last Synchronization	เวลาล่าสุด
Exception	ความผิดปกติ

สำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ช่องโหว่ทางเทคนิคอาจเกิดขึ้นในหลายชั้นของบริการคลาวด์ ตั้งแต่ระบบปฏิบัติการ แอปพลิเคชัน แพลตฟอร์ม ไปจนถึงโครงสร้างพื้นฐาน โดยขอบเขตที่ CSC หรือ CSP สามารถตรวจสอบและแก้ไขช่องโหว่ได้จะแตกต่างกันตามรูปแบบบริการคลาวด์และขอบเขตการควบคุม

การจัดการช่องโหว่จึงควรดำเนินการอย่างต่อเนื่อง ตั้งแต่การรับข้อมูลหรือค้นหาช่องโหว่ การประเมินและจัดลำดับตามความเสี่ยง การแก้ไขหรือลดความเสี่ยง การตรวจสอบยืนยันผล และการติดตามสถานะ โดยควรมีการประสานงานระหว่าง CSC และ CSP ในกรณีที่ช่องโหว่หรือมาตรการแก้ไขเกี่ยวข้องกับความรับผิดชอบของทั้งสองฝ่าย

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ ผู้ใช้บริการคลาวด์ ต้องระบุช่องโหว่ทางเทคนิคที่ผู้ใช้บริการคลาวด์ จะเป็นผู้รับผิดชอบในการจัดการและกำหนดกระบวนการในการจัดการให้ชัดเจน	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูล ผู้ใช้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ

วัตถุประสงค์ (Objective)

1. เพื่อให้สามารถระบุ ประเมิน และจัดลำดับความสำคัญของช่องโหว่ทางเทคนิคตามระดับความเสี่ยงได้อย่างเป็นระบบ
2. เพื่อให้มีการดำเนินการแก้ไข ลดความเสี่ยง และตรวจสอบยืนยันผลภายในระยะเวลาที่เหมาะสม
3. เพื่อให้ CSC และ CSP สามารถประสานข้อมูลและการดำเนินการด้านช่องโหว่ตามขอบเขตความรับผิดชอบของแต่ละฝ่าย
4.

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรจัดให้มีกระบวนการบริหารจัดการช่องโหว่ทางเทคนิคที่เหมาะสมกับระบบและบริการที่ใช้งาน โดยควรดำเนินการดังต่อไปนี้

1. การระบุและค้นหาช่องโหว่ (Vulnerability Identification)

ผู้ใช้บริการคลาวด์ควรมีแนวทางในการค้นหาและระบุช่องโหว่ที่อาจเกิดขึ้นกับระบบสารสนเทศ แอปพลิเคชัน และองค์ประกอบที่อยู่ภายใต้ความรับผิดชอบของตน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

แหล่งข้อมูลสำหรับการระบุช่องโหว่อาจประกอบด้วย

- ฐานข้อมูลช่องโหว่สาธารณะ (Public Vulnerability Database)
- ประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory)
- ผลการตรวจประเมินช่องโหว่ (Vulnerability Assessment)
- ผลการทดสอบเจาะระบบ (Penetration Testing)
- รายงานจากผู้ผลิตซอฟต์แวร์ (Vendor Security Bulletin)

2. การประเมินและจัดลำดับความสำคัญของช่องโหว่ (Vulnerability Assessment and Prioritization)

ผู้ใช้บริการคลาวด์ควรประเมินระดับความเสี่ยงของช่องโหว่ (Vulnerability Risk Assessment) เพื่อกำหนดลำดับความสำคัญในการแก้ไข

ปัจจัยที่ควรพิจารณา ได้แก่

- ระดับความรุนแรงของช่องโหว่ (Severity Level)
- ความสามารถในการถูกใช้โจมตี (Exploitability)
- ผลกระทบต่อระบบ (System Impact)
- ความสำคัญของสินทรัพย์ (Asset Criticality)
- ความเกี่ยวข้องกับข้อมูลสำคัญ (Sensitive Information Impact)

องค์กรอาจใช้มาตรฐานการให้คะแนน เช่น Common Vulnerability Scoring System (CVSS) หรือรูปแบบมาตรฐานที่องค์กรกำหนดเอง เพื่อสนับสนุนการประเมินความรุนแรงของช่องโหว่

3. การดำเนินการแก้ไขช่องโหว่ (Vulnerability Remediation)

ผู้ใช้บริการคลาวด์ควรกำหนดแนวทางการจัดการช่องโหว่ตามระดับความเสี่ยง เช่น

- การติดตั้งโปรแกรมแก้ไข (Security Patch Installation)
- การปรับปรุงค่าการตั้งค่า (Security Configuration Hardening)
- การปิดบริการที่ไม่จำเป็น (Disable Unnecessary Services)
- การใช้มาตรการควบคุมทดแทน (Compensating Controls)

ในกรณีที่ไม่สามารถแก้ไขช่องโหว่ได้ทันที ควรมีการประเมินและกำหนดมาตรการลดความเสี่ยงชั่วคราว (Risk Mitigation)

4. การตรวจสอบยืนยันหลังการแก้ไข (Remediation Verification)

หลังจากดำเนินการแก้ไขช่องโหว่ ควรมีการตรวจสอบเพื่อยืนยันว่ามาตรการแก้ไขสามารถลดหรือกำจัดความเสี่ยงได้

ร่างประกาศฯ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กิจกรรมที่ควรพิจารณา ได้แก่

- การตรวจสอบซ้ำ (Re-scan)
- การทดสอบการทำงานของระบบ (System Validation)
- การทบทวนค่าการตั้งค่า (Configuration Review)
- การปรับปรุงสถานะช่องโหว่ (Vulnerability Status Update)

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีมาตรการบริหารจัดการช่องโหว่ที่เกี่ยวข้องกับโครงสร้างพื้นฐานและบริการคลาวด์ เพื่อรักษาความมั่นคงปลอดภัยของบริการที่ให้แก่ผู้ใช้บริการ

1. การบริหารจัดการช่องโหว่ของโครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure Vulnerability Management)

ผู้ให้บริการคลาวด์ควรมีกระบวนการจัดการช่องโหว่ขององค์ประกอบที่อยู่ภายใต้ความรับผิดชอบ เช่น

- ระบบปฏิบัติการโครงสร้างพื้นฐาน (Infrastructure Operating Systems)
- อุปกรณ์เครือข่าย (Network Devices)
- ระบบบริหารจัดการคลาวด์ (Cloud Management Platform)
- ซอฟต์แวร์สนับสนุนบริการ (Supporting Software)

2. การแจ้งข้อมูลช่องโหว่ที่เกี่ยวข้องแก่ผู้ใช้บริการ (Customer Vulnerability Notification)

ผู้ให้บริการคลาวด์ควรมีกระบวนการแจ้งข้อมูลช่องโหว่ที่อาจส่งผลกระทบต่อผู้ใช้บริการ ตามระดับความเหมาะสมและข้อจำกัดด้านความมั่นคงปลอดภัย

ข้อมูลที่อาจแจ้ง ได้แก่

รายการ	**รายละเอียด**
รายละเอียดช่องโหว่ (Vulnerability Description)	ลักษณะของช่องโหว่
ผลกระทบ (Impact)	บริการหรือข้อมูลที่เกี่ยวข้อง
ระดับความรุนแรง (Severity)	ระดับความเสี่ยง
แนวทางดำเนินการ (Recommended Action)	คำแนะนำสำหรับผู้ใช้บริการ

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

3. การบริหารจัดการช่องโหว่ตามระดับความเสี่ยง (Risk-Based Vulnerability Management)

ผู้ให้บริการคลาวด์ควรจัดลำดับความสำคัญในการแก้ไขช่องโหว่ตามระดับความเสี่ยง เพื่อให้สามารถลดผลกระทบที่อาจเกิดขึ้นได้อย่างเหมาะสม

แนวทางดังกล่าวควรพิจารณา

- ความรุนแรงของช่องโหว่
- ความสามารถในการโจมตี
- ผลกระทบต่อบริการ
- ความสำคัญของระบบที่เกี่ยวข้อง

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. วงจรชีวิตการบริหารจัดการช่องโหว่ (Vulnerability Management Lifecycle)

การจัดการช่องโหว่ทางเทคนิคควรดำเนินการอย่างต่อเนื่องตั้งแต่การระบุช่องโหว่ การประเมินและจัดลำดับความสำคัญ การแก้ไขหรือลดความเสี่ยง การตรวจสอบยืนยันผล และการติดตามสถานะ เพื่อให้ความเสี่ยงจากช่องโหว่ได้รับการจัดการอย่างเป็นระบบ ดังแสดงในรูปต่อไปนี้



รูปที่ 9 วงจรชีวิตการบริหารจัดการช่องโหว่ทางเทคนิค

เทศน์ - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

ช่องโหว่ทางเทคนิคเป็นหนึ่งในปัจจัยสำคัญที่อาจนำไปสู่การถูกโจมตี การเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือการสูญเสียความพร้อมใช้งานของบริการ การมีกระบวนการบริหารจัดการช่องโหว่ที่เป็นระบบช่วยให้องค์กรสามารถลดความเสี่ยงและรักษาระดับความมั่นคงปลอดภัยของบริการคลาวด์ได้อย่างต่อเนื่อง

การกำหนดแนวทางแบบอิงความเสี่ยง (Risk-Based Approach) ช่วยให้องค์กรและผู้ให้บริการคลาวด์สามารถจัดลำดับความสำคัญของการแก้ไขได้อย่างเหมาะสม โดยมุ่งเน้นทรัพยากรไปยังช่องโหว่ที่มีผลกระทบสูงก่อน

2. การกำหนดระยะเวลาเป้าหมายในการแก้ไข (Remediation Target)

องค์กรควรกำหนดระยะเวลาเป้าหมายในการแก้ไขช่องโหว่ (Remediation Target Timeline) ตามระดับความรุนแรง เช่น

ระดับความเสี่ยง	แนวทาง
สูงมาก (Critical)	ดำเนินการโดยเร่งด่วน
สูง (High)	กำหนดระยะเวลาแก้ไขที่เหมาะสม
ปานกลาง (Medium)	วางแผนดำเนินการตามรอบ
ต่ำ (Low)	พิจารณาตามความเหมาะสม

3. การเชื่อมโยงกับกระบวนการบริหารความเสี่ยง (Risk Management Integration)

การจัดการช่องโหว่ควรเชื่อมโยงกับกระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) เพื่อให้สามารถพิจารณาความเสี่ยงในภาพรวม ไม่ใช่พิจารณาเฉพาะตัวช่องโหว่

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานด้านการบริหารจัดการช่องโหว่ควรสามารถแสดงวงจรตั้งแต่การระบุและประเมินช่องโหว่ การจัดลำดับความสำคัญ การกำหนดแนวทางและระยะเวลาในการแก้ไข ตลอดจนการตรวจสอบยืนยันผลหลังการดำเนินการ

ตัวอย่างหลักฐานที่อาจใช้ประกอบการพิจารณา ได้แก่ ผลการตรวจประเมินช่องโหว่ (Vulnerability Assessment Report) ผลการสแกน รายงานการทดสอบเจาะระบบ ประกาศแจ้งเตือนช่องโหว่ แผนหรือบันทึกการแก้ไข และผลการตรวจสอบยืนยันหลังการแก้ไข

องค์กรอาจใช้**ทะเบียนบริหารจัดการช่องโหว่ (Vulnerability Management Register)** เพื่อสนับสนุนการติดตามสถานะ โดยข้อมูลอาจประกอบด้วยรายการต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

รายการ	รายละเอียด
Vulnerability ID	หมายเลขอ้างอิง
Asset/System	ระบบที่เกี่ยวข้อง
Description	รายละเอียดช่องโหว่
Severity/CVSS	ระดับความรุนแรง
Risk Rating	ระดับความเสี่ยง
Remediation Plan	แผนแก้ไข
Status	สถานะดำเนินการ
Verification Result	ผลตรวจสอบ

5.2.6.9 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน (Separation of Development, Testing and Operational Environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงมีวัตถุประสงค์และระดับความเสี่ยงแตกต่างกัน หากไม่มีการแบ่งแยกและควบคุมที่เหมาะสม ความผิดพลาด การทดสอบ การเปลี่ยนแปลง หรือการเข้าถึงจากสภาพแวดล้อมที่ไม่ใช่ระบบปฏิบัติงานจริงอาจส่งผลกระทบต่อระบบและข้อมูลที่ให้บริการจริงได้

การแบ่งแยกมิได้หมายความว่าต้องใช้โครงสร้างพื้นฐานทางกายภาพแยกจากกันในทุกกรณี แต่สามารถใช้การแบ่งแยกเชิงตรรกะ การแยกบัญชีหรือโครงการ การแบ่งแยกเครือข่าย การควบคุมสิทธิ และการควบคุมการนำระบบขึ้นใช้งานตามระดับความเสี่ยง ทั้งนี้ การใช้ข้อมูล Production ใน Non-Production Environment ควรได้รับการควบคุมอย่างเหมาะสม โดยเฉพาะเมื่อเกี่ยวข้องกับข้อมูลส่วนบุคคลหรือข้อมูลที่มีความอ่อนไหว

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด	ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด

วัตถุประสงค์ (Objective)

ร่างประกาศ Public Hearing ฉบับ - ห้ามใช้อ้างอิง

1. เพื่อให้สภาพแวดล้อม Development, Testing และ Production มีขอบเขตการควบคุมที่เหมาะสมกับวัตถุประสงค์และระดับความเสี่ยง
2. เพื่อป้องกันไม่ให้กิจกรรมการพัฒนา การทดสอบ หรือการเปลี่ยนแปลงที่ไม่ได้รับอนุมัติส่งผลกระทบต่อระบบปฏิบัติงานจริง
3. เพื่อให้การเข้าถึง การใช้ข้อมูล การเชื่อมต่อระหว่างสภาพแวดล้อม และการนำการเปลี่ยนแปลงเข้าสู่ Production ได้รับการควบคุมและสามารถตรวจสอบได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 1: ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดมาตรการแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงตามระดับความเสี่ยงและความสำคัญของระบบ โดยควรครอบคลุมประเด็นสำคัญดังต่อไปนี้

1. การแบ่งแยกสภาพแวดล้อม (Environment Separation)

ผู้ใช้บริการคลาวด์ควรแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงให้เหมาะสม เพื่อป้องกันไม่ให้กิจกรรมในสภาพแวดล้อมหนึ่งส่งผลกระทบโดยไม่เหมาะสมต่ออีกสภาพแวดล้อมหนึ่ง

แนวทางการแบ่งแยกอาจประกอบด้วย การใช้บัญชีคลาวด์ (Cloud Account) โครงการ (Project) เครือข่าย (Network) ทรัพยากร (Resource) หรือกลไกการแบ่งแยกเชิงตรรกะอื่นที่เหมาะสม

2. การควบคุมการเข้าถึงแต่ละสภาพแวดล้อม (Environment Access Control)

ผู้ใช้บริการคลาวด์ควรกำหนดสิทธิการเข้าถึงแต่ละสภาพแวดล้อมตามบทบาทและหน้าที่ความรับผิดชอบ (Roles and Responsibilities) โดยยึดหลักสิทธิเท่าที่จำเป็น (Principle of Least Privilege)

โดยเฉพาะอย่างยิ่ง การเข้าถึงสภาพแวดล้อมปฏิบัติการจริง (Production Environment) ควรจำกัดเฉพาะบุคลากรที่มีความจำเป็นและได้รับอนุญาตอย่างเหมาะสม

การกำหนดสิทธิอาจพิจารณาในลักษณะดังนี้

สภาพแวดล้อม	แนวทางการควบคุม
การพัฒนา (Development)	อนุญาตตามบทบาทของผู้พัฒนาและผู้เกี่ยวข้อง
การทดสอบ (Testing)	จำกัดตามหน้าที่ในการทดสอบและตรวจสอบ
การปฏิบัติงานจริง (Production)	จำกัดเฉพาะผู้ได้รับอนุญาตและมีความจำเป็นทางปฏิบัติการ

3. การควบคุมการนำการเปลี่ยนแปลงเข้าสู่ระบบปฏิบัติการจริง (Production Deployment Control)

การนำซอฟต์แวร์ การตั้งค่า หรือองค์ประกอบอื่นเข้าสู่สภาพแวดล้อมปฏิบัติการจริงควรผ่านกระบวนการที่ได้รับอนุมัติและสามารถตรวจสอบย้อนหลังได้

ควรพิจารณาอย่างน้อยถึง

- การอนุมัติการเปลี่ยนแปลง (Change Approval)
- การทดสอบก่อนนำไปใช้งาน (Pre-deployment Testing)
- การบันทึกการนำขึ้นระบบ (Deployment Record)
- การกำหนดแนวทางย้อนกลับเมื่อเกิดปัญหา (Rollback Arrangement)

ทั้งนี้ ควรเชื่อมโยงกับกระบวนการจัดการการเปลี่ยนแปลง (Change Management) ตามข้อ 5.2.6.1 โดยไม่จำเป็นต้องกำหนดกระบวนการซ้ำขึ้นใหม่

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

4. การใช้ข้อมูลในสภาพแวดล้อมที่ไม่ใช่ระบบปฏิบัติการจริง (Use of Production Data in Non-Production Environments)

ผู้ใช้บริการคลาวด์ควรหลีกเลี่ยงการนำข้อมูลจากระบบปฏิบัติการจริง (Production Data) โดยเฉพาะข้อมูลสำคัญหรือข้อมูลที่มีความอ่อนไหว (Sensitive Information) ไปใช้ในสภาพแวดล้อมสำหรับการพัฒนาหรือการทดสอบโดยไม่มีความจำเป็น

หากมีความจำเป็นต้องใช้ ควรกำหนดมาตรการป้องกันที่เหมาะสม เช่น การปกปิดข้อมูล (Data Masking) การทำข้อมูลให้ไม่สามารถระบุตัวบุคคลได้ (Anonymization) การใช้นามแฝงแทนข้อมูล (Pseudonymization) หรือมาตรการควบคุมการเข้าถึงตามความเหมาะสม

ส่วนที่ 2: ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถและกลไกที่สนับสนุนให้ผู้ใช้บริการสามารถแบ่งแยกและควบคุมสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงได้อย่างเหมาะสม

1. การสนับสนุนการแบ่งแยกสภาพแวดล้อม (Environment Isolation Capability)

ผู้ให้บริการคลาวด์ควรมีความสามารถในการสนับสนุนการแบ่งแยกทรัพยากรและสภาพแวดล้อมตามความเหมาะสมกับรูปแบบบริการ เช่น

- การแบ่งแยกบัญชีหรือโครงการ (Account/Project Separation)
- การแบ่งแยกเครือข่าย (Network Segmentation)
- การแบ่งแยกทรัพยากร (Resource Isolation)
- การกำหนดนโยบายและสิทธิการเข้าถึงแยกตามสภาพแวดล้อม (Environment-specific Access Policy)

2. การสนับสนุนการควบคุมสิทธิ (Access Control Capability)

ผู้ให้บริการคลาวด์ควรจัดให้มีกลไกสำหรับกำหนดและควบคุมสิทธิการเข้าถึงทรัพยากรในแต่ละสภาพแวดล้อม เช่น การควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control: RBAC) หรือกลไกอื่นที่มีวัตถุประสงค์เทียบเท่า

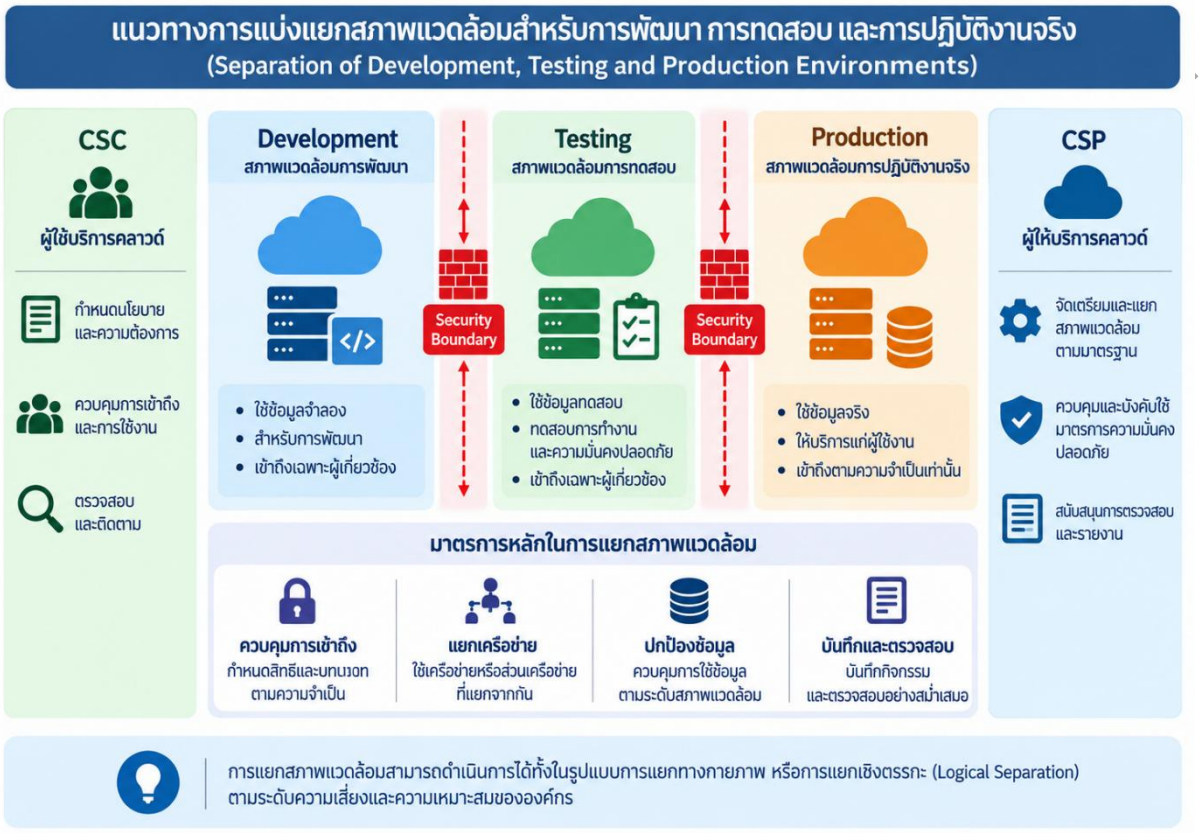
3. การสนับสนุนการตรวจสอบย้อนหลัง (Auditability)

ผู้ให้บริการคลาวด์ควรสนับสนุนความสามารถในการบันทึกกิจกรรมสำคัญที่เกี่ยวข้องกับการบริหารจัดการและการเปลี่ยนแปลงในแต่ละสภาพแวดล้อม เพื่อให้สามารถตรวจสอบย้อนหลังได้ตามขอบเขตของบริการ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 3: แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การแบ่งแยกสภาพแวดล้อมควรพิจารณาทั้งขอบเขตการเข้าถึง เครือข่าย ข้อมูล และกระบวนการนำการเปลี่ยนแปลงเข้าสู่ระบบปฏิบัติงานจริง โดยไม่จำเป็นต้องเป็นการแบ่งแยกทางกายภาพในทุกกรณี หากสามารถใช้มาตรการแบ่งแยกเชิงตรรกะที่เหมาะสมกับระดับความเสี่ยงได้ ดังแสดงในรูปต่อไปนี้



รูปที่ 10 แนวทางการแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริง

เหตุผลและความจำเป็น (Rationale)

การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงานจริงช่วยลดความเสี่ยงที่ความผิดพลาด การทดสอบ หรือกิจกรรมของผู้พัฒนาจะส่งผลกระทบต่อระบบที่ให้บริการจริง รวมถึงช่วยลดโอกาสของการเข้าถึงหรือเปลี่ยนแปลงระบบปฏิบัติการจริงโดยไม่ได้รับอนุญาต

สำหรับบริการคลาวด์ การแบ่งแยกเชิงตรรกะที่เหมาะสมประกอบกับการควบคุมสิทธิ การแบ่งแยกเครือข่าย การปกป้องข้อมูล และการตรวจสอบย้อนหลัง สามารถสนับสนุนการแบ่งแยกสภาพแวดล้อมได้โดยไม่จำเป็นต้องกำหนดเทคโนโลยีหรือสถาปัตยกรรมเฉพาะราย จึงรักษาความเป็นกลางทางเทคโนโลยี (Technology Neutrality) และเปิดโอกาสให้ผู้ให้บริการคลาวด์สามารถแสดงความสามารถด้านการแบ่งแยกและการควบคุมที่มีประสิทธิผลตามสถาปัตยกรรมของตน

การเคลื่อนย้ายหรือปรับเปลี่ยนซอฟต์แวร์ การตั้งค่า หรือองค์ประกอบระหว่างสภาพแวดล้อมควรผ่านช่องทางและกระบวนการที่กำหนด (Controlled Promotion Path) และไม่ควรเปิดให้มีการนำการเปลี่ยนแปลงเข้าสู่ระบบปฏิบัติการจริงโดยข้ามกระบวนการควบคุมที่กำหนด เว้นแต่เป็นกรณีฉุกเฉินที่ดำเนินการตามกระบวนการจัดการการเปลี่ยนแปลงฉุกเฉิน (Emergency Change Management)

นอกจากนี้ การแบ่งแยกควรพิจารณาอย่างน้อย 4 มิติ ได้แก่ **การแบ่งแยกทรัพยากร (Resource Separation), การแบ่งแยกการเข้าถึง (Access Separation), การแบ่งแยกข้อมูล (Data Separation) และการควบคุมการนำขึ้นระบบ (Deployment Control)** โดยระดับความเข้มงวดควรสอดคล้องกับผลการประเมินความเสี่ยง

หลักฐานที่ควรพิจารณา (Recommended Evidence)

หลักฐานอาจประกอบด้วยแผนภาพสถาปัตยกรรม (Architecture Diagram) ตารางสิทธิการเข้าถึง (Access Control Matrix) บันทึกการเปลี่ยนแปลง (Change Record) และบันทึกการนำระบบขึ้นใช้งาน (Deployment Record) ตามความเหมาะสม

องค์กรอาจใช้ **ตารางการแบ่งแยกสภาพแวดล้อม (Environment Separation Matrix)** เพื่อเชื่อมโยงสภาพแวดล้อม บัญชีหรือโครงการ เครือข่าย บทบาทการเข้าถึง ประเภทข้อมูล และการควบคุมการนำระบบขึ้นใช้งาน ทั้งนี้ สามารถใช้ข้อมูลจากเอกสารหรือระบบที่มีอยู่แทนได้ หากสามารถยืนยันการแบ่งแยกและการควบคุมได้อย่างเพียงพอ

สรุปข้อกำหนดและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security Requirements and Responsibility Summary)

1. หลักการ (Principle)

การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security) ของบริการคลาวด์เป็นความรับผิดชอบร่วม (Shared Responsibility) ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยขอบเขตความรับผิดชอบของแต่ละฝ่ายอาจแตกต่างกันตามรูปแบบบริการคลาวด์ (Cloud Service Model) ขอบเขตการควบคุมทางเทคนิค (Technical Control Boundary) และข้อตกลงการให้บริการ (Service Agreement)

ผู้ใช้บริการคลาวด์ยังคงมีหน้าที่ในการกำหนดความต้องการด้านความมั่นคงปลอดภัย ประเมินความเสี่ยง กำหนดค่าบริการและควบคุมทรัพยากรที่อยู่ภายใต้ความรับผิดชอบของตน ขณะที่ผู้ให้บริการคลาวด์มีหน้าที่จัดให้มีมาตรการควบคุมและความสามารถด้านความมั่นคงปลอดภัยสำหรับโครงสร้างพื้นฐาน แพลตฟอร์ม หรือบริการที่อยู่ภายใต้ขอบเขตความรับผิดชอบของผู้ให้บริการ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ทั้งสองฝ่ายควรทำความเข้าใจและกำหนดขอบเขตความรับผิดชอบดังกล่าวอย่างชัดเจน เพื่อป้องกันช่องว่างของการควบคุม (Control Gap) หรือความเข้าใจคลาดเคลื่อนเกี่ยวกับความรับผิดชอบด้านความมั่นคงปลอดภัย (Responsibility Misalignment)

2. สรุปความรับผิดชอบของผู้ใช้บริการและผู้ให้บริการคลาวด์ (Cloud Security Responsibility Summary)

หัวข้อ	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
5.2.6.1 การจัดการการเปลี่ยนแปลง (Change Management)	กำหนด ควบคุม อนุมัติ และตรวจสอบการเปลี่ยนแปลงของระบบและทรัพยากรที่อยู่ภายใต้ความรับผิดชอบ	ควบคุมการเปลี่ยนแปลงของโครงสร้างพื้นฐานและบริการภายใต้ความรับผิดชอบ และบริหารผลกระทบต่อบริการ
5.2.6.2 การบริหารจัดการความจุ (Capacity Management)	ประเมินความต้องการ ติดตามการใช้ทรัพยากร และวางแผนความจุตามความต้องการของระบบ	บริหารความจุของโครงสร้างพื้นฐานและจัดให้มีความสามารถในการขยายทรัพยากรตามลักษณะบริการ
5.2.6.3 การสำรองข้อมูล (Information Backup)	กำหนดข้อมูลที่ต้องสำรอง ความถี่ ระยะเวลาจัดเก็บ RPO/RTO และทดสอบการกู้คืนตามความรับผิดชอบ	จัดให้มีความสามารถในการสำรองและกู้คืนตามขอบเขตของบริการ พร้อมปกป้องโครงสร้างพื้นฐานที่เกี่ยวข้อง
5.2.6.4 การบันทึกเหตุการณ์ (Event Logging)	กำหนดเหตุการณ์ที่ต้องบันทึก รวบรวม ตรวจสอบ และวิเคราะห์ Log ของระบบที่รับผิดชอบ	จัดให้มี Logging Capability และช่องทางเข้าถึงหรือส่งออก Log ตามขอบเขตของบริการ
5.2.6.5 การปกป้องข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)	ป้องกัน Log ที่จัดเก็บหรือบริหารโดย CSC จากการเข้าถึง แก้ไข หรือลบโดยไม่ได้รับอนุญาต	ปกป้อง Log ที่อยู่ภายใต้การควบคุมของ CSP รวมถึงการแบ่งแยกข้อมูลของผู้ใช้บริการตามความเหมาะสม
5.2.6.6 การบันทึกกิจกรรมของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)	บันทึกและทบทวนกิจกรรมของบัญชีสิทธิพิเศษภายใต้การควบคุมของ CSC	บันทึกและควบคุมกิจกรรมของผู้ดูแลระบบ CSP ที่เกี่ยวข้องกับบริการตามขอบเขตที่รับผิดชอบ
5.2.6.7 การประสานเวลาของระบบ (Clock Synchronization)	กำหนดและควบคุมเวลาของระบบที่ CSC สามารถบริหารจัดการได้	รักษาความถูกต้องและความสอดคล้องของเวลาสำหรับ

ร่างสำหรับ Public Hearing เท่านั้น ยังไม่ใช่ร่างที่ใช้งานจริง

		โครงสร้างพื้นฐานและบริการที่ CSP รับผิดชอบ
5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)	ระบุ ประเมิน จัดลำดับ แก้ไข และตรวจสอบช่องโหว่ของระบบที่อยู่ภายใต้ความรับผิดชอบ	บริหารจัดการช่องโหว่ของโครงสร้างพื้นฐาน แพลตฟอร์ม หรือองค์ประกอบที่อยู่ภายใต้ความรับผิดชอบของ CSP
5.2.6.9 การแยกสภาพแวดล้อม (Separation of Development, Testing and Operational Environments)	กำหนดและควบคุมการแบ่งแยก Dev/Test/Production รวมถึงสิทธิข้อมูล และการนำขึ้นระบบ	จัดให้มีกลไกที่สนับสนุนการแบ่งแยกทรัพยากร เครือข่าย บัญชี/โครงการ และสิทธิการเข้าถึงตามลักษณะบริการ

3. การประยุกต์ใช้ตามรูปแบบบริการคลาวด์ (Application by Cloud Service Model)

ขอบเขตความรับผิดชอบควรพิจารณาตามรูปแบบบริการคลาวด์ โดยไม่ควรกำหนดให้ผู้ให้บริการคลาวด์รับผิดชอบทุกมาตรการโดยอัตโนมัติ

โดยหลักการ เมื่อผู้ใช้บริการมีอำนาจควบคุมองค์ประกอบของระบบมากขึ้น ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยการปฏิบัติการของผู้ใช้บริการย่อมเพิ่มขึ้นตามไปด้วย ในทางกลับกัน เมื่อองค์ประกอบของบริการได้รับการบริหารจัดการโดยผู้ให้บริการมากขึ้น ความรับผิดชอบในการควบคุมองค์ประกอบดังกล่าวย่อมอยู่กับผู้ให้บริการมากขึ้น

ตัวอย่างเชิงหลักการสามารถสรุปได้ดังนี้

ขอบเขต	IaaS	PaaS	SaaS
โครงสร้างพื้นฐานทางกายภาพ (Physical Infrastructure)	CSP	CSP	CSP
โครงสร้างพื้นฐานเสมือน (Virtualization Infrastructure)	CSP	CSP	CSP
ระบบปฏิบัติการ (Operating System)	CSC เป็นหลัก	CSP เป็นหลัก	CSP
แพลตฟอร์ม/Runtime	CSC เป็นหลัก	CSP	CSP

สำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

แอปพลิเคชัน (Application)	CSC	CSC/CSP ตามบริการ	CSP เป็นหลัก
ข้อมูลและการกำหนดสิทธิ (Data and Access Configuration)	CSC	CSC	CSC และ CSP ตามขอบเขตบริการ
การกำหนดค่าบริการของผู้ใช้ (Customer Configuration)	CSC	CSC	CSC

ตารางดังกล่าวควรใช้เป็น **แนวทางเชิงหลักการ (Indicative Guidance)** ไม่ใช่ข้อกำหนดตายตัว เนื่องจากขอบเขตความรับผิดชอบจริงขึ้นอยู่กับรายละเอียดของบริการและข้อตกลงระหว่างคู่สัญญา

4. หลักฐานประกอบการประเมิน (Assessment Evidence)

ในการประเมินความสอดคล้อง ผู้ประเมินควรพิจารณาทั้งเอกสาร กระบวนการ และหลักฐานทางเทคนิค (Technical Evidence) ที่แสดงให้เห็นว่ามาตรการควบคุมได้รับการนำไปปฏิบัติจริง

หลักฐานอาจประกอบด้วย นโยบายและขั้นตอนปฏิบัติงาน (Policies and Procedures) การตั้งค่าระบบ (System Configuration) รายงานจากเครื่องมือบริหารจัดการ (Management Reports) บันทึกเหตุการณ์ (Logs) รายงานการตรวจสอบ (Audit Reports) รายงานการทดสอบ (Test Reports) และหลักฐานอื่นที่สามารถแสดงประสิทธิผลของมาตรการควบคุม (Control Effectiveness)

ไม่ควรกำหนดให้ผู้ให้บริการต้องเปิดเผยรายละเอียดทางเทคนิคที่อาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานโดยไม่จำเป็น หากสามารถใช้หลักฐานอื่นที่ให้ความเชื่อมั่นในระดับเทียบเท่า (Equivalent Assurance) ได้

5. การใช้หลักฐานรับรองจากบุคคลที่สาม (Independent Assurance)

ในการประเมินมาตรการด้านการรักษาความมั่นคงปลอดภัยการปฏิบัติการ อาจพิจารณาหลักฐานการรับรองหรือรายงานการตรวจประเมินจากบุคคลที่สามที่มีความน่าเชื่อถือ (Independent Third-Party Assurance) ประกอบการประเมินได้ โดยต้องพิจารณาว่าขอบเขต (Scope) ระยะเวลาที่ครอบคลุม (Coverage Period) และมาตรการควบคุมที่ได้รับการประเมิน (Control Coverage) สอดคล้องกับบริการคลาวด์ที่อยู่ระหว่างการประเมิน

ตัวอย่างหลักฐานอาจรวมถึงใบรับรองมาตรฐาน (Certification) รายงานการตรวจประเมินจากบุคคลที่สาม (Third-Party Audit Report) หรือรายงานการรับรองอื่นที่ได้รับการยอมรับ ทั้งนี้ การมีใบรับรองเพียงอย่างเดียวไม่ควรถือเป็นหลักฐานว่าข้อกำหนดทุกประการได้รับการปฏิบัติตามโดยอัตโนมัติ

6. การกำหนดความรับผิดชอบร่วม (Shared Responsibility Determination)

ร่างหลักเกณฑ์ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ก่อนนำบริการคลาวด์มาใช้งาน ผู้ใช้บริการควรทำความเข้าใจและประเมินขอบเขตความรับผิดชอบด้านความมั่นคงปลอดภัยระหว่างผู้ใช้บริการและผู้ให้บริการ เพื่อให้มั่นใจว่ามาตรการควบคุมที่จำเป็นได้รับการกำหนดผู้รับผิดชอบอย่างครบถ้วน

ในกรณีที่ความรับผิดชอบเกี่ยวข้องกับทั้งสองฝ่าย ควรกำหนดให้ชัดเจนว่าแต่ละฝ่ายมีหน้าที่ดำเนินการในส่วนใด รวมถึงข้อมูลหรือการประสานงานที่จำเป็นระหว่างกัน เพื่อป้องกันมิให้เกิดช่องว่างของการควบคุม (Control Gap)

สามารถกำหนดหลักการได้ว่า

ความรับผิดชอบร่วม (Shared Responsibility) มิได้หมายถึงความรับผิดชอบที่ซ้ำซ้อน แต่หมายถึงการกำหนดขอบเขตหน้าที่ของแต่ละฝ่ายให้ต่อเนื่องและครอบคลุมตลอดห่วงโซ่การควบคุม (Control Chain)

องค์กรไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มใหม่สำหรับหัวข้อนี้ หากข้อมูลจากระบบ เอกสารที่มีอยู่ รายงานการปฏิบัติงาน หรือหลักฐานจาก CSP สามารถใช้ยืนยันการดำเนินการตามข้อกำหนดได้อย่างเพียงพอและตรวจสอบย้อนกลับได้

การใช้หลักฐานจากผู้ให้บริการและการรับรองโดยหน่วยงานอิสระ

การประเมินการปฏิบัติตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยการปฏิบัติการไม่ควรพิจารณาจากการมีใบรับรองหรือรายงานการตรวจประเมินของผู้ให้บริการคลาวด์เพียงอย่างเดียว แต่ควรพิจารณาความเกี่ยวข้องของขอบเขตการรับรอง ความครอบคลุมของบริการที่ใช้งาน ระยะเวลาของหลักฐาน ตลอดจนข้อจำกัดหรือข้อยกเว้นที่ระบุไว้ในรายงาน

รายงานการตรวจประเมินโดยหน่วยงานอิสระ ใบรับรองมาตรฐาน หรือรายงานการประเมินอื่น สามารถใช้เป็นหลักฐานประกอบการพิจารณาได้ หากมีขอบเขตที่เกี่ยวข้องและมีความน่าเชื่อถือเพียงพอ อย่างไรก็ตาม การมีหลักฐานดังกล่าวไม่ควรถูกตีความโดยอัตโนมัติว่าข้อกำหนดทุกประเด็นได้รับการปฏิบัติอย่างครบถ้วน เนื่องจากความรับผิดชอบบางส่วนอาจยังอยู่ภายใต้การควบคุมของ CSC หรือเป็นความรับผิดชอบร่วมระหว่าง CSC และ CSP

การประเมินจึงควรพิจารณาร่วมกันระหว่างขอบเขตการควบคุม (Control Boundary) รูปแบบบริการคลาวด์ (Cloud Service Model) ข้อตกลงการให้บริการ (Service Agreement) หลักฐานที่เกี่ยวข้อง และผลการประเมินความเสี่ยง เพื่อให้สามารถระบุได้อย่างชัดเจนว่ามาตรการใดอยู่ในความรับผิดชอบของ CSC มาตรการใดอยู่ในความรับผิดชอบของ CSP และมาตรการใดจำเป็นต้องดำเนินการร่วมกัน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

แบบประเมินความรับผิดชอบร่วมด้านการรักษาความมั่นคงปลอดภัยการปฏิบัติการของบริการคลาวด์ (Cloud Operations Security Shared Responsibility Assessment)

1. วัตถุประสงค์ (Objective)

แบบประเมินนี้มีวัตถุประสงค์เพื่อสนับสนุนผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ในการพิจารณาขอบเขตความรับผิดชอบร่วม (Shared Responsibility) ระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) สำหรับมาตรการด้านการรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

แบบประเมินนี้ควรใช้เพื่อระบุว่ามาตรการควบคุมแต่ละรายการอยู่ภายใต้ความรับผิดชอบของฝ่ายใด มีหลักฐานสนับสนุนเพียงพอหรือไม่ และมีช่องว่างของการควบคุม (Control Gap) ที่จำเป็นต้องดำเนินการเพิ่มเติมหรือไม่

การใช้แบบประเมินควรพิจารณาร่วมกับรูปแบบบริการคลาวด์ (Cloud Service Model) ได้แก่ การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) และการให้บริการซอฟต์แวร์ (Software as a Service: SaaS) รวมถึงข้อตกลงการให้บริการ (Service Agreement) และผลการประเมินความเสี่ยงของหน่วยงาน

2. ข้อมูลทั่วไปของบริการคลาวด์ (Cloud Service Information)

รายการ	**รายละเอียด**
ชื่อบริการคลาวด์ (Cloud Service Name)	
ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)	
หน่วยงาน/ระบบที่ใช้บริการ (Customer/System)	
รูปแบบบริการ (Service Model)	☐ IaaS ☐ PaaS ☐ SaaS ☐ อื่น ๆ
รูปแบบการติดตั้งใช้งาน (Deployment Model)	☐ Public ☐ Private ☐ Hybrid ☐ อื่น ๆ
ระดับความสำคัญของระบบ (System Criticality)	
ระดับชั้นข้อมูล (Information Classification)	
ผู้รับผิดชอบการประเมิน (Assessor/Owner)	
วันที่ประเมิน (Assessment Date)	
วันที่ทบทวนครั้งถัดไป (Next Review Date)	

ร่างเพื่อการรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

3. การกำหนดสถานะความรับผิดชอบ (Responsibility Classification)

เพื่อให้การประเมินเป็นไปในแนวทางเดียวกัน ควรกำหนดสถานะความรับผิดชอบ ดังนี้

สถานะ	ความหมาย
CSC	ผู้ใช้บริการคลาวด์เป็นผู้รับผิดชอบหลัก (Customer Responsibility)
CSP	ผู้ให้บริการคลาวด์เป็นผู้รับผิดชอบหลัก (Provider Responsibility)
Shared	ทั้ง CSC และ CSP มีความรับผิดชอบในส่วนที่แตกต่างหรือเกี่ยวเนื่องกัน (Shared Responsibility)
N/A	ไม่สามารถนำมาประยุกต์ใช้กับบริการนั้นได้ (Not Applicable) โดยควรระบุเหตุผล

ข้อควรระวัง: คำว่า “Shared” ไม่ควรตีความว่าทั้งสองฝ่ายต้องดำเนินมาตรการเดียวกันซ้ำกัน แต่หมายถึงแต่ละฝ่ายมีหน้าที่ในองค์ประกอบที่อยู่ภายใต้ขอบเขตการควบคุม (Control Boundary) ของตน และหน้าที่ของทั้งสองฝ่ายเมื่อพิจารณาร่วมกันแล้วควรครอบคลุมความเสี่ยงที่เกี่ยวข้องอย่างเพียงพอ

4. แบบประเมิน (Assessment Checklist)

ข้อ	ประเด็นประเมิน (Assessment Criteria)	ความรับผิดชอบ	หลักฐาน (Evidence)	สถานะ/ช่องว่าง (Status/Gap)
5.2.6.1	**การจัดการการเปลี่ยนแปลง (Change Management)**			
1	มีกระบวนการควบคุมและอนุมัติการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อบริการคลาวด์	CSC / CSP / Shared		
2	มีการประเมินผลกระทบและความเสี่ยงก่อนดำเนินการเปลี่ยนแปลงตามความเหมาะสม	CSC / CSP / Shared		
3	มีการทดสอบและแนวทางย้อนกลับ (Rollback) สำหรับการเปลี่ยนแปลงที่มีนัยสำคัญ	CSC / CSP / Shared		
4	CSP มีกลไกแจ้งการเปลี่ยนแปลงที่มีนัยสำคัญต่อ CSC ตามเงื่อนไขของบริการ	CSP		
5.2.6.2	**การบริหารจัดการความจุ (Capacity Management)**			
5	มีการติดตามการใช้ทรัพยากร (Resource Utilization) ที่สำคัญ	CSC / CSP / Shared		
6	มีการวิเคราะห์แนวโน้มและวางแผนความจุตามความต้องการของระบบ	CSC / CSP / Shared		

ร่างเอกสาร Public Hearing ฉบับ - ห้ามใช้อ้างอิง

7	บริการรองรับการปรับเพิ่มหรือลดทรัพยากรตามความเหมาะสม	CSP / Shared		
5.2.6.3	**การสำรองข้อมูล (Information Backup)**			
8	มีการกำหนดขอบเขต ความถี่ และระยะเวลาเก็บรักษาข้อมูลสำรอง	CSC / CSP / Shared		
9	มีมาตรการปกป้องข้อมูลสำรองจากการเข้าถึง แก้ไข หรือลบโดยไม่ได้รับอนุญาต	CSC / CSP / Shared		
10	มีการตรวจสอบสถานะและความสำเร็จของการสำรองข้อมูล	CSC / CSP / Shared		
11	มีการทดสอบการกู้คืนข้อมูล (Restore Testing) ตามความเหมาะสม	CSC / CSP / Shared		
5.2.6.4	**การบันทึกเหตุการณ์ (Event Logging)**			
12	มีการกำหนดเหตุการณ์สำคัญที่ต้องบันทึก (Logging Requirements)	CSC / CSP / Shared		
13	Log มีข้อมูลเพียงพอสำหรับการตรวจสอบและเชื่อมโยงเหตุการณ์	CSC / CSP / Shared		
14	สามารถเข้าถึง ส่งออก หรือเชื่อมต่อ Log เพื่อสนับสนุนการตรวจสอบตามขอบเขตบริการ	CSP / Shared		
5.2.6.5	**การปกป้องข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)**			
15	มีการควบคุมสิทธิการเข้าถึง Log	CSC / CSP / Shared		
16	มีมาตรการป้องกันการแก้ไขหรือลบ Log โดยไม่ได้รับอนุญาต	CSC / CSP / Shared		
17	มีการกำหนดและควบคุมระยะเวลาเก็บรักษา Log	CSC / CSP / Shared		
5.2.6.6	**การบันทึกกิจกรรมของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)**			
18	มีการบันทึกกิจกรรมของบัญชีที่มีสิทธิพิเศษ (Privileged Accounts)	CSC / CSP / Shared		
19	สามารถระบุตัวตน เวลา กิจกรรม และผลการดำเนินการของผู้ดูแลระบบได้	CSC / CSP / Shared		

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

20	มีการทบทวนกิจกรรมที่มีความเสี่ยงหรือผิดปกติตามความเหมาะสม	CSC / CSP / Shared		
5.2.6.7	**การประสานเวลาของระบบ (Clock Synchronization)**			
21	ระบบใช้แหล่งอ้างอิงเวลาที่เชื่อถือได้ (Trusted Time Source)	CSC / CSP / Shared		
22	Timestamp ของระบบที่เกี่ยวข้องมีความสอดคล้องเพียงพอต่อการตรวจสอบเหตุการณ์	CSC / CSP / Shared		
5.2.6.8	**การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)**			
23	มีกระบวนการระบุและติดตามช่องโหว่ที่เกี่ยวข้องกับระบบหรือบริการ	CSC / CSP / Shared		
24	มีการประเมินและจัดลำดับความสำคัญของช่องโหว่ตามความเสี่ยง	CSC / CSP / Shared		
25	มีการดำเนินการแก้ไขหรือลดความเสี่ยง (Remediation/Mitigation)	CSC / CSP / Shared		
26	มีการตรวจสอบยืนยันหลังดำเนินการแก้ไข (Remediation Verification)	CSC / CSP / Shared		
5.2.6.9	**การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน (Separation of Development, Testing and Operational Environments)**			
27	มีการแบ่งแยก Development, Testing และ Production ตามระดับความเสี่ยง	CSC / CSP / Shared		
28	มีการแบ่งแยกและควบคุมสิทธิการเข้าถึงแต่ละสภาพแวดล้อม	CSC / CSP / Shared		
29	มีการควบคุมการนำการเปลี่ยนแปลงเข้าสู่ Production	CSC / CSP / Shared		
30	การใช้ข้อมูล Production ใน Non-Production Environment ได้รับการควบคุมอย่างเหมาะสม	CSC / CSP / Shared		

5. เกณฑ์การประเมินสถานะ (Assessment Status)

ร่างเอกสาร Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ควรใช้สถานะเชิงคุณภาพ (Qualitative Status) ดังนี้

สถานะ	หลักเกณฑ์
สอดคล้อง (Conform)	มีมาตรการและหลักฐานเพียงพอแสดงว่าข้อกำหนดได้รับการดำเนินการอย่างเหมาะสม
สอดคล้องบางส่วน (Partially Conform)	มีมาตรการแล้ว แต่ยังมีข้อจำกัดหรือหลักฐานบางส่วนที่ต้องปรับปรุง
ไม่สอดคล้อง (Not Conform)	ยังไม่มีมาตรการ หรือมาตรการไม่เพียงพอต่อข้อกำหนด
ไม่เกี่ยวข้อง (Not Applicable: N/A)	ไม่สามารถนำข้อกำหนดนั้นมาประยุกต์ใช้กับบริการได้ โดยต้องระบุเหตุผล

การใช้ **N/A ต้องมีเหตุผลประกอบ (Justification)** และไม่ควรใช้เพียงเพราะมาตรการนั้นดำเนินการโดย CSP หาก CSP เป็นผู้รับผิดชอบ มาตรการดังกล่าวยังถือว่า *Applicable* แต่หลักฐานอาจมาจาก CSP

6. แนวทางพิจารณาหลักฐาน (Evidence Consideration)

หลักฐานประกอบการประเมินไม่จำเป็นต้องมีรูปแบบเดียวกันสำหรับผู้ให้บริการทุกราย ผู้ประเมินควรพิจารณาความเพียงพอ ความเกี่ยวข้อง และความน่าเชื่อถือของหลักฐาน (Sufficiency, Relevance and Reliability of Evidence) ตามลักษณะของบริการและความเสี่ยง

ตัวอย่างหลักฐานที่อาจนำมาพิจารณา ได้แก่ เอกสารนโยบายและขั้นตอนปฏิบัติงาน (Policies and Procedures) ภาพหรือข้อมูลการตั้งค่าระบบ (Configuration Evidence) รายงานการปฏิบัติงาน (Operational Reports) บันทึกเหตุการณ์ (Logs) รายงานการทดสอบ (Test Reports) ข้อตกลงการให้บริการ (Service Agreement) เอกสารอธิบายความรับผิดชอบร่วม (Shared Responsibility Documentation) และหลักฐานการรับรองจากบุคคลที่สาม (Independent Assurance)

สำหรับมาตรการที่อยู่ภายใต้การควบคุมของ CSP ผู้ประเมินอาจยอมรับหลักฐานที่ให้ระดับความเชื่อมั่นเทียบเท่า (Equivalent Assurance) แทนการเข้าถึงระบบภายในของ CSP โดยตรงได้ หากหลักฐานดังกล่าวมีขอบเขตและความน่าเชื่อถือเพียงพอต่อวัตถุประสงค์ของการประเมิน

7. การจัดการช่องว่าง (Gap Management)

หากพบช่องว่างจากการประเมิน ควรระบุอย่างน้อยถึง **ช่องว่างที่พบ (Identified Gap) ระดับความเสี่ยง (Risk Level) ผู้รับผิดชอบ (Responsible Party) แนวทางดำเนินการ (Action Plan) และระยะเวลาดำเนินการ (Target Date)**

ในกรณีที่ช่องว่างอยู่ภายใต้ความรับผิดชอบของ CSP ผู้ใช้บริการควรพิจารณาวิธีการที่เหมาะสม เช่น การขอข้อมูลหรือหลักฐานเพิ่มเติม การเปิดใช้ความสามารถด้านความมั่นคงปลอดภัยเพิ่มเติม (Security Capability) การ

ร่างเอกสารเพื่อรับฟังความคิดเห็นสาธารณะ (Public Hearing) เท่านั้น - ห้ามนำไปใช้อ้างอิง

กำหนดค่าบริการเพิ่มเติม การกำหนดมาตรการชดเชย (Compensating Control) หรือการบริหารความเสี่ยงตามกระบวนการของหน่วยงาน

5.2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security) เป็นมาตรการสำคัญในการปกป้องข้อมูลและระบบสารสนเทศที่มีการเชื่อมต่อหรือรับส่งข้อมูลผ่านเครือข่าย โดยมีวัตถุประสงค์เพื่อลดความเสี่ยงจากการเข้าถึง การดักรับ การเปิดเผย การแก้ไข หรือการถ่ายโอนข้อมูลโดยไม่ได้รับอนุญาต รวมถึงสนับสนุนการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและบริการ

สำหรับสภาพแวดล้อมระบบคลาวด์ การรักษาความมั่นคงปลอดภัยเครือข่ายควรพิจารณาทั้งการปกป้องข้อมูลระหว่างการถ่ายโอน (Information Transfer Protection) และการแบ่งแยกเครือข่าย (Network Segregation) ให้เหมาะสมกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ลักษณะของบริการคลาวด์ สถาปัตยกรรมระบบ และผลการประเมินความเสี่ยง โดยเฉพาะการแบ่งแยกระหว่างผู้เช่า (Tenant Isolation) ในสภาพแวดล้อมที่มีผู้เช่าหลายราย (Multi-tenant Environment) และการแบ่งแยกระหว่างสภาพแวดล้อมการบริหารจัดการของผู้ให้บริการคลาวด์กับสภาพแวดล้อมการประมวลผลของผู้ใช้บริการคลาวด์ ซึ่งเป็นสาระที่ข้อกำหนดเดิมกำหนดไว้โดยตรง

มาตรการที่นำมาใช้ควรมีความเหมาะสมและได้สัดส่วนกับความเสี่ยง (Risk-based and Proportionate) โดยคำนึงถึงระดับความสำคัญและความอ่อนไหวของข้อมูลหรือระบบสารสนเทศ ตลอดจนความสามารถและข้อจำกัดของบริการคลาวด์ เพื่อให้สามารถรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิผลโดยไม่ก่อให้เกิดภาระหรือความซับซ้อนเกินความจำเป็น ทั้งนี้ แนวทางดังกล่าวสอดคล้องกับกรอบของประกาศที่กำหนดข้อกำหนดขั้นต่ำตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

หมายเหตุ

การรักษาความมั่นคงปลอดภัยเครือข่ายในสภาพแวดล้อมระบบคลาวด์อาจเป็นความรับผิดชอบร่วมระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยขอบเขตความรับผิดชอบอาจแตกต่างกันตามประเภทบริการคลาวด์ รูปแบบการให้บริการ และสถาปัตยกรรมที่นำมาใช้

ผู้ใช้บริการคลาวด์ควรพิจารณาหลักการแบ่งความรับผิดชอบ (Shared Responsibility Model) เพื่อกำหนดขอบเขตการควบคุมที่หน่วยงานต้องดำเนินการเอง และส่วนที่ผู้ให้บริการคลาวด์เป็นผู้ดำเนินการ รวมถึงพิจารณาข้อมูลหรือหลักฐานที่จำเป็นสำหรับการตรวจสอบความเหมาะสมและประสิทธิผลของมาตรการดังกล่าว

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้อ้างอิง



แสดงกรอบแนวคิดของการรักษาความมั่นคงปลอดภัยเครือข่ายสำหรับบริการคลาวด์ โดยแบ่งออกเป็น 2 มาตรการหลัก ได้แก่ การถ่ายโอนข้อมูล (Information Transfer) และ การแบ่งแยกเครือข่าย (Network Segregation) ซึ่งควรนำมาประยุกต์ใช้ร่วมกันตามระดับผลกระทบของข้อมูล สถาปัตยกรรมของบริการคลาวด์ และผลการประเมินความเสี่ยง เพื่อสนับสนุนการปกป้องข้อมูลระหว่างการสื่อสารและลดโอกาสของการเข้าถึงหรือการเคลื่อนย้ายภายในระบบโดยไม่ได้รับอนุญาต

ความสัมพันธ์กับมาตรการควบคุมอื่น (Relationship with Other Security Controls)

การแบ่งแยกเครือข่ายเป็นมาตรการควบคุมที่สนับสนุนการรักษาความมั่นคงปลอดภัยของบริการคลาวด์ร่วมกับมาตรการด้านอื่น โดยไม่ควรนำมาใช้เป็นมาตรการเพียงมาตรการเดียวในการลดความเสี่ยง ทั้งนี้ หน่วยงานควรพิจารณาประยุกต์ใช้ร่วมกับมาตรการควบคุมที่เกี่ยวข้องตามความเหมาะสม ดังนี้

- การควบคุมการเข้าถึง (Access Control) เพื่อกำหนดสิทธิ์การเข้าถึงทรัพยากรและการสื่อสารระหว่างส่วนเครือข่าย
- การเข้ารหัส (Cryptography) เพื่อปกป้องข้อมูลที่มีการรับส่งระหว่างส่วนเครือข่ายหรือระหว่างสภาพแวดล้อมที่ได้รับการแบ่งแยก

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing

- การรักษาความมั่นคงปลอดภัยในการดำเนินงาน (Operations Security) เพื่อสนับสนุนการกำหนดค่า การเปลี่ยนแปลง การเฝ้าระวัง และการบริหารจัดการองค์ประกอบของเครือข่ายให้สอดคล้องกับมาตรการแบ่งแยกที่กำหนด
- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) เพื่อจำกัดขอบเขตของผลกระทบ (Impact Containment) และสนับสนุนการตอบสนองต่อเหตุการณ์เมื่อเกิดการละเมิดความมั่นคงปลอดภัย

การเลือกใช้มาตรการควบคุมควรอาศัยผลการประเมินความเสี่ยง และไม่ควรพึ่งพาการแบ่งแยกเครือข่ายเพียงอย่างเดียวในการปกป้องข้อมูลหรือระบบสารสนเทศ

5.2.7.1 นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ	ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ
ข) ผู้ใช้บริการคลาวด์ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง	ข) หากเป็นไปได้ ต้องขอให้ผู้ใช้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง

วัตถุประสงค์ (Objective)

เพื่อกำหนดหลักเกณฑ์และแนวทางในการถ่ายโอนข้อมูล (Information Transfer) ที่เกี่ยวข้องกับการใช้บริการคลาวด์ให้มีความมั่นคงปลอดภัย เหมาะสมกับประเภทและระดับผลกระทบของข้อมูล ช่องทางที่ใช้ในการถ่ายโอน และผลการประเมินความเสี่ยง เพื่อป้องกันการเข้าถึง การดักรับ การเปิดเผย การแก้ไข การสูญหาย หรือการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาตระหว่างกระบวนการถ่ายโอนข้อมูล

การกำหนดมาตรการควบคุมควรครอบคลุมการถ่ายโอนข้อมูลผ่านช่องทางอิเล็กทรอนิกส์ (Electronic Information Transfer) และการถ่ายโอนผ่านสื่อทางกายภาพ (Physical Media Transfer) ตามความเหมาะสม โดยมาตรการที่นำมาใช้ควรสอดคล้องกับระดับความสำคัญและความอ่อนไหวของข้อมูล รวมถึงข้อกำหนดทางกฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา และข้อกำหนดอื่นที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ต้องกำหนดและดำเนินการตามมาตรการสำหรับการถ่ายโอนข้อมูลที่เกี่ยวข้องกับบริการคลาวด์ โดยคำนึงถึงประเภทข้อมูล ระดับผลกระทบ ช่องทางการถ่ายโอน ปลายทางของข้อมูล และความเสี่ยงที่เกี่ยวข้อง

ในกรณีที่มีการใช้สื่อทางกายภาพ (Physical Media) สำหรับการถ่ายโอนข้อมูล ต้องมีการบันทึกข้อมูลเกี่ยวกับสื่อทางกายภาพที่รับเข้าหรือส่งออกซึ่งมีข้อมูลส่วนบุคคล โดยอย่างน้อยต้องสามารถระบุประเภทของสื่อ ผู้ส่งและผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ ทั้งนี้ เพื่อให้สามารถควบคุมและตรวจสอบย้อนกลับ (Traceability) การเคลื่อนย้ายข้อมูลได้อย่างเหมาะสมตามข้อกำหนดของประกาศ

นอกจากนี้ ผู้ใช้บริการคลาวด์ต้องกำหนดให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติมตามความเหมาะสม เช่น การเข้ารหัส (Encryption) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะ ณ จุดปลายทางที่ได้รับอนุญาต และได้รับการปกป้องอย่างเหมาะสมระหว่างการถ่ายโอน

โดยควรดำเนินการดังต่อไปนี้

1. การกำหนดข้อกำหนดสำหรับการถ่ายโอนข้อมูล (Information Transfer Requirements)

หน่วยงานควรกำหนดหลักเกณฑ์สำหรับการถ่ายโอนข้อมูลที่เกี่ยวข้องกับบริการคลาวด์ให้เหมาะสมกับประเภทข้อมูล ระดับผลกระทบ และความเสี่ยง โดยพิจารณาตลอดเส้นทางการถ่ายโอนข้อมูลตั้งแต่ต้นทาง (Source) ช่องทางการถ่ายโอน (Transfer Channel) จนถึงปลายทางที่ได้รับอนุญาต (Authorized Destination)

อย่างน้อยควรพิจารณาประเด็นดังต่อไปนี้

1. ประเภทและระดับของข้อมูลที่อนุญาตให้ถ่ายโอน
2. ผู้ส่งและผู้รับข้อมูลที่ได้รับอนุญาต (Authorized Sender and Recipient)
3. ช่องทางหรือวิธีการถ่ายโอนข้อมูลที่ได้รับอนุญาต (Approved Transfer Method)
4. มาตรการป้องกันข้อมูลที่เหมาะสมกับระดับผลกระทบและความเสี่ยง
5. ข้อกำหนดในการตรวจสอบหรือบันทึกกิจกรรมที่เกี่ยวข้องกับการถ่ายโอนข้อมูลตามความจำเป็น
6. ข้อกำหนดทางกฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา หรือข้อกำหนดอื่นที่เกี่ยวข้องกับข้อมูลที่มีการถ่ายโอน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หน่วยงานควรหลีกเลี่ยงการกำหนดช่องทางหรือมาตรการสำหรับการถ่ายโอนข้อมูลในลักษณะเดียวกันสำหรับข้อมูลทุกประเภท โดยควรใช้แนวทางตามความเสี่ยง (Risk-based Approach) เพื่อให้ระดับของมาตรการควบคุมมีความเหมาะสมและได้สัดส่วนกับผลกระทบที่อาจเกิดขึ้น

ตัวอย่างแนวทาง

ลักษณะข้อมูล	ตัวอย่างแนวทางการถ่ายโอน
ข้อมูลที่เปิดเผยต่อสาธารณะ (Public Information)	สามารถใช้ช่องทางทั่วไปที่หน่วยงานอนุญาต
ข้อมูลใช้ภายใน (Internal Information)	ใช้ช่องทางที่หน่วยงานอนุญาตและมีการควบคุมการเข้าถึงตามความเหมาะสม
ข้อมูลที่มีความอ่อนไหวหรือมีผลกระทบสูง (Sensitive or High-impact Information)	ใช้ช่องทางที่มีมาตรการป้องกันข้อมูลระหว่างการถ่ายโอนและจำกัดปลายทางเฉพาะผู้ได้รับอนุญาต
ข้อมูลที่ถ่ายโอนผ่านสื่อทางกายภาพ (Physical Media)	ใช้มาตรการป้องกันตามความเสี่ยงและจัดให้มีบันทึกการรับ–ส่งสื่อ

หมายเหตุ: ตารางดังกล่าวเป็นเพียงตัวอย่างประกอบการพิจารณา หน่วยงานควรกำหนดมาตรการให้สอดคล้องกับระบบการจัดระดับข้อมูล (Data Classification) และระดับผลกระทบของข้อมูลหรือระบบสารสนเทศที่หน่วยงานกำหนด

เหตุผลและความจำเป็น (Rationale)

ข้อมูลที่มีการถ่ายโอนระหว่างระบบ ผู้ใช้งาน หน่วยงาน หรือบริการคลาวด์อาจเผชิญความเสี่ยงจากการเข้าถึง การดักรับ การเปิดเผย การแก้ไข การสูญหาย หรือการส่งข้อมูลไปยังปลายทางที่ไม่ได้รับอนุญาต การกำหนดข้อกำหนดสำหรับการถ่ายโอนข้อมูลตามประเภทและระดับผลกระทบของข้อมูลจะช่วยให้หน่วยงานสามารถเลือกใช้ช่องทางและมาตรการควบคุมได้อย่างเหมาะสมกับความเสี่ยง โดยไม่กำหนดมาตรการที่มากเกินความจำเป็น

2. การปกป้องข้อมูลระหว่างการถ่ายโอน (Protection of Information in Transfer)

หน่วยงานควรกำหนดมาตรการปกป้องข้อมูลระหว่างการถ่ายโอนให้เหมาะสมกับประเภทข้อมูล ระดับผลกระทบ ช่องทางการสื่อสาร ปลายทางของข้อมูล และผลการประเมินความเสี่ยง เพื่อให้ข้อมูลได้รับการปกป้องจากการเข้าถึง การดักรับ การเปิดเผย การแก้ไข หรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตตลอดกระบวนการถ่ายโอน

การถ่ายโอนข้อมูลที่มีความสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลที่อาจก่อให้เกิดผลกระทบต่อหน่วยงาน ควรดำเนินการผ่านช่องทางที่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยหน่วยงานควรพิจารณาความสามารถในการปกป้องข้อมูลตั้งแต่ต้นทาง (Source) ระหว่างการถ่ายโอน (In Transit) จนถึงปลายทางที่ได้รับอนุญาต (Authorized Destination)

โดยควรพิจารณาดำเนินการดังต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. ใช้ช่องทางการถ่ายโอนข้อมูลที่ได้รับอนุญาต (Approved Transfer Channel) และเหมาะสมกับระดับผลกระทบของข้อมูล
2. ใช้มาตรการปกป้องข้อมูลระหว่างการถ่ายโอน (Data-in-Transit Protection) ที่เหมาะสมกับความเสี่ยง รวมถึงการเข้ารหัส (Encryption) ในกรณีที่จำเป็น โดยให้เป็นไปตามข้อกำหนดด้านการเข้ารหัสของหน่วยงาน
3. ตรวจสอบความถูกต้องของต้นทางและปลายทาง (Source and Destination Verification) ตามความเหมาะสม เพื่อช่วยลดความเสี่ยงจากการส่งข้อมูลไปยังบุคคล ระบบ หรือปลายทางที่ไม่ได้รับอนุญาต
4. จำกัดการเข้าถึงข้อมูลให้เฉพาะบุคคล ระบบ หรือบริการที่ได้รับอนุญาต (Authorized Entity) ตามหลักการควบคุมการเข้าถึงของหน่วยงาน
5. พิจารณามาตรการเพื่อรักษาความถูกต้องครบถ้วนของข้อมูล (Data Integrity) เพื่อให้สามารถป้องกันหรือตรวจพบการแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตระหว่างการถ่ายโอน ตามระดับความเสี่ยง
6. หลีกเลี่ยงการถ่ายโอนข้อมูลสำคัญผ่านช่องทางที่ไม่ได้รับอนุญาต หรือช่องทางที่ไม่มีมาตรการรักษาความมั่นคงปลอดภัยเพียงพอ
7. ในกรณีที่การถ่ายโอนข้อมูลอาศัยความสามารถของผู้ให้บริการคลาวด์ หน่วยงานควรพิจารณาว่าบริการดังกล่าวมีมาตรการหรือความสามารถในการปกป้องข้อมูลระหว่างการถ่ายโอนที่สอดคล้องกับข้อกำหนดของหน่วยงาน

ความสัมพันธ์กับมาตรการควบคุมอื่น การปกป้องข้อมูลระหว่างการถ่ายโอนอาจเกี่ยวข้องกับมาตรการควบคุมด้านอื่น เช่น การควบคุมการเข้าถึง (Access Control) การพิสูจน์ตัวตน (Authentication) และการเข้ารหัส (Cryptography) ดังนั้น หน่วยงานควรนำมาตรการดังกล่าวมาประยุกต์ใช้ร่วมกันตามความเหมาะสม โดยไม่จำเป็นต้องกำหนดมาตรการซ้ำซ้อน

สำหรับรายละเอียดเกี่ยวกับอัลกอริทึมการเข้ารหัส โพรโทคอลการเข้ารหัส ชุดรหัส (Cipher Suite) ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) และการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management) ให้พิจารณาตามข้อ **5.2.4 การเข้ารหัส (Cryptography)** ที่เกี่ยวข้อง

ตัวอย่างแนวทางการปกป้องข้อมูลระหว่างการถ่ายโอน

สถานการณ์	แนวทางที่ควรพิจารณา
การเชื่อมต่อผู้ใช้งานเข้าสู่บริการคลาวด์	ใช้ช่องทางการสื่อสารที่มั่นคงปลอดภัยและมีการพิสูจน์ตัวตนตามความเหมาะสม
การรับส่งข้อมูลระหว่างระบบ	ใช้กลไกปกป้องข้อมูลระหว่างการถ่ายโอนและจำกัดการเชื่อมต่อเฉพาะระบบที่ได้รับอนุญาต
การเชื่อมต่อระหว่างระบบของหน่วยงานกับระบบคลาวด์	กำหนดช่องทางการเชื่อมต่อและมาตรการปกป้องให้เหมาะสมกับระดับผลกระทบและความเสี่ยง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

การถ่ายโอนข้อมูลสำคัญไปยังบุคคลหรือหน่วยงานภายนอก	ตรวจสอบผู้รับและปลายทาง ใช้ช่องทางที่ได้รับอนุญาต และใช้มาตรการปกป้องตามระดับความเสี่ยง
การใช้ความสามารถในการรับส่งข้อมูลของ CSP	ตรวจสอบความสามารถและข้อจำกัดด้านความมั่นคงปลอดภัยของบริการก่อนนำมาใช้งาน

เหตุผลและความจำเป็น (Rationale)

ข้อมูลที่มีการถ่ายโอนผ่านเครือข่ายอาจถูกดักรับ เปิดเผย แก้ไข หรือเปลี่ยนเส้นทางไปยังปลายทางที่ไม่ได้รับอนุญาตได้ หากไม่มีมาตรการปกป้องที่เหมาะสม การกำหนดช่องทางการถ่ายโอนและมาตรการรักษาความมั่นคงปลอดภัยตามระดับผลกระทบและความเสี่ยงจึงช่วยลดโอกาสและผลกระทบจากเหตุการณ์ดังกล่าว ตลอดจนช่วยให้หน่วยงานสามารถใช้ความสามารถด้านความมั่นคงปลอดภัยของบริการคลาวด์ได้อย่างเหมาะสม

ทั้งนี้ การกำหนดมาตรการควรใช้หลักตามความเสี่ยง (Risk-based Approach) และหลีกเลี่ยงการกำหนดเทคโนโลยีหรือรูปแบบการเชื่อมต่อเฉพาะ เว้นแต่มีข้อกำหนดทางกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือผลการประเมินความเสี่ยงที่รองรับ

3. การควบคุมการถ่ายโอนข้อมูลผ่านสื่อทางกายภาพ (Physical Media Transfer Control)

ในกรณีที่หน่วยงานมีการถ่ายโอนข้อมูลที่เกี่ยวข้องกับบริการคลาวด์ผ่านสื่อทางกายภาพ (Physical Media) หน่วยงานต้องกำหนดมาตรการควบคุมการรับ การส่ง และการเคลื่อนย้ายสื่อดังกล่าวให้เหมาะสมกับประเภทข้อมูล ระดับผลกระทบ และผลการประเมินความเสี่ยง เพื่อป้องกันการสูญหาย การเข้าถึง การเปิดเผย การแก้ไข หรือการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาตระหว่างการถ่ายโอน

สื่อทางกายภาพในบริบทนี้อาจรวมถึงสื่อบันทึกข้อมูลแบบถอดหรือเคลื่อนย้ายได้ (Removable or Portable Storage Media) หรือสื่ออื่นที่ใช้สำหรับการรับ–ส่งข้อมูลระหว่างหน่วยงาน ผู้ให้บริการคลาวด์ หรือบุคคลภายนอก ทั้งนี้ ให้พิจารณาตามลักษณะการใช้งานจริงของหน่วยงาน โดยไม่จำเป็นต้องกำหนดประเภทของเทคโนโลยีหรือสื่อไว้เป็นการเฉพาะ

เมื่อมีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูลส่วนบุคคล ต้องจัดให้มีการบันทึกการรับเข้าและส่งออกของสื่อดังกล่าว โดยอย่างน้อยต้องสามารถระบุประเภทของสื่อทางกายภาพ ผู้ส่งและผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ ตามข้อกำหนดของประกาศ

หน่วยงานควรพิจารณาดำเนินการดังต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

1. **กำหนดผู้ส่งและผู้รับที่ได้รับอนุญาต (Authorized Sender and Recipient)** ให้ชัดเจน และตรวจสอบว่าการถ่ายโอนสื่อดำเนินการระหว่างบุคคลหรือหน่วยงานที่มีอำนาจและความจำเป็นในการรับข้อมูล
2. **จัดทำบันทึกการรับ–ส่งสื่อทางกายภาพ (Physical Media Transfer Record)** เพื่อให้สามารถตรวจสอบสถานะและติดตามการเคลื่อนย้ายของสื่อได้ตลอดกระบวนการ
3. **ใช้มาตรการป้องกันสื่อระหว่างการเคลื่อนย้าย (Media Protection in Transit)** ให้เหมาะสมกับระดับผลกระทบของข้อมูลและความเสี่ยง เช่น การป้องกันการเปิดหรือเข้าถึงสื่อโดยไม่ได้รับอนุญาต และการใช้มาตรการเข้ารหัส (Encryption) ในกรณีที่เหมาะสม
4. **กำหนดวิธีการส่งมอบที่สามารถตรวจสอบได้ (Traceable Delivery Method)** สำหรับข้อมูลที่มีความสำคัญหรือมีผลกระทบสูงตามความเหมาะสม เพื่อให้สามารถยืนยันการส่งมอบและผู้รับปลายทางได้
5. **ตรวจสอบการรับมอบ (Receipt Verification)** เมื่อสื่อถึงปลายทางตามความเหมาะสม เพื่อยืนยันว่าสื่อถูกส่งมอบให้แก่ผู้รับที่ได้รับอนุญาต และไม่มีเหตุผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล
6. **ดำเนินการต่อสื่อภายหลังการใช้งาน (Post-transfer Media Handling)** ตามข้อกำหนดด้านการจัดการสื่อและข้อมูลของหน่วยงาน เช่น การนำกลับมาใช้ใหม่ (Reuse) การเก็บรักษา (Retention) หรือการทำลายอย่างมั่นคงปลอดภัย (Secure Disposal) เมื่อไม่มีความจำเป็นต้องใช้งานต่อไป

ในกรณีที่การรับ–ส่งสื่อทางกายภาพดำเนินการโดยผู้ให้บริการคลาวด์หรือผู้ให้บริการภายนอก หน่วยงานควรพิจารณาความเหมาะสมของมาตรการรักษาความมั่นคงปลอดภัยและความสามารถในการติดตามตรวจสอบการรับ–ส่งสื่อดังกล่าวตามระดับความเสี่ยง

ตัวอย่างกระบวนการควบคุมการรับ–ส่งสื่อทางกายภาพ

สามารถกำหนดกระบวนการในลักษณะดังต่อไปนี้

ระบุข้อมูลและสื่อที่จะถ่ายโอน

↓

ตรวจสอบระดับผลกระทบและความจำเป็น

↓

ตรวจสอบผู้ส่งและผู้รับที่ได้รับอนุญาต

↓

กำหนดมาตรการป้องกันสื่อ

↓

บันทึกการส่งออก

↓

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ถ่ายโอนและติดตามการส่งมอบ

↓

ยืนยันการรับมอบ

↓

บันทึกผลและเก็บรักษาหลักฐาน

รูปนี้ช่วยให้เห็นจุดควบคุมตั้งแต่ต้นทางจนถึงปลายทาง โดยไม่จำเป็นต้องลงรายละเอียดเป็นขั้นตอนปฏิบัติงานระดับปฏิบัติการมากเกินไป

แบบบันทึกการรับ–ส่งสื่อทางกายภาพ (Physical Media Transfer Log)

ควรมีแบบฟอร์ม เพราะข้อกำหนดต้นทางระบุข้อมูลที่ต้องบันทึกไว้อย่างชัดเจน

โครงสร้างขั้นต่ำของแบบบันทึกควรเป็นดังนี้

รายการ	**รายละเอียด**
เลขที่รายการ (Record No.)	หมายเลขอ้างอิงรายการรับ–ส่ง
ประเภทการดำเนินการ (Transfer Type)	รับเข้า (Inbound) / ส่งออก (Outbound)
ประเภทสื่อ (Media Type)	ประเภทของสื่อทางกายภาพ
รายละเอียดข้อมูล (Information Description)	คำอธิบายข้อมูลโดยสังเขป โดยหลีกเลี่ยงการบันทึกข้อมูลสำคัญเกินความจำเป็น
ระดับข้อมูล/ผลกระทบ (Classification/Impact Level)	ระดับตามที่หน่วยงานกำหนด
จำนวนสื่อ (Quantity)	จำนวนสื่อ
ผู้ส่งที่ได้รับอนุญาต (Authorized Sender)	ชื่อหรือข้อมูลระบุตัวผู้ส่ง
ผู้รับที่ได้รับอนุญาต (Authorized Recipient)	ชื่อหรือข้อมูลระบุตัวผู้รับ
วันที่และเวลาส่ง (Dispatch Date and Time)	วันที่และเวลา
วันที่และเวลารับ (Receipt Date and Time)	วันที่และเวลา
วิธีการถ่ายโอน (Transfer Method)	วิธีการหรือช่องทางการส่งมอบ
มาตรการป้องกัน (Protection Measures)	มาตรการที่ใช้ตามความเหมาะสม
การยืนยันการรับมอบ (Receipt Confirmation)	ผลการยืนยันการรับมอบ
หมายเหตุ (Remarks)	ข้อมูลเพิ่มเติมที่จำเป็น

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

โดย **5 รายการที่มาจากข้อกำหนดโดยตรง** ได้แก่ ประเภทสื่อ ผู้ส่ง ผู้รับ วันที่และเวลา และจำนวนสื่อ ส่วนรายการอื่นเป็นข้อเสนอเพื่อเพิ่มความสามารถในการตรวจสอบย้อนกลับ (Traceability)

เหตุผลและความจำเป็น (Rationale)

การถ่ายโอนข้อมูลผ่านสื่อทางกายภาพมีความเสี่ยงแตกต่างจากการรับส่งข้อมูลผ่านเครือข่าย เนื่องจากสื่ออาจสูญหาย ถูกนำออกนอกพื้นที่ควบคุม ถูกส่งมอบผิดปลายทาง หรือถูกเข้าถึงระหว่างการเคลื่อนย้าย การจัดให้มีมาตรการป้องกันและบันทึกการรับ–ส่งที่เหมาะสมจึงช่วยให้หน่วยงานสามารถควบคุมและตรวจสอบย้อนกลับการเคลื่อนย้ายข้อมูล ตลอดจนสนับสนุนการตรวจสอบและการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเมื่อเกิดความผิดปกติ

ทั้งนี้ ควรกำหนดระดับของมาตรการตามความเสี่ยง (Risk-based Approach) และหลีกเลี่ยงการกำหนดขั้นตอนที่สร้างภาระเกินความจำเป็น โดยเฉพาะกรณีที่ไม่มีการใช้สื่อทางกายภาพในการถ่ายโอนข้อมูลในการให้บริการคลาวด์

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ควรจัดให้มีความสามารถและมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมสำหรับการถ่ายโอนข้อมูลที่อยู่ภายใต้ขอบเขตความรับผิดชอบของตน โดยคำนึงถึงลักษณะของบริการคลาวด์ รูปแบบการให้บริการ สถาปัตยกรรมของระบบ และความเสี่ยงที่เกี่ยวข้อง

ผู้ให้บริการคลาวด์ควรให้ข้อมูลที่เพียงพอแก่ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) เพื่อให้สามารถพิจารณาเลือกใช้และกำหนดค่าความสามารถด้านการรักษาความมั่นคงปลอดภัยสำหรับการถ่ายโอนข้อมูลให้สอดคล้องกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และข้อกำหนดของหน่วยงาน

1. ความสามารถในการปกป้องข้อมูลระหว่างการถ่ายโอน (Secure Information Transfer Capability)

ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถในการปกป้องข้อมูลระหว่างการถ่ายโอน (Data-in-Transit Protection) ที่เหมาะสมกับลักษณะของบริการและขอบเขตความรับผิดชอบของผู้ให้บริการ เพื่อช่วยลดความเสี่ยงจากการดักรับ การเปิดเผย การแก้ไข หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตระหว่างการรับส่งข้อมูล

ความสามารถดังกล่าวควรสนับสนุนให้ผู้ใช้บริการคลาวด์สามารถเลือกใช้หรือกำหนดมาตรการรักษาความมั่นคงปลอดภัยได้อย่างเหมาะสมกับระดับผลกระทบและความเสี่ยงของข้อมูล โดยควรพิจารณาประเด็นดังต่อไปนี้

1. **การปกป้องข้อมูลระหว่างการรับส่ง (Data-in-Transit Protection)** จัดให้มีหรือรองรับกลไกสำหรับปกป้องข้อมูลที่มีการรับส่งผ่านเครือข่ายตามลักษณะของบริการ โดยอาจรวมถึงการใช้ช่องทางการสื่อสารที่มั่นคงปลอดภัย (Secure Communication Channel) และการเข้ารหัสข้อมูลระหว่างการรับส่ง (Encryption in Transit) ตามความเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2. **การปกป้องการเชื่อมต่อกับบริการคลาวด์ (Cloud Service Connection Protection)** รองรับการเชื่อมต่อระหว่างผู้ใช้บริการ ระบบของหน่วยงาน และบริการคลาวด์ผ่านกลไกที่สามารถปกป้องข้อมูลจากการเข้าถึงหรือการดักรับโดยไม่ได้รับอนุญาต โดยระดับของการปกป้องควรสอดคล้องกับลักษณะและความเสี่ยงของการเชื่อมต่อนั้น
3. **การจำกัดการสื่อสารเฉพาะปลายทางที่ได้รับอนุญาต (Authorized Destination Restriction)** ควรมีความสามารถที่ช่วยให้ผู้ใช้บริการคลาวด์สามารถกำหนดหรือจำกัดการรับส่งข้อมูลไปยังระบบ บริการหรือปลายทางที่ได้รับอนุญาต ตามความสามารถของบริการและรูปแบบความรับผิดชอบร่วมที่เกี่ยวข้อง
4. **การรักษาความถูกต้องครบถ้วนของข้อมูลระหว่างการถ่ายโอน (Integrity Protection in Transit)** ควรรองรับมาตรการที่ช่วยป้องกันหรือตรวจพบการแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตระหว่างการถ่ายโอน ตามความเหมาะสมกับลักษณะของบริการและความเสี่ยง
5. **การสนับสนุนทางเลือกด้านการเชื่อมต่อที่เหมาะสมกับความเสี่ยง (Risk-appropriate Connectivity Options)** ในกรณีที่บริการรองรับ ผู้ให้บริการคลาวด์ควรมีทางเลือกในการเชื่อมต่อหรือรับส่งข้อมูลที่มีระดับการปกป้องแตกต่างกัน เพื่อให้ผู้ใช้บริการสามารถเลือกใช้ให้เหมาะสมกับระดับผลกระทบ ความต้องการด้านความมั่นคงปลอดภัย และสถาปัตยกรรมของระบบ
6. **การให้ข้อมูลเกี่ยวกับความสามารถและข้อจำกัด (Capability and Limitation Information)** ควรให้ข้อมูลเกี่ยวกับความสามารถด้านการรักษาความมั่นคงปลอดภัยสำหรับการถ่ายโอนข้อมูล รวมถึงขอบเขตความรับผิดชอบ การกำหนดค่าที่ผู้ใช้บริการต้องดำเนินการ และข้อจำกัดที่สำคัญของบริการอย่างเพียงพอ เพื่อสนับสนุนการประเมินและการตัดสินใจของผู้ใช้บริการคลาวด์

หลักการกำหนดความสามารถของผู้ให้บริการคลาวด์

การกำหนดข้อกำหนดสำหรับผู้ให้บริการคลาวด์ควรมุ่งเน้นที่ **ผลลัพธ์ด้านความมั่นคงปลอดภัย (Security Outcome)** และ **ความสามารถของบริการ (Service Capability)** มากกว่าการกำหนดเทคโนโลยี ผลิตภัณฑ์หรือรูปแบบการเชื่อมต่อเฉพาะ เพื่อให้สามารถประยุกต์ใช้กับผู้ให้บริการคลาวด์และรูปแบบบริการที่แตกต่างกันได้อย่างเป็นกลางทางเทคโนโลยี (Technology-neutral)

ตัวอย่างแนวทางการประเมินสามารถกำหนดได้ดังนี้

ประเด็นประเมิน	**ความสามารถที่ควรพิจารณา**
การปกป้องข้อมูลระหว่างการรับส่ง	มีความสามารถในการปกป้องข้อมูลระหว่างการถ่ายโอนตามความเหมาะสม
การเชื่อมต่อกับบริการคลาวด์	มีทางเลือกในการเชื่อมต่อที่เหมาะสมกับระดับความเสี่ยง
การจำกัดต้นทางและปลายทาง	สามารถกำหนดหรือสนับสนุนการควบคุมการสื่อสารระหว่างระบบหรือบริการที่ได้รับอนุญาต

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ความถูกต้องครบถ้วนของข้อมูล	รองรับกลไกป้องกันหรือตรวจพบการเปลี่ยนแปลงข้อมูลระหว่างการรับส่งตามความเหมาะสม
การกำหนดค่าของ CSC	มีข้อมูลเกี่ยวกับการกำหนดค่าที่ CSC ต้องรับผิดชอบ
ข้อจำกัดของบริการ	มีข้อมูลเพียงพอให้ CSC สามารถประเมินความเหมาะสมและความเสี่ยงของบริการ

ความสัมพันธ์กับข้อกำหนดด้านการเข้ารหัส

ในกรณีที่ใช้การเข้ารหัส (Encryption) เป็นมาตรการสำหรับปกป้องข้อมูลระหว่างการถ่ายโอน รายละเอียดเกี่ยวกับมาตรฐานการเข้ารหัส โพรโทคอล ชุดรหัส (Cipher Suite) ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) และการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management) **ไม่ควรกำหนดซ้ำในหัวข้อนี้** แต่ให้เป็นไปตามข้อ **5.2.4 การเข้ารหัส (Cryptography)** ที่เกี่ยวข้อง

เหตุผลและความจำเป็น (Rationale)

ในสภาพแวดล้อมระบบคลาวด์ กลไกสำหรับการรับส่งข้อมูลบางส่วนอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์ ขณะที่การเลือกใช้ การกำหนดค่า และการกำหนดปลายทางของการรับส่งข้อมูลบางส่วนอาจเป็นความรับผิดชอบของผู้ใช้บริการคลาวด์ ดังนั้น การมีความสามารถด้านการรักษาความมั่นคงปลอดภัยที่เหมาะสม พร้อมข้อมูลเกี่ยวกับขอบเขตความรับผิดชอบและข้อจำกัดของบริการที่ชัดเจน จะช่วยให้ผู้ใช้บริการสามารถกำหนดมาตรการปกป้องข้อมูลได้สอดคล้องกับระดับผลกระทบและความเสี่ยง

2. การสนับสนุนการควบคุมและตรวจสอบการถ่ายโอนข้อมูล (Information Transfer Security Support and Assurance)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ควรจัดให้มีข้อมูล ความสามารถ หรือหลักฐานที่เหมาะสมเพื่อสนับสนุนให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) สามารถกำหนด ใช้งาน และตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยสำหรับการถ่ายโอนข้อมูลที่เกี่ยวข้องกับบริการคลาวด์ได้อย่างเหมาะสมตามขอบเขตความรับผิดชอบร่วม (Shared Responsibility)

การสนับสนุนดังกล่าวควรมีความเพียงพอให้ผู้ใช้บริการคลาวด์สามารถประเมินได้ว่า ความสามารถของบริการคลาวด์ที่เลือกใช้สอดคล้องกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ข้อกำหนดด้านความมั่นคงปลอดภัย และผลการประเมินความเสี่ยงของหน่วยงาน โดยไม่จำเป็นต้องเปิดเผยข้อมูลทางเทคนิคที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ควรพิจารณาดำเนินการในประเด็นสำคัญ ดังต่อไปนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

1. **การให้ข้อมูลเกี่ยวกับกลไกการปกป้องข้อมูล (Information Protection Mechanism Information)** ควรมีข้อมูลเกี่ยวกับกลไกหรือความสามารถที่บริการจัดให้สำหรับการปกป้องข้อมูลระหว่างการถ่ายโอน รวมถึงขอบเขตของมาตรการที่ผู้ให้บริการเป็นผู้ดำเนินการ และมาตรการที่ผู้ใช้บริการต้องเลือกใช้หรือกำหนดค่าเพิ่มเติม
2. **การระบุขอบเขตความรับผิดชอบ (Responsibility Boundary)** ควรระบุขอบเขตความรับผิดชอบระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ที่เกี่ยวข้องกับการรับส่งข้อมูลให้มีความชัดเจนตามรูปแบบของบริการ เพื่อช่วยลดความเสี่ยงจากช่องว่างของความรับผิดชอบ (Responsibility Gap) หรือความเข้าใจที่ไม่สอดคล้องกันเกี่ยวกับมาตรการที่แต่ละฝ่ายต้องดำเนินการ
3. **การสนับสนุนการกำหนดค่าที่มั่นคงปลอดภัย (Secure Configuration Support)** ในกรณีที่ผู้ใช้บริการมีหน้าที่กำหนดค่าความมั่นคงปลอดภัยสำหรับการรับส่งข้อมูล ผู้ให้บริการคลาวด์ควรจัดให้มีข้อมูลหรือแนวทางที่เหมาะสมเพื่อสนับสนุนการกำหนดค่าดังกล่าว และช่วยให้ผู้ใช้บริการสามารถหลีกเลี่ยงการกำหนดค่าที่อาจก่อให้เกิดความเสี่ยงโดยไม่จำเป็น
4. **การสนับสนุนการตรวจสอบและหลักฐาน (Verification and Evidence Support)** ควรมีข้อมูลหรือหลักฐานที่เหมาะสมตามลักษณะของบริการ เพื่อสนับสนุนให้ผู้ใช้บริการสามารถตรวจสอบหรือประเมินความเหมาะสมของมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการถ่ายโอนข้อมูล ทั้งนี้ รูปแบบและระดับของหลักฐานควรพิจารณาตามความเสี่ยง ขอบเขตบริการ และข้อจำกัดด้านการรักษาความลับและความมั่นคงปลอดภัยของผู้ให้บริการ
5. **การแจ้งข้อจำกัดที่มีนัยสำคัญของบริการ (Material Service Limitation Disclosure)** ควรให้ข้อมูลเกี่ยวกับข้อจำกัดที่มีนัยสำคัญของความสามารถด้านการรักษาความมั่นคงปลอดภัยสำหรับการถ่ายโอนข้อมูล ซึ่งอาจมีผลต่อการตัดสินใจเลือกใช้บริการหรือการกำหนดมาตรการเพิ่มเติมของผู้ใช้บริการคลาวด์
6.

แนวทางเกี่ยวกับหลักฐานประกอบการประเมิน (Assessment Evidence)

หลักฐานที่ใช้ประกอบการประเมินไม่จำเป็นต้องอยู่ในรูปแบบเดียวกันสำหรับผู้ให้บริการคลาวด์ทุกราย โดยอาจพิจารณาจากลักษณะของบริการและระดับความเสี่ยง เช่น เอกสารอธิบายสถาปัตยกรรมหรือความสามารถด้านความมั่นคงปลอดภัย (Security Architecture or Capability Documentation) เอกสารแสดงขอบเขตความรับผิดชอบร่วม (Shared Responsibility Documentation) รายงานหรือผลการประเมินโดยหน่วยงานที่เป็นอิสระ (Independent Assessment or Assurance Report) การรับรองตามมาตรฐานที่เกี่ยวข้อง (Relevant Certification) หรือหลักฐานอื่นที่สามารถแสดงให้เห็นถึงการดำเนินมาตรการที่เกี่ยวข้องได้อย่างเหมาะสม

ทั้งนี้ การมีใบรับรองหรือรายงานการตรวจประเมินเพียงอย่างเดียว **ไม่ควรถูกพิจารณาว่าเป็นหลักฐานที่เพียงพอโดยอัตโนมัติ** หากขอบเขตของการรับรองหรือการตรวจประเมินดังกล่าวไม่ครอบคลุมบริการ ความสามารถหรือมาตรการที่หน่วยงานนำมาใช้งาน

ร่างคำสั่งฯ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักการพิจารณาความเพียงพอของหลักฐาน

การประเมินควรพิจารณา **สาระและขอบเขตของหลักฐาน (Substance and Scope of Evidence)** มากกว่าการกำหนดให้ต้องใช้เอกสารหรือใบรับรองประเภทใดประเภทหนึ่งโดยเฉพาะ เพื่อรักษาความเป็นกลางต่อผู้ให้บริการและรูปแบบบริการคลาวด์ที่แตกต่างกัน

แนวทางนี้ยังเปิดโอกาสให้ผู้ให้บริการที่มีระบบบริหารจัดการและการประกันความมั่นคงปลอดภัยที่มีวุฒิภาวะสูง (Security Assurance Maturity) สามารถใช้หลักฐานที่มีอยู่เพื่อแสดงความสามารถได้ โดยไม่สร้างภาระในการจัดทำหลักฐานซ้ำซ้อนโดยไม่จำเป็น

ตัวอย่างหลักฐานที่อาจใช้ประกอบการประเมิน

ประเด็น	ตัวอย่างหลักฐาน
การปกป้องข้อมูลระหว่างการถ่ายโอน	เอกสารอธิบายความสามารถหรือข้อกำหนดด้านความมั่นคงปลอดภัยของบริการ
ขอบเขตความรับผิดชอบ	เอกสารความรับผิดชอบร่วม (Shared Responsibility Documentation)
การกำหนดค่าความมั่นคงปลอดภัย	แนวทางการกำหนดค่าหรือเอกสารประกอบบริการ
การประกันความมั่นคงปลอดภัย	รายงานการประเมิน การรับรอง หรือหลักฐานจากบุคคลที่เป็นอิสระตามความเหมาะสม
ข้อจำกัดของบริการ	เอกสารข้อกำหนด ข้อจำกัด หรือเงื่อนไขที่เกี่ยวข้องกับบริการ

เหตุผลและความจำเป็น (Rationale)

การใช้บริการคลาวด์ทำให้มาตรการรักษาความมั่นคงปลอดภัยบางส่วนอยู่ภายใต้การดำเนินการของผู้ให้บริการคลาวด์ ขณะที่มาตรการบางส่วนขึ้นอยู่กับการเลือกใช้และการกำหนดค่าของผู้ใช้บริการ ดังนั้น การมีข้อมูลเกี่ยวกับความสามารถ ขอบเขตความรับผิดชอบ ข้อจำกัด และหลักฐานที่เหมาะสม จะช่วยให้ผู้ใช้บริการสามารถประเมินความเพียงพอของมาตรการและกำหนดมาตรการเพิ่มเติมได้อย่างเหมาะสมกับความเสี่ยง

อย่างไรก็ตาม การร้องขอหลักฐานจากผู้ให้บริการควรคำนึงถึงหลักความได้สัดส่วน (Proportionality) และข้อจำกัดด้านความมั่นคงปลอดภัยและการรักษาความลับ โดยไม่ควรกำหนดให้ผู้ให้บริการเปิดเผยรายละเอียดทางเทคนิคที่อาจเพิ่มความเสี่ยงต่อระบบคลาวด์หรือผู้ใช้บริการรายอื่น

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การกำหนดมาตรการด้านการถ่ายโอนข้อมูล (Information Transfer) ควรดำเนินการให้สอดคล้องกับระดับผลกระทบของข้อมูล ผลการประเมินความเสี่ยง ลักษณะของบริการคลาวด์ และรูปแบบความรับผิดชอบร่วม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้อ้างอิง

(Shared Responsibility Model) ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)

หน่วยงานควรออกแบบมาตรการควบคุมให้ครอบคลุมวงจรการถ่ายโอนข้อมูลตั้งแต่ต้นทาง (Source) ระหว่างการถ่ายโอน (In Transit) จนถึงปลายทาง (Destination) รวมถึงสามารถตรวจสอบย้อนกลับ (Traceability) และรองรับการตรวจประเมินได้ตามความเหมาะสม

1. การจำแนกข้อมูลก่อนการถ่ายโอน (Information Classification before Transfer)

ก่อนมีการถ่ายโอนข้อมูล หน่วยงานควรกำหนดระดับชั้นข้อมูล (Data Classification) และประเมินระดับผลกระทบของข้อมูล เพื่อใช้กำหนดมาตรการควบคุมที่เหมาะสม โดยข้อมูลที่มีความอ่อนไหวหรือมีผลกระทบสูงควรได้รับการปกป้องด้วยมาตรการที่เข้มงวดกว่าข้อมูลทั่วไป

2. การเลือกช่องทางการถ่ายโอนข้อมูล (Selection of Information Transfer Channel)

หน่วยงานควรเลือกช่องทางการถ่ายโอนข้อมูลให้เหมาะสมกับระดับความเสี่ยง โดยพิจารณาปัจจัย เช่น

- ระดับผลกระทบของข้อมูล
- ความน่าเชื่อถือของเครือข่าย
- ผู้รับข้อมูล
- ข้อกำหนดด้านกฎหมาย ระเบียบ หรือสัญญา
- ความสามารถด้านความมั่นคงปลอดภัยของบริการคลาวด์

ไม่ควรใช้ช่องทางเดียวกันสำหรับข้อมูลทุกประเภท หากความเสี่ยงแตกต่างกัน

3. การปกป้องข้อมูลระหว่างการถ่ายโอน (Protection during Information Transfer)

หน่วยงานควรใช้มาตรการป้องกันข้อมูลระหว่างการถ่ายโอนให้เหมาะสมกับความเสี่ยง เช่น

- การเข้ารหัสข้อมูล (Encryption)
- การพิสูจน์ตัวตน (Authentication)
- การตรวจสอบความถูกต้องของปลายทาง (Destination Verification)
- การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity Protection)
- การจำกัดผู้รับข้อมูลเฉพาะผู้ได้รับอนุญาต

รายละเอียดด้านการเข้ารหัสให้เป็นไปตามข้อ 5.2.4 การเข้ารหัส (Cryptography)

4. การควบคุมการถ่ายโอนข้อมูลผ่านสื่อทางกายภาพ (Physical Media Transfer)

หากมีการใช้สื่อทางกายภาพในการถ่ายโอนข้อมูล หน่วยงานควร

- กำหนดผู้ส่งและผู้รับที่ได้รับอนุญาต

ร่างประกาศ Public Hearing เท่านั้น - ห้ามใช้งานจริง

- จัดทำบันทึกการรับ–ส่งสื่อ
- ใช้มาตรการป้องกันระหว่างการขนส่ง
- ตรวจสอบการส่งมอบ
- เก็บรักษาหลักฐานการรับ–ส่ง
- จัดการสื่อภายหลังการใช้งานตามนโยบายขององค์กร

5. การตรวจสอบและการติดตาม (Monitoring and Verification)

หน่วยงานควรตรวจสอบความเหมาะสมของมาตรการที่ใช้ในการถ่ายโอนข้อมูลเป็นระยะ เพื่อให้มั่นใจว่าช่องทางการถ่ายโอนข้อมูลและมาตรการปกป้องข้อมูลยังคงสอดคล้องกับระดับผลกระทบของข้อมูล ผลการประเมินความเสี่ยง และข้อกำหนดของหน่วยงาน

การตรวจสอบอาจครอบคลุมประเด็น เช่น

- ความเหมาะสมของช่องทางการถ่ายโอนข้อมูลที่ได้รับอนุญาต
- ความเพียงพอของมาตรการปกป้องข้อมูลระหว่างการถ่ายโอน
- ความสอดคล้องของการกำหนดค่ากับนโยบายของหน่วยงาน
- ความสามารถของบริการคลาวด์ในการรองรับมาตรการด้านการถ่ายโอนข้อมูล
- การทบทวนเมื่อมีการเปลี่ยนแปลงบริการคลาวด์หรือผลการประเมินความเสี่ยง

รายละเอียดเกี่ยวกับการบันทึกเหตุการณ์ (Logging) การติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Monitoring) และการตรวจสอบบันทึกเหตุการณ์ ให้เป็นไปตามข้อกำหนดที่เกี่ยวข้องในหมวด **5.2.6 การรักษาความมั่นคงปลอดภัยในการดำเนินงาน (Operations Security)**

6. การกำหนดบทบาทและความรับผิดชอบ (Roles and Responsibilities)

การกำหนดมาตรการด้านการถ่ายโอนข้อมูลควรพิจารณาขอบเขตความรับผิดชอบร่วม (Shared Responsibility Model) ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ให้สอดคล้องกับรูปแบบของบริการคลาวด์ เพื่อให้แต่ละฝ่ายสามารถดำเนินมาตรการด้านการรักษาความมั่นคงปลอดภัยในการสื่อสารได้อย่างเหมาะสม

ตัวอย่างความรับผิดชอบที่ควรพิจารณา มีดังนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ผู้รับผิดชอบ	ตัวอย่างหน้าที่
ผู้ใช้บริการคลาวด์ (CSC)	กำหนดข้อกำหนดด้านการถ่ายโอนข้อมูล เลือกใช้ช่องทางการถ่ายโอนที่เหมาะสม และกำหนดมาตรการควบคุมตามระดับความเสี่ยง
ผู้ให้บริการคลาวด์ (CSP)	จัดให้มีความสามารถด้านการรักษาความมั่นคงปลอดภัยสำหรับการถ่ายโอนข้อมูล และให้ข้อมูลเกี่ยวกับขอบเขตความรับผิดชอบและข้อจำกัดของบริการ
ทั้ง CSC และ CSP	ประสานการดำเนินมาตรการในส่วนที่เป็นความรับผิดชอบร่วม และกำหนดแนวทางในการตรวจสอบหรือยืนยันความเพียงพอของมาตรการตามความเหมาะสม

7. การทบทวนและปรับปรุงมาตรการ (Review and Continual Improvement)

มาตรการด้านการถ่ายโอนข้อมูลควรได้รับการทบทวนเป็นระยะ หรือเมื่อมีการเปลี่ยนแปลง เช่น

- การเปลี่ยนผู้ให้บริการคลาวด์
- การเปลี่ยนสถาปัตยกรรมระบบ
- การเปลี่ยนระดับผลกระทบของข้อมูล
- การเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
- การเปลี่ยนแปลงข้อกำหนดทางกฎหมายหรือข้อกำหนดขององค์กร

เพื่อให้มาตรการยังคงเหมาะสมกับความเสี่ยงที่เปลี่ยนแปลงไป

รูป วงจรการถ่ายโอนข้อมูลอย่างมั่นคงปลอดภัยในบริการคลาวด์ (Secure Information Transfer Lifecycle for Cloud Services)

จำแนกประเภทข้อมูล

(Information Classification)

↓

ประเมินระดับผลกระทบและความเสี่ยง

(Impact and Risk Assessment)

↓

เลือกช่องทางการถ่ายโอน

(Approved Transfer Channel)

↓

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กำหนดมาตรการปกป้องข้อมูล

(Authentication / Encryption /

Integrity Protection)

↓

ตรวจสอบผู้ส่งและผู้รับ

(Sender / Recipient Verification)

↓

ถ่ายโอนข้อมูล

(Information Transfer)

↓

ยืนยันการรับข้อมูล

(Receipt Verification)

↓

บันทึกและติดตามการถ่ายโอน

(Logging and Traceability)

ร่างเพื่อการรับฟังความคิดเห็นสาธารณะ (Public Hearing) เท่านั้น - ห้ามใช้อ้างอิง

รูปดังกล่าวแสดงแนวคิดของการควบคุมการถ่ายโอนข้อมูลตลอดวงจรชีวิต (Information Transfer Lifecycle) ตั้งแต่การจำแนกประเภทข้อมูล การประเมินความเสี่ยง การเลือกช่องทางการถ่ายโอน การปกป้องข้อมูลระหว่างการถ่ายโอน การตรวจสอบผู้ส่งและผู้รับ การยืนยันการรับข้อมูล ตลอดจนการบันทึกและการตรวจสอบย้อนกลับ (Traceability) ซึ่งสามารถใช้เป็นภาพอ้างอิงร่วมกันสำหรับทั้งผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)

แบบฟอร์ม/หลักฐานที่แนะนำ (Recommended Forms / Evidence)

หน่วยงานควรจัดทำเอกสาร หลักฐาน หรือบันทึกที่เหมาะสม เพื่อสนับสนุนการบริหารจัดการ การตรวจสอบย้อนกลับ (Traceability) และการตรวจประเมินความสอดคล้องของมาตรการด้านการถ่ายโอนข้อมูล ทั้งนี้ รูปแบบของเอกสารสามารถปรับให้เหมาะสมกับขนาด ลักษณะขององค์กร และผลการประเมินความเสี่ยง โดยไม่จำเป็นต้องใช้รูปแบบเดียวกันทุกหน่วยงาน

ตัวอย่างแบบฟอร์มที่แนะนำ

2. แบบบันทึกการถ่ายโอนข้อมูล (Information Transfer Log)

รายการ	รายละเอียด
วันและเวลา	วันที่และเวลาที่ถ่ายโอน
ผู้ส่ง	ผู้ดำเนินการส่ง
ผู้รับ	ผู้รับข้อมูล
วิธีการถ่ายโอน	ช่องทางที่ใช้
สถานะ	สำเร็จ / ไม่สำเร็จ
หมายเหตุ	เหตุผิดปกติ (ถ้ามี)

ตัวอย่างหลักฐานที่ใช้ในการตรวจประเมิน (Assessment Evidence)

หน่วยงานอาจใช้เอกสารหรือหลักฐานต่อไปนี้เพื่อแสดงความสอดคล้องกับข้อกำหนดด้านการถ่ายโอนข้อมูล

- นโยบายการถ่ายโอนข้อมูล (Information Transfer Policy)
- ขั้นตอนปฏิบัติการถ่ายโอนข้อมูล (Information Transfer Procedure)
- บันทึกการถ่ายโอนข้อมูล (Information Transfer Log)
- บันทึกการรับ–ส่งสื่อทางกายภาพ (Physical Media Transfer Log)
- หลักฐานการเข้ารหัสข้อมูลระหว่างการถ่ายโอน (Encryption Configuration)

5.2.7.2 การแบ่งแยกในเครือข่าย (Segregation in Networks)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องจัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่า (Tenant) ในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน และตรวจสอบว่า ผู้ให้บริการคลาวด์ มีคุณสมบัติตรงตามข้อกำหนดเหล่านั้นหรือไม่	ก) ผู้ให้บริการคลาวด์ ต้องบังคับใช้การแยกการเข้าถึงเครือข่ายในกรณีต่อไปนี้ – การแบ่งแยกระหว่างผู้เช่าในสภาพแวดล้อมที่มีผู้เช่าหลายราย – การแยกระหว่างสภาพแวดล้อมการดูแลระบบภายในของ ผู้ให้บริการคลาวด์ และสภาพแวดล้อมการประมวลผลบนคลาวด์ของ ผู้ใช้บริการคลาวด์

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ข) ผู้ให้บริการคลาวด์ ต้องช่วย ผู้ใช้บริการคลาวด์ ตรวจสอบการแบ่งแยกที่ดำเนินการโดยผู้ให้บริการคลาวด์

วัตถุประสงค์ (Objective)

เพื่อกำหนดหลักเกณฑ์และแนวทางในการแบ่งแยกเครือข่าย (Network Segregation) และสภาพแวดล้อมที่เกี่ยวข้องกับการให้บริการคลาวด์อย่างเหมาะสม เพื่อจำกัดการเข้าถึงและการสื่อสารระหว่างระบบ เครือข่าย ทรัพยากร หรือสภาพแวดล้อมที่มีระดับความสำคัญ ความไว้วางใจ หรือความต้องการด้านความมั่นคงปลอดภัยแตกต่างกัน และลดความเสี่ยงจากการเข้าถึง การเชื่อมต่อ หรือการเคลื่อนย้ายระหว่างส่วนของเครือข่ายโดยไม่ได้รับอนุญาต (Unauthorized Lateral Movement)

สำหรับสภาพแวดล้อมระบบคลาวด์ การแบ่งแยกเครือข่ายควรให้ความสำคัญกับการแยกระหว่างผู้เช่า (Tenant Isolation) ในสภาพแวดล้อมที่มีผู้เช่าหลายราย (Multi-tenant Environment) และการแบ่งแยกระหว่างสภาพแวดล้อมการบริหารจัดการของผู้ให้บริการคลาวด์ (CSP Management Environment) กับสภาพแวดล้อมการประมวลผลของผู้ใช้บริการคลาวด์ (CSC Cloud Processing Environment) ตามที่ข้อกำหนดของประกาศกำหนดไว้

มาตรการแบ่งแยกเครือข่ายควรได้รับการกำหนดตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ สถาปัตยกรรมระบบ ลักษณะของภาระงาน (Workload) รูปแบบบริการคลาวด์ และผลการประเมินความเสี่ยง โดยไม่จำเป็นต้องใช้รูปแบบหรือเทคโนโลยีในการแบ่งแยกเดียวกันสำหรับทุกระบบ

หลักการแบ่งแยกเครือข่าย (Network Segregation Principles)

การแบ่งแยกเครือข่ายควรดำเนินการตามหลักความจำเป็นและความเสี่ยง (Need- and Risk-based Segregation) โดยกำหนดขอบเขตการแบ่งแยก (Segregation Boundary) และควบคุมการสื่อสารระหว่างขอบเขตดังกล่าวให้สอดคล้องกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยของหน่วยงาน

ควรพิจารณาหลักการสำคัญดังต่อไปนี้

1. **การแบ่งแยกตามระดับความไว้วางใจ (Segregation by Trust Level)** ระบบ เครือข่าย หรือทรัพยากรที่มีระดับความไว้วางใจแตกต่างกันควรได้รับการแบ่งแยกตามความเหมาะสม เพื่อจำกัดการเชื่อมต่อหรือการเข้าถึงโดยไม่จำเป็น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามเผยแพร่

2. **การแบ่งแยกตามระดับผลกระทบและความสำคัญ (Segregation by Impact and Criticality)** ระบบหรือภาระงานที่มีระดับผลกระทบหรือความสำคัญแตกต่างกันควรได้รับการพิจารณาแบ่งแยกตามผลการประเมินความเสี่ยง เพื่อจำกัดผลกระทบในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
3. **การจำกัดการสื่อสารระหว่างส่วนเครือข่าย (Inter-segment Communication Restriction)** การสื่อสารระหว่างส่วนเครือข่ายที่ได้รับการแบ่งแยกควรได้รับอนุญาตเฉพาะเท่าที่จำเป็นต่อการดำเนินงานและเป็นไปตามนโยบายการควบคุมการเข้าถึง (Access Control Policy) ของหน่วยงาน
4. **การแยกระหว่างผู้เช่า (Tenant Isolation)** ในสภาพแวดล้อมที่มีผู้เช่าหลายราย ผู้ให้บริการคลาวด์ต้องมีกลไกแบ่งแยกที่เหมาะสมเพื่อป้องกันมิให้ผู้เช่ารายหนึ่งสามารถเข้าถึงเครือข่าย ข้อมูล หรือทรัพยากรของผู้เช่ารายอื่นโดยไม่ได้รับอนุญาต ซึ่งเป็นข้อกำหนดที่ประกาศกำหนดไว้โดยตรง
5. **การแบ่งแยกสภาพแวดล้อมการบริหารจัดการ (Management Environment Segregation)** สภาพแวดล้อมการดูแลระบบภายในของผู้ให้บริการคลาวด์ควรได้รับการแบ่งแยกออกจากสภาพแวดล้อมการประมวลผลของผู้ใช้บริการคลาวด์อย่างเหมาะสม เพื่อลดความเสี่ยงจากการเข้าถึงหรือการเชื่อมต่อข้ามขอบเขตโดยไม่ได้รับอนุญาต
6. **การตรวจสอบประสิทธิผลของการแบ่งแยก (Segregation Effectiveness Verification)** การแบ่งแยกเครือข่ายควรสามารถตรวจสอบหรือประเมินประสิทธิผลได้ตามความเหมาะสม โดยใช้ข้อมูล การกำหนดค่า ผลการทดสอบ หรือหลักฐานอื่นที่เพียงพอต่อระดับความเสี่ยงและขอบเขตความรับผิดชอบของแต่ละฝ่าย

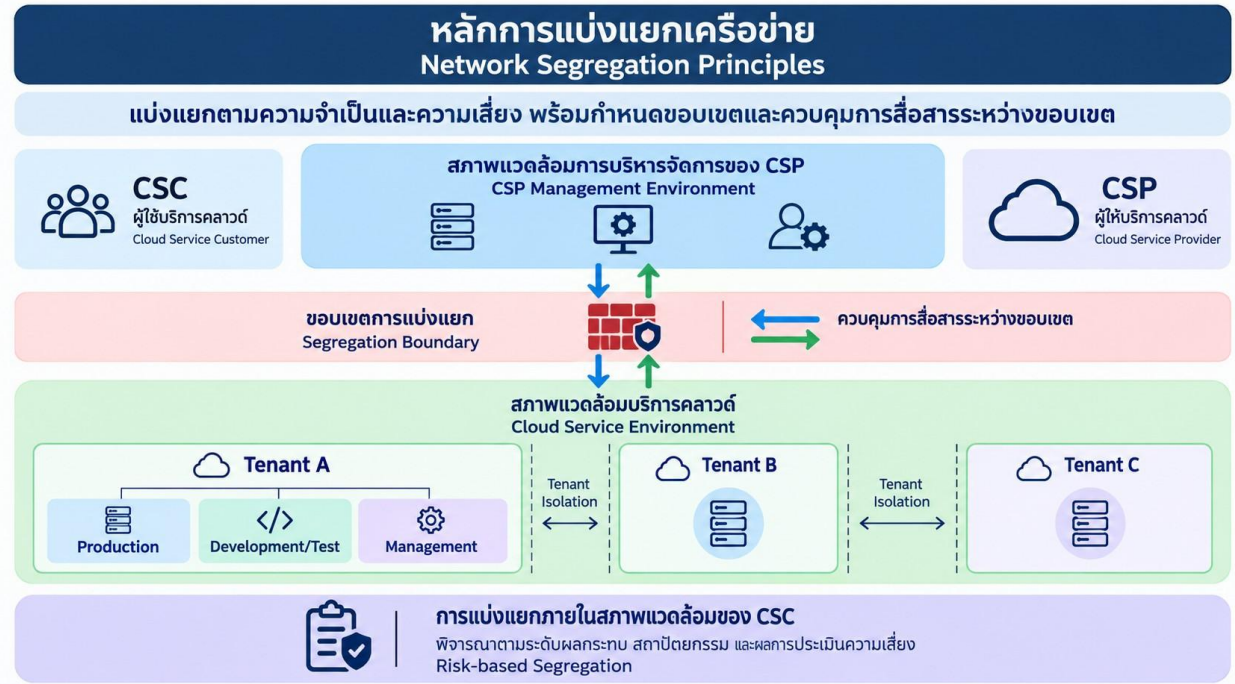
แนวคิดการแบ่งแยกเครือข่ายตามความเสี่ยง

ในทางปฏิบัติ ไม่ควรตีความการแบ่งแยกเครือข่ายว่าระบบทุกประเภทต้องได้รับการแยกทางกายภาพ (Physical Segregation) เนื่องจากสภาพแวดล้อมระบบคลาวด์อาจใช้กลไกการแบ่งแยกทั้งในระดับกายภาพและเชิงตรรกะ (Physical and Logical Segregation) ตามสถาปัตยกรรมของบริการ

แนวคิดที่เหมาะสมสามารถพิจารณาได้ดังนี้

ปัจจัยพิจารณา	แนวทาง
ระดับผลกระทบของข้อมูลหรือระบบ	ระดับผลกระทบสูงขึ้นอาจต้องใช้มาตรการแบ่งแยกและควบคุมการสื่อสารที่เข้มงวดขึ้น
ระดับความไว้วางใจ	สภาพแวดล้อมที่มีระดับความไว้วางใจแตกต่างกันควรพิจารณาแบ่งแยก
ลักษณะของภาระงาน (Workload)	พิจารณาความสำคัญและความสัมพันธ์ระหว่างภาระงาน
ผู้เช่า (Tenant)	ต้องมีการแบ่งแยกที่ป้องกันการเข้าถึงข้ามผู้เช่าโดยไม่ได้รับอนุญาต
สภาพแวดล้อมการบริหารจัดการ	ควรแยกออกจากสภาพแวดล้อมการประมวลผลของผู้ใช้บริการอย่างเหมาะสม
ความจำเป็นในการสื่อสาร	อนุญาตการสื่อสารข้ามขอบเขตเฉพาะเท่าที่จำเป็นและได้รับอนุญาต

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ควรกำหนดข้อกำหนดด้านการแบ่งแยกเครือข่ายให้เหมาะสมกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ลักษณะของภาระงาน (Workload) สถาปัตยกรรมระบบ รูปแบบบริการคลาวด์ และผลการประเมินความเสี่ยง รวมถึงพิจารณาขอบเขตความรับผิดชอบระหว่าง CSC และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)

1. การกำหนดข้อกำหนดการแบ่งแยกเครือข่าย (Network Segregation Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดความต้องการด้านการแบ่งแยกเครือข่าย (Network Segregation Requirements) ก่อนหรือระหว่างการออกแบบและนำบริการคลาวด์มาใช้งาน เพื่อให้ทรัพยากร ระบบ และภาระงานที่มีความต้องการด้านความมั่นคงปลอดภัยแตกต่างกันได้รับการแบ่งแยกและควบคุมการสื่อสารอย่างเหมาะสม

การกำหนดข้อกำหนดดังกล่าวควรพิจารณาอย่างน้อยจากระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ระดับความไว้วางใจ (Trust Level) ความสำคัญของระบบ ความจำเป็นในการเชื่อมต่อ และผลการประเมินความเสี่ยง โดยควรพิจารณาประเด็นสำคัญดังต่อไปนี้

1. **การกำหนดขอบเขตเครือข่าย (Network Boundary Definition)** ควรระบุขอบเขตของเครือข่าย ระบบ หรือกลุ่มทรัพยากรที่จำเป็นต้องได้รับการแบ่งแยก โดยพิจารณาจากหน้าที่การใช้งาน ระดับผลกระทบความสำคัญ และระดับความไว้วางใจของระบบ

สำนักงานปลัดกระทรวง Public Hearing เท่านั้น

2. **การกำหนดระดับการแบ่งแยกตามความเสี่ยง (Risk-based Segregation Level)** ควรกำหนดระดับและความเข้มงวดของการแบ่งแยกให้เหมาะสมกับความเสี่ยง โดยระบบที่มีระดับผลกระทบหรือความสำคัญสูงอาจจำเป็นต้องใช้มาตรการแบ่งแยกและควบคุมการสื่อสารที่เข้มงวดกว่าระบบทั่วไป
3. **การกำหนดการสื่อสารระหว่างขอบเขตเครือข่าย (Inter-segment Communication Requirements)** ควรกำหนดว่าระบบหรือส่วนเครือข่ายใดมีความจำเป็นต้องสื่อสารระหว่างกัน และกำหนดการสื่อสารดังกล่าวเฉพาะเท่าที่จำเป็นตามวัตถุประสงค์ทางธุรกิจและการปฏิบัติงาน
4. **การพิจารณาระดับความไว้วางใจ (Trust Level Consideration)** ระบบหรือทรัพยากรที่มีระดับความไว้วางใจแตกต่างกันควรได้รับการพิจารณาแบ่งแยกตามความเหมาะสม โดยเฉพาะการเชื่อมต่อระหว่างเครือข่ายหรือระบบภายในกับเครือข่ายหรือระบบที่อยู่นอกขอบเขตการควบคุมของหน่วยงาน
5. **การพิจารณาสภาพแวดล้อมของระบบ (Environment Consideration)** ควรพิจารณาความจำเป็นในการแบ่งแยกสภาพแวดล้อมที่มีวัตถุประสงค์การใช้งานแตกต่างกัน เช่น สภาพแวดล้อมการผลิต (Production Environment) สภาพแวดล้อมการพัฒนา (Development Environment) และสภาพแวดล้อมการทดสอบ (Test Environment) ตามระดับผลกระทบและผลการประเมินความเสี่ยง
6. **การพิจารณาขอบเขตความรับผิดชอบร่วม (Shared Responsibility Consideration)** ควรระบุว่ามาตรการแบ่งแยกส่วนใดอยู่ภายใต้ความรับผิดชอบของ CSC และส่วนใดเป็นความรับผิดชอบของ CSP รวมถึงการกำหนดค่าหรือมาตรการเพิ่มเติมที่ CSC ต้องดำเนินการเพื่อให้การแบ่งแยกมีประสิทธิผล

แนวทางการกำหนดระดับการแบ่งแยก

การกำหนดระดับการแบ่งแยกไม่ควรใช้หลักว่า **“ยิ่งแยกมากยิ่งปลอดภัย”** เพียงอย่างเดียว เนื่องจากการแบ่งแยกที่มากเกินความจำเป็นอาจเพิ่มความซับซ้อนในการบริหารจัดการ การกำหนดค่า และการตรวจสอบ ซึ่งอาจก่อให้เกิดความเสี่ยงจากการกำหนดค่าที่ไม่ถูกต้อง (Misconfiguration) ได้

ดังนั้น ควรใช้หลัก **การแบ่งแยกที่เหมาะสมกับความเสี่ยง (Risk-appropriate Segregation)** โดยพิจารณาความสมดุลระหว่างระดับการป้องกัน ความจำเป็นทางธุรกิจ และความสามารถในการบริหารจัดการ

ตัวอย่างแนวทางประกอบการพิจารณา:

ปัจจัย	แนวทางพิจารณาการแบ่งแยก
ระดับผลกระทบสูง	พิจารณาขอบเขตที่ชัดเจนและควบคุมการสื่อสารระหว่างขอบเขตอย่างเข้มงวด
ระดับความไว้วางใจแตกต่างกัน	ควรพิจารณาแบ่งแยกและควบคุมการเชื่อมต่อ
ระบบมีหน้าที่แตกต่างกันอย่างมีนัยสำคัญ	พิจารณาการแบ่งแยกตามหน้าที่และความเสี่ยง
Production กับ Development/Test	พิจารณาการแบ่งแยกตามความเสี่ยงและลักษณะการใช้งาน

ร่างเอกสารเพื่อ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

ระบบจำเป็นต้องสื่อสารระหว่างกัน	อนุญาตเฉพาะการสื่อสารที่จำเป็นและได้รับอนุญาต
ระบบไม่มีความจำเป็นต้องสื่อสารกัน	ควรจำกัดหรือไม่อนุญาตการสื่อสารระหว่างกันตามความเหมาะสม

การจัดทำเอกสารประกอบ (Documentation)

หน่วยงานควรมีข้อมูลหรือเอกสารที่เพียงพอสำหรับแสดงขอบเขตและความสัมพันธ์ของเครือข่ายที่มีนัยสำคัญต่อความมั่นคงปลอดภัย เช่น แผนภาพสถาปัตยกรรมเครือข่าย (Network Architecture Diagram) หรือแผนภาพการแบ่งแยกเครือข่าย (Network Segmentation Diagram) ตามความเหมาะสม

เอกสารดังกล่าวควรมีรายละเอียดในระดับที่เพียงพอสำหรับการบริหารความเสี่ยง การทบทวน และการตรวจสอบ โดย **ไม่จำเป็นต้องกำหนดให้เอกสารมาตรฐานฉบับนี้เก็บรายละเอียดทางเทคนิคระดับกฎการควบคุมเครือข่าย (Network Control Rules) ทุกรายการ**

เหตุผลและความจำเป็น (Rationale)

การกำหนดขอบเขตการแบ่งแยกเครือข่ายอย่างเหมาะสมช่วยลดพื้นที่ที่อาจได้รับผลกระทบ (Blast Radius) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย และช่วยจำกัดการเคลื่อนย้ายระหว่างระบบหรือส่วนเครือข่ายโดยไม่ได้รับอนุญาต (Unauthorized Lateral Movement)

อย่างไรก็ตาม การแบ่งแยกเครือข่ายควรสัมพันธ์กับระดับผลกระทบและความเสี่ยง มิใช่กำหนดให้ทุกระบบใช้รูปแบบการแบ่งแยกเดียวกัน ซึ่งช่วยให้ข้อกำหนดสามารถประยุกต์ใช้ได้กับสถาปัตยกรรมและรูปแบบบริการคลาวด์ที่หลากหลาย

2. การแบ่งแยกสภาพแวดล้อมและภาระงาน (Environment and Workload Segregation)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ควรพิจารณาแบ่งแยกสภาพแวดล้อม (Environment) ระบบ (System) และภาระงาน (Workload) ที่มีวัตถุประสงค์การใช้งาน ระดับผลกระทบ ระดับความไว้วางใจ (Trust Level) หรือข้อกำหนดด้านความมั่นคงปลอดภัยแตกต่างกัน เพื่อจำกัดการเข้าถึงและการสื่อสารระหว่างส่วนที่ไม่มีความจำเป็นต้องเชื่อมต่อกัน ลดโอกาสของการเคลื่อนย้ายภายในระบบโดยไม่ได้รับอนุญาต (Unauthorized Lateral Movement) และจำกัดขอบเขตของผลกระทบ (Impact Containment) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

การกำหนดระดับและรูปแบบของการแบ่งแยกควรเป็นไปตามผลการประเมินความเสี่ยง (Risk Assessment) ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ สถาปัตยกรรมของระบบ ลักษณะของบริการคลาวด์ และขอบเขตความรับผิดชอบร่วม (Shared Responsibility) ระหว่างผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (Cloud

ร่างเพื่อรับฟังความคิดเห็นสาธารณะ (Public Hearing) ห้ามนำไปอ้างอิง

Service Provider: CSP) ทั้งนี้ ไม่จำเป็นต้องกำหนดรูปแบบหรือระดับของการแบ่งแยกในลักษณะเดียวกันสำหรับทุกระบบหรือทุกภาระงาน

หน่วยงานควรพิจารณาประเด็นสำคัญ ดังต่อไปนี้

1. **การแบ่งแยกตามวัตถุประสงค์ของสภาพแวดล้อม (Segregation by Environment Purpose)** พิจารณาแบ่งแยกสภาพแวดล้อมที่มีวัตถุประสงค์แตกต่างกัน เช่น สภาพแวดล้อมการผลิต (Production Environment) สภาพแวดล้อมการพัฒนา (Development Environment) และสภาพแวดล้อมการทดสอบ (Test Environment) ตามระดับผลกระทบของข้อมูล ความสำคัญของระบบ และผลการประเมินความเสี่ยง เพื่อป้องกันการเข้าถึง การเปลี่ยนแปลง หรือการใช้ทรัพยากรข้ามสภาพแวดล้อมโดยไม่จำเป็น
2. **การแบ่งแยกตามระดับผลกระทบและความสำคัญ (Segregation by Impact and Criticality)** ระบบหรือภาระงานที่มีระดับผลกระทบหรือความสำคัญแตกต่างกันอย่างมีนัยสำคัญ ควรได้รับการพิจารณาแบ่งแยกตามความเหมาะสม เพื่อช่วยจำกัดผลกระทบเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย และลดโอกาสที่เหตุการณ์จากระบบหนึ่งจะส่งผลกระทบต่อระบบหรือบริการอื่น
3. **การแบ่งแยกตามระดับความไว้วางใจ (Segregation by Trust Level)** ระบบ ภาระงาน หรือทรัพยากรที่มีระดับความไว้วางใจแตกต่างกัน ควรได้รับการแบ่งแยกและควบคุมการสื่อสารระหว่างกันตามหลักความจำเป็น (Need-to-Communicate Principle) และนโยบายการควบคุมการเข้าถึง (Access Control Policy)
4. **การแบ่งแยกภาระงานที่มีข้อกำหนดเฉพาะ (Segregation of Workloads with Specific Requirements)** ภาระงานที่ประมวลผลข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลที่อยู่ภายใต้ข้อกำหนดทางกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือสัญญาที่แตกต่างจากภาระงานทั่วไป ควรได้รับการพิจารณาแบ่งแยกตามระดับความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง
5. **การควบคุมการสื่อสารระหว่างสภาพแวดล้อม (Inter-environment Communication Control)** การสื่อสารระหว่างสภาพแวดล้อมหรือภาระงานที่ได้รับการแบ่งแยกควรได้รับอนุญาตเฉพาะเท่าที่จำเป็นต่อการดำเนินงาน และอยู่ภายใต้นโยบายการควบคุมการเข้าถึงของหน่วยงาน โดยควรสามารถกำหนด ตรวจสอบ และติดตามการเชื่อมต่อระหว่างสภาพแวดล้อมได้ตามความเหมาะสม
6. **การจำกัดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Impact Containment)** การออกแบบการแบ่งแยกควรคำนึงถึงการจำกัดขอบเขตของผลกระทบ (Blast Radius Reduction) และป้องกันการแพร่กระจายของเหตุการณ์ด้านความมั่นคงปลอดภัยจากระบบหรือภาระงานหนึ่งไปยังส่วนอื่นที่ไม่เกี่ยวข้อง เพื่อสนับสนุนการตอบสนองและการกู้คืนระบบอย่างมีประสิทธิภาพ

การแบ่งแยกสภาพแวดล้อมสามารถดำเนินการได้ทั้งในลักษณะ **เชิงตรรกะ (Logical Segregation)** และ **เชิงกายภาพ (Physical Segregation)** ตามความเหมาะสมกับสถาปัตยกรรมของบริการคลาวด์ ผลการประเมินความเสี่ยง และระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ทั้งนี้ ไม่ควรตีความว่าทุกสภาพแวดล้อมจำเป็นต้องแยก

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้งานจริง

โครงสร้างพื้นฐานทางกายภาพออกจากกันเสมอไป หากมาตรการแบ่งแยกเชิงตรรกะสามารถให้ระดับการป้องกันที่เพียงพอต่อความเสี่ยงที่ยอมรับได้

ตัวอย่างแนวทางในการพิจารณา มีดังนี้

สถานการณ์	**แนวทางที่ควรพิจารณา**
Production ประมวลผลข้อมูลที่มีผลกระทบสูง	แบ่งแยกจาก Development/Test และควบคุมสิทธิ์การเข้าถึงอย่างเข้มงวด
Development/Test ไม่จำเป็นต้องใช้ข้อมูลจริง	หลีกเลี่ยงการเข้าถึงข้อมูลจาก Production และใช้ข้อมูลจำลองหรือข้อมูลที่ผ่านการปกปิดข้อมูล (Masked Data) ตามความเหมาะสม
จำเป็นต้องมีการเชื่อมต่อระหว่างสภาพแวดล้อม	อนุญาตเฉพาะการเชื่อมต่อที่จำเป็น พร้อมกำหนดมาตรการควบคุมและตรวจสอบ
ภาระงานมีระดับผลกระทบแตกต่างกัน	พิจารณาแบ่งแยกและกำหนดมาตรการควบคุมตามระดับความเสี่ยง
ภาระงานมีระดับความเสี่ยงใกล้เคียงกัน	สามารถใช้สภาพแวดล้อมร่วมกันได้ หากผลการประเมินความเสี่ยงและสถาปัตยกรรมรองรับ

เหตุผลและความจำเป็น (Rationale)

การแบ่งแยกสภาพแวดล้อมและภาระงานเป็นมาตรการสำคัญในการลดพื้นที่ที่อาจได้รับผลกระทบ (Blast Radius) จำกัดการเคลื่อนย้ายภายในระบบโดยไม่ได้รับอนุญาต (Unauthorized Lateral Movement) และลดโอกาสที่เหตุการณ์ด้านความมั่นคงปลอดภัยจะส่งผลกระทบข้ามระบบหรือข้ามภาระงาน ทั้งนี้ การกำหนดระดับของการแบ่งแยกควรเป็นไปตามหลักการบริหารความเสี่ยง (Risk-based Approach) และมีความได้สัดส่วนกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ โดยคำนึงถึงประสิทธิผลในการรักษาความมั่นคงปลอดภัย ควบคู่กับความสามารถในการบริหารจัดการและการดำเนินงานของหน่วยงาน

3. การตรวจสอบความสามารถในการแบ่งแยกของผู้ให้บริการคลาวด์ (CSP Segregation Capability Verification)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ควรพิจารณาและตรวจสอบความสามารถของผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ในการแบ่งแยกเครือข่าย ระบบ และทรัพยากรที่เกี่ยวข้องกับบริการคลาวด์ เพื่อให้มั่นใจว่ากลไกการแบ่งแยกที่ผู้ให้บริการจัดให้มีความเหมาะสมกับระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ลักษณะของบริการ สถาปัตยกรรม และผลการประเมินความเสี่ยงของหน่วยงาน

การตรวจสอบดังกล่าวควรพิจารณาตามขอบเขตความรับผิดชอบร่วม (Shared Responsibility) โดยไม่จำเป็นต้องกำหนดให้ CSC สามารถเข้าถึงหรือตรวจสอบรายละเอียดทางเทคนิคทั้งหมดของโครงสร้างพื้นฐาน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ภายในของ CSP หากสามารถใช้ข้อมูลหรือหลักฐานอื่นที่เหมาะสมและเพียงพอในการประเมินความสามารถดังกล่าวได้

CSC ควรพิจารณาประเด็นสำคัญ ดังต่อไปนี้

1. การแบ่งแยกระหว่างผู้เช่า (Tenant Isolation)

CSC ควรตรวจสอบว่า CSP มีกลไกที่เหมาะสมสำหรับการแบ่งแยกเครือข่าย ระบบ ข้อมูล หรือทรัพยากรระหว่างผู้เช่า (Tenant) ในสภาพแวดล้อมที่มีผู้เช่าหลายราย (Multi-tenant Environment) เพื่อป้องกันการเข้าถึงหรือการสื่อสารข้ามผู้เช่าโดยไม่ได้รับอนุญาต (Unauthorized Cross-tenant Access)

การตรวจสอบควรมุ่งเน้นที่ **ผลลัพธ์ของการแบ่งแยก (Isolation Outcome)** มากกว่าการกำหนดเทคโนโลยีที่ CSP ต้องนำมาใช้ เนื่องจากกลไกการแบ่งแยกอาจแตกต่างกันตามสถาปัตยกรรมและรูปแบบบริการคลาวด์

2. การแบ่งแยกสภาพแวดล้อมการบริหารจัดการของ CSP (CSP Management Environment Segregation)

CSC ควรพิจารณาว่า CSP มีมาตรการที่เหมาะสมในการแบ่งแยกสภาพแวดล้อมที่ใช้สำหรับการบริหารจัดการบริการหรือโครงสร้างพื้นฐานของ CSP (CSP Management Environment) ออกจากสภาพแวดล้อมการประมวลผลที่ให้บริการแก่ CSC (CSC Cloud Processing Environment)

การแบ่งแยกดังกล่าวควรช่วยลดความเสี่ยงจากการเข้าถึง การเชื่อมต่อ หรือการดำเนินการข้ามขอบเขตโดยไม่ได้รับอนุญาต และควรสัมพันธ์กับมาตรการควบคุมการเข้าถึงสำหรับผู้ดูแลระบบหรือบัญชีที่มีสิทธิ์ระดับสูง (Privileged Access) ของ CSP ตามขอบเขตที่เกี่ยวข้อง

3. การป้องกันการสื่อสารข้ามขอบเขตโดยไม่ได้รับอนุญาต (Unauthorized Cross-boundary Communication Prevention)

CSC ควรพิจารณาความสามารถของบริการในการควบคุมหรือจำกัดการสื่อสารข้ามขอบเขตการแบ่งแยก โดยการสื่อสารระหว่างเครือข่าย ระบบ หรือทรัพยากรที่ได้รับการแบ่งแยกควรเกิดขึ้นเฉพาะเมื่อมีความจำเป็นและได้รับอนุญาตตามนโยบายที่กำหนด

หลักการดังกล่าวสอดคล้องกับแนวคิด **การสื่อสารตามสิทธิ์เท่าที่จำเป็น (Least-privilege Communication)** ซึ่งช่วยลดโอกาสในการเคลื่อนที่ด้านข้าง (Lateral Movement) เมื่อระบบหรือบัญชีส่วนหนึ่ง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ถูกประนีประนอม (Compromised) โดยเอกสาร Zero Trust ที่นำมาใช้ประกอบระบุ Micro-segmentation เป็นกลไกหนึ่งในการจำกัดการเชื่อมต่อระหว่าง Workload และ Asset ตามความจำเป็น

อย่างไรก็ตาม ข้อกำหนดนี้ **ไม่ควรตีความว่า CSP ต้องใช้ Micro-segmentation โดยเฉพาะ** หากสามารถใช้กลไกอื่นที่ให้ผลลัพธ์ด้านความมั่นคงปลอดภัยเทียบเท่าและเหมาะสมกับความเสี่ยง

4. การสนับสนุนการตรวจสอบประสิทธิผลของการแบ่งแยก (Segregation Effectiveness Verification Support)

CSC ควรพิจารณาว่า CSP สามารถจัดให้มีข้อมูล หลักฐาน หรือความสามารถที่เหมาะสม เพื่อสนับสนุนการตรวจสอบว่ากลไกการแบ่งแยกที่เกี่ยวข้องกับบริการมีการนำไปใช้และมีประสิทธิผลตามขอบเขตที่เกี่ยวข้อง

การตรวจสอบอาจดำเนินการโดยใช้เอกสารประกอบบริการ ข้อมูลเกี่ยวกับสถาปัตยกรรมหรือมาตรการควบคุม รายงานการประเมินโดยบุคคลที่เป็นอิสระ (Independent Assessment) การรับรองตามมาตรฐานที่เกี่ยวข้อง (Relevant Certification) ผลการทดสอบ หรือหลักฐานอื่นที่มีความเหมาะสมกับระดับความเสี่ยงและรูปแบบบริการ

ทั้งนี้ CSC ไม่ควรกำหนดให้ CSP เปิดเผยข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน ผู้เช่ารายอื่น หรือข้อมูลที่มีข้อจำกัดด้านการรักษาความลับ หากมีหลักฐานอื่นที่เพียงพอสำหรับการประเมิน

5. การพิจารณาข้อจำกัดและความรับผิดชอบของบริการ (Service Limitations and Responsibilities)

CSC ควรทำความเข้าใจขอบเขตและข้อจำกัดของกลไกการแบ่งแยกที่ CSP จัดให้ รวมถึงส่วนที่ CSC ต้องดำเนินการหรือกำหนดค่าเพิ่มเติม เพื่อป้องกันมิให้เกิดช่องว่างของความรับผิดชอบ (Responsibility Gap)

โดยเฉพาะในกรณีที่ CSC สามารถกำหนดค่าการเชื่อมต่อระหว่างเครือข่าย ระบบ หรือภาระงานได้เอง CSC ควรรับผิดชอบในการกำหนดค่าดังกล่าวให้สอดคล้องกับข้อกำหนดด้านการแบ่งแยกและผลการประเมินความเสี่ยงของหน่วยงาน

แนวทางการพิจารณาหลักฐาน (Evidence Consideration)

ความเพียงพอของหลักฐานตามลักษณะบริการและระดับความเสี่ยง ตัวอย่างเช่น

ประเด็นที่ตรวจสอบ	ตัวอย่างหลักฐานที่อาจพิจารณา
การแบ่งแยกระหว่างผู้เช่า (Tenant Isolation)	เอกสารอธิบายกลไกการแบ่งแยกหรือหลักฐานการประเมินที่เกี่ยวข้อง
การแบ่งแยก Management Environment	เอกสารสถาปัตยกรรมหรือคำอธิบายมาตรการควบคุมในระดับที่เหมาะสม
การควบคุมการสื่อสารข้ามขอบเขต	เอกสารความสามารถของบริการหรือแนวทางการกำหนดค่า

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

ประสิทธิผลของมาตรการ	ผลการทดสอบ รายงานการประเมิน หรือการรับรองที่มีขอบเขตเกี่ยวข้อง
ความรับผิดชอบของ CSC/CSP	เอกสารความรับผิดชอบร่วม (Shared Responsibility Documentation)
ข้อจำกัดของบริการ	เอกสารข้อกำหนด เงื่อนไข หรือข้อจำกัดของบริการ

การมีใบรับรองมาตรฐานหรือรายงานการตรวจประเมิน **ไม่ควรถือว่าเพียงพอโดยอัตโนมัติ** CSC ควรพิจารณาว่าขอบเขตของหลักฐานนั้นครอบคลุมบริการและความสามารถด้านการแบ่งแยกที่หน่วยงานนำมาใช้งานจริงหรือไม่

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ต้องจัดให้มีและบังคับใช้มาตรการแบ่งแยกเครือข่าย (Network Segregation) ที่เหมาะสมกับลักษณะของบริการคลาวด์ สถาปัตยกรรมระบบ และความเสี่ยงที่เกี่ยวข้อง เพื่อป้องกันการเข้าถึงหรือการสื่อสารข้ามขอบเขตโดยไม่ได้รับอนุญาต และรักษาการแบ่งแยกระหว่างผู้ใช้บริการและสภาพแวดล้อมที่มีวัตถุประสงค์หรือระดับความไว้วางใจแตกต่างกัน

มาตรการดังกล่าวควรสามารถรักษาผลลัพธ์ด้านการแบ่งแยก (Segregation Outcome) ได้อย่างมีประสิทธิผล โดยไม่จำเป็นต้องกำหนดเทคโนโลยีหรือกลไกทางเทคนิคเฉพาะ ทั้งนี้ CSP ควรสามารถให้ข้อมูลหรือหลักฐานที่เหมาะสมเพื่อสนับสนุนให้ CSC สามารถประเมินความเพียงพอและประสิทธิผลของมาตรการที่เกี่ยวข้องได้

1. การแบ่งแยกระหว่างผู้เช่า (Tenant Isolation)

ในสภาพแวดล้อมระบบคลาวด์ที่มีผู้เช่าหลายราย (Multi-tenant Environment) ผู้ให้บริการคลาวด์ต้องจัดให้มีและบังคับใช้กลไกการแบ่งแยกระหว่างผู้เช่า (Tenant Isolation) เพื่อป้องกันมิให้ผู้เช่ารายหนึ่งสามารถเข้าถึงเครือข่าย ข้อมูล ระบบ หรือทรัพยากรของผู้เช่ารายอื่นโดยไม่ได้รับอนุญาต ซึ่งสอดคล้องโดยตรงกับข้อกำหนดของประกาศ

การแบ่งแยกดังกล่าวอาจดำเนินการโดยใช้กลไกเชิงกายภาพ (Physical Isolation) เชิงตรรกะ (Logical Isolation) หรือกลไกอื่นที่เหมาะสมกับสถาปัตยกรรมและรูปแบบบริการ โดยควรมุ่งเน้นที่ความสามารถในการบรรลุผลลัพธ์ด้านความมั่นคงปลอดภัย มากกว่าการกำหนดรูปแบบเทคโนโลยีเฉพาะ

CSP ควรพิจารณาประเด็นสำคัญดังต่อไปนี้

1. **การป้องกันการเข้าถึงข้ามผู้เช่าโดยไม่ได้รับอนุญาต (Unauthorized Cross-tenant Access Prevention)** ต้องมีกลไกที่เหมาะสมเพื่อป้องกันมิให้ผู้ใช้ ระบบ บริการ หรือภาระงาน (Workload) ของผู้เช่ารายหนึ่งสามารถเข้าถึงทรัพยากรของผู้เช่ารายอื่นโดยไม่ได้รับอนุญาต

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2. **การแบ่งแยกการสื่อสารระหว่างผู้เช่า (Cross-tenant Communication Isolation)** การสื่อสารระหว่างทรัพยากรของผู้เช่าที่แตกต่างกันควรได้รับการแบ่งแยกตามสถาปัตยกรรมของบริการ เว้นแต่เป็นการสื่อสารที่ได้รับอนุญาตอย่างชัดเจนตามรูปแบบและวัตถุประสงค์ของบริการ
3. **การแบ่งแยกทรัพยากรเชิงตรรกะ (Logical Resource Isolation)** ในกรณีที่มีการใช้โครงสร้างพื้นฐานหรือทรัพยากรร่วมกัน (Shared Infrastructure or Resources) CSP ควรมีกลไกเชิงตรรกะที่เหมาะสมสำหรับรักษาขอบเขตระหว่างผู้เช่า เพื่อป้องกันการเข้าถึงข้ามขอบเขตโดยไม่ได้รับอนุญาต
4. **การควบคุมการระบุตัวตนและขอบเขตของทรัพยากร (Tenant and Resource Boundary Control)** CSP ควรมีกลไกที่สามารถระบุและบังคับใช้ขอบเขตของทรัพยากรที่เกี่ยวข้องกับผู้เช่าแต่ละรายตามความเหมาะสม เพื่อสนับสนุนให้การควบคุมการเข้าถึงและการสื่อสารเป็นไปตามขอบเขตที่กำหนด
5. **การป้องกันการเคลื่อนที่ข้ามขอบเขตโดยไม่ได้รับอนุญาต (Unauthorized Cross-boundary Movement Prevention)** กลไกการแบ่งแยกควรช่วยลดความเสี่ยงที่เหตุการณ์ด้านความมั่นคงปลอดภัยจากผู้เช่าหรือภาระงานหนึ่งจะสามารถขยายผลหรือเคลื่อนที่ไปยังทรัพยากรของผู้เช่ารายอื่นโดยไม่ได้รับอนุญาต
6. **การรักษาประสิทธิผลของการแบ่งแยก (Isolation Effectiveness)** CSP ควรจัดให้มีกระบวนการหรือกลไกที่เหมาะสมสำหรับรักษาและตรวจสอบประสิทธิผลของการแบ่งแยกระหว่างผู้เช่า ตามลักษณะของบริการและระดับความเสี่ยง
7.

หลักการไม่ให้ความเชื่อมั่นโดยปริยาย (No Implicit Trust)

การที่ทรัพยากรอยู่ภายในโครงสร้างพื้นฐานหรือสภาพแวดล้อมคลาวด์เดียวกัน ไม่ควรเป็นเหตุให้ได้รับอนุญาตให้เข้าถึงหรือสื่อสารระหว่างกันโดยปริยาย การอนุญาตการเข้าถึงควรพิจารณาตามขอบเขตของผู้เช่า สิทธิ์ที่ได้รับอนุญาต และนโยบายการควบคุมที่เกี่ยวข้อง

หลักการนี้สอดคล้องกับแนวคิด Zero Trust ที่ไม่ถือว่าตำแหน่งของเครือข่ายเป็นฐานของความเชื่อมั่นโดยอัตโนมัติ และใช้การแบ่งส่วนเครือข่าย (Network Segmentation) หรือการแบ่งส่วนในระดับที่ละเอียดขึ้น (Micro-segmentation) เพื่อจำกัดการสื่อสารและการเคลื่อนที่ด้านข้าง (Lateral Movement) ระหว่างทรัพยากรตามความเหมาะสม อย่างไรก็ตาม CSP สามารถใช้กลไกอื่นที่บรรลุผลลัพธ์ด้านการแบ่งแยกและการป้องกันการเข้าถึงข้ามผู้เช่าได้อย่างมีประสิทธิผล

การใช้ทรัพยากรร่วมกัน (Shared Resource Consideration)

การใช้ทรัพยากรหรือโครงสร้างพื้นฐานร่วมกันระหว่างผู้เช่า **ไม่ควรถูกตีความว่าไม่สอดคล้องกับข้อกำหนดโดยอัตโนมัติ** เนื่องจากการใช้ทรัพยากรร่วมกัน (Resource Pooling) เป็นลักษณะหนึ่งที่สามารถพบได้ในสถาปัตยกรรมบริการคลาวด์

ประเด็นสำคัญในการประเมินจึงไม่ใช่ว่า CSP ใช้ทรัพยากรร่วมกันหรือไม่ แต่ควรพิจารณาว่า

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing ไม่ใช่ฉบับจริง

ทรัพยากรร่วมกัน (Shared Resources)

⟶ มีขอบเขตการแบ่งแยกที่เหมาะสม (Appropriate Isolation Boundary)

⟶ มีการควบคุมการเข้าถึง (Access Control)

⟶ ป้องกันการเข้าถึงข้ามผู้เช่า (Cross-tenant Access Prevention)

⟶ สามารถแสดงประสิทธิผลของการแบ่งแยกได้ (Isolation Assurance)

แนวทางนี้ทำให้ข้อกำหนดรองรับทั้งบริการที่ใช้ทรัพยากรร่วมกัน (Shared Infrastructure) และบริการที่จัดสรรทรัพยากรเฉพาะ (Dedicated Resources) โดยไม่สร้างข้อได้เปรียบหรือข้อเสียจากรูปแบบสถาปัตยกรรมเพียงอย่างเดียว

การตรวจสอบประสิทธิผลของการแบ่งแยกระหว่างผู้เช่า (Tenant Isolation Verification)

CSP ควรจัดให้มีกลไกหรือกระบวนการที่เหมาะสมสำหรับตรวจสอบว่าการแบ่งแยกระหว่างผู้เช่ายังคงมีประสิทธิผล โดยอาจใช้การทดสอบ การตรวจสอบการกำหนดค่า การประเมินด้านความมั่นคงปลอดภัย หรือวิธีการอื่นตามความเหมาะสมกับลักษณะของบริการและระดับความเสี่ยง

CSP ควรสามารถให้ข้อมูลหรือหลักฐานที่เพียงพอแก่ CSC เพื่อสนับสนุนการประเมินความสามารถดังกล่าว โดยคำนึงถึงข้อจำกัดด้านการรักษาความลับ ความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน และการคุ้มครองข้อมูลของผู้ใช้บริการรายอื่น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เหตุผลและความจำเป็น (Rationale)

สภาพแวดล้อมระบบคลาวด์อาจมีผู้ใช้บริการหลายรายใช้ทรัพยากรหรือโครงสร้างพื้นฐานบางส่วนร่วมกัน หากกลไกการแบ่งแยกระหว่างผู้เช่าไม่มีประสิทธิผล อาจก่อให้เกิดความเสี่ยงจากการเข้าถึงข้อมูล ระบบ หรือทรัพยากรของผู้ใช้บริการรายอื่นโดยไม่ได้รับอนุญาต

การกำหนดให้มีการแบ่งแยกระหว่างผู้เช่าที่เหมาะสมจึงเป็นมาตรการพื้นฐานสำหรับรักษาขอบเขตความมั่นคงปลอดภัยของบริการคลาวด์ และสนับสนุนการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและบริการ

2. การแบ่งแยกสภาพแวดล้อมการบริหารจัดการของผู้ให้บริการคลาวด์ (CSP Management Environment Segregation)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ต้องจัดให้มีและบังคับใช้มาตรการแบ่งแยกสภาพแวดล้อมที่ใช้สำหรับการบริหารจัดการบริการและโครงสร้างพื้นฐานของผู้ให้บริการคลาวด์ (CSP Management Environment) ออกจากสภาพแวดล้อมการประมวลผลที่ให้บริการแก่ผู้ใช้บริการคลาวด์ (CSC Cloud Processing Environment) อย่างเหมาะสม เพื่อป้องกันการเข้าถึง การเชื่อมต่อ หรือการดำเนินการข้ามขอบเขตโดยไม่ได้รับอนุญาต ซึ่งเป็นสาระที่ข้อกำหนดต้นทางกำหนดไว้โดยตรง

การแบ่งแยกดังกล่าวควรได้รับการออกแบบและบังคับใช้ให้เหมาะสมกับสถาปัตยกรรมของบริการ รูปแบบการให้บริการ และความเสี่ยงที่เกี่ยวข้อง โดยอาจใช้การแบ่งแยกเชิงกายภาพ (Physical Segregation) การแบ่งแยกเชิงตรรกะ (Logical Segregation) หรือกลไกอื่นที่สามารถบรรลุผลลัพธ์ด้านความมั่นคงปลอดภัยที่เทียบเท่า

CSP ควรพิจารณาประเด็นสำคัญดังต่อไปนี้

1. **การกำหนดขอบเขตสภาพแวดล้อมการบริหารจัดการ (Management Environment Boundary)** ควรกำหนดขอบเขตของระบบ เครือข่าย บริการ หรือองค์ประกอบที่ใช้สำหรับการบริหารจัดการโครงสร้างพื้นฐานและบริการคลาวด์ให้มีความเหมาะสมและสามารถแยกออกจากสภาพแวดล้อมการประมวลผลของ CSC ได้อย่างชัดเจนตามสถาปัตยกรรมของบริการ
2. **การควบคุมการเข้าถึงสภาพแวดล้อมการบริหารจัดการ (Management Environment Access Control)** การเข้าถึงสภาพแวดล้อมการบริหารจัดการควรจำกัดเฉพาะบุคคล ระบบ หรือกระบวนการที่ได้รับอนุญาตและมีความจำเป็นต่อการปฏิบัติหน้าที่ โดยสอดคล้องกับหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และการแบ่งแยกหน้าที่ (Segregation of Duties) ตามความเหมาะสม
3. **การควบคุมการสื่อสารข้ามขอบเขต (Cross-boundary Communication Control)** การสื่อสารระหว่างสภาพแวดล้อมการบริหารจัดการของ CSP กับสภาพแวดล้อมการประมวลผลของ CSC ควรจำกัดเฉพาะการสื่อสารที่มีความจำเป็นต่อการให้บริการ การบริหารจัดการ การบำรุงรักษา หรือการสนับสนุนบริการ และต้องได้รับอนุญาตตามกลไกควบคุมที่กำหนด
4. **การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากสภาพแวดล้อมของ CSC (Unauthorized Access from CSC Environment Prevention)** ควรมีกลไกที่เหมาะสมเพื่อป้องกันมิให้ระบบ ภาระงาน หรือผู้ใช้งานในสภาพแวดล้อมการประมวลผลของ CSC สามารถเข้าถึงสภาพแวดล้อมการบริหารจัดการภายในของ CSP โดยไม่ได้รับอนุญาต
5. **การควบคุมการเข้าถึงจากสภาพแวดล้อมการบริหารจัดการเข้าสู่ทรัพยากรของ CSC (Controlled Administrative Access to CSC Resources)** ในกรณีที่ CSP มีความจำเป็นต้องเข้าถึงทรัพยากรหรือสภาพแวดล้อมของ CSC เพื่อวัตถุประสงค์ในการบริหารจัดการ บำรุงรักษา สนับสนุน หรือแก้ไขเหตุขัดข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การเข้าถึงดังกล่าวควรอยู่ภายใต้มาตรการควบคุมที่เหมาะสมกับความเสี่ยงและขอบเขตความรับผิดชอบของบริการ

6. **การป้องกันการเคลื่อนที่ข้ามขอบเขตโดยไม่ได้รับอนุญาต (Unauthorized Cross-boundary Movement Prevention)** การออกแบบการแบ่งแยกควรช่วยลดความเสี่ยงที่การประนีประนอม (Compromise) ของระบบหรือองค์ประกอบในสภาพแวดล้อมหนึ่งจะสามารถนำไปสู่การเข้าถึงหรือการเคลื่อนที่ไปยังอีกสภาพแวดล้อมหนึ่งโดยไม่ได้รับอนุญาต
7. **การรักษาและตรวจสอบประสิทธิผลของการแบ่งแยก (Segregation Maintenance and Verification)** CSP ควรจัดให้มีกระบวนการหรือกลไกที่เหมาะสมสำหรับรักษาและตรวจสอบว่าการแบ่งแยกระหว่างสภาพแวดล้อมการบริหารจัดการกับสภาพแวดล้อมการประมวลผลของ CSC ยังคงมีประสิทธิผล โดยเฉพาะเมื่อมีการเปลี่ยนแปลงสถาปัตยกรรมหรือองค์ประกอบของบริการที่มีนัยสำคัญ

การเข้าถึงเพื่อการบริหารจัดการ (Administrative Access)

เนื่องจากบริการคลาวด์บางรูปแบบอาจมีความจำเป็นทางเทคนิคหรือการปฏิบัติงานที่ CSP ต้องดำเนินการบางอย่างภายในขอบเขตบริการที่ตนรับผิดชอบ ดังนั้น หลักการที่เหมาะสมควรเป็น

มีความจำเป็นและวัตถุประสงค์ที่ชอบด้วยหน้าที่ (Legitimate Operational Need)

⟶ ได้รับอนุญาต (Authorized)

⟶ จำกัดสิทธิ์เท่าที่จำเป็น (Least Privilege)

⟶ ดำเนินการผ่านช่องทางหรือกลไกที่ควบคุม (Controlled Administrative Access)

⟶ สามารถตรวจสอบได้ตามความเหมาะสม (Accountable and Verifiable)

แนวทางนี้ช่วยหลีกเลี่ยงการกำหนดข้อห้ามที่ไม่สอดคล้องกับลักษณะการให้บริการคลาวด์ ขณะเดียวกันยังรักษาหลักการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจน

ความสัมพันธ์กับหลักการไม่ให้ความเชื่อมั่นโดยปริยาย (No Implicit Trust)

การที่ระบบหรือบัญชีเป็นส่วนหนึ่งของสภาพแวดล้อมการบริหารจัดการของ CSP ไม่ควรทำให้ได้รับสิทธิ์ในการเข้าถึงทรัพยากรของ CSC โดยปริยาย การเข้าถึงควรสัมพันธ์กับหน้าที่ สิทธิ์ และเงื่อนไขที่กำหนดไว้

หลักการดังกล่าวสอดคล้องกับแนวคิด Zero Trust ซึ่งเน้นการไม่ให้ความเชื่อมั่นโดยอัตโนมัติจากตำแหน่งเครือข่าย การให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และการตรวจสอบก่อนอนุญาตการเข้าถึงทรัพยากร

หลักฐานประกอบการประเมิน (Assessment Evidence)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

เพื่อสนับสนุนให้ CSC สามารถประเมินความเหมาะสมของการแบ่งแยก CSP อาจใช้หลักฐานในรูปแบบที่เหมาะสมกับลักษณะบริการ เช่น

ประเด็น	ตัวอย่างหลักฐานที่อาจพิจารณา
ขอบเขต Management Environment	เอกสารอธิบายสถาปัตยกรรมหรือขอบเขตการควบคุมในระดับที่เหมาะสม
การแบ่งแยกจาก CSC Environment	เอกสารอธิบายมาตรการหรือกลไกการแบ่งแยก
Administrative Access	นโยบายหรือคำอธิบายมาตรการควบคุมการเข้าถึงเพื่อการบริหารจัดการ
ประสิทธิผลของการแบ่งแยก	รายงานการประเมิน ผลการทดสอบ หรือหลักฐานการรับรองที่มีขอบเขตเกี่ยวข้อง
ความรับผิดชอบของ CSC/CSP	เอกสารความรับผิดชอบร่วม (Shared Responsibility Documentation)

ทั้งนี้ ไม่กำหนดให้ CSP ต้องเปิดเผย แผนผังเครือข่ายภายในโดยละเอียด (Detailed Internal Network Diagram) รายการกฎการควบคุมเครือข่ายทั้งหมด หรือข้อมูลทางเทคนิคที่อาจเพิ่มความเสี่ยงต่อโครงสร้างพื้นฐานและผู้ใช้บริการรายอื่น หากสามารถใช้หลักฐานอื่นที่เพียงพอในการแสดงประสิทธิผลของมาตรการได้

เหตุผลและความจำเป็น (Rationale)

สภาพแวดล้อมการบริหารจัดการของ CSP อาจมีความสามารถในการควบคุมหรือบริหารองค์ประกอบสำคัญของบริการคลาวด์ หากไม่มีการแบ่งแยกและควบคุมการเข้าถึงอย่างเหมาะสม การโจมตีองค์ประกอบด้านการบริหารจัดการอาจส่งผลกระทบต่อสภาพแวดล้อมการประมวลผลของ CSC ได้

การแบ่งแยกสภาพแวดล้อมดังกล่าวจึงช่วยลดเส้นทางการเข้าถึงที่ไม่จำเป็น จำกัดขอบเขตผลกระทบ และสนับสนุนให้การเข้าถึงเพื่อการบริหารจัดการเกิดขึ้นเฉพาะตามความจำเป็นและอยู่ภายใต้การควบคุมที่เหมาะสม

3. การสนับสนุนการตรวจสอบประสิทธิผลของการแบ่งแยก (Segregation Verification and Assurance Support)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ต้องสนับสนุนให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) สามารถตรวจสอบหรือประเมินความเหมาะสมและประสิทธิผลของมาตรการแบ่งแยกที่อยู่ภายใต้ความรับผิดชอบของ CSP โดยเฉพาะการแบ่งแยกระหว่างผู้เช่า (Tenant Isolation) และการแบ่งแยกระหว่างสภาพแวดล้อมการบริหารจัดการของ CSP (CSP Management Environment) กับสภาพแวดล้อมการประมวลผลของ CSC (CSC Cloud Processing Environment) ตามข้อกำหนดของประกาศ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การสนับสนุนดังกล่าวควรดำเนินการในระดับที่เหมาะสมกับลักษณะของบริการคลาวด์ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และผลการประเมินความเสี่ยง โดยคำนึงถึงขอบเขตความรับผิดชอบร่วม (Shared Responsibility) ตลอดจนข้อจำกัดด้านการรักษาความลับและความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน ผู้ใช้บริการ และผู้เช่ารายอื่น

CSP ควรพิจารณาดำเนินการในประเด็นสำคัญ ดังต่อไปนี้

1. **การให้ข้อมูลเกี่ยวกับกลไกการแบ่งแยก (Segregation Mechanism Information)** ควรให้ข้อมูลในระดับที่เหมาะสมเกี่ยวกับหลักการหรือกลไกที่ใช้ในการแบ่งแยกระหว่างผู้เช่า และการแบ่งแยกสภาพแวดล้อมการบริหารจัดการของ CSP ออกจากสภาพแวดล้อมการประมวลผลของ CSC เพื่อให้ CSC สามารถประเมินความเหมาะสมของมาตรการกับความต้องการด้านความมั่นคงปลอดภัยของตนได้
2. **การให้ข้อมูลเกี่ยวกับขอบเขตความรับผิดชอบ (Responsibility Boundary Information)** ควรระบุให้ชัดเจนว่ามาตรการแบ่งแยกส่วนใดอยู่ภายใต้ความรับผิดชอบของ CSP และส่วนใดเป็นความรับผิดชอบของ CSC รวมถึงการกำหนดค่าหรือมาตรการเพิ่มเติมที่ CSC ต้องดำเนินการเพื่อให้การแบ่งแยกมีประสิทธิผลตามวัตถุประสงค์
3. **การสนับสนุนหลักฐานประกอบการประเมิน (Assessment Evidence Support)** ควรจัดให้มีข้อมูลหรือหลักฐานที่เหมาะสมเพื่อสนับสนุนการประเมินประสิทธิผลของมาตรการแบ่งแยก โดยรูปแบบของหลักฐานอาจแตกต่างกันตามประเภทและลักษณะของบริการ และไม่จำเป็นต้องกำหนดให้ใช้หลักฐานประเภทเดียวกันสำหรับผู้ให้บริการคลาวด์ทุกราย
4. **การสนับสนุนการตรวจสอบหรือการทดสอบตามความเหมาะสม (Verification or Testing Support)** ในกรณีที่เหมาะสมกับลักษณะบริการและระดับความเสี่ยง CSP ควรมีแนวทางหรือกลไกที่สนับสนุนการตรวจสอบหรือการทดสอบประสิทธิผลของการแบ่งแยก ทั้งนี้ การดำเนินการดังกล่าวต้องอยู่ภายใต้เงื่อนไขที่ไม่ก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัย ความพร้อมใช้งาน หรือผู้ใช้บริการรายอื่น
5. **การให้ข้อมูลเกี่ยวกับข้อจำกัดที่มีนัยสำคัญ (Material Limitation Information)** ควรให้ข้อมูลเกี่ยวกับข้อจำกัดของกลไกการแบ่งแยกที่อาจมีนัยสำคัญต่อการประเมินความเสี่ยงหรือการออกแบบมาตรการเพิ่มเติมของ CSC เพื่อให้ CSC สามารถพิจารณาความเสี่ยงคงเหลือ (Residual Risk) และกำหนดมาตรการที่เหมาะสมได้
6. **การรักษาความต่อเนื่องของการประกันความมั่นคงปลอดภัย (Ongoing Security Assurance)** CSP ควรมีกระบวนการที่เหมาะสมในการรักษาความมีประสิทธิผลของมาตรการแบ่งแยกตลอดระยะเวลาการให้บริการ รวมถึงพิจารณาทบทวนหรือประเมินใหม่เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อสถาปัตยกรรมหรือกลไกการแบ่งแยก

หลักฐานประกอบการประเมิน (Assessment Evidence)

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น ห้ามใช้งานอย่างอื่น

หลักฐานที่ใช้สนับสนุนการตรวจสอบไม่จำเป็นต้องเป็นการเปิดให้ CSC ตรวจสอบโครงสร้างพื้นฐานของ CSP โดยตรง แต่อาจใช้หลักฐานหลายรูปแบบตามความเหมาะสม เช่น เอกสารอธิบายสถาปัตยกรรมหรือมาตรการควบคุม (Architecture or Control Documentation) รายงานการประเมินโดยบุคคลที่เป็นอิสระ (Independent Assessment Report) การรับรองตามมาตรฐานที่เกี่ยวข้อง (Relevant Certification) ผลการทดสอบด้านความมั่นคงปลอดภัย (Security Testing Results) หรือหลักฐานอื่นที่สามารถแสดงให้เห็นถึงประสิทธิผลของมาตรการได้

การพิจารณาหลักฐานควรให้ความสำคัญกับ **ขอบเขต (Scope) ความเกี่ยวข้อง (Relevance) ความน่าเชื่อถือ (Reliability) และความเป็นปัจจุบัน (Currency)** ของหลักฐาน มากกว่าการพิจารณาเพียงว่าผู้ให้บริการมีใบรับรองหรือเอกสารประเภทใดประเภทหนึ่งหรือไม่

ตัวอย่างแนวทางสามารถสรุปได้ดังนี้

ประเด็นที่ต้องการความเชื่อมั่น	**ตัวอย่างหลักฐานที่อาจใช้**
การแบ่งแยกระหว่างผู้เช่า (Tenant Isolation)	เอกสารอธิบายมาตรการ รายงานการประเมิน หรือผลการทดสอบที่เกี่ยวข้อง
การแบ่งแยก CSP Management Environment	เอกสารสถาปัตยกรรมหรือคำอธิบายมาตรการควบคุมในระดับที่เหมาะสม
ประสิทธิผลของการแบ่งแยก	รายงานการทดสอบ การประเมินโดยบุคคลที่เป็นอิสระ หรือหลักฐานอื่นที่เกี่ยวข้อง
ขอบเขตความรับผิดชอบ	เอกสารความรับผิดชอบร่วม (Shared Responsibility Documentation)
การกำหนดค่าของ CSC	เอกสารหรือแนวทางการกำหนดค่าที่มั่นคงปลอดภัย (Secure Configuration Guidance)
ข้อจำกัดของกลไก	เอกสารข้อกำหนด เงื่อนไข หรือข้อจำกัดของบริการ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้อ้างอิง

การตรวจสอบโดย CSC และบุคคลที่เป็นอิสระ

การสนับสนุนการตรวจสอบ **ไม่ควรตีความว่า CSC ต้องได้รับสิทธิ์ในการดำเนินการทดสอบเจาะระบบ (Penetration Testing) หรือการตรวจสอบทางเทคนิคต่อโครงสร้างพื้นฐานของ CSP ได้โดยไม่มีข้อจำกัด**

ในสภาพแวดล้อมที่มีผู้เช่าหลายราย การทดสอบดังกล่าวอาจส่งผลกระทบต่อความพร้อมใช้งาน ความมั่นคงปลอดภัย หรือผู้ใช้บริการรายอื่น ดังนั้น CSP สามารถกำหนดเงื่อนไข ขอบเขต กระบวนการอนุมัติ หรือวิธีการทดสอบที่เหมาะสมได้

ในกรณีที่ CSC ไม่สามารถตรวจสอบมาตรการบางส่วนได้โดยตรง อาจใช้การประกันโดยบุคคลที่เป็นอิสระ (Independent Assurance) หรือหลักฐานอื่นที่มีความน่าเชื่อถือและมีขอบเขตครอบคลุมมาตรการที่ต้องการประเมินแทนได้

เหตุผลและความจำเป็น (Rationale)

เนื่องจากมาตรการแบ่งแยกบางส่วนของบริการคลาวด์อยู่ภายใต้การออกแบบ การดำเนินการ และการควบคุมของ CSP โดยตรง CSC อาจไม่สามารถตรวจสอบมาตรการดังกล่าวด้วยตนเองได้ทั้งหมด การจัดให้มีข้อมูล หลักฐาน และกลไกการประกันความมั่นคงปลอดภัยที่เหมาะสมจึงมีความสำคัญต่อการช่วยให้ CSC สามารถประเมินว่าบริการคลาวด์มีระดับการแบ่งแยกที่สอดคล้องกับความต้องการและระดับความเสี่ยงของหน่วยงาน

ในขณะเดียวกัน การกำหนดหลักฐานควรใช้หลักความได้สัดส่วน (Proportionality) และไม่สร้างภาระในการเปิดเผยข้อมูลหรือการตรวจประเมินซ้ำซ้อนโดยไม่จำเป็น โดยเฉพาะเมื่อ CSP มีหลักฐานการประเมินจากบุคคลที่เป็นอิสระที่น่าเชื่อถือและมีขอบเขตครอบคลุมมาตรการที่เกี่ยวข้อง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. แนวทางการออกแบบการแบ่งแยกเครือข่ายตามความเสี่ยง (Risk-based Network Segregation)

การออกแบบการแบ่งแยกเครือข่าย (Network Segregation) สำหรับระบบคลาวด์ควรดำเนินการบนพื้นฐานของระดับผลกระทบ ความสำคัญของระบบ ระดับความไว้วางใจ ลักษณะของภาระงาน (Workload) ความจำเป็นในการสื่อสาร และผลการประเมินความเสี่ยง โดยไม่จำเป็นต้องใช้รูปแบบหรือระดับการแบ่งแยกเดียวกันสำหรับทุกระบบ

การแบ่งแยกควรมุ่งให้เกิดผลลัพธ์ด้านความมั่นคงปลอดภัย (Security Outcome) ที่สำคัญ ได้แก่ การจำกัดการเข้าถึงโดยไม่ได้รับอนุญาต การลดเส้นทางการสื่อสารที่ไม่จำเป็น การจำกัดการเคลื่อนที่ด้านข้าง (Lateral Movement) และการจำกัดขอบเขตผลกระทบ (Impact Containment) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

แนวทางการออกแบบควรพิจารณาประเด็นสำคัญ ดังต่อไปนี้

1. **ระบุทรัพยากรและภาระงานที่ต้องได้รับการปกป้อง (Identify Resources and Workloads)** ระบุระบบ ข้อมูล บริการ และภาระงานที่อยู่ภายในขอบเขต รวมถึงพิจารณาระดับผลกระทบ ความสำคัญ และข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง เพื่อใช้เป็นพื้นฐานในการกำหนดขอบเขตการแบ่งแยก
2. **กำหนดขอบเขตตามความเสี่ยงและระดับความไว้วางใจ (Define Risk and Trust Boundaries)** พิจารณาจัดกลุ่มและแบ่งแยกทรัพยากรที่มีระดับผลกระทบ วัตถุประสงค์ หรือระดับความไว้วางใจแตกต่าง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กันอย่างมีนัยสำคัญ โดยขอบเขตดังกล่าวอาจเป็นการแบ่งแยกเชิงกายภาพ (Physical Segregation) หรือเชิงตรรกะ (Logical Segregation) ตามความเหมาะสม

3. **ระบุความจำเป็นในการสื่อสาร (Identify Communication Requirements)** ระบุว่าระบบ ภาระงาน หรือขอบเขตใดจำเป็นต้องสื่อสารระหว่างกัน รวมถึงวัตถุประสงค์ของการสื่อสาร เพื่อหลีกเลี่ยงการเปิดให้มีการเชื่อมต่อระหว่างส่วนต่าง ๆ โดยไม่มีความจำเป็น
4. **จำกัดการสื่อสารตามความจำเป็น (Restrict Communication Based on Need)** การสื่อสารข้ามขอบเขตควรได้รับอนุญาตเฉพาะเท่าที่จำเป็นต่อวัตถุประสงค์ของระบบและการดำเนินงาน ซึ่งสอดคล้องกับหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และช่วยลดเส้นทางที่อาจถูกใช้สำหรับการเคลื่อนที่ด้านข้าง
5. **ไม่ใช้ตำแหน่งของเครือข่ายเป็นฐานความเชื่อมั่นเพียงอย่างเดียว (Do Not Rely Solely on Network Location for Trust)** การที่ผู้ใช้ อุปกรณ์ ระบบ หรือภาระงานอยู่ภายในเครือข่ายหรือขอบเขตเดียวกัน ไม่ควรถูกใช้เป็นเหตุผลเพียงประการเดียวในการอนุญาตการเข้าถึงหรือการสื่อสาร แต่ควรพิจารณาสิทธิ์ ความจำเป็น และนโยบายการควบคุมที่เกี่ยวข้องประกอบกัน

   หลักการนี้สัมพันธ์กับแนวคิด Zero Trust ที่กำหนดว่าเครือข่ายไม่ควรได้รับความเชื่อมั่นโดยอัตโนมัติ และการสื่อสารควรได้รับการรักษาความมั่นคงปลอดภัยโดยไม่ขึ้นกับตำแหน่งของเครือข่าย

6. **พิจารณาการแบ่งส่วนในระดับที่ละเอียดขึ้นตามความเสี่ยง (Consider Granular Segmentation Based on Risk)** สำหรับระบบหรือภาระงานที่มีระดับผลกระทบหรือความเสี่ยงสูง อาจพิจารณาการแบ่งส่วนเครือข่ายในระดับที่ละเอียดขึ้น รวมถึงการแบ่งส่วนย่อย (Micro-segmentation) หากเหมาะสมกับสถาปัตยกรรมและความต้องการของระบบ
7. **ตรวจสอบและทบทวนความเหมาะสมของการแบ่งแยก (Verify and Review Segregation)** ควรทบทวนขอบเขตการแบ่งแยกและการสื่อสารที่ได้รับอนุญาตเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้มั่นใจว่าการแบ่งแยกยังคงเหมาะสมกับสถาปัตยกรรม การใช้งาน และระดับความเสี่ยง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กระบวนการออกแบบการแบ่งแยกเครือข่าย

เพื่อให้สามารถนำหลักการดังกล่าวไปประยุกต์ใช้ได้อย่างเป็นระบบ สามารถพิจารณากระบวนการดังต่อไปนี้

ระบุระบบ ข้อมูล และภาระงาน

(Identify Systems, Information and Workloads)

↓

ประเมินระดับผลกระทบ ความสำคัญ และความเสี่ยง

(Assess Impact, Criticality and Risk)

↓

กำหนดขอบเขตและระดับความไว้วางใจ

(Define Segregation and Trust Boundaries)

↓

ระบุการสื่อสารที่จำเป็น

(Identify Required Communications)

↓

กำหนดและบังคับใช้การแบ่งแยกและการควบคุมการสื่อสาร

(Implement Segregation and Communication Controls)

↓

ตรวจสอบประสิทธิผล

(Verify Effectiveness)

↓

ทบทวนเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(Review upon Significant Changes)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กระบวนการ 7 ขั้นตอนนี้ช่วยเปลี่ยนเนื้อหาเชิงหลักการให้เป็นแนวทางที่หน่วยงานนำไปปฏิบัติได้ โดยไม่ต้องลงรายละเอียดถึงผลิตภัณฑ์หรือการกำหนดค่าเฉพาะ

การประยุกต์ใช้ตามระดับความเสี่ยง

แนวทางการแบ่งแยกควรใช้หลักความได้สัดส่วน (Proportionality) โดยอาจพิจารณาในลักษณะดังนี้

ลักษณะของระบบหรือความเสี่ยง	**แนวทางการแบ่งแยกที่ควรพิจารณา**
ระบบทั่วไปที่มีความเสี่ยงจำกัด	กำหนดขอบเขตและควบคุมการสื่อสารตามความจำเป็น
ระบบที่มีระดับผลกระทบหรือความสำคัญสูง	เพิ่มความเข้มงวดของขอบเขตและการควบคุมการสื่อสาร

ระบบที่มีระดับความไว้วางใจแตกต่างกัน	พิจารณาแบ่งแยกและควบคุมการสื่อสารข้ามขอบเขต
ระบบที่มีภาระงานหลายประเภท	พิจารณาแบ่งแยกตามหน้าที่ ความสำคัญ และความเสี่ยง
ระบบที่มีความเสี่ยงต่อ Lateral Movement สูง	พิจารณาการแบ่งส่วนที่ละเอียดขึ้นตามความเหมาะสม
สภาพแวดล้อมแบบ Multi-tenant	ต้องคำนึงถึงประสิทธิผลของ Tenant Isolation ที่ CSP จัดให้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักการสำคัญในการนำไปใช้

สาระสำคัญสามารถสรุปได้เป็นลำดับดังนี้

Risk & Impact

⟶ Segregation Boundary

⟶ No Implicit Trust

⟶ Least-privilege Communication

⟶ Lateral Movement Restriction

⟶ Verification & Review

แนวทางดังกล่าวนำหลักการที่เกี่ยวข้องจาก Zero Trust มาใช้สนับสนุนการแบ่งแยกเครือข่าย โดยยังรักษาขอบเขตของมาตรฐานนี้ไว้ที่ **การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)** มิได้กำหนดให้หน่วยงานต้องนำสถาปัตยกรรม Zero Trust (Zero Trust Architecture: ZTA) มาใช้เต็มรูปแบบ

2. แนวทางการตรวจสอบและทบทวนการแบ่งแยกเครือข่าย (Network Segregation Verification and Review)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ควรตรวจสอบและทบทวนความเหมาะสมและประสิทธิผลของการแบ่งแยกเครือข่าย (Network Segregation) ตามขอบเขตความรับผิดชอบของแต่ละฝ่าย เพื่อให้มั่นใจว่าขอบเขตการแบ่งแยกและการควบคุมการสื่อสารยังคงสอดคล้องกับวัตถุประสงค์ของระบบ ระดับผลกระทบ สถาปัตยกรรม และความเสี่ยงที่เกี่ยวข้อง

การตรวจสอบและทบทวนควรดำเนินการตามระดับความเสี่ยงและความมีนัยสำคัญของระบบ โดยไม่จำเป็นต้องกำหนดวิธีการหรือความถี่เดียวกันสำหรับทุกระบบ ทั้งนี้ ควรให้ความสำคัญกับการตรวจสอบ **ผลลัพธ์ของการควบคุม (Control Outcome)** มากกว่าการกำหนดให้ใช้เทคโนโลยีหรือเครื่องมือเฉพาะ

แนวทางการตรวจสอบและทบทวนควรพิจารณาประเด็นสำคัญ ดังต่อไปนี้

1. **การตรวจสอบความสอดคล้องกับขอบเขตที่กำหนด (Segregation Boundary Verification)** ควรตรวจสอบว่าขอบเขตการแบ่งแยกที่นำไปใช้สอดคล้องกับสถาปัตยกรรมและข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ รวมถึงไม่มีการเชื่อมต่อข้ามขอบเขตที่ไม่จำเป็นหรือไม่ได้รับอนุญาต
2. **การตรวจสอบการสื่อสารที่ได้รับอนุญาต (Authorized Communication Verification)** ควรตรวจสอบว่าการสื่อสารระหว่างเครือข่าย ระบบ สภาพแวดล้อม หรือภาระงานที่ได้รับการแบ่งแยกยังคงมีความจำเป็นต่อการดำเนินงาน และได้รับอนุญาตตามนโยบายหรือข้อกำหนดที่เกี่ยวข้อง

ร่างเพื่อรับฟังความคิดเห็น (Public Hearing เท่านั้น) - ห้ามใช้อ้างอิง

3. **การตรวจสอบประสิทธิผลของการแบ่งแยก (Segregation Effectiveness Verification)** ควรพิจารณาว่ามาตรการแบ่งแยกสามารถป้องกันหรือจำกัดการเข้าถึงและการสื่อสารข้ามขอบเขตโดยไม่ได้รับอนุญาตได้อย่างเหมาะสม รวมถึงสามารถช่วยจำกัดการเคลื่อนที่ด้านข้าง (Lateral Movement) และขอบเขตของผลกระทบเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
4. **การตรวจสอบการแบ่งแยกระหว่างผู้เช่า (Tenant Isolation Verification)** สำหรับบริการคลาวด์ที่มีสภาพแวดล้อมแบบผู้เช่าหลายราย (Multi-tenant Environment) ควรมีข้อมูลหรือหลักฐานที่เหมาะสมเพื่อสร้างความเชื่อมั่นว่าการแบ่งแยกระหว่างผู้เช่ายังคงมีประสิทธิผล โดยเฉพาะการป้องกันการเข้าถึงเครือข่าย ข้อมูล หรือทรัพยากรของผู้เช่ารายอื่นโดยไม่ได้รับอนุญาต
5. **การตรวจสอบการแบ่งแยกสภาพแวดล้อมการบริหารจัดการ (Management Environment Segregation Verification)** ควรตรวจสอบหรือมีหลักฐานที่เพียงพอว่าสภาพแวดล้อมการบริหารจัดการของ CSP (CSP Management Environment) ได้รับการแบ่งแยกออกจากสภาพแวดล้อมการประมวลผลของ CSC (CSC Cloud Processing Environment) และการเข้าถึงข้ามขอบเขตอยู่ภายใต้มาตรการควบคุมที่เหมาะสม
6. **การทบทวนเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ (Review upon Significant Changes)** ควรทบทวนความเหมาะสมของการแบ่งแยกเมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อความเสี่ยงหรือขอบเขตด้านความมั่นคงปลอดภัย เช่น การเปลี่ยนแปลงสถาปัตยกรรม การเพิ่มระบบหรือภาระงาน การเปลี่ยนแปลงรูปแบบการเชื่อมต่อ หรือการเปลี่ยนระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
7. **การดำเนินการเมื่อพบความไม่เหมาะสม (Corrective Action)** เมื่อพบว่าขอบเขตการแบ่งแยก การสื่อสารที่ได้รับอนุญาต หรือมาตรการควบคุมไม่เหมาะสมกับความเสี่ยง ควรดำเนินการปรับปรุงตามระดับความสำคัญและความเสี่ยง พร้อมติดตามผลเพื่อให้มั่นใจว่าประเด็นดังกล่าวได้รับการจัดการอย่างเหมาะสม

การตรวจสอบตามขอบเขตความรับผิดชอบร่วม (Verification under Shared Responsibility)

การตรวจสอบควรพิจารณาตามขอบเขตความรับผิดชอบระหว่าง CSC และ CSP โดยไม่ควรตีความว่า CSC ต้องสามารถตรวจสอบองค์ประกอบทุกส่วนของโครงสร้างพื้นฐานคลาวด์ได้โดยตรง

สามารถแบ่งแนวทางได้ดังนี้

ขอบเขต	แนวทางการตรวจสอบ
การแบ่งแยกที่ CSC กำหนดค่าและควบคุม	CSC ควรสามารถตรวจสอบการกำหนดค่าและประสิทธิผลได้ตามความเหมาะสม
การแบ่งแยกระหว่าง Workload ของ CSC	CSC ตรวจสอบตามสถาปัตยกรรมและข้อกำหนดที่ตนกำหนด
Tenant Isolation ที่ CSP รับผิดชอบ	ใช้ข้อมูล หลักฐาน ผลการประเมิน หรือการรับรองที่เหมาะสมจาก CSP

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

CSP Management Environment	ใช้ข้อมูลหรือหลักฐานที่ CSP สามารถเปิดเผยได้อย่างเหมาะสม
Shared Responsibility	ตรวจสอบว่าหน้าที่ของแต่ละฝ่ายได้รับการกำหนดและดำเนินการครบถ้วน

หลักการสำคัญคือ **“ตรวจสอบในส่วนที่ตนควบคุม และสร้างความเชื่อมั่นในส่วนที่อีกฝ่ายควบคุม” (Verify What You Control, Obtain Assurance for What You Do Not Control)** แนวคิดนี้เหมาะสมกับบริการคลาวด์มากกว่าการกำหนดให้ CSC ต้องสามารถตรวจสอบทุกองค์ประกอบของ CSP ด้วยตนเอง

การทบทวนตามความเสี่ยง (Risk-based Review)

การทบทวนไม่จำเป็นต้องดำเนินการด้วยระดับความเข้มงวดเดียวกันในทุกระบบ แต่ควรกำหนดตามระดับผลกระทบ ความสำคัญ และความเสี่ยงของระบบ

ตัวอย่างเช่น ระบบที่มีระดับผลกระทบสูงหรือมีการเปลี่ยนแปลงสถาปัตยกรรมอย่างมีนัยสำคัญอาจต้องได้รับการตรวจสอบในรายละเอียดมากกว่าระบบทั่วไป ขณะที่การเปลี่ยนแปลงเล็กน้อยซึ่งไม่ส่งผลต่อขอบเขตการแบ่งแยกหรือความเสี่ยงอย่างมีนัยสำคัญอาจดำเนินการตามกระบวนการบริหารการเปลี่ยนแปลงตามปกติ

จึงไม่ควรกำหนดในหัวข้อนี้ว่า **“ต้องทบทวนทุก 6 เดือน” หรือ “ต้องทบทวนปีละครั้ง”** เป็นการเฉพาะ หากข้อกำหนดต้นทางไม่ได้กำหนดไว้ เพราะจะกลายเป็นการสร้างภาระหรือข้อกำหนดเพิ่มเติมโดยไม่จำเป็น

ความสัมพันธ์กับหลักการตรวจสอบอย่างต่อเนื่อง (Continuous Verification)

หลักการตรวจสอบอย่างต่อเนื่อง (Continuous Verification) จากแนวคิด Zero Trust สามารถนำมาใช้เป็นแนวคิดสนับสนุน โดยไม่ควรตีความว่าหน่วยงานต้องดำเนินการตรวจสอบทางเทคนิคแบบเวลาจริง (Real-time Verification) ต่อทุกการสื่อสาร

ในบริบทของการแบ่งแยกเครือข่าย หลักการดังกล่าวหมายถึงการไม่ตั้งสมมติฐานว่ามาตรการที่เคยได้รับการตรวจสอบแล้วจะยังคงมีประสิทธิผลตลอดไป แต่ควรมีการติดตาม ตรวจสอบ หรือทบทวนตามความเสี่ยงและการเปลี่ยนแปลงที่เกี่ยวข้อง ซึ่งสอดคล้องกับแนวคิด Continuous Verification ในเอกสาร Zero Trust ที่นำมาใช้ประกอบ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

วงจรการแบ่งแยกเครือข่าย (Network Segregation Lifecycle)

เมื่อรวมกับหัวข้อก่อนหน้า กระบวนการทั้งหมดสามารถสรุปเป็นวงจรได้ว่า

ประเมินความเสี่ยง (Assess Risk)

⟶ ออกแบบขอบเขต (Design Boundaries)

⟶ กำหนดการสื่อสารที่จำเป็น (Define Required Communications)

⟶ นำมาตรการไปใช้ (Implement Controls)

⟶ ตรวจสอบประสิทธิผล (Verify Effectiveness)

⟶ ทบทวนเมื่อมีการเปลี่ยนแปลง (Review upon Change)

⟶ ปรับปรุง (Improve)

หลักฐานที่ควรเก็บรักษา

หลักฐานควรเก็บรักษาเท่าที่จำเป็นและเหมาะสมกับความเสี่ยง เช่น เอกสารหรือแผนภาพแสดงขอบเขตการแบ่งแยก ผลการทบทวนการสื่อสารที่ได้รับอนุญาต ผลการตรวจสอบหรือทดสอบที่เกี่ยวข้อง หลักฐานจาก CSP และรายการปรับปรุงที่เกิดจากการทบทวน

สรุปข้อกำหนดและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security Requirements and Responsibility Summary).

1. หลักการ (Principle)

การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security) สำหรับบริการคลาวด์เป็นความรับผิดชอบร่วม (Shared Responsibility) ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยขอบเขตความรับผิดชอบของแต่ละฝ่ายอาจแตกต่างกันตามรูปแบบบริการคลาวด์ (Cloud Service Model) สถาปัตยกรรมของบริการ และข้อตกลงการให้บริการ (Service Agreement)

ผู้ใช้บริการคลาวด์ยังคงมีหน้าที่กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยของการสื่อสาร การเลือกใช้มาตรการที่เหมาะสมกับระดับผลกระทบของข้อมูล และการตรวจสอบว่าผู้ให้บริการคลาวด์สามารถรองรับข้อกำหนดดังกล่าวได้ ขณะที่ผู้ให้บริการคลาวด์ควรจัดให้มีความสามารถด้านการรักษาความมั่นคงปลอดภัยของการถ่ายโอนข้อมูลและการแบ่งแยกเครือข่ายภายในขอบเขตความรับผิดชอบของตน พร้อมทั้งให้ข้อมูลหรือหลักฐานที่จำเป็นเพื่อสนับสนุนการประเมินของผู้ใช้บริการคลาวด์

การกำหนดความรับผิดชอบควรอาศัยหลักการแบ่งความรับผิดชอบ (Shared Responsibility Model) และผลการประเมินความเสี่ยง เพื่อให้มั่นใจว่ามาตรการควบคุมได้รับการกำหนดผู้รับผิดชอบอย่างครบถ้วน และไม่เกิดช่องว่างของการควบคุม (Control Gap)

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

2. สรุปข้อกำหนดและความรับผิดชอบ

หัวข้อ	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
5.2.7.1 นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)	กำหนดข้อกำหนดการถ่ายโอนข้อมูล เลือกช่องทางการถ่ายโอนที่เหมาะสม กำหนดมาตรการปกป้องข้อมูล และควบคุมการใช้สื่อทางกายภาพตามระดับความเสี่ยง	จัดให้มีความสามารถในการปกป้องข้อมูลระหว่างการถ่ายโอน สนับสนุนการกำหนดค่าที่มั่นคงปลอดภัย ระบุขอบเขตความรับผิดชอบ และจัดเตรียมข้อมูลหรือหลักฐานที่จำเป็นเกี่ยวกับบริการ
5.2.7.2 การแบ่งแยกในเครือข่าย (Segregation in Networks)	กำหนดข้อกำหนดด้านการแบ่งแยกเครือข่ายให้เหมาะสมกับระดับผลกระทบของข้อมูล ผลการประเมินความเสี่ยง และตรวจสอบว่าการแบ่งแยกของผู้ให้บริการสอดคล้องกับข้อกำหนดของหน่วยงาน	บังคับใช้การแบ่งแยกผู้เช่า (Tenant Isolation) การแบ่งแยกสภาพแวดล้อมการบริหารจัดการ และสนับสนุนการตรวจสอบประสิทธิผลของมาตรการแบ่งแยกเครือข่าย

3. หลักการประยุกต์ใช้ (Application Considerations)

ในการนำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยเครือข่ายไปประยุกต์ใช้ หน่วยงานควรพิจารณาปัจจัยดังต่อไปนี้

- รูปแบบบริการคลาวด์ (Cloud Service Model)
- ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
- ผลการประเมินความเสี่ยง (Risk Assessment)
- ขอบเขตความรับผิดชอบร่วม (Shared Responsibility)
- ความสามารถและข้อจำกัดของบริการคลาวด์
- ข้อกำหนดทางกฎหมาย กฎ ระเบียบ ข้อบังคับ และสัญญาที่เกี่ยวข้อง

ทั้งนี้ การเลือกใช้มาตรการควบคุมควรเป็นไปตามหลักการบริหารความเสี่ยง (Risk-based Approach) และไม่ควรกำหนดเทคโนโลยี ผลิตภัณฑ์ หรือสถาปัตยกรรมเฉพาะ เว้นแต่มีข้อกำหนดทางกฎหมายหรือผลการประเมินความเสี่ยงรองรับ

ร่างเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

5.2.8 การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)

การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ควรคำนึงถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตั้งแต่ระยะเริ่มต้น เพื่อให้การเลือกใช้ การพัฒนา การปรับปรุง และการนำระบบหรือบริการไปใช้งาน มีระดับการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับลักษณะการใช้งาน ความสำคัญของข้อมูล ผลกระทบ และความเสี่ยงที่เกี่ยวข้อง

สำหรับการจัดหาหรือเลือกใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ควรกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่จำเป็น และใช้ข้อกำหนดดังกล่าวเป็นเกณฑ์ในการประเมินว่าบริการของผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) สามารถตอบสนองความต้องการของหน่วยงานได้อย่างเพียงพอหรือไม่ โดย CSC ควรได้รับข้อมูลเกี่ยวกับความสามารถด้านความมั่นคงปลอดภัยของบริการจาก CSP ในระดับที่เหมาะสมต่อการประเมิน ขณะที่ CSP ควรให้ข้อมูลดังกล่าวโดยคำนึงถึงการป้องกันข้อมูลที่มีความอ่อนไหวด้านความมั่นคงปลอดภัย ซึ่งหากเปิดเผยโดยไม่เหมาะสมอาจก่อให้เกิดความเสี่ยงต่อบริการหรือโครงสร้างพื้นฐานของ CSP

หลักการดังกล่าวตรงกับข้อกำหนด 5.2.8.1 ของประกาศ ซึ่งกำหนดให้ CSC กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการใช้บริการคลาวด์ ประเมินว่าบริการสามารถตอบสนองข้อกำหนดดังกล่าวได้หรือไม่ และขอข้อมูลเกี่ยวกับความสามารถด้านความมั่นคงปลอดภัยจาก CSP ขณะที่ CSP มีหน้าที่ให้ข้อมูลที่จำเป็นโดยไม่เปิดเผยข้อมูลที่อาจเป็นประโยชน์ต่อบุคคลที่มีเจตนาร้าย

ในกรณีที่มีการพัฒนา ปรับแต่ง หรือเชื่อมต่อระบบหรือซอฟต์แวร์กับบริการคลาวด์ ควรนำหลักการพัฒนาที่มั่นคงปลอดภัย (Secure Development) มาประยุกต์ใช้ตามขอบเขตที่แต่ละฝ่ายสามารถควบคุมและรับผิดชอบได้ โดยพิจารณาความมั่นคงปลอดภัยเป็นส่วนหนึ่งของกระบวนการพัฒนา และกำหนดระดับความเข้มงวดของการดำเนินการให้เหมาะสมกับความสำคัญและความเสี่ยงของระบบ

ในกรณีที่ CSC ไม่ได้เป็นผู้พัฒนาระบบหรือไม่สามารถควบคุมกระบวนการพัฒนาของ CSP ได้โดยตรง การดำเนินการควรมุ่งเน้นการขอและพิจารณาข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของ CSP เพื่อให้มีความเชื่อมั่นในระดับที่เหมาะสมกับความเสี่ยงของบริการ โดยไม่จำเป็นต้องกำหนดวิธีการหรือมาตรการทางเทคนิคภายในของ CSP โดยตรง ทั้งนี้ สอดคล้องกับข้อ 5.2.8.2 ซึ่งกำหนดให้ CSC ขอข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัย และให้ CSP ให้ข้อมูลดังกล่าวภายใต้ขอบเขตที่สอดคล้องกับนโยบายการเปิดเผยข้อมูลของตน

การดำเนินการตามหัวข้อนี้จึงมุ่งเน้นสาระสำคัญ 2 ประการ ได้แก่

1. **การวิเคราะห์และกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ** (Information Security Requirements Analysis and Specification) เพื่อให้สามารถกำหนดความต้องการด้านความมั่นคงปลอดภัยและประเมินความสามารถของบริการคลาวด์ก่อนการเลือกใช้หรือใช้งานบริการ

ร่างเพื่อรับฟังความคิดเห็น Public Hearing ยังไม่ใช่ประกาศ

2. **การพัฒนาที่มั่นคงปลอดภัย** (Secure Development) เพื่อให้ CSC สามารถพิจารณาความเหมาะสมของกระบวนการพัฒนาที่เกี่ยวข้องกับบริการคลาวด์ และให้ CSP สามารถแสดงข้อมูลเกี่ยวกับกระบวนการพัฒนาที่ปลอดภัยได้ในระดับที่เหมาะสม

การนำแนวทางดังกล่าวไปปฏิบัติควรพิจารณาตามรูปแบบบริการคลาวด์ ขอบเขตบริการ ลักษณะและความสำคัญของระบบและข้อมูล ตลอดจนขอบเขตความรับผิดชอบของ CSC และ CSP โดยใช้แนวทางที่อิงความเสี่ยง (Risk-based Approach) และไม่ควรกำหนดมาตรการหรือเอกสารเพิ่มเติมเกินความจำเป็น หากกระบวนการหรือหลักฐานที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

หมายเหตุ

รายละเอียดของมาตรการควบคุมเฉพาะด้าน เช่น การควบคุมการเข้าถึง การเข้ารหัส การบันทึกเหตุการณ์ การรักษาความมั่นคงปลอดภัยของเครือข่าย การจัดการช่องโหว่ และการจัดการเหตุการณ์ ควรอ้างอิงข้อกำหนดและแนวทางในหัวข้อที่เกี่ยวข้องของประกาศ โดยไม่จำเป็นต้องกำหนดรายละเอียดซ้ำในหัวข้อ 5.2.8

5.2.8.1 การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

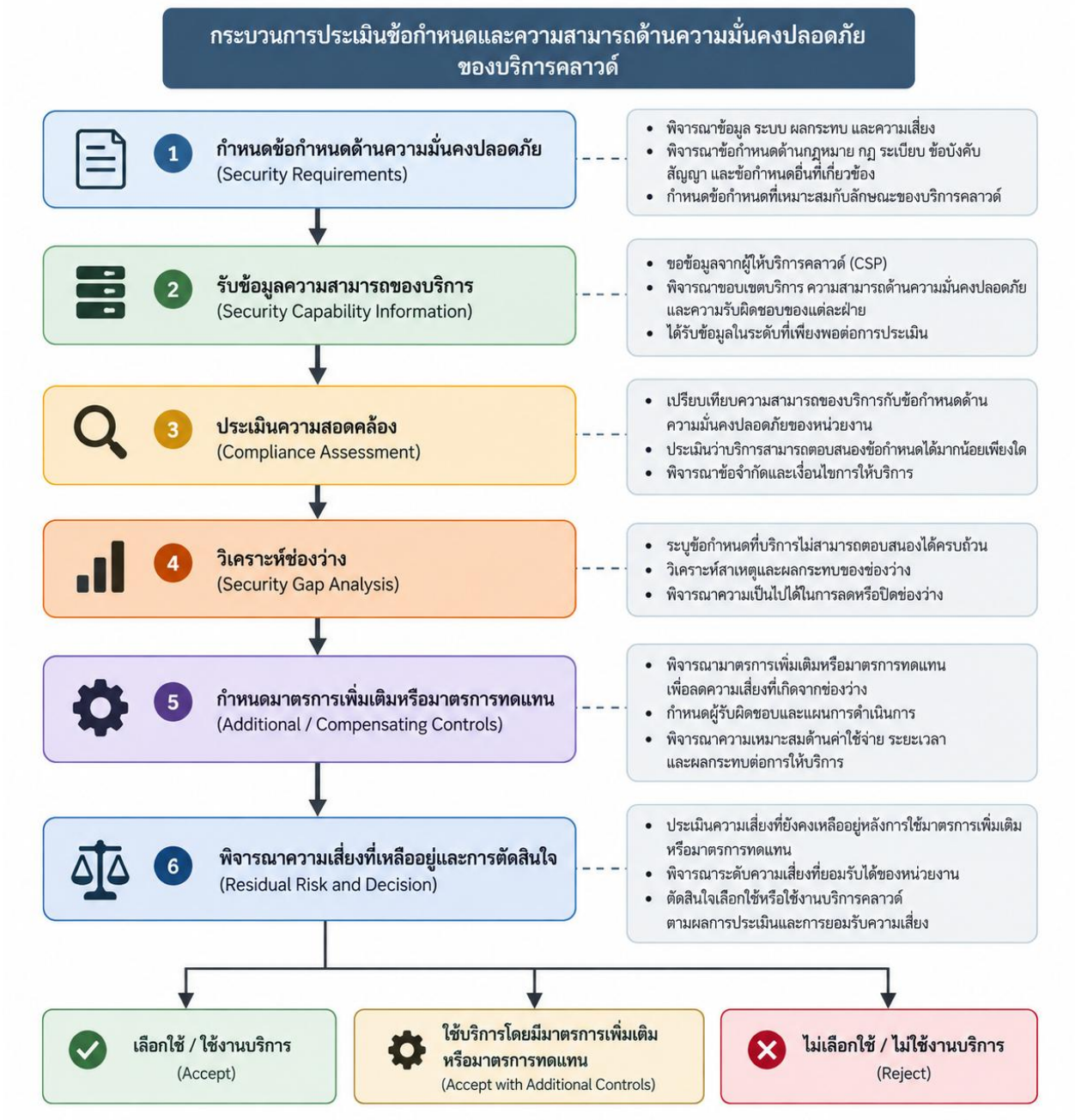
ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ จากนั้นประเมินว่าบริการของผู้ให้บริการคลาวด์ สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่ ข) สำหรับการประเมินนี้ ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจาก ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลแก่ ผู้ใช้บริการคลาวด์ เกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ตนใช้ ข้อมูลนี้ต้องเป็นข้อมูลโดยไม่เปิดเผยข้อมูลที่อาจเป็นประโยชน์ต่อบุคคลที่มีเจตนาร้าย

วัตถุประสงค์ (Objective)

เพื่อให้ผู้ใช้บริการคลาวด์สามารถกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสมกับระบบข้อมูล และลักษณะการใช้บริการคลาวด์ และใช้ข้อกำหนดดังกล่าวเป็นเกณฑ์ในการประเมินว่าบริการคลาวด์ที่พิจารณาเลือกใช้หรือใช้งานอยู่สามารถตอบสนองความต้องการด้านความมั่นคงปลอดภัยของหน่วยงานได้อย่างเพียงพอหรือไม่

การกำหนดข้อกำหนดควรพิจารณาจากความสำคัญของข้อมูลและระบบ ระดับผลกระทบ ความเสี่ยง ตลอดจนข้อกำหนดด้านกฎหมาย กฎ ระเบียบ ข้อบังคับ และพันธกรณีที่เกี่ยวข้อง โดย CSC ควรได้รับข้อมูลเกี่ยวกับความสามารถด้านความมั่นคงปลอดภัยของบริการจาก CSP ในระดับที่เพียงพอต่อการประเมิน

ร่างสำหรับประชาพิจารณ์ Public Hearing ร่างนี้ - ห้ามใช้อ้างอิง



กระบวนการประเมินข้อกำหนดและความสามารถด้านความมั่นคงปลอดภัยของบริการคลาวด์

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ควรกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศก่อนการจัดหา เลือกใช้ หรือเปลี่ยนแปลงบริการคลาวด์ที่มีนัยสำคัญ และประเมินความสามารถของบริการเทียบกับข้อกำหนดดังกล่าว

การดำเนินการไม่จำเป็นต้องจัดทำเป็นกระบวนการหรือเอกสารแยกต่างหาก หากหน่วยงานมีกระบวนการจัดหา การประเมินความเสี่ยง การกำหนดความต้องการของระบบ หรือการประเมินผู้ให้บริการที่สามารถรองรับประเด็นดังกล่าวได้อย่างเพียงพอ

CSC ควรดำเนินการอย่างน้อยในประเด็นต่อไปนี้

1. การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Security Requirements)

CSC ควรกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยให้เหมาะสมกับระบบ ข้อมูล และบริการคลาวด์ที่จะนำมาใช้ โดยพิจารณาอย่างน้อยจาก

ประเด็นที่พิจารณา	แนวทาง
ความสำคัญของข้อมูลและระบบ	พิจารณาความต้องการด้านการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้
ผลกระทบและความเสี่ยง	พิจารณาระดับผลกระทบและผลการประเมินความเสี่ยงที่เกี่ยวข้อง
กฎหมายและข้อกำหนด	พิจารณากฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา และข้อกำหนดเฉพาะที่เกี่ยวข้อง
มาตรการด้านความมั่นคงปลอดภัย	ระบุความสามารถหรือมาตรการที่บริการจำเป็นต้องรองรับตามความเสี่ยงและลักษณะการใช้งาน

ตัวอย่างเช่น หากหน่วยงานมีข้อกำหนดเกี่ยวกับการควบคุมการเข้าถึง การเข้ารหัส การบันทึกเหตุการณ์ หรือความมั่นคงปลอดภัยของเครือข่าย ควรระบุเป็นความต้องการที่บริการคลาวด์ต้องรองรับ ส่วนรายละเอียดของมาตรการให้พิจารณาตามข้อกำหนดในหัวข้อที่เกี่ยวข้องของประกาศ

2. การขอข้อมูลความสามารถด้านความมั่นคงปลอดภัยจาก CSP (Security Capability Information)

CSC ควรขอหรือรวบรวมข้อมูลจาก CSP ในระดับที่เพียงพอต่อการประเมินว่าบริการสามารถตอบสนองข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ได้หรือไม่

ข้อมูลที่ใช้ประกอบการประเมินอาจอยู่ในรูปแบบที่แตกต่างกันตามลักษณะของบริการและระดับความเสี่ยง เช่น

- เอกสารอธิบายความสามารถด้านความมั่นคงปลอดภัยของบริการ
- ข้อกำหนดหรือรายละเอียดทางเทคนิคของบริการ
- ข้อตกลงการให้บริการหรือเงื่อนไขการให้บริการ
- รายงานหรือผลการประเมินจากหน่วยงานอิสระ
- การรับรองตามมาตรฐานที่เกี่ยวข้อง
- ข้อมูลหรือหลักฐานอื่นที่ CSP จัดให้เพื่อสนับสนุนการประเมิน

3. การประเมินความสามารถของบริการคลาวด์ (Cloud Service Security Capability Assessment)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

เมื่อกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยและได้รับข้อมูลจาก CSP แล้ว CSC ควรประเมินว่าความสามารถของบริการสามารถตอบสนองต่อข้อกำหนดที่กำหนดไว้ได้หรือไม่

การประเมินอาจจำแนกผลเป็น

ผลการประเมิน	ความหมาย
สอดคล้อง (Compliant)	บริการสามารถตอบสนองข้อกำหนดที่กำหนดไว้ได้อย่างเพียงพอ
สอดคล้องบางส่วน (Partially Compliant)	บริการสามารถตอบสนองข้อกำหนดได้บางส่วน หรือจำเป็นต้องมีมาตรการเพิ่มเติม
ไม่สอดคล้อง (Non-Compliant)	บริการไม่สามารถตอบสนองข้อกำหนดที่กำหนดไว้ได้

4. การจัดการช่องว่างและความเสี่ยงที่เหลืออยู่ (Security Gap and Residual Risk)

หากผลการประเมินพบว่าบริการตอบสนองข้อกำหนดได้เพียงบางส่วนหรือไม่สามารถตอบสนองข้อกำหนดบางประการได้ CSC ควรพิจารณาความสำคัญของช่องว่างดังกล่าวและดำเนินการตามความเหมาะสม เช่น

- กำหนดมาตรการเพิ่มเติมที่อยู่ภายใต้ความรับผิดชอบของ CSC
- พิจารณามาตรการทดแทน (Compensating Controls)
- ขอให้ CSP ให้ข้อมูลหรือดำเนินการเพิ่มเติม หากอยู่ภายใต้ขอบเขตบริการ
- พิจารณาความเสี่ยงที่เหลืออยู่ก่อนการตัดสินใจใช้บริการ

หากความเสี่ยงที่เหลืออยู่สูงกว่าระดับที่หน่วยงานยอมรับได้ ควรดำเนินการจัดการความเสี่ยงตามกระบวนการบริหารความเสี่ยงของหน่วยงานก่อนตัดสินใจใช้หรือดำเนินการต่อกับบริการดังกล่าว

กระบวนการโดยสรุป

กำหนดข้อกำหนดด้านความมั่นคงปลอดภัย

(Security Requirements)

↓

ขอข้อมูลความสามารถด้านความมั่นคงปลอดภัยจาก CSP

(Security Capability Information)

↓

ประเมินความสามารถของบริการ

(Security Capability Assessment)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

↓

ระบุช่องว่างและกำหนดมาตรการที่เหมาะสม

(Security Gap and Additional / Compensating Controls)

↓

พิจารณาความเสี่ยงที่เหลืออยู่และตัดสินใจ

(Residual Risk and Decision)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักฐานที่ควรมี (Recommended Evidence)

เพื่อแสดงถึงการนำข้อกำหนดไปปฏิบัติ CSC ควรมีหลักฐานที่เหมาะสมกับลักษณะและความเสี่ยงของบริการ โดยอาจประกอบด้วย

- ข้อกำหนดของระบบหรือบริการที่มีข้อกำหนดด้านความมั่นคงปลอดภัย
- ผลการประเมินความเสี่ยงที่เกี่ยวข้อง
- ข้อมูลความสามารถด้านความมั่นคงปลอดภัยที่ได้รับจาก CSP
- ผลการประเมินหรือเปรียบเทียบข้อกำหนดของ CSC กับความสามารถของ CSP
- บันทึกการพิจารณาช่องว่าง มาตรการเพิ่มเติมหรือมาตรการทดแทน และความเสี่ยงที่เหลืออยู่ ตามความเหมาะสม
- หลักฐานการพิจารณาหรืออนุมัติการเลือกใช้บริการ ตามกระบวนการของหน่วยงาน

ทั้งนี้ ไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มแยกต่างหากสำหรับข้อ 5.2.8.1 หากหน่วยงานมีเอกสาร ระบบหรือกระบวนการที่สามารถแสดงหลักฐานดังกล่าวได้อย่างเพียงพอ

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ควรให้ข้อมูลเกี่ยวกับความสามารถด้านความมั่นคงปลอดภัยสารสนเทศของบริการแก่ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ในระดับที่เพียงพอต่อการประเมินว่าบริการสามารถตอบสนองข้อกำหนดด้านความมั่นคงปลอดภัยของ CSC ได้หรือไม่

การให้ข้อมูลควรคำนึงถึงความสมดุลระหว่าง **ความเพียงพอของข้อมูลสำหรับการประเมิน** และ **การป้องกันข้อมูลที่มีความอ่อนไหวด้านความมั่นคงปลอดภัย** โดย CSP ไม่จำเป็นต้องเปิดเผยรายละเอียดภายในที่อาจเพิ่มความเสี่ยงต่อระบบ โครงสร้างพื้นฐาน หรือมาตรการรักษาความมั่นคงปลอดภัยของตน

1. การให้ข้อมูลความสามารถด้านความมั่นคงปลอดภัย

CSP ควรจัดให้มีข้อมูลที่สามารถใช้ประกอบการประเมินความสามารถด้านความมั่นคงปลอดภัยของบริการ โดยรายละเอียดและระดับของข้อมูลควรเหมาะสมกับประเภทของบริการ ขอบเขตบริการ และความเสี่ยงที่เกี่ยวข้อง

ข้อมูลดังกล่าวอาจครอบคลุมประเด็น เช่น

ประเด็น	**แนวทาง**
ขอบเขตบริการ	ระบุขอบเขตของบริการและองค์ประกอบที่ CSP รับผิดชอบ
ความสามารถด้านความมั่นคงปลอดภัย	ให้ข้อมูลเกี่ยวกับมาตรการหรือความสามารถด้านความมั่นคงปลอดภัยที่บริการรองรับ
บทบาทและความรับผิดชอบ	ระบุขอบเขตความรับผิดชอบของ CSP และส่วนที่ CSC ต้องดำเนินการเอง
ข้อจำกัดของบริการ	ระบุข้อจำกัดที่อาจมีผลต่อการปฏิบัติตามข้อกำหนดของ CSC ตามความเหมาะสม
หลักฐานประกอบ	ให้เอกสาร รายงาน การรับรอง หรือหลักฐานอื่นที่สามารถใช้สนับสนุนการประเมินได้ ตามความเหมาะสม

ทั้งนี้ ตารางดังกล่าวเป็นแนวทางสำหรับการให้ข้อมูล มิได้หมายความว่า CSP ต้องจัดทำเอกสารใหม่ทุกประเภท หากข้อมูลหรือหลักฐานที่มีอยู่สามารถสนับสนุนการประเมินของ CSC ได้อย่างเพียงพอ

2. ความเพียงพอและความเหมาะสมของข้อมูล

ข้อมูลที่ CSP ให้แก่ CSC ควรมีรายละเอียดเพียงพอให้ CSC สามารถพิจารณาได้ว่า

รูปข้อกำหนดของ CSC ⟶ ความสามารถของบริการ ⟶ ช่องว่างหรือข้อจำกัด ⟶ ความเสี่ยงที่ต้องพิจารณา

CSP ไม่จำเป็นต้องรับรองว่าบริการของตนสามารถตอบสนองข้อกำหนดทุกประการของ CSC แต่ควรให้ข้อมูลอย่างเพียงพอเพื่อให้ CSC สามารถประเมินและตัดสินใจได้อย่างเหมาะสม

ในกรณีที่ข้อกำหนดบางประการอยู่นอกขอบเขตความรับผิดชอบของ CSP หรือขึ้นอยู่กับการกำหนดค่าและการใช้งานของ CSC ควรมีข้อมูลที่ทำให้สามารถเข้าใจขอบเขตความรับผิดชอบดังกล่าวได้อย่างเหมาะสม

3. การป้องกันข้อมูลที่มีความอ่อนไหวด้านความมั่นคงปลอดภัย

การให้ข้อมูลแก่ CSC ต้องไม่ส่งผลให้เกิดการเปิดเผยข้อมูลที่อาจถูกนำไปใช้เพื่อหลีกเลี่ยง ลดประสิทธิผล หรือโจมตีมาตรการรักษาความมั่นคงปลอดภัยของ CSP

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ข้อมูลที่ควรพิจารณาจำกัดการเปิดเผยอาจรวมถึง รายละเอียดการกำหนดค่าความมั่นคงปลอดภัยภายใน ข้อมูลประจำตัวหรือข้อมูลลับ รายละเอียดเชิงลึกของกลไกการป้องกัน ตลอดจนรายละเอียดของช่องโหว่ที่ยังไม่ได้รับการแก้ไข

หากจำเป็นต้องเปิดเผยข้อมูลที่มีความอ่อนไหวเพื่อประกอบการประเมิน CSP ควรกำหนดมาตรการที่เหมาะสมในการควบคุมการเข้าถึง การส่งต่อ การจัดเก็บ และการใช้ข้อมูล โดยจำกัดการเปิดเผยเฉพาะผู้ที่มีความจำเป็นต้องใช้ข้อมูลดังกล่าว

ดังนั้น หลักการสำหรับ CSP สามารถสรุปได้เป็น

ให้ข้อมูลที่เพียงพอต่อการประเมิน

(Sufficient Security Information)

↓

แสดงขอบเขตและความสามารถของบริการ

(Service Scope and Security Capability)

↓

ระบุข้อจำกัดและความรับผิดชอบที่เกี่ยวข้อง

(Limitations and Responsibilities)

↓

ป้องกันข้อมูลที่มีความอ่อนไหวด้านความมั่นคงปลอดภัย

(Protection of Security-Sensitive Information)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักฐานที่ควรมี (Recommended Evidence)

เพื่อสนับสนุนการแสดงการปฏิบัติตามข้อกำหนด CSP ควรสามารถแสดงหลักฐานตามความเหมาะสม เช่น เอกสารอธิบายความสามารถด้านความมั่นคงปลอดภัยของบริการ ขอบเขตและรายละเอียดของบริการ ข้อมูลเกี่ยวกับบทบาทและความรับผิดชอบ ข้อตกลงหรือเงื่อนไขการให้บริการ รายงานหรือการรับรองจากหน่วยงานอิสระ และแนวทางหรือนโยบายเกี่ยวกับการเปิดเผยข้อมูลด้านความมั่นคงปลอดภัย

ไม่จำเป็นต้องมีหลักฐานทุกประเภทดังกล่าว หากข้อมูลที่มีอยู่สามารถแสดงความสามารถของบริการและสนับสนุนการประเมินของ CSC ได้อย่างเพียงพอ

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดตาม 5.2.8.1 ไปปฏิบัติควรดำเนินการโดยเชื่อมโยง **ข้อกำหนดด้านความมั่นคงปลอดภัยของ CSC** กับ **ความสามารถด้านความมั่นคงปลอดภัยของบริการที่ CSP จัดให้** เพื่อให้สามารถระบุช่องว่างและพิจารณาความเสี่ยงก่อนการเลือกใช้หรือใช้งานบริการคลาวด์

การดำเนินการสามารถประยุกต์ใช้ร่วมกับกระบวนการที่หน่วยงานมีอยู่เดิมได้ โดยไม่จำเป็นต้องสร้างกระบวนการใหม่ หากกระบวนการเดิมสามารถรองรับการกำหนดข้อกำหนด การประเมินความสามารถของบริการและการพิจารณาความเสี่ยงได้อย่างเพียงพอ

ขั้นตอน	CSC	CSP	ผลลัพธ์ที่คาดหวัง
1. กำหนดข้อกำหนด	กำหนดข้อกำหนดตามข้อมูลระบบ ความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง	—	ข้อกำหนดด้านความมั่นคงปลอดภัย
2. ขอและให้ข้อมูล	ขอข้อมูลที่จำเป็นต่อการประเมิน	ให้ข้อมูลความสามารถของบริการในระดับที่เหมาะสม	ข้อมูลความสามารถของบริการ
3. ประเมินความสอดคล้อง	เปรียบเทียบข้อกำหนดกับความสามารถของบริการ	ให้ข้อมูลเพิ่มเติมตามความเหมาะสม	ผลการประเมิน
4. จัดการช่องว่าง	พิจารณามาตรการเพิ่มเติม มาตรการทดแทน หรือแนวทางจัดการความเสี่ยง	สนับสนุนตามขอบเขตบริการและความรับผิดชอบ	ช่องว่างและแนวทางจัดการ
5. พิจารณาความเสี่ยงและตัดสินใจ	พิจารณาความเสี่ยงที่เหลืออยู่และตัดสินใจตามกระบวนการของหน่วยงาน	—	ผลการพิจารณาเลือกใช้หรือใช้งานบริการ

การประยุกต์ใช้ตามระดับความเสี่ยง

ระดับรายละเอียดของการประเมินควรเหมาะสมกับความสำคัญและความเสี่ยงของระบบหรือบริการ โดยไม่จำเป็นต้องใช้ระดับการประเมินเดียวกันกับบริการคลาวด์ทุกประเภท

สำหรับบริการที่มีความเสี่ยงไม่สูง อาจใช้ข้อมูลมาตรฐานของ CSP ข้อกำหนดการให้บริการ เอกสารแสดงความสามารถของบริการ หรือการรับรองที่เกี่ยวข้องเป็นข้อมูลประกอบการประเมินได้

สำหรับบริการที่มีความสำคัญหรือมีความเสี่ยงสูง อาจจำเป็นต้องขอข้อมูลหรือหลักฐานเพิ่มเติม เพื่อให้สามารถประเมินประเด็นที่มีความสำคัญต่อหน่วยงานได้อย่างเพียงพอ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

ดังนั้น แนวทางนี้จึง **ไม่กำหนดว่าทุกองค์กรต้องตรวจสอบ CSP ในระดับเดียวกัน** แต่ให้ระดับการประเมินสัมพันธ์กับความเสี่ยงของการใช้บริการ

การใช้กระบวนการและเอกสารที่มีอยู่เดิม

CSC สามารถนำกระบวนการที่มีอยู่เดิม เช่น การจัดหา การประเมินผู้ให้บริการ การประเมินความเสี่ยง การทบทวนสัญญา หรือการอนุมัติระบบสารสนเทศ มาประยุกต์ใช้เพื่อรองรับข้อกำหนดตาม 5.2.8.1 ได้ โดยไม่จำเป็นต้องจัดทำกระบวนการแยกสำหรับบริการคลาวด์ หากกระบวนการดังกล่าวสามารถแสดงได้ว่า

มีการกำหนดข้อกำหนด ⟶ ได้รับข้อมูลจาก CSP ⟶ มีการประเมิน ⟶ มีการจัดการช่องว่างหรือความเสี่ยง ⟶ มีผลการตัดสินใจ

หลักฐานที่ควรมี (Recommended Evidence)

ประเด็น	**ตัวอย่างหลักฐาน**
ข้อกำหนดด้านความมั่นคงปลอดภัย	Security Requirements / TOR / Specification / Requirement Checklist
ความเสี่ยง	Risk Assessment / Risk Register ที่เกี่ยวข้อง
ความสามารถของ CSP	Security Capability Information / Service Documentation
ขอบเขตความรับผิดชอบ	Service Agreement / Shared Responsibility Information
การประเมิน	Cloud Security Assessment / Supplier Assessment / Checklist
ช่องว่าง	Security Gap / Compensating Control
ความเสี่ยงที่เหลืออยู่	Residual Risk Assessment หรือบันทึกการพิจารณาที่เกี่ยวข้อง
การตัดสินใจ	Approval / Procurement Record / Risk Acceptance ตามความเหมาะสม

ทั้งนี้ ไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มใหม่ หากสามารถใช้ระบบ กระบวนการ หรือเอกสารที่มีอยู่เดิมเป็นหลักฐานได้อย่างเพียงพอ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

5.2.8.2 นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของ ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลเกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาความปลอดภัยของตนในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล

สาระสำคัญของข้อกำหนดนี้มุ่งให้ผู้ใช้บริการคลาวด์ (CSC) สามารถได้รับข้อมูลที่เพียงพอเพื่อพิจารณาว่า ผู้ให้บริการคลาวด์ (CSP) มีขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยหรือไม่ ขณะที่ CSP มีหน้าที่ให้ข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติดังกล่าวภายใต้ขอบเขตที่สามารถเปิดเผยได้

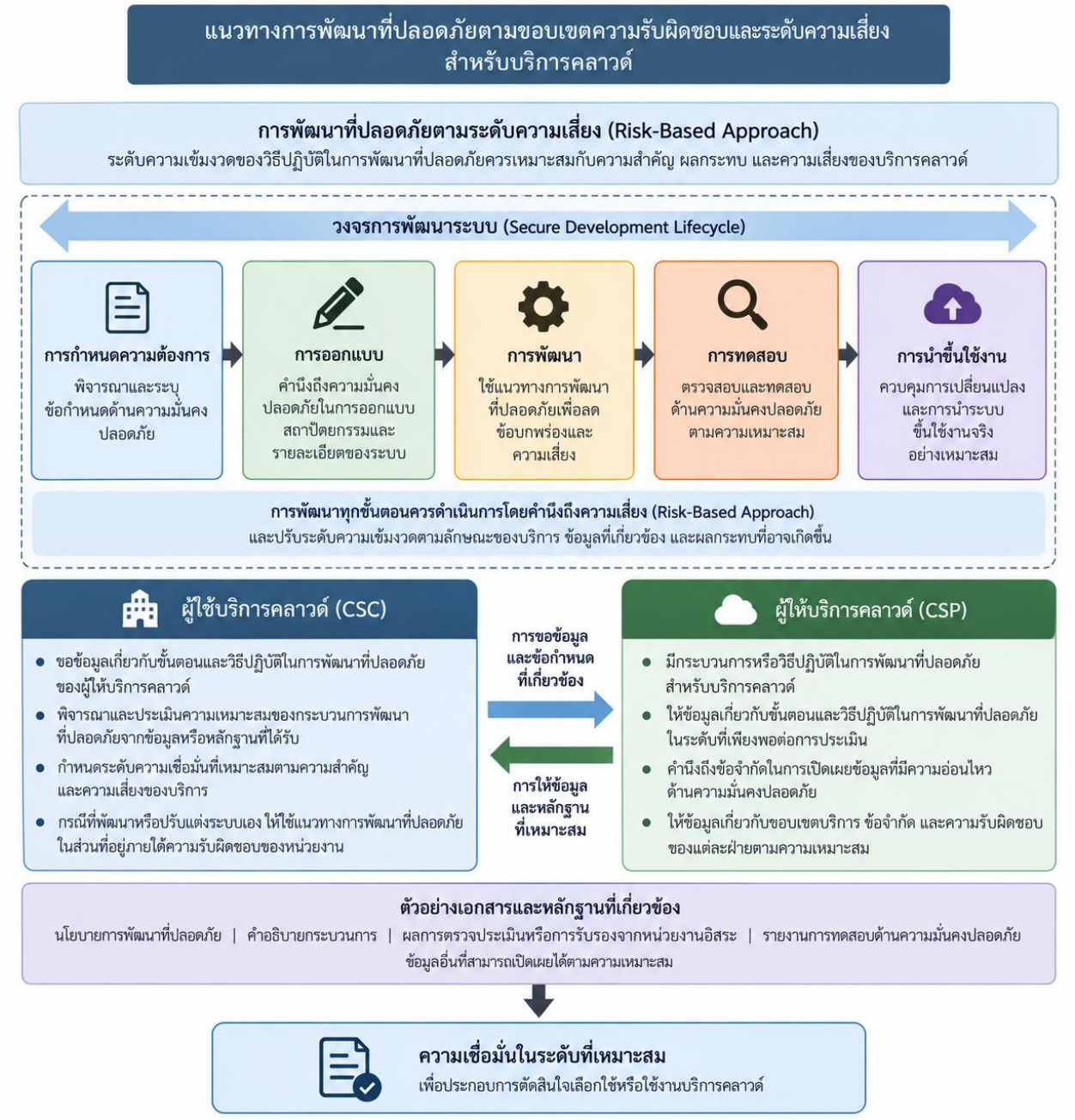
ดังนั้น การนำข้อกำหนดนี้ไปปฏิบัติ **ไม่ควรตีความว่า CSC ต้องเข้าไปกำหนดหรือควบคุมกระบวนการพัฒนาภายในของ CSP** แต่ควรมุ่งเน้นการสร้างความเชื่อมั่นว่าบริการคลาวด์ที่เลือกใช้ได้รับการพัฒนาโดยคำนึงถึงความมั่นคงปลอดภัยอย่างเหมาะสม

วัตถุประสงค์ (Objective)

เพื่อให้ CSC สามารถพิจารณาความเหมาะสมของแนวทางการพัฒนาที่ปลอดภัยของ CSP โดยอาศัยข้อมูลหรือหลักฐานที่ CSP สามารถเปิดเผยได้ และเพื่อให้ CSP สามารถแสดงให้เห็นว่ามีกระบวนการหรือวิธีปฏิบัติด้านการพัฒนาที่คำนึงถึงความมั่นคงปลอดภัยอย่างเหมาะสมกับลักษณะและความเสี่ยงของบริการ

สำหรับกรณีที่ CSC มีการพัฒนา ปรับแต่ง หรือเชื่อมต่อระบบกับบริการคลาวด์ภายใต้ความรับผิดชอบของตนเอง CSC ควรนำหลักการพัฒนาที่ปลอดภัยมาประยุกต์ใช้ตามความเหมาะสมกับลักษณะของระบบและระดับความเสี่ย

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



แนวทางการพัฒนาที่ปลอดภัยตามขอบเขตความรับผิดชอบและระดับความเสี่ยงสำหรับบริการคลาวด์

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

CSC ควรขอและพิจารณาข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของ CSP เพื่อให้สามารถประเมินได้ว่ากระบวนการดังกล่าวมีความเหมาะสมกับลักษณะ ความสำคัญ และความเสี่ยงของบริการคลาวด์ที่หน่วยงานประสงค์จะใช้หรือใช้งานอยู่

1. การขอข้อมูลเกี่ยวกับการพัฒนาที่ปลอดภัย

CSC ควรขอหรือรวบรวมข้อมูลที่สามารถแสดงให้เห็นว่า CSP มีแนวทางหรือกระบวนการสำหรับการพัฒนาที่ปลอดภัย โดยไม่จำเป็นต้องกำหนดรูปแบบของหลักฐานไว้ตายตัว

ข้อมูลที่ใช้ประกอบการพิจารณาอาจเป็นนโยบายหรือคำอธิบายกระบวนการพัฒนาที่ปลอดภัย เอกสารเกี่ยวกับวงจรการพัฒนาระบบที่ CSP สามารถเปิดเผยได้ ผลการตรวจประเมินหรือการรับรองจากหน่วยงานอิสระ รายงานการทดสอบด้านความมั่นคงปลอดภัย หรือข้อมูลอื่นที่สามารถสร้างความเชื่อมั่นได้อย่างเหมาะสม

CSC ไม่จำเป็นต้องได้รับเอกสารภายในหรือรายละเอียดทางเทคนิคทั้งหมดของ CSP หากข้อมูลที่ได้รับเพียงพอสำหรับการประเมินตามระดับความเสี่ยงของบริการ

2. การพิจารณาความเหมาะสมของกระบวนการพัฒนาที่ปลอดภัย

CSC ควรพิจารณาข้อมูลที่ได้รับจาก CSP เพื่อให้เกิดความเชื่อมั่นในระดับที่เหมาะสมว่า มีการคำนึงถึงความมั่นคงปลอดภัยในกระบวนการพัฒนาบริการ

การพิจารณาอาจครอบคลุมวงจรสำคัญของการพัฒนา เช่น

ขั้นตอน	ประเด็นที่ควรพิจารณาในระดับหลักการ
การกำหนดความต้องการ	มีการนำข้อกำหนดด้านความมั่นคงปลอดภัยมาพิจารณา
การออกแบบ	มีการพิจารณาความเสี่ยงและความมั่นคงปลอดภัยในการออกแบบ
การพัฒนา	มีวิธีปฏิบัติเพื่อลดข้อบกพร่องหรือช่องโหว่ที่เกิดจากการพัฒนา
การทดสอบ	มีการตรวจสอบหรือทดสอบด้านความมั่นคงปลอดภัยตามความเหมาะสม
การนำขึ้นใช้งาน	มีการควบคุมก่อนนำระบบหรือการเปลี่ยนแปลงขึ้นใช้งานจริง

3. การประเมินตามระดับความเสี่ยง

ระดับรายละเอียดของการประเมินควรสัมพันธ์กับความสำคัญและความเสี่ยงของบริการ โดยไม่จำเป็นต้องขอหลักฐานในระดับเดียวกันสำหรับบริการคลาวด์ทุกประเภท

สำหรับบริการที่มีความเสี่ยงไม่สูง CSC อาจพิจารณาข้อมูลมาตรฐานที่ CSP เปิดเผย คำอธิบายกระบวนการพัฒนา การรับรอง หรือรายงานจากหน่วยงานอิสระที่เกี่ยวข้องได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

สำหรับบริการที่มีความสำคัญหรือมีความเสี่ยงสูง CSC อาจพิจารณาขอข้อมูลหรือหลักฐานเพิ่มเติมเกี่ยวกับกระบวนการพัฒนาและการทดสอบด้านความมั่นคงปลอดภัย เพื่อให้เกิดความเชื่อมั่นในระดับที่เหมาะสม

ทั้งนี้ ไม่จำเป็นต้องกำหนดระดับความเข้มงวดของกระบวนการพัฒนาและการประเมินให้เท่ากันสำหรับทุกระบบหรือบริการ โดยควรกำหนดระดับการดำเนินการให้สัมพันธ์กับความสำคัญ ผลกระทบ และความเสี่ยงที่เกี่ยวข้อง

4. กรณี CSC เป็นผู้พัฒนาหรือปรับแต่งระบบ

ในกรณีที่ CSC พัฒนา ปรับแต่ง หรือเชื่อมต่อระบบหรือซอฟต์แวร์กับบริการคลาวด์ และกิจกรรมดังกล่าวอยู่ภายใต้ความรับผิดชอบหรือการควบคุมของ CSC หน่วยงานควรนำแนวทางการพัฒนาที่ปลอดภัยมาประยุกต์ใช้กับส่วนที่ตนรับผิดชอบ โดยกำหนดระดับความเข้มงวดให้เหมาะสมกับความสำคัญ ผลกระทบ และความเสี่ยงของระบบ

อย่างน้อยควรพิจารณาให้ข้อกำหนดด้านความมั่นคงปลอดภัยได้รับการนำเข้าสู่กระบวนการพัฒนา มีการพิจารณาความมั่นคงปลอดภัยในการออกแบบและพัฒนา มีการตรวจสอบหรือทดสอบก่อนนำระบบขึ้นใช้งาน และมีการอนุมัติการนำระบบหรือการเปลี่ยนแปลงที่สำคัญขึ้นใช้งานตามกระบวนการของหน่วยงาน

หลักฐานที่ควรมี (Recommended Evidence)

ประเด็น	ตัวอย่างหลักฐาน
การกำหนดแนวทางพัฒนาที่ปลอดภัย	Secure Development Policy / Secure SDLC Description
ข้อมูลจาก CSP	CSP Security / Secure Development Documentation
การประเมินของ CSC	Supplier Assessment / Cloud Security Assessment
การตรวจประเมินจากหน่วยงานอิสระ	Certification / Independent Assessment Report
การทดสอบด้านความมั่นคงปลอดภัย	Security Test Summary / Assessment Report ตามความเหมาะสม
กรณี CSC พัฒนาเอง	System Requirements / Design Review / Code Review / Security Test / Release Approval ตามความเหมาะสม

ทั้งนี้ ไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มใหม่ หากสามารถใช้เอกสาร ระบบ หรือหลักฐานจากกระบวนการที่มีอยู่เพื่อแสดงการดำเนินการได้อย่างเพียงพอ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

CSP ควรสามารถให้ข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของบริการแก่ CSC ในระดับที่เพียงพอต่อการพิจารณา โดยคำนึงถึงนโยบายและข้อจำกัดในการเปิดเผยข้อมูลของ CSP

1. การมีแนวทางหรือกระบวนการพัฒนาที่ปลอดภัย

CSP ควรมีกระบวนการหรือวิธีปฏิบัติที่ทำให้ความมั่นคงปลอดภัยได้รับการพิจารณาอย่างเหมาะสมตลอดวงจรการพัฒนาบริการ

แนวทางดังกล่าวอาจครอบคลุมการกำหนดความต้องการ การออกแบบ การพัฒนา การทดสอบ และการนำขึ้นใช้งาน โดยระดับของมาตรการควรเหมาะสมกับลักษณะและความเสี่ยงของบริการ

2. การให้ข้อมูลแก่ CSC

CSP ควรให้ข้อมูลเกี่ยวกับกระบวนการพัฒนาที่ปลอดภัยในระดับที่ CSC สามารถนำไปประกอบการประเมินได้ โดยข้อมูลอาจอยู่ในรูปของคำอธิบายกระบวนการ นโยบาย มาตรฐานหรือแนวทางที่ใช้ ผลการตรวจประเมิน การรับรอง หรือหลักฐานอื่นที่เหมาะสม

การให้ข้อมูลไม่จำเป็นต้องเปิดเผยรายละเอียดของกระบวนการพัฒนาภายในทั้งหมด แต่ควรเพียงพอให้ CSC สามารถพิจารณาความเหมาะสมของกระบวนการได้ตามระดับความเสี่ยงของบริการ

3. การจำกัดการเปิดเผยข้อมูล

CSP สามารถจำกัดการเปิดเผยข้อมูลที่มีความอ่อนไหว หรือข้อมูลที่การเปิดเผยอาจเพิ่มความเสี่ยงต่อบริการ ระบบ หรือกระบวนการพัฒนาของ CSP ได้ โดยควรให้ข้อมูลในระดับที่ยังสามารถสนับสนุนการประเมินของ CSC ได้อย่างเหมาะสม

ในกรณีที่ไม่สามารถเปิดเผยรายละเอียดโดยตรง อาจใช้หลักฐานในรูปแบบอื่นที่สามารถสร้างความเชื่อมั่นได้ เช่น ผลการตรวจประเมินหรือการรับรองจากหน่วยงานอิสระ ตามความเหมาะสม

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การดำเนินการตามข้อ 5.2.8.2 ควรใช้แนวทางตามระดับความเสี่ยง โดย CSC และ CSP ควรดำเนินการตามขอบเขตความรับผิดชอบของตน ดังนี้

CSC กำหนดระดับความเชื่อมั่นที่ต้องการ

↓

CSC ขอข้อมูลเกี่ยวกับการพัฒนาที่ปลอดภัยจาก CSP

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

↓

CSP ให้ข้อมูลหรือหลักฐานในขอบเขตที่สามารถเปิดเผยได้

↓

CSC พิจารณาความเหมาะสมตามความสำคัญและความเสี่ยงของบริการ

↓

หากข้อมูลไม่เพียงพอ ให้ขอข้อมูลเพิ่มเติมหรือพิจารณาความเสี่ยงก่อนตัดสินใจ

สำหรับส่วนของระบบที่ CSC เป็นผู้พัฒนา ปรับแต่ง หรือควบคุมเอง ให้ CSC ใช้กระบวนการพัฒนาที่ปลอดภัยของหน่วยงานตามระดับความเสี่ยง โดยสามารถใช้กระบวนการและหลักฐานที่มีอยู่เดิมได้ ไม่จำเป็นต้องสร้างกระบวนการ Secure SDLC สำหรับคลาวด์แยกต่างหาก หากกระบวนการเดิมครอบคลุมอย่างเพียงพอ

หลักฐานที่ควรมี (Recommended Evidence)

ฝ่าย	ตัวอย่างหลักฐาน
CSC	บันทึกการขอหรือรวบรวมข้อมูล Secure Development ของ CSP
CSC	ผลการประเมิน CSP หรือ Supplier/Cloud Security Assessment
CSC	ผลการพิจารณาความเสี่ยง หากมีข้อจำกัดหรือข้อมูลไม่เพียงพอ
CSP	Secure Development Policy หรือคำอธิบายกระบวนการที่สามารถเปิดเผยได้
CSP	รายงานการตรวจประเมิน การรับรอง หรือหลักฐานที่เกี่ยวข้อง
CSC กรณีพัฒนาเอง	หลักฐานจากกระบวนการพัฒนาและทดสอบตามความเหมาะสม

ไม่จำเป็นต้องมีหลักฐานทุกรายการ และไม่จำเป็นต้องจัดทำเอกสารใหม่ หากหลักฐานที่มีอยู่สามารถแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

สรุปข้อกำหนดและความรับผิดชอบ (System Acquisition, Development, and Maintenance Requirements and Responsibility Summary)

การดำเนินการตามข้อ 5.2.8 ควรพิจารณาความรับผิดชอบระหว่างผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) ให้สอดคล้องกับลักษณะบริการ ขอบเขตบริการ และความรับผิดชอบของแต่ละฝ่าย

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้งานอื่น

สาระสำคัญแบ่งออกเป็น 2 ด้าน ได้แก่

5.2.8.1 การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยของ CSC และการประเมินความสามารถของบริการคลาวด์ และ

5.2.8.2 การพิจารณากระบวนการพัฒนาที่ปลอดภัย โดย CSC ขอและพิจารณาข้อมูลที่เกี่ยวข้อง ขณะที่ CSP ให้ข้อมูลภายใต้ขอบเขตที่สามารถเปิดเผยได้

1. สรุปความรับผิดชอบของ CSC และ CSP

ประเด็น	CSC	CSP
กำหนดข้อกำหนดด้านความมั่นคงปลอดภัย	**รับผิดชอบหลัก** โดยกำหนดตามระบบข้อมูล ความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง	สนับสนุนข้อมูลเกี่ยวกับความสามารถของบริการ
ขอข้อมูลความสามารถด้านความมั่นคงปลอดภัย	**รับผิดชอบหลัก** ในการกำหนดข้อมูลที่จำเป็นต่อการประเมิน	ให้ข้อมูลตามขอบเขตที่เหมาะสม
ให้ข้อมูลความสามารถของบริการ	รับและนำข้อมูลมาใช้ประกอบการประเมิน	**รับผิดชอบหลัก**
ประเมินบริการเทียบกับข้อกำหนด	**รับผิดชอบหลัก**	สนับสนุนข้อมูลเพิ่มเติมตามความเหมาะสม
พิจารณาช่องว่าง	**รับผิดชอบหลัก**	สนับสนุนตามขอบเขตบริการ
พิจารณาความเสี่ยงที่เหลืออยู่	**รับผิดชอบหลัก**	ให้ข้อมูลที่เกี่ยวข้องตามความเหมาะสม
ตัดสินใจเลือกใช้หรือใช้งานบริการ	**รับผิดชอบหลัก**	—
มีกระบวนการพัฒนาที่ปลอดภัยสำหรับบริการที่ CSP พัฒนา	พิจารณาความเหมาะสมจากข้อมูลที่ได้รับ	**รับผิดชอบหลัก**
ขอข้อมูลเกี่ยวกับการพัฒนาที่ปลอดภัยของ CSP	**รับผิดชอบหลัก**	ให้ข้อมูลตามขอบเขตที่สามารถเปิดเผยได้
การพัฒนา/ปรับแต่งระบบที่ CSC ควบคุมเอง	**รับผิดชอบหลัก** ในส่วนที่อยู่ภายใต้การควบคุมของ CSC	สนับสนุนตามขอบเขตบริการ
ป้องกันข้อมูลที่มีความอ่อนไหวของ CSP	ใช้และปกป้องข้อมูลที่ได้รับตามเงื่อนไขที่เกี่ยวข้อง	**รับผิดชอบหลัก** ในการกำหนดขอบเขตการเปิดเผย

ร่างเอกสารเพื่อ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

ตารางนี้เป็น **สรุปความรับผิดชอบในระดับแนวทาง** มิใช่การกำหนดตารางความรับผิดชอบแบบตายตัว เนื่องจากขอบเขตความรับผิดชอบจริงอาจแตกต่างกันตามรูปแบบบริการ เช่น IaaS, PaaS และ SaaS ตลอดจนขอบเขตและข้อตกลงการให้บริการ

2. หลักฐานที่ควรพิจารณา (Recommended Evidence)

เพื่อสนับสนุนการตรวจสอบการนำข้อกำหนด 5.2.8 ไปปฏิบัติ CSC และ CSP ควรมีหลักฐานที่เหมาะสมกับลักษณะ ความสำคัญ และความเสี่ยงของบริการ โดยไม่จำเป็นต้องมีหลักฐานทุกประเภทในทุกกรณี

ประเด็น	ตัวอย่างหลักฐาน
1. ข้อกำหนดด้านความมั่นคงปลอดภัย	Security Requirements / System Requirements / TOR / Specification หรือเอกสารอื่นที่แสดงความต้องการด้านความมั่นคงปลอดภัย
2. ข้อมูลความสามารถของบริการ	Security Capability Information / Service Documentation / Security Documentation ของ CSP
3. ผลการประเมิน	Cloud Security Assessment / Supplier Assessment / Checklist หรือหลักฐานการประเมินในรูปแบบอื่น
4. ช่องว่างและความเสี่ยง	Security Gap / Risk Assessment / Residual Risk / Risk Acceptance ตามความเหมาะสม
5. ข้อมูลเกี่ยวกับการพัฒนาที่ปลอดภัย	Secure Development Policy / Secure SDLC Description / Certification / Independent Assessment หรือข้อมูลอื่นที่ CSP สามารถเปิดเผยได้
6. กรณี CSC พัฒนาหรือปรับแต่งระบบเอง	Requirements / Design Review / Code Review / Security Test / Release Approval หรือหลักฐานจากกระบวนการพัฒนาที่มีอยู่ ตามความเหมาะสม

ทั้งนี้ ไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มแยกต่างหากสำหรับข้อ 5.2.8 หากหน่วยงานมีระบบ กระบวนการ หรือเอกสารที่สามารถใช้เป็นหลักฐานและแสดงการปฏิบัติตามข้อกำหนดได้อย่างเพียงพอ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

5.2.9 การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

การใช้บริการคลาวด์ทำให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ต้องพึ่งพาผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) รวมถึงผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่เกี่ยวข้องกับการให้บริการคลาวด์ ดังนั้น ความสัมพันธ์และข้อตกลงกับผู้ให้บริการภายนอกจึงเป็นส่วนสำคัญในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

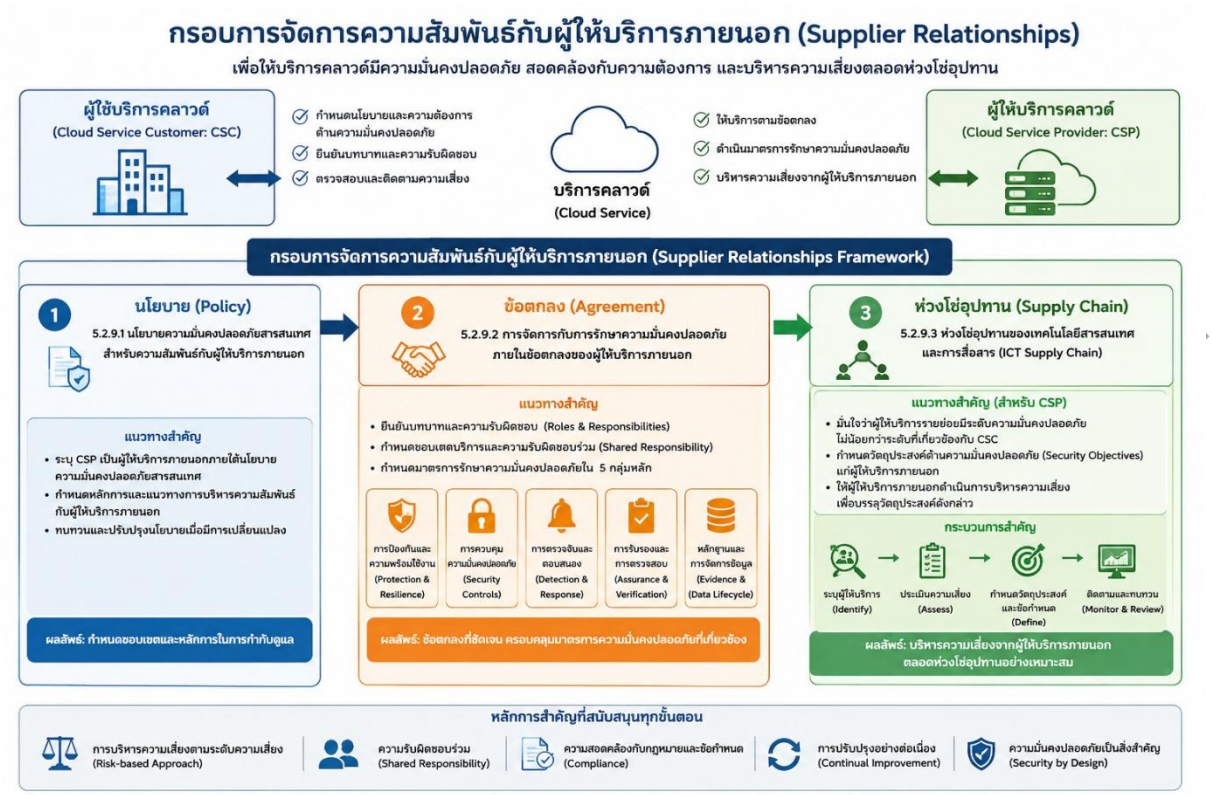
การจัดการผู้ให้บริการภายนอกควรครอบคลุมตั้งแต่การกำหนดนโยบาย การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในข้อตกลงการให้บริการ ตลอดจนการบริหารความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

สำหรับบริการคลาวด์ การรักษาความมั่นคงปลอดภัยเป็น ความรับผิดชอบร่วม (Shared Responsibility) ระหว่าง CSC และ CSP โดยขอบเขตความรับผิดชอบของแต่ละฝ่ายอาจแตกต่างกันตามประเภทบริการคลาวด์ รูปแบบการให้บริการ สถาปัตยกรรมของระบบ และข้อตกลงการให้บริการ

มาตรการที่กำหนดควรมีความเหมาะสมและได้สัดส่วนกับความเสี่ยง (Risk-based and Proportionate) โดยคำนึงถึงระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ลักษณะของบริการ และความเสี่ยงที่เกี่ยวข้อง ทั้งนี้ การกำหนดข้อกำหนดหรือการขอหลักฐานจาก CSP ควรพิจารณาตามความจำเป็นและไม่ควรก่อให้เกิดภาระหรือข้อกำหนดที่เกินความจำเป็น

การควบคุมด้าน Cloud ควรพิจารณาตามระดับผลกระทบ ความเสี่ยง ข้อจำกัดของบริการ และ Shared Responsibility แทนการกำหนดมาตรการแบบเดียวกันสำหรับทุกบริการ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งาน



กรอบการจัดการความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships Framework) แสดงกรอบการจัดการความสัมพันธ์ระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ผ่าน 3 องค์ประกอบหลัก ได้แก่ นโยบาย (Policy) ข้อตกลง (Agreement) และห่วงโซ่อุปทาน (Supply Chain) โดยมุ่งให้มีการกำหนดบทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน การบริหารความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายนอก และการทบทวนการดำเนินงานตามความเหมาะสม ทั้งนี้ การนำกรอบดังกล่าวไปใช้ควรยึดหลัก การบริหารตามความเสี่ยง (Risk-based Approach) ความรับผิดชอบร่วม (Shared Responsibility) และ ความได้สัดส่วน (Proportionality) เพื่อให้การกำหนดมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศสอดคล้องกับลักษณะของบริการและระดับความเสี่ยงที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing

หลักการสำคัญ (Key Principles)

การจัดการความสัมพันธ์กับผู้ให้บริการภายนอกควรอยู่บนหลักการสำคัญ 4 ประการ ดังนี้

1. ความรับผิดชอบร่วม (Shared Responsibility)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) มีความรับผิดชอบร่วมกันในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยขอบเขตและรายละเอียดของความ

รับผิดชอบของแต่ละฝ่ายควรพิจารณาตาม **ประเภทและรูปแบบของบริการคลาวด์ (Cloud Service Model)** ลักษณะของบริการ และข้อตกลงการให้บริการ

2. การบริหารตามความเสี่ยงและความได้สัดส่วน (Risk-based and Proportionate Approach)

การกำหนดข้อกำหนดและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศควรพิจารณาตาม **ระดับความเสี่ยงและผลกระทบ** ที่เกี่ยวข้องกับข้อมูล ระบบสารสนเทศ และบริการคลาวด์ โดยมาตรการที่กำหนดควรมีความเหมาะสมกับลักษณะของบริการและไม่ก่อให้เกิดข้อกำหนดหรือภาระที่เกินความจำเป็น

3. การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยผ่านข้อตกลง (Security by Agreement)

บทบาท ความรับผิดชอบ และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ควรกำหนดไว้อย่างชัดเจนใน **ข้อตกลงการให้บริการ (Service Agreement)** หรือเอกสารที่เกี่ยวข้อง เพื่อให้ CSC และ CSP มีความเข้าใจที่ตรงกันเกี่ยวกับขอบเขตการดำเนินงานและมาตรการรักษาความมั่นคงปลอดภัยของแต่ละฝ่าย

4. การรักษาความมั่นคงปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security)

CSP ควรบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกิดจาก **ผู้ให้บริการภายนอก (External Provider)** หรือ **ผู้ให้บริการรายย่อย (Sub-provider)** ที่เกี่ยวข้องกับการให้บริการคลาวด์ โดยกำหนดวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัยที่เหมาะสม และติดตามการบริหารความเสี่ยงตามขอบเขตที่เกี่ยวข้อง

ความสัมพันธ์กับมาตรการควบคุมอื่น (Relationship with Other Security Controls)

การจัดการผู้ให้บริการภายนอกเป็นมาตรการที่เกี่ยวข้องกับการควบคุมด้านความมั่นคงปลอดภัยอื่นของบริการคลาวด์ โดยเฉพาะมาตรการที่เกี่ยวข้องกับการเข้าถึงข้อมูล การดำเนินงาน การจัดการเหตุการณ์ และการจัดหาและพัฒนาระบบ ทั้งนี้ หน่วยงานควรพิจารณาความสัมพันธ์ระหว่างมาตรการเหล่านี้ตามขอบเขตความรับผิดชอบและผลการประเมินความเสี่ยง เพื่อให้ข้อกำหนดที่กำหนดในความสัมพันธ์กับผู้ให้บริการภายนอกมีความสอดคล้องและไม่เกิดช่องว่างของการควบคุม

มาตรการที่เกี่ยวข้อง	ความสัมพันธ์กับ Supplier Relationships
Access Control	กำหนดความรับผิดชอบเกี่ยวกับการยืนยันตัวตน การจัดการข้อมูลประจำตัว และการควบคุมการเข้าถึง
Cryptography	กำหนดข้อกำหนดหรือความรับผิดชอบด้านการเข้ารหัสที่เกี่ยวข้องกับบริการ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

Operations Security	กำหนดความรับผิดชอบด้านการสำรองข้อมูล ช่องโหว่ การตรวจสอบ และมาตรการปฏิบัติการ
System Acquisition, Development and Maintenance	พิจารณาความมั่นคงปลอดภัยของผู้ให้บริการหรือ Third Party ที่เกี่ยวข้องกับการพัฒนาและบำรุงรักษา
Information Security Incident Management	กำหนดบทบาทและการประสานงานเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
Compliance	พิจารณาข้อกำหนดทางกฎหมาย กฎ ระเบียบ และข้อกำหนดที่เกี่ยวข้องกับบริการ

5.2.9.1 นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องระบุว่า ผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูล ผู้ใช้บริการคลาวด์ ของ ผู้ให้บริการคลาวด์	

วัตถุประสงค์ (Objective)

เพื่อกำหนดหลักการสำหรับการบริหารความสัมพันธ์กับผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการคลาวด์ โดยให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) สามารถกำหนดและสื่อสารข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ได้อย่างเหมาะสมกับลักษณะของบริการและความเสี่ยงที่เกี่ยวข้อง

ทั้งนี้ ผู้ให้บริการคลาวด์ควรถูกพิจารณาเป็นผู้ให้บริการภายนอกประเภทหนึ่งภายใต้กรอบนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกของ CSC

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ต้องดำเนินการดังต่อไปนี้:

1. การกำหนด CSP เป็นผู้ให้บริการภายนอก

CSC ต้องระบุผู้ให้บริการคลาวด์ (CSP) เป็นผู้ให้บริการภายนอกประเภทหนึ่งภายใต้นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกของหน่วยงาน

การกำหนดดังกล่าวควรทำให้เกิดความชัดเจนว่า การใช้บริการคลาวด์และการพึ่งพา CSP เป็นส่วนหนึ่งของความสัมพันธ์กับผู้ให้บริการภายนอก และอยู่ภายใต้หลักเกณฑ์การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของหน่วยงาน

2. การเชื่อมโยงกับการบริหารความเสี่ยง

CSC ควรพิจารณาความเสี่ยงที่เกิดจากการใช้บริการ CSP ภายใต้กรอบการบริหารความเสี่ยงของหน่วยงาน โดยพิจารณาตามความเหมาะสม เช่น

- ประเภทและลักษณะของบริการคลาวด์
- ข้อมูลหรือระบบสารสนเทศที่นำไปใช้กับบริการ
- ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
- ขอบเขตความรับผิดชอบระหว่าง CSC และ CSP
- การพึ่งพาบริการของ CSP

3. การกำหนดผู้รับผิดชอบ

CSC ควรกำหนดหน่วยงานหรือผู้รับผิดชอบในการบริหารความสัมพันธ์ด้านความมั่นคงปลอดภัยกับ CSP ให้เหมาะสมกับโครงสร้างของหน่วยงาน

ผู้รับผิดชอบดังกล่าวอาจทำหน้าที่ประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง เช่น ผู้ใช้งานบริการ Cloud, IT/Cloud Team, Information Security, Procurement และ Legal ตามความเหมาะสม

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

CSP ควรสนับสนุน CSC ในการดำเนินการตามนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ภายใต้ขอบเขตความรับผิดชอบของ CSP และตามที่กำหนดไว้ในข้อตกลงการให้บริการ

รายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยที่ CSP ต้องดำเนินการ รวมถึงบทบาทและความรับผิดชอบของ CSP ให้พิจารณาตามข้อ 5.2.9.2 และ 5.2.9.3 ของเอกสารฉบับนี้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดด้านนโยบายไปใช้ควรพิจารณาตามขอบเขตของบริการและความเสี่ยงที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดรูปแบบนโยบายเดียวกันสำหรับทุกหน่วยงานหรือทุกบริการคลาวด์

1. ระบุ CSP ภายใต้นโยบาย

CSC ควรตรวจสอบว่านโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกครอบคลุม CSP ที่หน่วยงานใช้งานอยู่

ตัวอย่างเช่น

"ผู้ให้บริการคลาวด์ที่หน่วยงานใช้บริการถือเป็นผู้ให้บริการภายนอก และอยู่ภายใต้หลักเกณฑ์การบริหารความมั่นคงปลอดภัยของผู้ให้บริการภายนอกตามนโยบายของหน่วยงาน"

ไม่จำเป็นต้องบังคับให้ใช้ข้อความนี้ เป็นเพียงตัวอย่างเพื่อช่วยให้หน่วยงานนำไปใช้

2. กำหนดขอบเขตของความสัมพันธ์

หน่วยงานควรระบุขอบเขตของความสัมพันธ์กับ CSP ตามความเหมาะสม เช่น

- บริการคลาวด์ที่อยู่ภายใต้ข้อตกลง
- ข้อมูลหรือระบบสารสนเทศที่เกี่ยวข้อง
- หน้าที่และความรับผิดชอบของ CSC
- หน้าที่และความรับผิดชอบของ CSP
- ผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่เกี่ยวข้อง หากมี

ทั้งนี้ ไม่จำเป็นต้องนำรายละเอียดทางเทคนิคของ Cloud Architecture มาใส่ใน Policy

3. การเชื่อมโยงนโยบายกับข้อตกลงกับผู้ให้บริการภายนอก

นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกควรใช้เป็นกรอบในการกำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในข้อตกลงกับผู้ให้บริการคลาวด์ โดยควรมีความสอดคล้องและเชื่อมโยงกันในแต่ละระดับ ดังนี้

- **นโยบาย (Policy)** กำหนดหลักการและกรอบการบริหารความสัมพันธ์กับผู้ให้บริการภายนอก
- **ข้อตกลงกับผู้ให้บริการ (Supplier Agreement)** กำหนดบทบาท ความรับผิดชอบ และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง
- **การดำเนินการ (Implementation)** ดำเนินมาตรการตามบทบาทและความรับผิดชอบที่กำหนดไว้

เอกสารสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- **การทบทวน (Review)** ทบทวนความเหมาะสมของข้อกำหนดและการดำเนินงานเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญหรือเมื่อมีการเปลี่ยนแปลงของความเสี่ยงที่เกี่ยวข้อง

ทั้งนี้ รายละเอียดของข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศภายในข้อตกลงให้เป็นไปตามแนวทางที่กำหนดไว้ในข้อ **5.2.9.2 การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)**

4. ทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่สำคัญ

CSC ควรทบทวนความเหมาะสมของนโยบายหรือข้อกำหนดที่เกี่ยวข้องกับ CSP เมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อความมั่นคงปลอดภัย เช่น

- มีการนำบริการ Cloud ใหม่มาใช้งาน
- มีการเปลี่ยนแปลงประเภทหรือขอบเขตบริการ
- มีการเปลี่ยนแปลงความรับผิดชอบระหว่าง CSC และ CSP
- มีเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับ CSP
- มีการเปลี่ยนแปลงข้อกำหนดทางกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

เหตุผลและความจำเป็น (Rationale)

การใช้บริการคลาวด์ทำให้ CSC ต้องพึ่งพาความสามารถและการดำเนินงานของ CSP ในบางส่วนของการรักษาความมั่นคงปลอดภัยสารสนเทศ การระบุ CSP เป็นผู้ให้บริการภายนอกภายใต้นโยบายที่เกี่ยวข้องจึงช่วยให้ความสัมพันธ์ดังกล่าวอยู่ภายใต้กรอบการบริหารความเสี่ยงและการกำกับดูแลของหน่วยงานอย่างชัดเจน

ทั้งนี้ การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยควรคำนึงถึงลักษณะของบริการคลาวด์ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และขอบเขตความรับผิดชอบระหว่าง CSC และ CSP เพื่อไม่ให้เกิดข้อกำหนดที่ซ้ำซ้อนหรือเกินความจำเป็น

หลักฐานที่ควรเก็บรักษา

หลักฐาน	วัตถุประสงค์
Information Security Policy	แสดงว่า CSP อยู่ภายใต้ Supplier Relationship Policy
รายการ/ทะเบียน CSP ที่เกี่ยวข้อง	แสดงขอบเขตของผู้ให้บริการที่อยู่ภายใต้นโยบาย
การอนุมัติหรือทบทวนนโยบาย	แสดงการกำกับดูแลตามกระบวนการของหน่วยงาน
เอกสารที่เชื่อมโยง Policy กับ Supplier Agreement	แสดงการนำหลักการไปใช้กับความสัมพันธ์จริง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักฐานควรจัดเก็บเท่าที่จำเป็นและเหมาะสมกับระดับความเสี่ยง โดยไม่จำเป็นต้องจัดทำเอกสารเพิ่มเติมหากหน่วยงานมีเอกสารหรือหลักฐานที่มีอยู่แล้วและสามารถแสดงให้เห็นถึงการดำเนินการตามข้อกำหนดได้อย่างเพียงพอ

5.2.9.2 การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ดังที่อธิบายไว้ในข้อตกลงการให้บริการ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้ – การป้องกันมัลแวร์ – การสำรองข้อมูล – มาตรการควบคุมการเข้ารหัส – การจัดการช่องโหว่ – การจัดการเหตุการณ์ – การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค – การทดสอบความปลอดภัย – การตรวจสอบ – การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ – การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ – การยืนยันตัวตน และการควบคุมการเข้าถึง – การจัดการข้อมูลประจำตัวและการเข้าถึง	ก) ผู้ให้บริการคลาวด์ ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่งผู้ให้บริการคลาวด์ จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่าง ผู้ให้บริการคลาวด์ และ ผู้ใช้บริการคลาวด์ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้ – การป้องกันมัลแวร์ – การสำรองข้อมูล – มาตรการควบคุมการเข้ารหัส – การจัดการช่องโหว่ – การจัดการเหตุการณ์ – การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค – การทดสอบความปลอดภัย – การตรวจสอบ – การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ – การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ – การยืนยันตัวตน และการควบคุมการเข้าถึง – การจัดการข้อมูลประจำตัวและการเข้าถึง ข) มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการคลาวด์ จะใช้อาจแตกต่างกันออกไปตามประเภทของบริการคลาวด์ที่ ผู้ใช้บริการคลาวด์ใช้งานอยู่

ร่างสำหรับ Public Hearing เท่านั้น

วัตถุประสงค์ (Objective)

เพื่อให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) มีความเข้าใจที่ชัดเจนเกี่ยวกับบทบาท ความรับผิดชอบ และมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ โดยกำหนดรายละเอียดที่เกี่ยวข้องไว้ในข้อตกลงการให้บริการ (Service Agreement) หรือเอกสารที่เกี่ยวข้อง

การกำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศควรพิจารณาตามประเภทและรูปแบบของบริการคลาวด์ ขอบเขตความรับผิดชอบของแต่ละฝ่าย ลักษณะของข้อมูลหรือระบบสารสนเทศ และระดับความเสี่ยงที่เกี่ยวข้อง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ (CSC) ต้องยืนยันบทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ไว้ในข้อตกลงการให้บริการ หรือเอกสารที่เกี่ยวข้อง เพื่อให้เกิดความชัดเจนเกี่ยวกับขอบเขตการดำเนินงานและความรับผิดชอบของแต่ละฝ่าย

1. การกำหนดบทบาทและความรับผิดชอบ

CSC ควรตรวจสอบให้ข้อตกลงมีการกำหนดหรืออ้างอิงถึงประเด็นต่อไปนี้ตามความเหมาะสม

- ขอบเขตของบริการคลาวด์
- บทบาทและความรับผิดชอบของ CSC
- บทบาทและความรับผิดชอบของ CSP
- มาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่อยู่ภายใต้ความรับผิดชอบของแต่ละฝ่าย
- การประสานงานระหว่าง CSC และ CSP ในประเด็นด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ทั้งนี้ การกำหนดบทบาทและความรับผิดชอบควรสอดคล้องกับ **แบบจำลองความรับผิดชอบร่วม (Shared Responsibility Model)** ของบริการคลาวด์ที่เกี่ยวข้อง

2. ประเด็นด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง

CSC ควรพิจารณาประเด็นด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ และกำหนดไว้ในข้อตกลงหรือเอกสารที่เกี่ยวข้องตามความเหมาะสม โดยอาจครอบคลุมประเด็นดังต่อไปนี้

2.1 การป้องกันมัลแวร์ (Malware Protection)

กำหนดบทบาทและความรับผิดชอบในการป้องกัน ตรวจจับ และจัดการมัลแวร์ที่เกี่ยวข้องกับบริการคลาวด์ตามขอบเขตความรับผิดชอบของแต่ละฝ่าย

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

2.2 การสำรองข้อมูล (Backup)

กำหนดบทบาทและความรับผิดชอบเกี่ยวกับการสำรองข้อมูล รวมถึงขอบเขตของข้อมูลที่อยู่ภายใต้การสำรองข้อมูลของ CSC และ CSP ตามลักษณะของบริการ

2.3 มาตรการควบคุมการเข้ารหัส (Encryption Controls)

กำหนดความรับผิดชอบเกี่ยวกับการใช้และการจัดการมาตรการเข้ารหัสข้อมูลตามขอบเขตของบริการ รวมถึงกรณีที่การเข้ารหัสเป็นความสามารถของ CSP หรือเป็นการตั้งค่าที่ CSC ต้องดำเนินการ

2.4 การจัดการช่องโหว่ (Vulnerability Management)

กำหนดความรับผิดชอบในการระบุ ประเมิน และจัดการช่องโหว่ขององค์ประกอบที่อยู่ภายใต้การควบคุมของแต่ละฝ่าย

2.5 การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

กำหนดบทบาท ความรับผิดชอบ และแนวทางการประสานงานระหว่าง CSC และ CSP เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ

2.6 การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค (Technical Compliance)

กำหนดแนวทางหรือกลไกที่เหมาะสมในการประเมินการปฏิบัติตามข้อกำหนดทางเทคนิคด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ

2.7 การทดสอบความมั่นคงปลอดภัย (Security Testing)

กำหนดขอบเขตและแนวทางในการสนับสนุนการทดสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ โดยคำนึงถึงข้อจำกัดของสภาพแวดล้อมคลาวด์และความรับผิดชอบของแต่ละฝ่าย

2.8 การตรวจสอบ (Audit)

กำหนดสิทธิหรือกลไกที่เหมาะสมสำหรับการตรวจสอบหรือการได้รับหลักฐานเกี่ยวกับการปฏิบัติตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยคำนึงถึงขอบเขตบริการ ความลับของข้อมูล และข้อจำกัดของสภาพแวดล้อมคลาวด์

2.9 การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน (Collection, Maintenance and Protection of Evidence)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

กำหนดความรับผิดชอบเกี่ยวกับการรวบรวม การบำรุงรักษา และการปกป้องหลักฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึง **บันทึก (Logs)** และ **เส้นทางการตรวจสอบ (Audit Trails)** ตามความเหมาะสม

2.10 การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ (Data Protection at Service Termination)

กำหนดความรับผิดชอบในการจัดการข้อมูลเมื่อสิ้นสุดการให้บริการ เช่น การคืนข้อมูล การลบข้อมูล การยุติการเข้าถึง และการดำเนินการอื่นที่เกี่ยวข้องตามข้อตกลงและข้อกำหนดที่เกี่ยวข้อง

2.11 การยืนยันตัวตนและการควบคุมการเข้าถึง (Authentication and Access Control)

กำหนดบทบาทและความรับผิดชอบในการยืนยันตัวตนและการควบคุมการเข้าถึงทรัพยากรและบริการคลาวด์ตามขอบเขตความรับผิดชอบของแต่ละฝ่าย

2.12 การจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management)

กำหนดความรับผิดชอบในการจัดการข้อมูลประจำตัว สิทธิ์การเข้าถึง และการบริหารจัดการบัญชีผู้ใช้งานที่เกี่ยวข้องกับบริการคลาวด์

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ (CSP) ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง ซึ่ง CSP จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงการให้บริการ หรือเอกสารที่เกี่ยวข้อง เพื่อให้ CSC สามารถเข้าใจขอบเขตของมาตรการและความรับผิดชอบของ CSP ได้อย่างชัดเจน

1. การกำหนดขอบเขตความรับผิดชอบ

CSP ควรจัดให้มีข้อมูลที่เพียงพอสำหรับให้ CSC สามารถเข้าใจว่า มาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศใดอยู่ภายใต้ความรับผิดชอบของ CSP และมาตรการใดอยู่ภายใต้ความรับผิดชอบของ CSC

2. การกำหนดมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ

CSP ควรระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการไว้ในข้อตกลงหรือเอกสารที่เกี่ยวข้อง โดยพิจารณาตามลักษณะของบริการและขอบเขตความรับผิดชอบของ CSP

มาตรการดังกล่าวอาจครอบคลุมประเด็นที่เกี่ยวข้องกับ

- การป้องกันมัลแวร์ (Malware Protection)
- การสำรองข้อมูล (Backup)
- การเข้ารหัส (Encryption)
- การจัดการช่องโหว่ (Vulnerability Management)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- การจัดการเหตุการณ์ (Incident Management)
- การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค (Technical Compliance)
- การทดสอบความมั่นคงปลอดภัย (Security Testing)
- การตรวจสอบ (Audit)
- การจัดการหลักฐาน บันทึก และเส้นทางการตรวจสอบ (Evidence, Logs and Audit Trails)
- การปกป้องข้อมูลเมื่อสิ้นสุดการให้บริการ (Data Protection at Service Termination)
- การยืนยันตัวตนและการควบคุมการเข้าถึง (Authentication and Access Control)
- การจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management)

ทั้งนี้ มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ CSP นำมาใช้ **อาจแตกต่างกันตามประเภทและรูปแบบของบริการคลาวด์ที่ CSC ใช้งาน** และควรพิจารณาให้เหมาะสมกับขอบเขตความรับผิดชอบและระดับความเสี่ยงที่เกี่ยวข้อง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การกำหนดขอบเขตความรับผิดชอบ

CSC และ CSP ควรร่วมกันกำหนดขอบเขตความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ โดยพิจารณาตามแบบจำลองความรับผิดชอบร่วม (Shared Responsibility Model) ประเภทและรูปแบบของบริการ และลักษณะของระบบหรือข้อมูลที่เกี่ยวข้อง

2. การกำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

CSC ควรกำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่จำเป็นสำหรับบริการ โดยพิจารณาจาก

- ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ
- ผลการประเมินความเสี่ยง (Risk Assessment)
- ประเภทและรูปแบบของบริการคลาวด์
- ลักษณะของบริการ
- ข้อกำหนดทางกฎหมาย กฎ ระเบียบ หรือข้อกำหนดตามสัญญาที่เกี่ยวข้อง

3. การกำหนดประเด็นด้านความมั่นคงปลอดภัยในข้อตกลง

CSC และ CSP ควรพิจารณาประเด็นด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ และกำหนดไว้ในข้อตกลงหรือเอกสารที่เกี่ยวข้อง โดยพิจารณาตามขอบเขตความรับผิดชอบและระดับความเสี่ยง

การกำหนดรายละเอียดควรมีความชัดเจนเพียงพอที่จะทำให้แต่ละฝ่ายสามารถเข้าใจและปฏิบัติตามบทบาทและความรับผิดชอบของตนได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. การกำหนดหลักฐานเพื่อสนับสนุนการประเมิน

CSC ควรกำหนดประเภทของข้อมูลหรือหลักฐานที่จำเป็นสำหรับการประเมินการปฏิบัติตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ CSP ตามความเหมาะสม เช่น

- เอกสารด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- เอกสารแสดงขอบเขตความรับผิดชอบร่วม
- ใบรับรองหรือผลการประเมินจากหน่วยงานอิสระ
- ผลการทดสอบด้านความมั่นคงปลอดภัย
- ผลการประเมินหรือข้อมูลเกี่ยวกับการจัดการช่องโหว่
- ข้อมูลหรือหลักฐานเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัย
- บันทึกและหลักฐานการตรวจสอบที่เกี่ยวข้อง

การกำหนดและขอหลักฐานควรพิจารณาตามลักษณะของบริการ ขอบเขตความรับผิดชอบ และระดับความเสี่ยง และควรหลีกเลี่ยงการกำหนดหลักฐานที่ซ้ำซ้อนหรือเกินความจำเป็น

5. การทบทวนข้อกำหนด

CSC และ CSP ควรทบทวนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ในข้อตกลงเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น

- การเปลี่ยนแปลงบริการคลาวด์
- การเปลี่ยนแปลงประเภทหรือรูปแบบของบริการ
- การเปลี่ยนแปลงขอบเขตความรับผิดชอบ
- การเปลี่ยนแปลงประเภทหรือความสำคัญของข้อมูล
- การเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง
- การเปลี่ยนแปลงข้อกำหนดทางกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

6. การรักษาความสอดคล้องของข้อตกลง

CSC และ CSP ควรดูแลให้ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในข้อตกลงมีความสอดคล้องกับบริการและมาตรการที่ดำเนินการจริงตลอดระยะเวลาของการให้บริการ

เหตุผลและความจำเป็น (Rationale)

การกำหนดบทบาท ความรับผิดชอบ และมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศไว้ในข้อตกลงระหว่าง CSC และ CSP ช่วยให้แต่ละฝ่ายมีความเข้าใจที่ชัดเจนเกี่ยวกับขอบเขตการดำเนินงานและมาตรการที่อยู่ภายใต้ความรับผิดชอบของตน ซึ่งช่วยลดความเสี่ยงจากช่องว่างหรือความซ้ำซ้อนของการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

นอกจากนี้ การกำหนดข้อกำหนดดังกล่าวไว้ในข้อตกลงยังช่วยให้สามารถใช้เป็นกรอบในการติดตาม ประเมิน และทบทวนการปฏิบัติตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริการได้อย่างเหมาะสม

ทั้งนี้ การกำหนดข้อกำหนดและมาตรการควรพิจารณาตามลักษณะของบริการ ระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ และผลการประเมินความเสี่ยง โดยยึดหลักการบริหารตามความเสี่ยงและความได้สัดส่วน

หลักฐานประกอบการประเมิน (Assessment Evidence)

หลักฐานที่อาจใช้ประกอบการประเมินการดำเนินการตามข้อ 5.2.9.2 ได้แก่

ประเด็น	ตัวอย่างหลักฐาน
บทบาทและความรับผิดชอบ	ข้อตกลงการให้บริการ / เอกสารแสดงความรับผิดชอบร่วม
มาตรการด้านความมั่นคงปลอดภัย	Security Documentation / Service Documentation
การรับรองและการประเมิน	Certification / Independent Assessment Report
การจัดการช่องโหว่	Vulnerability Management Evidence
การจัดการเหตุการณ์	Incident Management / Notification Evidence
การทดสอบความมั่นคงปลอดภัย	Security Testing Results
การตรวจสอบ	Audit / Assurance Report
บันทึกและหลักฐาน	Logs / Audit Trails / Security Records
การปกป้องข้อมูลเมื่อสิ้นสุดบริการ	Data Return / Deletion Evidence
การควบคุมการเข้าถึง	Access Control / IAM Documentation

ทั้งนี้ การเลือกใช้หลักฐานควรพิจารณาตามลักษณะของบริการ ขอบเขตความรับผิดชอบ และระดับความเสี่ยง โดยไม่จำเป็นต้องกำหนดให้มีหลักฐานทุกประเภทสำหรับบริการคลาวด์ทุกประเภท

5.2.9.3 ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) หาก ผู้ให้บริการคลาวด์ ใช้บริการคลาวด์ของผู้ให้บริการรายย่อย ผู้ให้บริการคลาวด์ ต้องตรวจสอบให้แน่ใจว่าระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยนั้นได้รับการดูแลไม่น้อยกว่าผู้ใช้บริการคลาวด์ ข) เมื่อผู้ให้บริการคลาวด์ ให้บริการคลาวด์ตามห่วงโซ่อุปทาน ผู้ให้บริการคลาวด์ ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก และขอให้ผู้ให้บริการภายนอก

ร่างสำหรับ Public Hearing เท่านั้น - ไม่มีผลบังคับใช้

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	แต่ละรายดำเนินกิจกรรมการบริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์

วัตถุประสงค์ (Objective)

เพื่อให้มีการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกิดจากผู้ให้บริการภายนอก (External Provider) ผู้ให้บริการรายย่อย (Sub-provider) และผู้ให้บริการอื่นที่เกี่ยวข้องกับห่วงโซ่อุปทาน (Supply Chain) ของบริการคลาวด์ โดยให้ระดับการรักษาความมั่นคงปลอดภัยสารสนเทศของบริการมีความเหมาะสมและสอดคล้องกับระดับความเสี่ยงที่เกี่ยวข้อง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

แม้ข้อกำหนดในหัวข้อนี้มุ่งเน้นการดำเนินการของผู้ให้บริการคลาวด์ (CSP) แต่ผู้ใช้บริการคลาวด์ (CSC) ควรพิจารณาความเสี่ยงจากห่วงโซ่อุปทานของ CSP ในขอบเขตที่เกี่ยวข้องกับบริการคลาวด์ที่ CSC ใช้งาน

1. การพิจารณาการพึ่งพาผู้ให้บริการภายนอก

CSC ควรพิจารณาว่าบริการคลาวด์ที่ใช้งานมีการพึ่งพาผู้ให้บริการรายย่อย ผู้ให้บริการภายนอก หรือผู้ให้บริการโครงสร้างพื้นฐานและบริการสนับสนุนอื่นที่อาจมีผลกระทบต่อการรักษาความมั่นคงปลอดภัยของบริการหรือข้อมูลของ CSC หรือไม่

การพิจารณาดังกล่าวควรดำเนินการตามลักษณะของบริการ ขอบเขตความรับผิดชอบ และระดับความเสี่ยงที่เกี่ยวข้อง

2. การพิจารณาความเสี่ยงจากห่วงโซ่อุปทาน

ในกรณีที่การพึ่งพาผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยมีนัยสำคัญต่อบริการหรือข้อมูลของ CSC ควรพิจารณาข้อมูลที่เกี่ยวข้องกับการบริหารความเสี่ยงของ CSP ตามความเหมาะสม เช่น

- ข้อมูลเกี่ยวกับผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่เกี่ยวข้อง
- ข้อมูลเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ
- ผลการประเมินหรือการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัย
- ข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ในข้อตกลง
- ข้อมูลอื่นที่เกี่ยวข้องกับระดับความเสี่ยงของบริการ

ทั้งนี้ การพิจารณาควรใช้ข้อมูลเท่าที่จำเป็นและเหมาะสมกับระดับความเสี่ยง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานจริง

3. การกำหนดข้อกำหนดที่เกี่ยวข้องกับ CSP

ในกรณีที่ความเสี่ยงจากห่วงโซ่อุปทานมีนัยสำคัญ CSC ควรพิจารณากำหนดข้อกำหนดให้ CSP มีการบริหารความเสี่ยงของผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่เกี่ยวข้องตามขอบเขตที่เหมาะสม

ข้อกำหนดดังกล่าวควรเชื่อมโยงกับข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ใน **ข้อตกลงกับผู้ให้บริการ (Supplier Agreement)** ตามข้อ 5.2.9.2

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. การรักษาระดับความมั่นคงปลอดภัยของผู้ให้บริการรายย่อย

ในกรณีที่ CSP ใช้บริการคลาวด์ของผู้ให้บริการรายย่อย (Sub-provider) CSP ต้องตรวจสอบให้แน่ใจว่าระดับการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยนั้นได้รับการดูแลไม่น้อยกว่าผู้ใช้บริการคลาวด์ (CSC)

CSP ควรพิจารณาความเสี่ยงที่เกิดจากการพึ่งพาผู้ให้บริการรายย่อย และกำหนดมาตรการที่เหมาะสมเพื่อรักษาระดับความมั่นคงปลอดภัยสารสนเทศของบริการตามลักษณะของบริการและระดับความเสี่ยง

2. การกำหนดวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

เมื่อ CSP ให้บริการคลาวด์ผ่านห่วงโซ่อุปทาน CSP ต้องกำหนดวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Objectives) ให้แก่ผู้ให้บริการภายนอกที่เกี่ยวข้อง

ผู้ให้บริการภายนอกแต่ละรายควรดำเนินกิจกรรมการบริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

วัตถุประสงค์ดังกล่าวอาจครอบคลุมเป้าหมายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) รวมถึงข้อกำหนดสนับสนุนที่เกี่ยวข้อง เช่น การควบคุมการเข้าถึง (Access Control) การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) และการปฏิบัติตามข้อกำหนด (Compliance)

ทั้งนี้ การกำหนดวัตถุประสงค์และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศควรพิจารณาตามลักษณะของบริการ ขอบเขตความรับผิดชอบ และระดับความเสี่ยงของผู้ให้บริการแต่ละราย

ร่างเพื่อรับฟังความคิดเห็น (Public Hearing) ไม่ผูกพัน - ห้ามใช้อ้างอิง

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. การระบุผู้ให้บริการที่เกี่ยวข้องในห่วงโซ่อุปทาน

CSP ควรระบุผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่มีความเกี่ยวข้องอย่างมีนัยสำคัญต่อการให้บริการคลาวด์ โดยพิจารณาจากลักษณะของบริการและผลกระทบที่อาจเกิดขึ้นต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ

การระบุผู้ให้บริการควรมุ่งเน้นผู้ให้บริการที่มีนัยสำคัญต่อการรักษาความมั่นคงปลอดภัยของบริการ และไม่จำเป็นต้องครอบคลุมผู้ให้บริการทุกระดับของห่วงโซ่อุปทานที่ไม่มีนัยสำคัญต่อบริการ

2. การประเมินความเสี่ยงของห่วงโซ่อุปทาน

CSP ควรประเมินความเสี่ยงของผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่เกี่ยวข้องตามความเหมาะสม โดยพิจารณาปัจจัย เช่น

- ความสำคัญของบริการที่ได้รับ
- ประเภทและความสำคัญของข้อมูลที่เกี่ยวข้อง
- ระดับการเข้าถึงระบบหรือข้อมูล
- ผลกระทบที่อาจเกิดขึ้นหากบริการหยุดชะงัก
- ระดับการพึ่งพาผู้ให้บริการ
- ความสามารถในการทดแทนหรือเปลี่ยนผู้ให้บริการ

ทั้งนี้ วิธีการและระดับรายละเอียดของการประเมินความเสี่ยงควรสอดคล้องกับกระบวนการบริหารความเสี่ยงของ CSP และไม่จำเป็นต้องกำหนดวิธีการประเมินเฉพาะรูปแบบไว้ในเอกสารฉบับนี้

3. การกำหนดวัตถุประสงค์และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

CSP ควรกำหนดวัตถุประสงค์และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ให้บริการภายนอกตามผลการประเมินความเสี่ยง

ข้อกำหนดดังกล่าวควรถูกถ่ายทอดไว้ในข้อตกลงหรือเอกสารที่เกี่ยวข้องกับผู้ให้บริการตามความเหมาะสม โดยสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตามข้อ 5.2.9.2

4. การติดตามและทบทวนความเสี่ยง

CSP ควรติดตามและทบทวนความเสี่ยงของผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่มีนัยสำคัญตามความเหมาะสม โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่อาจส่งผลต่อระดับความเสี่ยง เช่น

- การเปลี่ยนแปลงผู้ให้บริการรายย่อย
- การเพิ่มหรือเปลี่ยนแปลงบริการ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- การเปลี่ยนแปลงสถาปัตยกรรมหรือรูปแบบการพึ่งพาบริการ
- การเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- การเปลี่ยนแปลงระดับความเสี่ยง
- การเปลี่ยนแปลงข้อกำหนดทางกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

เหตุผลและความจำเป็น (Rationale)

การให้บริการคลาวด์อาจมีการพึ่งพาผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยหลายระดับ ซึ่งอาจส่งผลต่อการรักษาความมั่นคงปลอดภัยของบริการและข้อมูลที่อยู่ภายใต้ความรับผิดชอบของ CSP หากผู้ให้บริการในห่วงโซ่อุปทานมีมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ไม่เหมาะสม อาจส่งผลกระทบต่อระดับการรักษาความมั่นคงปลอดภัยของบริการที่ CSP ให้แก่ CSC

การกำหนดวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และการบริหารความเสี่ยงของผู้ให้บริการที่เกี่ยวข้อง จึงช่วยให้ CSP สามารถควบคุมความเสี่ยงที่เกิดจากการพึ่งพาผู้ให้บริการภายนอก และรักษาระดับการรักษาความมั่นคงปลอดภัยของบริการให้สอดคล้องกับความต้องการของ CSC

หลักฐานประกอบการประเมิน

(Assessment Evidence)

หลักฐานที่อาจใช้ประกอบการประเมินการดำเนินการตามข้อ 5.2.9.3 ได้แก่

ประเด็น	ตัวอย่างหลักฐาน
ผู้ให้บริการในห่วงโซ่อุปทาน	ข้อมูลผู้ให้บริการภายนอกหรือผู้ให้บริการรายย่อยที่เกี่ยวข้อง
การประเมินความเสี่ยง	ผลการประเมินความเสี่ยงของผู้ให้บริการ
วัตถุประสงค์ด้านความมั่นคงปลอดภัย	Security Objectives / Security Requirements
ข้อกำหนดสำหรับผู้ให้บริการ	Contract / Agreement / Security Addendum
การให้ความเชื่อมั่น	Certification / Assessment Report
การติดตามและทบทวน	Supplier Review / Risk Review Evidence
การจัดการเหตุการณ์	Incident Records ที่เกี่ยวข้อง
การประเมินหรือให้ความเชื่อมั่นของผู้ให้บริการรายย่อย	Sub-provider Security Assessment / Assurance Evidence

ทั้งนี้ การเลือกใช้หลักฐานควรพิจารณาตามลักษณะของบริการ ความสำคัญของผู้ให้บริการ ขอบเขตความรับผิดชอบ และระดับความเสี่ยง โดยไม่จำเป็นต้องกำหนดให้มีหลักฐานทุกประเภทสำหรับผู้ให้บริการทุกราย

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

5.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

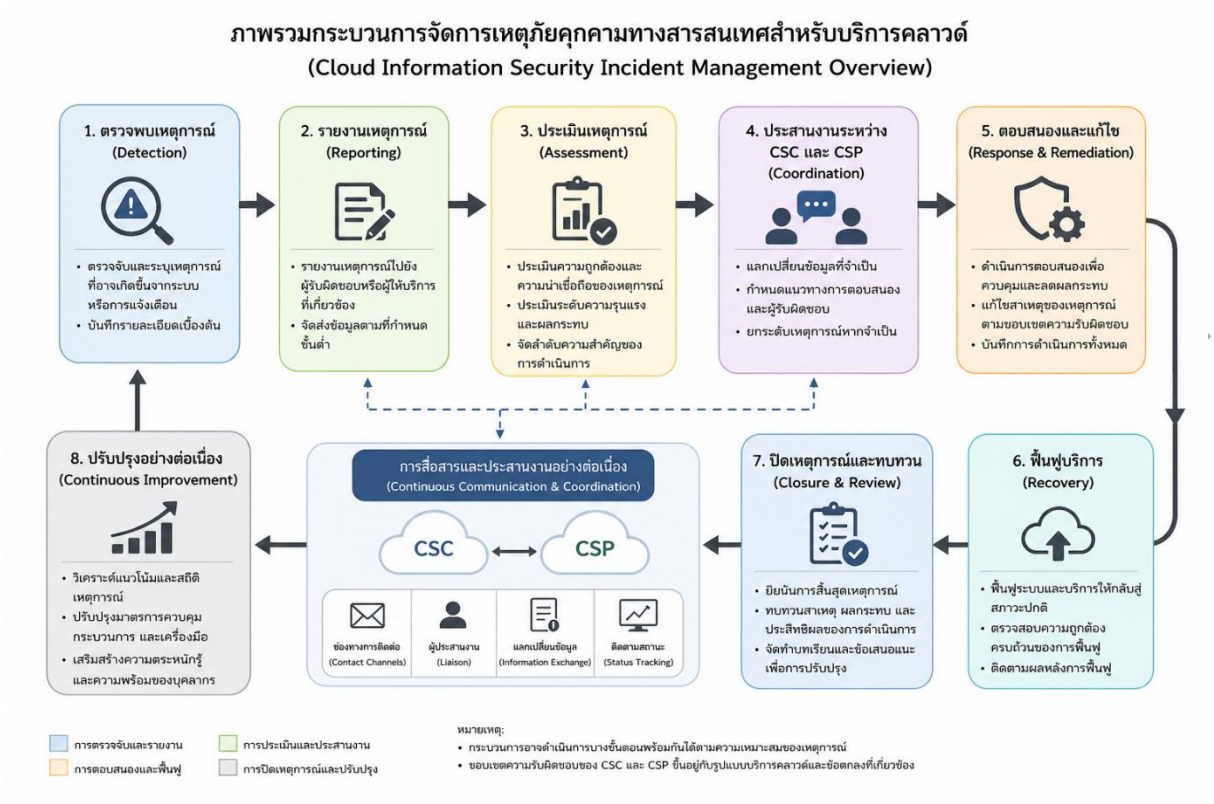
การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management) เป็นกระบวนการที่เกี่ยวข้องกับการตรวจพบ (Detection) การรายงาน (Reporting) การประเมิน (Assessment) การตอบสนอง (Response) และการติดตามเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ เพื่อจำกัดผลกระทบ ฟื้นฟูการให้บริการ และสนับสนุนการดำเนินการแก้ไขและปรับปรุงอย่างเหมาะสม

สำหรับบริการคลาวด์ (Cloud Services) การจัดการเหตุภัยคุกคามทางสารสนเทศอาจเกี่ยวข้องกับทั้งผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยขอบเขตความรับผิดชอบของแต่ละฝ่ายอาจแตกต่างกันตามรูปแบบบริการคลาวด์ (Cloud Service Model) ขอบเขตบริการ (Service Scope) สถาปัตยกรรมของบริการ และข้อตกลงการให้บริการ (Service Agreement) ดังนั้น หน่วยงานควรกำหนดบทบาทและความรับผิดชอบ ช่องทางการรายงานเหตุการณ์ การประสานงาน และการแลกเปลี่ยนข้อมูลระหว่าง CSC และ CSP ให้มีความชัดเจนและสอดคล้องกับหลักความรับผิดชอบร่วม (Shared Responsibility Model)

เหตุภัยคุกคามทางสารสนเทศควรนำไปสู่การทบทวนโดย CSC หรือการทบทวนร่วมกันระหว่าง CSC และ CSP ตามความเหมาะสม เพื่อประเมินประสิทธิผลของการจัดการเหตุการณ์ และพิจารณาว่าเหตุการณ์ดังกล่าวเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) หรือไม่ และดำเนินการตามกระบวนการและข้อกำหนดที่ใช้บังคับกับหน่วยงานนั้น

การจัดการเหตุภัยคุกคามทางสารสนเทศสำหรับบริการคลาวด์ควรดำเนินการตามแนวทางที่อิงความเสี่ยง (Risk-based Approach) โดยคำนึงถึงระดับความสำคัญของบริการ (Service Criticality) ผลกระทบของข้อมูลหรือระบบสารสนเทศ (Information or System Impact) รูปแบบบริการคลาวด์ และขอบเขตความรับผิดชอบของ CSC และ CSP ทั้งนี้ ไม่ควรกำหนดมาตรการทางเทคนิคหรือกระบวนการที่เฉพาะเจาะจงเกินความจำเป็น หากสามารถบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยได้ด้วยมาตรการที่เหมาะสมกับบริบทและความเสี่ยงของบริการ

ร่างสำหรับ Public Hearing ฉบับนี้ - ห้ามเผยแพร่



ภาพรวมกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศสำหรับบริการคลาวด์ เริ่มตั้งแต่การตรวจพบและรายงานเหตุการณ์ การประเมินและประสานงานระหว่างผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) การตอบสนองและแก้ไข การฟื้นฟูบริการ ตลอดจนการปิดและทบทวนเหตุการณ์และการปรับปรุงอย่างต่อเนื่อง ทั้งนี้ การดำเนินการในแต่ละขั้นตอนอาจแตกต่างกันตามลักษณะของเหตุการณ์ ระดับผลกระทบ รูปแบบบริการคลาวด์ และขอบเขตความรับผิดชอบของ CSC และ CSP

ร่างสำหรับ Public Hearing

5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และต้องตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์ ข) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์ หรือทบทวนร่วมกัน	ก) ผู้ให้บริการคลาวด์ ต้องกำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ใช้บริการคลาวด์ และ ผู้ให้บริการคลาวด์ โดยเป็นส่วนหนึ่งของข้อกำหนดบริการ ข) ผู้ให้บริการคลาวด์ ต้องจัดเตรียมเอกสารให้ผู้ใช้บริการคลาวด์ ครอบคลุม

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตน เพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่	– ขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ ผู้ให้บริการคลาวด์จะรายงานต่อผู้ใช้บริการคลาวด์ – ระดับการเปิดเผยการตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและการตอบสนองที่เกี่ยวข้อง – กรอบเวลาเป้าหมายที่จะมีการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศเกิดขึ้น – ขั้นตอนการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ – ข้อมูลติดต่อสำหรับการจัดการปัญหาที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ – การเยียวยาใด ๆ ที่สามารถนำไปใช้ได้หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศบางอย่างขึ้น ค) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์ หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตน เพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

วัตถุประสงค์ (Objective)

เพื่อให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) มีการกำหนดบทบาท ความรับผิดชอบ และขั้นตอนในการจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management) ที่ชัดเจนและเหมาะสมกับขอบเขตบริการคลาวด์ เพื่อให้สามารถตรวจพบ ประเมิน ตอบสนอง แก้ไข และฟื้นฟูจากเหตุการณ์ได้อย่างมีประสิทธิผล รวมทั้งสามารถประสานงานระหว่าง CSC และ CSP ได้อย่างเหมาะสม

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ต้องตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management) และต้องตรวจสอบให้แน่ใจว่าการจัดสรรดังกล่าวเป็นไปตามข้อกำหนดของ CSC โดยควรกำหนดบทบาท ความรับผิดชอบ และขั้นตอนที่เกี่ยวข้องให้มีความชัดเจนและสอดคล้องกับรูปแบบบริการคลาวด์ (Cloud Service Model) ขอบเขตบริการ (Service Scope) ข้อตกลงการให้บริการ (Service Agreement) และหลักความรับผิดชอบร่วม (Shared Responsibility Model)

การดำเนินการดังกล่าวควรเชื่อมโยงกับกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศที่มีอยู่ของหน่วยงาน และไม่จำเป็นต้องจัดทำกระบวนการแยกต่างหากสำหรับบริการคลาวด์ หากกระบวนการเดิมสามารถรองรับบริบทและความรับผิดชอบที่เกี่ยวข้องกับบริการคลาวด์ได้อย่างเพียงพอ

CSC ควรดำเนินการอย่างน้อยในประเด็นต่อไปนี้

1. การกำหนดบทบาทและความรับผิดชอบในการจัดการเหตุการณ์ (Incident Management Roles and Responsibilities)

CSC ควรกำหนดบุคคลหรือหน่วยงานที่มีหน้าที่รับผิดชอบในการจัดการและประสานงานเหตุภัยคุกคามทางสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ตั้งแต่การตรวจพบเหตุการณ์ (Incident Detection) การรายงานเหตุการณ์ (Incident Reporting) การประเมินผลกระทบ (Impact Assessment) การประสานงานกับ CSP การตอบสนองต่อเหตุการณ์ (Incident Response) และการติดตามภายหลังเหตุการณ์ (Post-Incident Follow-up)

การกำหนดบทบาทควรพิจารณาตามรูปแบบบริการคลาวด์ เช่น โครงสร้างพื้นฐานเป็นบริการ (Infrastructure as a Service: IaaS) แพลตฟอร์มเป็นบริการ (Platform as a Service: PaaS) และซอฟต์แวร์เป็นบริการ (Software as a Service: SaaS) เนื่องจากขอบเขตการควบคุมและความรับผิดชอบของ CSC และ CSP แตกต่างกันตามรูปแบบบริการ

CSC ควรกำหนด **ผู้รับผิดชอบหลักด้านการจัดการเหตุการณ์ (Incident Management Owner)** และช่องทางการติดต่อที่เหมาะสม โดยสามารถใช้บทบาทหรือหน้าที่ที่มีอยู่เดิมของหน่วยงาน เช่น ผู้ประสานงานเหตุการณ์ (Incident Coordinator) ผู้ดูแลบริการคลาวด์ (Cloud Service Administrator) ผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer) เจ้าของระบบหรือข้อมูล (System Owner / Data Owner) หรือผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ตามความเหมาะสม โดยไม่จำเป็นต้องจัดตั้งตำแหน่งใหม่โดยเฉพาะ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้งานอื่น

2. การกำหนดความรับผิดชอบร่วมระหว่าง CSC และ CSP (Shared Responsibility Definition)

CSC ควรกำหนดและทำความเข้าใจขอบเขตความรับผิดชอบระหว่าง CSC และ CSP สำหรับการจัดการเหตุภัยคุกคามทางสารสนเทศ โดยพิจารณาจากรูปแบบบริการคลาวด์ ขอบเขตบริการ สถาปัตยกรรมของบริการ และข้อตกลงการให้บริการ

การกำหนดความรับผิดชอบควรครอบคลุมทั้งกิจกรรมที่ CSC หรือ CSP เป็นผู้รับผิดชอบหลัก และกิจกรรมที่จำเป็นต้องดำเนินการร่วมกัน เพื่อป้องกันช่องว่างของความรับผิดชอบ (Responsibility Gap) หรือความซ้ำซ้อนในการดำเนินงาน

ตัวอย่างประเด็นที่ควรพิจารณา ได้แก่

กิจกรรม	CSC	CSP
การรายงานเหตุการณ์จากบัญชีผู้ใช้งานของ CSC	รับผิดชอบหลัก	สนับสนุนตามขอบเขตบริการ
การตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานคลาวด์	ประสานงานและติดตาม	รับผิดชอบหลัก
การประเมินผลกระทบต่อข้อมูลของ CSC	รับผิดชอบหลัก	สนับสนุนข้อมูลที่เกี่ยวข้อง
การจัดเตรียมข้อมูลเพื่อสนับสนุนการวิเคราะห์เหตุการณ์	จัดเตรียมข้อมูลในส่วนของ CSC	จัดเตรียมข้อมูลในส่วนของ CSP
การปรับปรุงมาตรการภายหลังเหตุการณ์	ดำเนินการในขอบเขตของ CSC	ดำเนินการในขอบเขตของ CSP

ตารางดังกล่าวเป็นเพียงตัวอย่างหลักการแบ่งความรับผิดชอบ และควรปรับให้เหมาะสมกับรูปแบบบริการและขอบเขตความรับผิดชอบจริงของแต่ละบริการคลาวด์

3. การจัดทำขั้นตอนการจัดการเหตุการณ์ (Incident Management Procedures)

CSC ควรจัดให้มีกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศที่สามารถรองรับเหตุการณ์ที่เกี่ยวข้องกับบริการคลาวด์ โดยกระบวนการดังกล่าวอาจเป็นส่วนหนึ่งของกระบวนการจัดการเหตุการณ์ที่มีอยู่ของหน่วยงาน และควรครอบคลุมกิจกรรมหลัก ได้แก่

1. การตรวจพบเหตุการณ์ (Detection)
2. การบันทึกและรายงานเหตุการณ์ (Logging and Reporting)
3. การประเมินและจำแนกระดับความรุนแรง (Assessment and Severity Classification)
4. การประสานงานกับ CSP (Coordination with CSP)
5. การตอบสนองและแก้ไขเหตุการณ์ (Response and Remediation)
6. การปิดเหตุการณ์และทบทวนบทเรียน (Incident Closure and Lessons Learned)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ทั้งนี้ หากหน่วยงานมีกระบวนการจัดการเหตุการณ์ตามระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) หรือกระบวนการอื่นที่เกี่ยวข้องอยู่แล้ว สามารถนำมาประยุกต์ใช้กับบริการคลาวด์ได้ โดยเพิ่มเติมเฉพาะประเด็นที่เกี่ยวข้องกับการประสานงาน การรายงาน และการแลกเปลี่ยนข้อมูลกับ CSP

4. การทบทวนเหตุการณ์และการปรับปรุง (Post-Incident Review and Improvement)

เหตุภัยคุกคามทางสารสนเทศควรนำไปสู่การทบทวนโดย CSC หรือการทบทวนร่วมกันระหว่าง CSC และ CSP ตามความเหมาะสม เพื่อประเมินประสิทธิผลของการจัดการเหตุการณ์ และพิจารณาว่าเหตุการณ์ดังกล่าวเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) หรือไม่

การทบทวนควรพิจารณาอย่างน้อยในประเด็นต่อไปนี้

- ลักษณะและสาเหตุของเหตุการณ์ (Incident Cause and Characteristics)
- ผลกระทบต่อระบบ ข้อมูล และบริการ (Impact on Systems, Data, and Services)
- ประสิทธิผลของการประสานงานระหว่าง CSC และ CSP (CSC–CSP Coordination Effectiveness)
- การแก้ไขและการปรับปรุงมาตรการควบคุม (Corrective and Improvement Actions)

หากเหตุการณ์เกี่ยวข้องกับข้อมูลส่วนบุคคล (Personal Data) CSC ควรประเมินเพิ่มเติมว่าเหตุการณ์ดังกล่าวเข้าข่ายการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) หรือไม่ และดำเนินการตามกฎหมาย กฎ ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

หลักฐานที่ควรมี (Recommended Evidence)

เพื่อแสดงถึงการนำข้อกำหนดไปปฏิบัติ CSC ควรมีหลักฐานที่เหมาะสมกับลักษณะและความเสี่ยงของบริการ เช่น

- กระบวนการจัดการเหตุการณ์ (Incident Management Procedure)
- การกำหนดบทบาทและความรับผิดชอบ (Roles and Responsibilities)
- ตารางความรับผิดชอบระหว่าง CSC และ CSP (Shared Responsibility Matrix)
- ข้อตกลงการให้บริการหรือ SLA (Service Agreement / SLA)
- บันทึกเหตุการณ์หรือระบบติดตามเหตุการณ์ (Incident Record / Ticket)
- บันทึกการทบทวนเหตุการณ์และการปรับปรุง (Post-Incident Review / Corrective Action)

ทั้งนี้ ไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มแยกต่างหาก หากหน่วยงานมีระบบหรือเอกสารที่สามารถแสดงหลักฐานดังกล่าวได้อย่างเพียงพอ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ควรกำหนดขอบเขตความรับผิดชอบ บทบาท และขั้นตอนในการจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management) ที่เกี่ยวข้องกับบริการคลาวด์ให้มีความชัดเจน เพื่อให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) สามารถทราบขอบเขตการดำเนินงาน การประสานงาน การแจ้งเหตุการณ์ และการสนับสนุนที่ CSP สามารถดำเนินการได้เมื่อเกิดเหตุการณ์

การกำหนดดังกล่าวควรสอดคล้องกับรูปแบบบริการคลาวด์ (Cloud Service Model) ขอบเขตบริการ (Service Scope) ข้อตกลงการให้บริการ (Service Agreement) และหลักความรับผิดชอบร่วม (Shared Responsibility Model) โดยแต่ละฝ่ายควรรับผิดชอบในส่วนที่อยู่ภายใต้การควบคุมของตน

CSP ควรดำเนินการอย่างน้อยในประเด็นต่อไปนี้

1. การกำหนดขอบเขตความรับผิดชอบในการจัดการเหตุการณ์ (Incident Management Responsibility Definition)

CSP ควรระบุขอบเขตและบทบาทความรับผิดชอบด้านการจัดการเหตุภัยคุกคามทางสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ไว้ในเอกสารหรือข้อตกลงที่เกี่ยวข้อง เช่น

- ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)
- ข้อตกลงการให้บริการคลาวด์ (Cloud Service Agreement)
- เงื่อนไขการให้บริการ (Service Terms and Conditions)
- เอกสารคำอธิบายบริการ (Service Description)

ข้อมูลดังกล่าวควรระบุขอบเขตความรับผิดชอบของ CSP และความสัมพันธ์กับความรับผิดชอบของ CSC อย่างเพียงพอ เพื่อให้สามารถระบุได้ว่าเหตุการณ์ประเภทใดอยู่ภายใต้ความรับผิดชอบของ CSP เหตุการณ์ใดอยู่ภายใต้ความรับผิดชอบของ CSC และเหตุการณ์ใดจำเป็นต้องดำเนินการร่วมกัน

ตัวอย่างเช่น

ลักษณะเหตุการณ์	แนวทางความรับผิดชอบ
เหตุการณ์ที่เกิดจากโครงสร้างพื้นฐานของ CSP	CSP รับผิดชอบหลัก
เหตุการณ์ที่เกิดจากการกำหนดค่าหรือการใช้งานภายใต้การควบคุมของ CSC	CSC รับผิดชอบหลัก
เหตุการณ์ที่เกี่ยวข้องกับข้อมูลของ CSC และองค์ประกอบของบริการ CSP	ดำเนินการร่วมกันตามขอบเขตความรับผิดชอบ
เหตุการณ์ที่ต้องใช้ข้อมูลจากทั้งสองฝ่ายเพื่อวิเคราะห์	CSC และ CSP สนับสนุนข้อมูลตามขอบเขตของตน

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้งานจริง

การแบ่งความรับผิดชอบดังกล่าวควรพิจารณาตามบริการจริง ไม่ควรกำหนดรูปแบบเดียวกันสำหรับบริการคลาวด์ทุกประเภท เนื่องจากขอบเขตการควบคุมของ CSC และ CSP แตกต่างกันตาม IaaS, PaaS และ SaaS

2. การกำหนดช่องทางและผู้ประสานงานด้านเหตุการณ์ (Incident Contact Point)

CSP ควรจัดให้มีช่องทางและผู้รับผิดชอบสำหรับการประสานงานด้านเหตุการณ์ (Incident Contact Point) เพื่อให้ CSC สามารถแจ้งเหตุ รับทราบข้อมูลสถานะ และติดตามความคืบหน้าของการดำเนินการได้อย่างเหมาะสม

ช่องทางดังกล่าวควรมีลักษณะอย่างน้อย ดังนี้

- สามารถเข้าถึงได้เมื่อเกิดเหตุการณ์ (Accessible During Incident)
- มีผู้รับผิดชอบที่ชัดเจน (Defined Responsible Contact)
- สามารถติดตามสถานะของเหตุการณ์ได้ (Incident Status Tracking)
- สามารถตรวจสอบประวัติการสื่อสารได้ตามความเหมาะสม (Communication Record)

ช่องทางอาจเป็นระบบแจ้งเหตุออนไลน์ (Incident Reporting Portal) ระบบบริหารคำร้องขอ (Ticket Management System) หรือช่องทางติดต่อเร่งด่วนด้านความมั่นคงปลอดภัย (Security Emergency Contact) ตามลักษณะบริการและระดับความสำคัญของเหตุการณ์

3. การแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Notification)

CSP ควรกำหนดหลักเกณฑ์และกระบวนการสำหรับการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ CSC ให้มีความชัดเจน โดยควรระบุไว้ในข้อกำหนดบริการ (Service Requirements) ข้อตกลงการให้บริการ (Service Agreement) หรือข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ตามความเหมาะสม

3.1 เหตุการณ์ที่ควรแจ้ง (Reportable Incident Criteria)

CSP ควรกำหนดหลักเกณฑ์สำหรับพิจารณาเหตุการณ์ที่ต้องแจ้ง CSC โดยคำนึงถึงลักษณะและผลกระทบของเหตุการณ์ เช่น

- เหตุการณ์ที่ส่งผลหรืออาจส่งผลต่อ **ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) หรือความพร้อมใช้งาน (Availability)** ของข้อมูลหรือบริการของ CSC
- เหตุการณ์ที่ทำให้บริการหยุดชะงักหรือมีประสิทธิภาพลดลงอย่างมีนัยสำคัญ (Significant Service Disruption or Degradation)
- การเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)
- เหตุการณ์ที่อาจเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)
- เหตุการณ์ที่อาจทำให้ CSC มีพันธกรณีในการรายงานต่อหน่วยงานกำกับดูแลหรือหน่วยงานของรัฐที่เกี่ยวข้อง

ทั้งนี้ ควรกำหนดหลักเกณฑ์ให้ชัดเจนเพียงพอที่จะลดความคลุมเครือว่าเหตุการณ์ประเภทใดอยู่ภายใต้หน้าที่ในการแจ้งของ CSP

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

3.2 กรอบเวลาเป้าหมายในการแจ้งเหตุการณ์ (Target Incident Notification Timeframe)

CSP ควรกำหนดกรอบเวลาเป้าหมายในการแจ้งเหตุการณ์ (Target Incident Notification Timeframe) ให้เหมาะสมกับระดับความรุนแรง ผลกระทบ ความสำคัญของบริการ

CSP และ CSC ควรกำหนดกรอบเวลาที่เหมาะสมไว้ใน SLA หรือข้อตกลงบริการ เช่น

ระดับความรุนแรง	แนวทางการแจ้ง
วิกฤต (Critical)	แจ้งโดยเร็วที่สุดภายหลังยืนยันเหตุการณ์ และรายงานความคืบหน้าอย่างเหมาะสม
สูง (High)	แจ้งภายในกรอบเวลาเร่งด่วนตาม SLA หรือข้อกำหนดที่เกี่ยวข้อง
ปานกลาง (Medium)	แจ้งตามกรอบเวลาของกระบวนการจัดการเหตุการณ์
ต่ำ (Low)	รายงานและติดตามตามกระบวนการปกติ

กรอบเวลาที่กำหนดควรเปิดโอกาสให้ CSC มีเวลาเพียงพอสำหรับการประเมินผลกระทบและดำเนินการตามพันธกรณีทางกฎหมายหรือการกำกับดูแลที่เกี่ยวข้อง

3.3 ข้อมูลขั้นต่ำในการแจ้งเหตุการณ์ (Minimum Incident Notification Information)

การแจ้งเหตุการณ์จาก CSP ควรมีข้อมูลที่เพียงพอให้ CSC สามารถประเมินสถานการณ์และดำเนินการที่เกี่ยวข้องได้ โดยอย่างน้อยควรพิจารณา

- หมายเลขอ้างอิงเหตุการณ์ (Incident Reference ID)
- วันและเวลาที่ตรวจพบเหตุการณ์ (Detection Date and Time)
- วันและเวลาที่เริ่มเกิดเหตุการณ์ หากทราบ (Incident Start Date and Time)
- รายละเอียดเหตุการณ์โดยสรุป (Incident Summary)
- บริการหรือระบบที่ได้รับผลกระทบ (Affected Services or Systems)
- ผลกระทบที่ทราบในขณะรายงาน (Known Impact)
- การดำเนินการตอบสนองหรือบรรเทาผลกระทบ (Response and Mitigation Actions)
- สถานะปัจจุบันของเหตุการณ์ (Current Incident Status)
- ช่องทางและผู้ประสานงานสำหรับการติดตามเหตุการณ์ (Contact Point and Follow-up Channel)

หากยังไม่สามารถระบุข้อมูลได้ครบถ้วนในการแจ้งครั้งแรก CSP สามารถจัดส่งข้อมูลเบื้องต้น (Initial Notification) และปรับปรุงข้อมูลเพิ่มเติม (Incident Update) เมื่อมีข้อมูลที่ได้รับการยืนยันแล้ว

ร่างมาตรฐาน Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง

4. การสนับสนุนข้อมูลเพื่อการวิเคราะห์และตอบสนองเหตุการณ์ (Incident Investigation and Response Support)

CSP ควรสนับสนุนข้อมูลที่เกี่ยวข้องกับบริการคลาวด์ตามขอบเขตความรับผิดชอบและข้อตกลงบริการ เพื่อให้ CSC สามารถวิเคราะห์ลักษณะ ขอบเขต และผลกระทบของเหตุการณ์ได้อย่างเหมาะสม

ข้อมูลที่อาจสนับสนุน ได้แก่

- วันและเวลาที่ตรวจพบเหตุการณ์ (Detection Date and Time)
- ลำดับเหตุการณ์ที่เกี่ยวข้อง (Incident Timeline)
- บริการหรือทรัพยากรคลาวด์ที่ได้รับผลกระทบ (Affected Cloud Services and Resources)
- บันทึกเหตุการณ์ที่เกี่ยวข้อง (Relevant Logs)
- กิจกรรมหรือพฤติกรรมที่ผิดปกติ (Suspicious Activities or Anomalies)
- บัญชีหรือสิทธิ์การเข้าถึงที่เกี่ยวข้อง (Relevant Accounts and Access Privileges)
- ตัวบ่งชี้การโจมตีหรือการบุกรุก หากมี (Indicators of Compromise: IoCs)
- ผลกระทบที่ตรวจพบหรือคาดว่าอาจเกิดขึ้น (Known or Potential Impact)
- มาตรการที่ CSP ได้ดำเนินการแล้ว (Actions Taken by CSP)

การสนับสนุนข้อมูลดังกล่าวต้องคำนึงถึงข้อจำกัดด้านการรักษาความลับ (Confidentiality) การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ความมั่นคงปลอดภัยของผู้ใช้บริการรายอื่น และข้อจำกัดตามกฎหมายหรือสัญญาที่เกี่ยวข้อง

การสนับสนุนบันทึกเหตุการณ์ (Log Support)

CSP ควรสามารถสนับสนุนบันทึกเหตุการณ์ (Log) ที่จำเป็นต่อการวิเคราะห์เหตุการณ์ตามขอบเขตความรับผิดชอบและความสามารถของบริการ

5. การเยียวยาและการติดตามผล (Remediation and Follow-up)

CSP ควรดำเนินการควบคุม แก้ไข และฟื้นฟูผลกระทบจากเหตุการณ์ภายในขอบเขตความรับผิดชอบของตน และประสานงานกับ CSC ตามความเหมาะสม

การดำเนินการอาจครอบคลุม

- การควบคุมหรือจำกัดผลกระทบ (Containment)
- การแก้ไขเหตุการณ์ (Remediation)
- การฟื้นฟูบริการ (Service Recovery)
- การติดตามสถานะและรายงานความคืบหน้า (Status Update)
- การสนับสนุนการวิเคราะห์สาเหตุ (Root Cause Analysis Support)
- การดำเนินการแก้ไขและปรับปรุง (Corrective and Improvement Actions)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

สำหรับเหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญ CSP ควรสนับสนุนข้อมูลที่จำเป็นสำหรับการวิเคราะห์สาเหตุ (Root Cause Analysis: RCA) ตามขอบเขตที่กำหนดไว้ในข้อกำหนดบริการ โดยสามารถจัดส่งข้อมูลเบื้องต้น (Preliminary Findings) ก่อน และจัดส่งผลการวิเคราะห์เพิ่มเติมเมื่อการตรวจสอบแล้วเสร็จ

หลักฐานที่ควรมี (Recommended Evidence)

CSP ควรมีเอกสารหรือหลักฐานที่สามารถแสดงขีดความสามารถและการดำเนินการตามข้อกำหนดที่เกี่ยวข้อง เช่น

- เอกสารกำหนดขอบเขตความรับผิดชอบ (Cloud Service Responsibility Description)
- ข้อตกลงหรือเงื่อนไขการแจ้งเหตุการณ์ (Incident Notification Agreement)
- ข้อมูลผู้ประสานงานและช่องทางการแจ้งเหตุการณ์ (Incident Contact Directory)
- กระบวนการจัดการเหตุการณ์ของ CSP (CSP Incident Management Procedure)
- บันทึกเหตุการณ์หรือรายงานเหตุการณ์ (Incident Ticket / Incident Report)
- หลักฐานการแจ้งเหตุและการติดตามสถานะ (Notification and Status Update Records)
- หลักฐานการดำเนินการแก้ไขหรือฟื้นฟูตามความเหมาะสม

ทั้งนี้ หลักฐานควรกำหนดตามระดับความรุนแรงของเหตุการณ์ ความสำคัญของบริการ และขอบเขตความรับผิดชอบ โดยไม่จำเป็นต้องกำหนดให้ทุกเหตุการณ์มีเอกสารในระดับเดียวกัน

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

การนำข้อกำหนดด้านการจัดการเหตุภัยคุกคามทางสารสนเทศไปปฏิบัติสำหรับบริการคลาวด์ (Cloud Services) ควรดำเนินการโดยคำนึงถึงรูปแบบบริการ ขอบเขตความรับผิดชอบ ระดับความสำคัญของบริการ และความเสี่ยงที่เกี่ยวข้อง โดย CSC และ CSP ควรกำหนดกลไกการประสานงานและการแลกเปลี่ยนข้อมูลให้สามารถดำเนินการได้อย่างเหมาะสมเมื่อเกิดเหตุการณ์

ทั้งนี้ หน่วยงานสามารถนำกระบวนการจัดการเหตุการณ์ที่มีอยู่เดิมมาประยุกต์ใช้กับบริการคลาวด์ได้ โดยเพิ่มเติมเฉพาะประเด็นที่เกี่ยวข้องกับความสัมพันธ์และการประสานงานระหว่าง CSC และ CSP

1. การกำหนดความรับผิดชอบร่วม (Shared Responsibility)

CSC และ CSP ควรกำหนดขอบเขตความรับผิดชอบด้านการจัดการเหตุภัยคุกคามทางสารสนเทศให้สอดคล้องกับรูปแบบบริการคลาวด์ (Cloud Service Model) และขอบเขตการควบคุมของแต่ละฝ่าย

การกำหนดความรับผิดชอบควรพิจารณาอย่างน้อยในกิจกรรมสำคัญ ได้แก่

- การตรวจพบเหตุการณ์ (Incident Detection)
- การรายงานและแจ้งเหตุการณ์ (Incident Reporting and Notification)
- การประเมินผลกระทบ (Impact Assessment)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- การวิเคราะห์เหตุการณ์ (Incident Analysis)
- การตอบสนองและแก้ไข (Response and Remediation)
- การฟื้นฟูบริการ (Service Recovery)
- การทบทวนภายหลังเหตุการณ์ (Post-Incident Review)

โดยอาจกำหนดความรับผิดชอบเป็น **CSC รับผิดชอบหลัก (CSC Responsibility), CSP รับผิดชอบหลัก (CSP Responsibility) หรือดำเนินการร่วมกัน (Joint Responsibility)** ตามลักษณะของบริการและเหตุการณ์

ตัวอย่างเช่น เหตุการณ์ที่เกิดจากการกำหนดค่าหรือการใช้งานที่อยู่ภายใต้การควบคุมของ CSC อาจอยู่ในความรับผิดชอบหลักของ CSC ขณะที่เหตุการณ์ที่เกิดจากโครงสร้างพื้นฐานของ CSP อาจอยู่ในความรับผิดชอบหลักของ CSP ส่วนเหตุการณ์ที่เกี่ยวข้องกับทั้งข้อมูลของ CSC และโครงสร้างพื้นฐานของ CSP ควรมีกลไกการประสานงานร่วมกัน

ตัวอย่างตารางความรับผิดชอบ

กิจกรรม	CSC	CSP
ตรวจพบเหตุจากระบบหรือทรัพยากรที่ CSC ควบคุม	รับผิดชอบหลัก	สนับสนุนตามความจำเป็น
ตรวจพบเหตุจากโครงสร้างพื้นฐานของ CSP	รับทราบและติดตาม	รับผิดชอบหลัก
แจ้งเหตุ CSC ⟶ CSP	รับผิดชอบหลัก	รับและดำเนินการ
แจ้งเหตุ CSP ⟶ CSC	รับและประเมินผลกระทบ	รับผิดชอบหลัก
วิเคราะห์สาเหตุ	ตามขอบเขต	ตามขอบเขต
แก้ไขเหตุการณ์	ตามขอบเขต	ตามขอบเขต
ฟื้นฟูบริการ	ตามขอบเขต	ตามขอบเขต

ตารางนี้เป็นเพียงตัวอย่างสำหรับใช้เป็นแนวทาง ไม่ควรนำไปใช้เป็นข้อกำหนดตายตัวกับบริการคลาวด์ทุกประเภท

2. การประสานงานและการยกระดับเหตุการณ์ (Incident Coordination and Escalation)

CSC และ CSP ควรกำหนดช่องทางและลำดับการประสานงาน (Incident Coordination) สำหรับเหตุการณ์ที่เกี่ยวข้องกับบริการคลาวด์ให้ชัดเจน โดยเฉพาะเหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญต่อข้อมูล ระบบ หรือความต่อเนื่องของบริการ

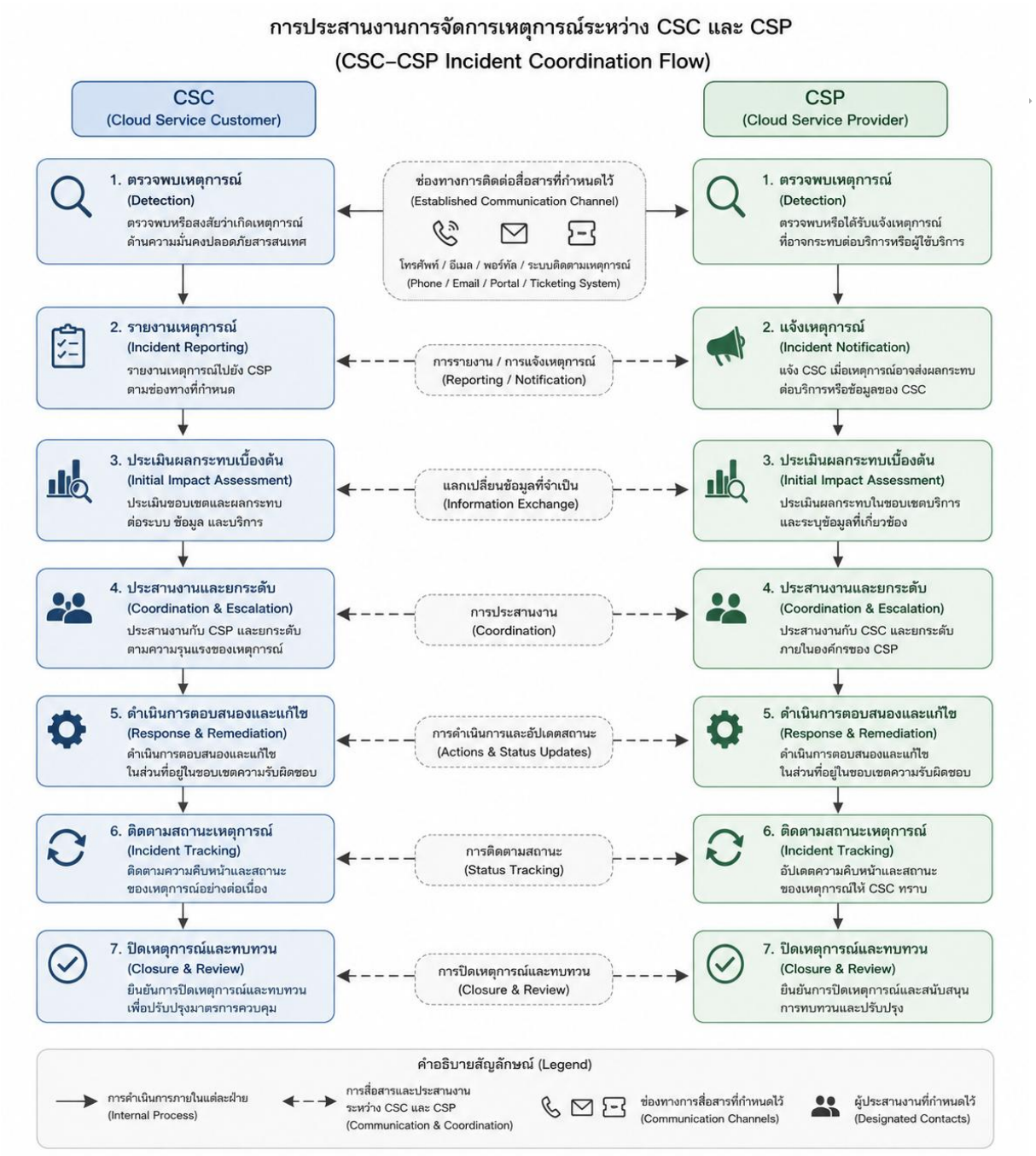
ควรกำหนดอย่างน้อย

- ผู้ประสานงานหลัก (Primary Contact)
- ผู้ประสานงานสำรอง (Alternate Contact)
- ช่องทางติดต่อกรณีเร่งด่วน (Emergency Contact Channel)
- ช่องทางติดตามสถานะ (Status Tracking Channel)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- แนวทางการยกระดับเหตุการณ์ (Escalation Path)

สำหรับเหตุการณ์ที่มีความรุนแรงสูงหรือมีแนวโน้มเพิ่มระดับผลกระทบ ควรมีกระบวนการยกระดับไปยังผู้รับผิดชอบที่เหมาะสมของทั้ง CSC และ CSP และควรติดตามสถานะจนกว่าเหตุการณ์จะได้รับการแก้ไขหรือปิดเหตุการณ์



แนวทางการประสานงานการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) โดยแสดงกระบวนการตั้งแต่การตรวจพบเหตุการณ์ (Detection) การรายงานหรือแจ้งเหตุการณ์ (Reporting / Notification) การประเมินผลกระทบเบื้องต้น (Initial Impact Assessment) การประสานงานและยกระดับเหตุการณ์ (Coordination and Escalation) การตอบสนองและแก้ไข (Response and Remediation) การติดตามสถานะ (Status Tracking) และการปิดเหตุการณ์และทบทวน (Closure and Review)

ทั้งนี้ การดำเนินการในแต่ละขั้นตอนขึ้นอยู่กับขอบเขตความรับผิดชอบของ CSC และ CSP ตามรูปแบบบริการคลาวด์ (Cloud Service Model) ขอบเขตบริการ (Service Scope) และข้อตกลงที่เกี่ยวข้อง โดยทั้งสองฝ่ายควรมีกลไกการสื่อสารและแลกเปลี่ยนข้อมูลที่เหมาะสม เพื่อให้สามารถประสานงานและตอบสนองต่อเหตุการณ์ได้อย่างต่อเนื่องและมีประสิทธิผล

3. การแจ้งเหตุการณ์และกรอบเวลา (Incident Notification and Timeframe)

CSP ควรกำหนดหลักเกณฑ์สำหรับเหตุการณ์ที่ต้องแจ้ง (Reportable Incident Criteria) และกรอบเวลาเป้าหมายในการแจ้ง (Target Notification Timeframe) ไว้ในข้อกำหนดบริการหรือข้อตกลงระหว่าง CSC และ CSP

เหตุการณ์ที่ควรพิจารณา ได้แก่ เหตุการณ์ที่กระทบหรืออาจกระทบต่อ **ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) หรือความพร้อมใช้งาน (Availability)** ของข้อมูลหรือบริการ เหตุการณ์ที่ส่งผลต่อความต่อเนื่องของบริการ เหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาต และเหตุการณ์ที่อาจเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล

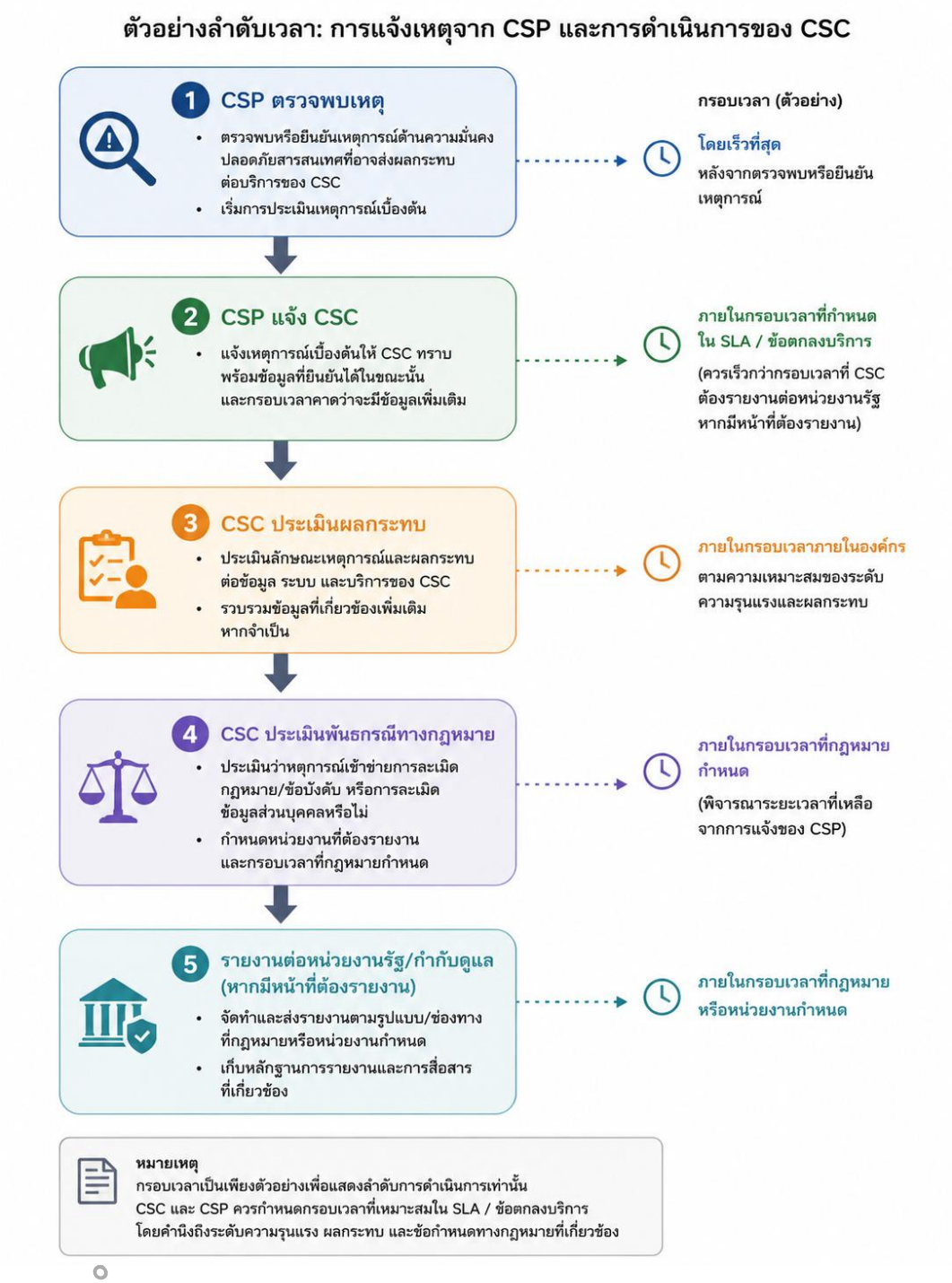
หลักการกำหนดกรอบเวลา

ไม่ควรกำหนดตัวเลขกรอบเวลาเดียวกันสำหรับทุกบริการ แต่ควรพิจารณาจาก

- ระดับความรุนแรงของเหตุการณ์ (Incident Severity)
- ผลกระทบต่อบริการและข้อมูล (Service and Information Impact)
- ความสำคัญของบริการ (Service Criticality)
- ข้อกำหนดใน SLA
- ข้อกำหนดทางกฎหมายและการกำกับดูแลที่เกี่ยวข้อง

สำหรับเหตุการณ์ที่อาจทำให้ CSC มีหน้าที่รายงานต่อหน่วยงานของรัฐหรือหน่วยงานกำกับดูแล ควรออกแบบกรอบเวลาการแจ้งของ CSP ให้ **เพียงพอสำหรับ CSC ในการประเมินและดำเนินการตามกรอบเวลาที่กฎหมายกำหนด** ไม่ควรรอจนถึงกรอบเวลาสูงสุดของ CSC

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปนี้แสดงตัวอย่างลำดับการดำเนินการเมื่อผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจส่งผลกระทบต่อผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) โดยเริ่มจากการตรวจพบและยืนยันเหตุการณ์ การแจ้งเหตุการณ์แก่ CSC การประเมินลักษณะ

และผลกระทบของเหตุการณ์ การประเมินพันธกรณีด้านกฎหมายและการกำกับดูแล และการรายงานต่อหน่วยงานของรัฐหรือหน่วยงานกำกับดูแลในกรณีที่มีหน้าที่ต้องรายงาน

ทั้งนี้ กรอบเวลาในการดำเนินการควรกำหนดให้เหมาะสมกับระดับความรุนแรงและผลกระทบของเหตุการณ์ รวมถึงข้อกำหนดในข้อตกลงการให้บริการ (Service Agreement) หรือข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และควรคำนึงถึงระยะเวลาที่ CSC จำเป็นต้องใช้ในการดำเนินการตามพันธกรณีทางกฎหมายหรือข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

ดังนั้น หลักการสำคัญคือ **CSP Notification Time ควรเร็วกว่ากรอบเวลาที่ CSC ต้องดำเนินการตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง**

4. ข้อมูลและการแลกเปลี่ยนข้อมูลเหตุการณ์ (Incident Information Exchange)

CSC และ CSP ควรกำหนดข้อมูลขั้นต่ำที่จำเป็นสำหรับการรายงาน การประเมิน และการติดตามเหตุการณ์ เพื่อให้สามารถแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิผล

ข้อมูลที่ควรพิจารณา ได้แก่

- หมายเลขอ้างอิงเหตุการณ์ (Incident Reference ID)
- วันและเวลาที่ตรวจพบ (Detection Date and Time)
- รายละเอียดเหตุการณ์ (Incident Summary)
- บริการหรือระบบที่ได้รับผลกระทบ (Affected Services or Systems)
- ผลกระทบที่ทราบ (Known Impact)
- การดำเนินการตอบสนอง (Response Actions)
- สถานะเหตุการณ์ (Incident Status)
- ผู้ประสานงานและช่องทางติดตาม (Contact Point and Follow-up Channel)

หากข้อมูลยังไม่ครบถ้วนในขณะที่แจ้งเหตุครั้งแรก สามารถจัดส่งข้อมูลเบื้องต้น (Initial Notification) และปรับปรุงข้อมูลเพิ่มเติม (Incident Update) เมื่อได้รับข้อมูลที่ยืนยันแล้ว

การแลกเปลี่ยนข้อมูลควรคำนึงถึงการรักษาความลับ (Confidentiality) การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ความมั่นคงปลอดภัยของผู้ใช้บริการรายอื่น และข้อจำกัดตามกฎหมายหรือสัญญาที่เกี่ยวข้อง

5. การสนับสนุนบันทึกเหตุการณ์และข้อมูลที่เกี่ยวข้อง (Log and Incident Information Support)

CSC และ CSP ควรกำหนดขอบเขตการเข้าถึงและการสนับสนุนบันทึกเหตุการณ์ (Log) ที่จำเป็นต่อการวิเคราะห์เหตุการณ์ไว้ล่วงหน้าตามรูปแบบบริการและขอบเขตความรับผิดชอบ

ตัวอย่างข้อมูลที่อาจเกี่ยวข้อง ได้แก่

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- บันทึกการพิสูจน์และยืนยันตัวตน (Authentication Log)
- บันทึกการเข้าถึง (Access Log)
- บันทึกกิจกรรมของผู้ดูแลระบบ (Administrative Activity Log)
- บันทึกกิจกรรมของบริการคลาวด์ (Cloud Service Activity Log)
- บันทึกด้านเครือข่าย (Network Log)
- บันทึกการแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Alert Log)

อย่างไรก็ตาม **ไม่ควรกำหนดให้ CSP ต้องส่งมอบ Log ทุกประเภทแก่ CSC** เนื่องจากขอบเขตการเข้าถึงและการเปิดเผยข้อมูลขึ้นอยู่กับรูปแบบบริการ สถาปัตยกรรม และขอบเขตความรับผิดชอบของแต่ละฝ่าย โดยควรกำหนดไว้ในข้อตกลงบริการว่า Log ประเภทใด CSC สามารถเข้าถึงได้โดยตรง และ Log ประเภทใดต้องร้องขอจาก CSP

ในกรณีที่ข้อมูลหรือ Log อาจถูกนำไปใช้เพื่อการตรวจสอบ การดำเนินการทางกฎหมาย หรือการรายงานต่อหน่วยงานกำกับดูแล ควรมีมาตรการรักษาความถูกต้องครบถ้วนของข้อมูล (Data Integrity) และสามารถตรวจสอบแหล่งที่มาได้ตามความเหมาะสม เช่น การควบคุมการเข้าถึง (Access Control) การบันทึกกิจกรรมการเข้าถึง (Access Logging) และการประทับเวลา (Timestamping)

6. การทบทวนและปรับปรุงภายหลังเหตุการณ์ (Post-Incident Review and Improvement)

ภายหลังเหตุการณ์ได้รับการแก้ไขและปิดเหตุการณ์แล้ว CSC และ CSP ควรทบทวนเหตุการณ์ตามความเหมาะสม โดยเฉพาะเหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญ เพื่อประเมินประสิทธิผลของการจัดการเหตุการณ์และระบุโอกาสในการปรับปรุง

การทบทวนควรพิจารณาอย่างน้อย

- สาเหตุและลักษณะของเหตุการณ์ (Incident Cause and Characteristics)
- ผลกระทบต่อระบบ ข้อมูล และบริการ (Impact on Systems, Data, and Services)
- ประสิทธิผลของการประสานงาน CSC–CSP (CSC–CSP Coordination Effectiveness)
- การดำเนินการแก้ไข (Corrective Actions)
- การปรับปรุงมาตรการเพื่อป้องกันการเกิดซ้ำ (Preventive or Improvement Actions)
- บทเรียนที่ได้รับ (Lessons Learned)

หลักฐานที่ควรมี (Recommended Evidence)

เพื่อสนับสนุนการนำแนวทางไปปฏิบัติ ควรพิจารณาหลักฐานที่เกี่ยวข้องตามความเหมาะสม เช่น

ประเด็น	ตัวอย่างหลักฐาน
ความรับผิดชอบ	Shared Responsibility Matrix
การประสานงาน	Contact Directory / Escalation Path
การแจ้งเหตุ	Incident Notification Record

ร่างเพื่อรับฟังความคิดเห็น (Public Hearing) ไม่ใช่ฉบับที่ใช้งานจริง

การติดตาม	Incident Ticket / Status Update
ข้อมูลเหตุการณ์	Incident Record / Relevant Logs
การตอบสนอง	Response / Remediation Record
การทบทวน	Post-Incident Review / Corrective Action

ทั้งนี้ หน่วยงานไม่จำเป็นต้องจัดทำเอกสารหรือแบบฟอร์มใหม่ หากสามารถใช้ระบบหรือเอกสารที่มีอยู่เดิมเป็นหลักฐานได้อย่างเพียงพอ

5.2.10.2 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับกลไกสำหรับ – ผู้ใช้บริการคลาวด์ รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบต่อผู้ให้บริการคลาวด์ – ผู้ให้บริการคลาวด์ เพื่อรับรายงานเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบโดยผู้ให้บริการคลาวด์ – ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน	ก) ผู้ให้บริการคลาวด์ ต้องมีกลไกสำหรับ – ผู้ใช้บริการคลาวด์ รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อ ผู้ให้บริการคลาวด์ – ผู้ให้บริการคลาวด์ เพื่อรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อ ผู้ใช้บริการคลาวด์ – ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน

วัตถุประสงค์ (Objective)

เพื่อให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) มีกลไกและช่องทางที่ชัดเจนสำหรับการรายงาน การรับแจ้ง และการติดตามสถานะเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Events) ที่เกี่ยวข้องกับบริการคลาวด์ เพื่อให้สามารถแลกเปลี่ยนข้อมูล ประสานงาน และดำเนินการต่อเหตุการณ์ได้อย่างเหมาะสมและทันเวลา

กลไกดังกล่าวควรรองรับการสื่อสารแบบสองทิศทาง (Two-way Communication) โดย CSC สามารถรายงานเหตุการณ์ที่ตรวจพบไปยัง CSP และ CSP สามารถแจ้งเหตุการณ์ที่อาจส่งผลกระทบต่อ CSC รวมทั้งจัดให้มีช่องทางสำหรับติดตามสถานะและความคืบหน้าของเหตุการณ์จนกว่าจะได้รับการแก้ไขหรือปิดเหตุการ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

ส่วนที่ 1 ข้อกำหนดสำหรับผู้ใช้บริการคลาวด์ (CSC Requirements)

CSC ควรขอและได้รับข้อมูลจาก CSP เกี่ยวกับกลไกสำหรับการรายงาน การรับแจ้ง และการติดตามสถานะเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ เพื่อให้สามารถดำเนินการและประสานงานเหตุการณ์ได้อย่างเหมาะสม

1. การรายงานเหตุการณ์ไปยัง CSP (CSC-to-CSP Incident Reporting)

CSC ควรสามารถรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบและอาจเกี่ยวข้องกับบริการหรือองค์ประกอบที่อยู่ภายใต้ความรับผิดชอบของ CSP ผ่านช่องทางที่ CSP กำหนดไว้

การรายงานเบื้องต้น (Initial Incident Reporting) ควรให้ข้อมูลเท่าที่จำเป็นต่อการเริ่มต้นประเมินและจัดการเหตุการณ์ โดยอาจประกอบด้วย

- วันและเวลาที่ตรวจพบเหตุการณ์ (Detection Date and Time)
- บริการหรือระบบที่เกี่ยวข้อง (Affected Service or System)
- รายละเอียดเหตุการณ์โดยสรุป (Incident Description)
- ผลกระทบที่ทราบในเบื้องต้น (Known Initial Impact)
- ผู้รายงานหรือผู้ประสานงาน (Reporter / Contact Point)

หากยังไม่สามารถระบุข้อมูลได้ครบถ้วน CSC ควรสามารถส่งข้อมูลเพิ่มเติมภายหลังได้ โดยไม่ควรทำให้การรายงานเหตุการณ์เบื้องต้นล่าช้าโดยไม่จำเป็น

2. การรับทราบและติดตามเหตุการณ์ (Incident Acknowledgement and Tracking)

CSC ควรสามารถตรวจสอบได้ว่า CSP ได้รับรายงานเหตุการณ์แล้ว และสามารถติดตามสถานะและความคืบหน้าของเหตุการณ์ผ่านหมายเลขอ้างอิงเหตุการณ์ (Incident Reference ID) หรือกลไกที่เทียบเท่า

สถานะของเหตุการณ์อาจกำหนดในระดับที่เหมาะสมกับการให้บริการ เช่น

รายงานแล้ว (Reported) ⟶ อยู่ระหว่างการประเมิน (Under Assessment) ⟶ อยู่ระหว่างดำเนินการ (In Progress) ⟶ แก้ไขแล้ว (Resolved) ⟶ ปิดเหตุการณ์ (Closed)

ไม่จำเป็นต้องกำหนดจำนวนสถานะมากเกินความจำเป็น หากไม่ได้ช่วยเพิ่มประสิทธิภาพในการประสานงานระหว่าง CSC และ CSP

ส่วนที่ 2 ข้อกำหนดสำหรับผู้ให้บริการคลาวด์ (CSP Requirements)

1. กลไกการรับรายงานจาก CSC (Incident Reporting Mechanism)

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

CSP ควรมีกลไกที่ทำให้ CSC สามารถรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างเหมาะสม โดยช่องทางดังกล่าวควรสอดคล้องกับระดับความสำคัญของบริการและระดับความรุนแรงของเหตุการณ์

ช่องทางอาจประกอบด้วย

- ระบบแจ้งเหตุการณ์ (Incident Reporting Portal)
- ระบบบริหารเหตุการณ์หรือ Ticketing (Incident Management / Ticketing System)
- อีเมลสำหรับเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Email)
- ช่องทางติดต่อกรณีเร่งด่วน (Emergency Contact Channel)

สำหรับบริการที่มีความสำคัญสูงหรือเหตุการณ์ที่มีความรุนแรงสูง ควรพิจารณาจัดให้มีช่องทางติดต่อเร่งด่วนเพิ่มเติมจากช่องทางปกติ

2. การแจ้งเหตุการณ์จาก CSP ไปยัง CSC (CSP-to-CSC Incident Notification)

เมื่อ CSP ตรวจพบหรือยืนยันเหตุการณ์ที่อาจส่งผลกระทบต่อข้อมูล ระบบ หรือบริการของ CSC CSP ควรแจ้ง CSC ตามหลักเกณฑ์และกรอบเวลาที่กำหนดไว้ในข้อกำหนดบริการ (Service Requirements) ข้อตกลงการให้บริการ (Service Agreement) หรือข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)

การแจ้งเบื้องต้น (Initial Notification) ควรให้ข้อมูลที่ได้รับการยืนยันแล้วเท่าที่มีอยู่ในขณะนั้น และควรระบุอย่างชัดเจนว่าข้อมูลส่วนใดยังอยู่ระหว่างการตรวจสอบ

CSP ไม่ควรชะลอการแจ้งเหตุการณ์ที่มีนัยสำคัญเพียงเพื่อรอผลการวิเคราะห์ที่สมบูรณ์ แต่ควรแจ้งข้อมูลเบื้องต้นและจัดส่งข้อมูลเพิ่มเติม (Subsequent Update) เมื่อได้รับข้อมูลที่มีความน่าเชื่อถือเพิ่มขึ้น

3. การติดตามสถานะเหตุการณ์ (Incident Status Tracking)

CSP ควรจัดให้ CSC สามารถติดตามสถานะของเหตุการณ์ที่ CSC รายงานหรือเหตุการณ์ที่ CSP แจ้งแก่ CSC เพื่อให้ทราบถึงความคืบหน้าของการประเมิน การตอบสนอง การแก้ไข และการฟื้นฟูบริการ

การติดตามอาจดำเนินการผ่านระบบบริหารเหตุการณ์ (Incident Management System) ระบบ Ticketing หรือช่องทางอื่นที่สามารถระบุหมายเลขอ้างอิงและสถานะของเหตุการณ์ได้อย่างชัดเจน

4. การยืนยันการรับรายงาน (Incident Report Acknowledgement)

เมื่อได้รับรายงานเหตุการณ์จาก CSC CSP ควรมีกลไกยืนยันการรับรายงาน (Acknowledgement) เพื่อให้ CSC ทราบว่ารายงานดังกล่าวได้รับเข้าสู่กระบวนการจัดการเหตุการณ์แล้ว

การยืนยันควรมีหมายเลขอ้างอิงเหตุการณ์ (Incident Reference ID) หรือข้อมูลที่สามารถใช้ติดตามสถานะของเหตุการณ์ได้

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้งานจริง

สำหรับเหตุการณ์ที่มีความรุนแรงสูง อาจกำหนดกรอบเวลาเป้าหมายสำหรับการยืนยันการรับรายงาน (Target Acknowledgement Time) และการเริ่มต้นประเมินเหตุการณ์ (Initial Assessment) ไว้ใน SLA ตามความเหมาะสม

ส่วนที่ 3 แนวทางการนำไปปฏิบัติ (Implementation Guidelines)

1. ช่องทางการรายงานและรับแจ้งเหตุการณ์ (Incident Reporting and Notification Channels)

CSC และ CSP ควรกำหนดช่องทางการรายงานและรับแจ้งเหตุการณ์ให้ชัดเจน และสื่อสารข้อมูลช่องทางดังกล่าวแก่บุคลากรที่เกี่ยวข้อง

ช่องทางควรได้รับการทบทวนและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ โดยพิจารณาตามระดับความสำคัญของบริการและระดับความรุนแรงของเหตุการณ์

ไม่จำเป็นต้องกำหนดเทคโนโลยีหรือช่องทางใดเป็นการเฉพาะ ตราบใดที่สามารถสนับสนุนการรายงาน รับแจ้ง และติดตามเหตุการณ์ได้อย่างมีประสิทธิผล

2. ข้อมูลขั้นต่ำสำหรับการรายงานและแจ้งเหตุการณ์ (Minimum Incident Reporting Information)

เพื่อให้สามารถเชื่อมโยงและติดตามเหตุการณ์ระหว่าง CSC และ CSP ได้อย่างมีประสิทธิผล ควรกำหนดชุดข้อมูลขั้นต่ำ (Minimum Information Set) เช่น

รายการ	รายละเอียด
หมายเลขอ้างอิงเหตุการณ์ (Incident ID)	ใช้ระบุและติดตามเหตุการณ์
วันและเวลาที่ตรวจพบ (Detection Date and Time)	เวลาที่ตรวจพบหรือรับทราบเหตุการณ์
ผู้รายงาน/ผู้ประสานงาน (Reporter / Contact Point)	ผู้รับผิดชอบการติดต่อ
บริการหรือระบบที่ได้รับผลกระทบ (Affected Service/System)	บริการคลาวด์หรือระบบที่เกี่ยวข้อง
รายละเอียดเหตุการณ์ (Incident Description)	รายละเอียดโดยสรุป
ระดับความรุนแรง (Severity Level)	ระดับตามเกณฑ์ที่กำหนด
ผลกระทบ (Impact)	ผลกระทบที่ทราบหรืออยู่ระหว่างประเมิน
การดำเนินการเบื้องต้น (Initial Actions)	การควบคุมหรือแก้ไขที่ดำเนินการแล้ว
สถานะเหตุการณ์ (Incident Status)	สถานะปัจจุบัน
การดำเนินการถัดไป (Next Action)	การดำเนินการที่ต้องติดตาม

รายการดังกล่าวเป็น **ข้อมูลขั้นต่ำสำหรับการประสานงาน** ไม่ใช่รายการข้อมูลที่ต้องมีครบถ้วนตั้งแต่การแจ้งครั้งแรก โดยสามารถเพิ่มเติมข้อมูลภายหลังตามความสำคัญของระบบ ลักษณะบริการ และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

เอกสารประกอบการ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

3. การรักษาความลับของข้อมูลการรายงาน (Confidentiality of Incident Reporting Information)

ข้อมูลที่เกี่ยวข้องกับการรายงานเหตุการณ์อาจมีข้อมูลที่มีความอ่อนไหว เช่น รายละเอียดช่องโหว่ (Vulnerability Information) ข้อมูลบัญชีผู้ใช้งาน การตั้งค่าระบบ บันทึกเหตุการณ์ (Logs) หรือข้อมูลส่วนบุคคล (Personal Data)

CSC และ CSP จึงควร

- ใช้ช่องทางการสื่อสารที่เหมาะสมและมีการป้องกัน
- จำกัดการเข้าถึงเฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง
- ป้องกันการเปิดเผยข้อมูลที่ไม่จำเป็น
- คำนึงถึงข้อกำหนดด้านการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล

โดยเฉพาะข้อมูลที่อาจส่งผลต่อความมั่นคงปลอดภัยของระบบหรือผู้ใช้บริการรายอื่น

ตัวอย่างโครงสร้างแบบรายงานและติดตามเหตุการณ์

(Example Structure of Cloud Information Security Incident Reporting and Tracking Form)

โดยสามารถครอบคลุมวงจรตั้งแต่การรายงานจนถึงการปิดเหตุการณ์ และแบ่งข้อมูลเป็น 6 ส่วน ได้แก่

1. ข้อมูลทั่วไปของเหตุการณ์ (Incident General Information)
2. การประเมินเหตุการณ์ (Incident Assessment)
3. ผลกระทบ (Impact)
4. การแจ้งและการประสานงาน (Notification and Coordination)
5. การตอบสนองและการแก้ไข (Response and Remediation)
6. การปิดและทบทวนเหตุการณ์ (Closure and Review)

สรุปข้อกำหนดและความรับผิดชอบ (Information Security Incident Management Requirements and Responsibility Summary)

1. หลักการ (Principles)

การจัดการเหตุภัยคุกคามทางสารสนเทศสำหรับบริการคลาวด์ควรดำเนินการตามหลักการสำคัญ ดังต่อไปนี้

1) ความรับผิดชอบร่วม (Shared Responsibility)

CSC และ CSP ควรกำหนดขอบเขตความรับผิดชอบที่ชัดเจนตามรูปแบบบริการคลาวด์ ขอบเขตบริการและข้อตกลงที่เกี่ยวข้อง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

2) **การประสานงานอย่างมีประสิทธิผล (Effective Coordination)**

ทั้งสองฝ่ายควรมีกลไกและช่องทางสำหรับการติดต่อ ประสานงาน ยกระดับเหตุการณ์ และติดตามสถานะอย่างเหมาะสม

3) **การรายงานอย่างทันเวลา (Timely Reporting)**

การรายงานเหตุการณ์ควรดำเนินการภายในกรอบเวลาที่เหมาะสมกับระดับความรุนแรง ความสำคัญของบริการ และข้อกำหนดที่เกี่ยวข้อง โดยไม่ควรรอข้อมูลที่สมบูรณ์จนทำให้การตอบสนองล่าช้า

4) **การแลกเปลี่ยนข้อมูลเท่าที่จำเป็น (Need-to-Know Information Exchange)**

ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ควรแลกเปลี่ยนเท่าที่จำเป็นต่อการประเมิน ตอบสนอง และติดตามเหตุการณ์ โดยคำนึงถึงการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล

5) **การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)**

เหตุการณ์ที่มีนัยสำคัญควรนำมาทบทวนเพื่อระบุบทเรียนและโอกาสในการปรับปรุงมาตรการควบคุมและกระบวนการที่เกี่ยวข้อง

หลักการดังกล่าวสอดคล้องกับแนวทางในฉบับเดิมที่เน้นการสื่อสารแบบสองทิศทางระหว่าง CSC และ CSP และการมีช่องทางที่ชัดเจนสำหรับการรายงาน รับรายงาน และติดตามสถานะเหตุการณ์

2. สรุปข้อกำหนดและความรับผิดชอบ (Requirements and Responsibility Summary)

ประเด็น	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
การกำหนดบทบาทและความรับผิดชอบ	กำหนดบทบาทภายในและขอบเขตความรับผิดชอบของตน	ระบุขอบเขตความรับผิดชอบของ CSP และความสัมพันธ์กับ CSC
กระบวนการจัดการเหตุการณ์	มีกระบวนการที่รองรับเหตุการณ์บนบริการคลาวด์	มีกระบวนการจัดการเหตุการณ์ภายในขอบเขตบริการ
ช่องทางรายงานเหตุการณ์	สามารถรายงานเหตุการณ์ไปยัง CSP ได้	จัดให้มีกลไกรับรายงานจาก CSC
การแจ้งเหตุการณ์	รับและประเมินเหตุการณ์ที่ CSP แจ้ง	แจ้ง CSC เมื่อเหตุการณ์อาจส่งผลกระทบต่อบริการหรือข้อมูลของ CSC
การประสานงาน	กำหนดผู้ประสานงานและช่องทางติดต่อ	กำหนดผู้ประสานงานและช่องทางติดต่อ
การประเมินผลกระทบ	ประเมินผลกระทบต่อข้อมูล ระบบ และบริการของ CSC	สนับสนุนข้อมูลภายในขอบเขตที่เกี่ยวข้อง
ข้อมูลและบันทึกเหตุการณ์	จัดเตรียมข้อมูลที่อยู่ภายใต้การควบคุมของ CSC	สนับสนุนข้อมูลและ Log ที่เกี่ยวข้องตามขอบเขตบริการ
การตอบสนองและแก้ไข	ดำเนินการในส่วนที่อยู่ภายใต้ความรับผิดชอบของ CSC	ดำเนินการในส่วนที่อยู่ภายใต้ความรับผิดชอบของ CSP

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

การติดตามสถานะ	สามารถติดตามสถานะเหตุการณ์ที่รายงานหรือได้รับแจ้ง	จัดให้มีกลไกสำหรับการติดตามสถานะ
การฟื้นฟูบริการ	ดำเนินการในส่วนที่อยู่ภายใต้ความรับผิดชอบของ CSC	ดำเนินการในส่วนที่อยู่ภายใต้ความรับผิดชอบของ CSP
การทบทวนภายหลังเหตุการณ์	ทบทวนผลกระทบและกำหนดการปรับปรุงตามความเหมาะสม	สนับสนุนการวิเคราะห์และการปรับปรุงตามขอบเขตที่เกี่ยวข้อง

ตารางนี้เป็น **สรุปความรับผิดชอบในระดับแนวทาง** ไม่ใช่การกำหนด Responsibility Matrix แบบตายตัว เนื่องจากขอบเขตความรับผิดชอบจริงแตกต่างกันตาม IaaS, PaaS, SaaS และข้อตกลงบริการ

3. หลักฐานขั้นต่ำที่ควรพิจารณา (Minimum Evidence)

เพื่อสนับสนุนการตรวจสอบการนำข้อกำหนดไปปฏิบัติ CSC และ CSP ควรมีหลักฐานที่เหมาะสมกับลักษณะบริการและความเสี่ยง โดยอาจประกอบด้วย

ประเด็น	ตัวอย่างหลักฐาน
บทบาทและความรับผิดชอบ	Roles and Responsibilities / Shared Responsibility Matrix
กระบวนการจัดการเหตุการณ์	Incident Management Procedure
ช่องทางการรายงาน	Incident Contact Point / Reporting Channel
การแจ้งและรับแจ้งเหตุการณ์	Incident Notification / Acknowledgement Record
การติดตามสถานะ	Incident Ticket / Status Tracking Record
การสนับสนุนข้อมูล	Relevant Logs / Incident Information
การตอบสนองและแก้ไข	Response / Remediation Record
การทบทวน	Post-Incident Review / Corrective Action

หลักฐานดังกล่าวเป็น **ตัวอย่างหลักฐาน (Examples of Evidence)** ไม่ใช่รายการเอกสารบังคับทั้งหมด และหน่วยงานสามารถใช้ระบบหรือเอกสารที่มีอยู่เดิมได้ หากสามารถแสดงให้เห็นถึงการดำเนินงานตามข้อกำหนดได้อย่างเพียงพอ

4. หลักการประยุกต์ใช้ (Application Considerations)

การนำข้อกำหนดนี้ไปใช้ควรพิจารณาปัจจัยต่อไปนี้

4.1 รูปแบบบริการคลาวด์ (Cloud Service Model)

ควรพิจารณาความแตกต่างระหว่าง IaaS, PaaS และ SaaS เนื่องจากระดับการควบคุมและความรับผิดชอบของ CSC และ CSP แตกต่างกัน

4.2 ความสำคัญของบริการ (Service Criticality)

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

บริการที่มีความสำคัญสูงหรือสนับสนุนภารกิจสำคัญของหน่วยงานควรมีช่องทางการประสานงานและการยกระดับเหตุการณ์ที่เหมาะสมกับระดับความสำคัญ

4.3 ระดับผลกระทบ (Impact Level)

ควรพิจารณาผลกระทบต่อ

- ความลับ (Confidentiality)
- ความถูกต้องครบถ้วน (Integrity)
- ความพร้อมใช้งาน (Availability)
- ข้อมูลส่วนบุคคล (Personal Data)
- ความต่อเนื่องของบริการ (Service Continuity)

4.4 ข้อกำหนดทางกฎหมายและการกำกับดูแล (Legal and Regulatory Requirements)

หากเหตุการณ์เกี่ยวข้องกับข้อกำหนดด้านกฎหมาย การกำกับดูแล หรือการรายงานต่อหน่วยงานรัฐ ให้ CSC และ CSP ดำเนินการตามข้อกำหนดที่ใช้บังคับกับกรณีนั้น โดย TF505 ไม่ควรกำหนดซ้ำหรือแทนที่ข้อกำหนดทางกฎหมายดังกล่าว

5.3 การใช้ทรัพยากรคลาวด์อย่างมีประสิทธิภาพและยั่งยืน (Efficient and Sustainable Use of Cloud Resources)

บริการคลาวด์มีคุณลักษณะที่ช่วยให้องค์กรสามารถจัดสรร ปรับเพิ่ม ปรับลด และยกเลิกทรัพยากรด้านการประมวลผล การจัดเก็บข้อมูล เครือข่าย และบริการที่เกี่ยวข้องได้ตามความต้องการ คุณลักษณะดังกล่าวสามารถสนับสนุนการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ หากมีการเลือก ออกแบบ ใช้งาน ติดตาม และปรับเปลี่ยนทรัพยากรให้เหมาะสมกับลักษณะของภาระงานตลอดวงจรชีวิตของบริการ

อย่างไรก็ตาม การใช้บริการคลาวด์มิได้ทำให้การใช้ทรัพยากร พลังงาน ค่าใช้จ่าย หรือผลกระทบต่อสิ่งแวดล้อมลดลงโดยอัตโนมัติ การจัดสรรทรัพยากรเกินความจำเป็น การเปิดใช้ทรัพยากรโดยไม่มีภาระงาน การเลือกทรัพยากรที่มีสมรรถนะสูงเกินความต้องการ การเก็บข้อมูลทั้งหมดไว้ในพื้นที่จัดเก็บระดับสมรรถนะสูง การสร้างสำเนาข้อมูลเกินความจำเป็น หรือการรับส่งข้อมูลซ้ำระหว่างพื้นที่ ล้วนสามารถเพิ่มการใช้ทรัพยากรของระบบคลาวด์ได้

ในทางกลับกัน การลดทรัพยากรหรือต้นทุนมากเกินไปอาจส่งผลต่อสมรรถนะ ความพร้อมใช้งาน ความต่อเนื่อง ความสามารถในการกู้คืน และความมั่นคงปลอดภัยของบริการ ดังนั้น เป้าหมายของการใช้ทรัพยากรอย่างมีประสิทธิภาพจึงมิใช่ **การใช้ทรัพยากรให้น้อยที่สุด** แต่เป็น **การใช้ทรัพยากรในระดับที่เหมาะสมกับภารกิจ ลักษณะของภาระงาน ระดับผลกระทบ และความเสี่ยง โดยหลีกเลี่ยงการใช้ทรัพยากรส่วนเกินที่ไม่มีความจำเป็น**

ร่างเอกสารเพื่อรับฟังความคิดเห็นสาธารณะ (Public Hearing) เท่านั้น ห้ามใช้อ้างอิง

แนวคิดดังกล่าวสอดคล้องกับทิศทางของมาตรฐานและแนวทางสากลด้านเทคโนโลยีดิจิทัลและความยั่งยืน โดย **ISO/IEC TS 20125-1:2026, Digital services ecodesign — Part 1: Ecopractices for life cycle stages** กำหนดข้อเสนอแนะและแนวปฏิบัติสำหรับลดผลกระทบด้านสิ่งแวดล้อมของบริการดิจิทัลตลอดช่วงของวงจรชีวิต ตั้งแต่การกำหนดความต้องการ การออกแบบ การพัฒนา การดำเนินงาน การบำรุงรักษา จนถึงการสิ้นสุดการใช้งาน

ในระดับการบริหารบริการ **ISO/IEC TS 20000-16:2025** กำหนดแนวทางเกี่ยวกับ Sustainability ภายในระบบบริหารจัดการบริการ โดยเชื่อมการบริหารบริการเข้ากับประเด็นด้านความยั่งยืนอย่างเป็นระบบ ขณะที่ ISO/IEC JTC 1/SC 39 มีขอบเขตการพัฒนามาตรฐานด้าน Sustainability, IT และ Data Centres ซึ่งรวมถึงประสิทธิภาพการใช้ทรัพยากรและตัวชี้วัดที่เกี่ยวข้อง

ในเชิงนโยบาย **OECD Digital Economy Outlook 2024** ชี้ให้เห็นว่าผลกระทบของเทคโนโลยีดิจิทัลต่อสิ่งแวดล้อมมีทั้งผลโดยตรง ผลที่เกิดจากการนำเทคโนโลยีไปใช้ และผลเชิงระบบ และผลกระทบสุทธิอาจมีความซับซ้อน จึงควรให้ความสำคัญกับการวัดและการประเมินผลอย่างเหมาะสม มากกว่าการสรุปว่าการเปลี่ยนไปใช้เทคโนโลยีดิจิทัลหรือคลาวด์จะทำให้ผลกระทบด้านสิ่งแวดล้อมลดลงโดยอัตโนมัติ

แนวทางในข้อ 5.3 จึงมุ่งเชื่อมโยง ความมั่นคงปลอดภัย ประสิทธิภาพของบริการ ความสามารถในการรองรับภาระงาน การใช้ทรัพยากร ต้นทุน และความยั่งยืน เข้าด้วยกัน โดยการตัดสินใจด้านประสิทธิภาพต้องไม่ทำให้ระดับการควบคุมด้านความมั่นคงปลอดภัยหรือความต่อเนื่องต่ำกว่าระดับที่เหมาะสมกับผลกระทบและความเสี่ยงของระบบ

ตารางที่ 1 กรอบ 6 Rights — หลัก 6 ประการในการใช้ทรัพยากรคลาวด์อย่างเหมาะสม

หลักการ	ความหมายและวัตถุประสงค์	ประเด็นที่ควรพิจารณา	ตัวอย่างแนวทางดำเนินการ	ผลที่คาดหวัง
ประเภทที่เหมาะสม (Right Type)	เลือกประเภทและคุณลักษณะของทรัพยากรคลาวด์ให้เหมาะสมกับลักษณะของภาระงานและความต้องการของบริการ โดยไม่เลือกทรัพยากรที่มีสมรรถนะหรือคุณลักษณะเกินความจำเป็น	ลักษณะภาระงาน การประมวลผล หน่วยความจำ พื้นที่จัดเก็บ เครือข่าย ฐานข้อมูล สมรรถนะ ความพร้อมใช้งาน และระดับผลกระทบ	วิเคราะห์ลักษณะภาระงาน เลือกประเภททรัพยากรให้สัมพันธ์กับงาน และทบทวนเมื่อรูปแบบการใช้งานเปลี่ยนแปลง	ลดการใช้ทรัพยากรที่ไม่เหมาะสม เพิ่มประสิทธิภาพ และรักษาสมรรถนะตามที่บริการต้องการ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้อ้างอิง

ขนาดที่เหมาะสม (Right Size)	กำหนดขนาด จำนวน และขีดความสามารถของทรัพยากรให้สัมพันธ์กับความต้องการจริง พร้อมส่วนเผื่อความสามารถที่เหมาะสมกับความเสี่ยงและความผันผวนของภาระงาน	ปริมาณการใช้งานปกติและสูงสุด แนวโน้มการเติบโต อัตราการใช้ประโยชน์ ส่วนเผื่อความสามารถสมรรถนะ และความต่อเนื่อง	การปรับขนาดทรัพยากรให้เหมาะสม (Right-sizing) การวางแผนขีดความสามารถ (Capacity Planning) และการปรับเพิ่มหรือลดทรัพยากรตามความต้องการ	ลดทรัพยากรส่วนเกินและทรัพยากรที่ไม่มีการใช้งาน โดยไม่ทำให้ความสามารถรองรับบริการต่ำกว่าระดับที่จำเป็น
รูปแบบการใช้ที่เหมาะสม (Right Use Case)	เลือกรูปแบบบริการ การจัดสรร และการปรับทรัพยากรให้เหมาะกับพฤติกรรม ความสำคัญ และช่วงเวลาการใช้งานของภาระงาน	ความคงที่หรือความผันผวนของภาระงาน ความสามารถในการคาดการณ์ ช่วงเวลาการใช้งาน ความเร่งด่วน ความสามารถในการยอมรับการหยุดชะงัก และระดับความสำคัญ	ใช้ทรัพยากรตามความต้องการ การปรับทรัพยากรตามกำหนดเวลา การปรับขนาดอัตโนมัติ การจัดตารางเปิด–ปิด และการใช้ทรัพยากรที่สามารถหยุดชั่วคราวได้สำหรับงานที่เหมาะสม	ใช้ทรัพยากรเฉพาะเมื่อจำเป็น รองรับความผันผวนของภาระงาน และลดระยะเวลาการเปิดใช้ทรัพยากรโดยไม่ก่อให้เกิดประโยชน์
ระดับชั้นที่เหมาะสม (Right Tier)	เลือกระดับชั้นของทรัพยากร โดยเฉพาะพื้นที่จัดเก็บข้อมูล ให้สัมพันธ์กับคุณค่า ความถี่ในการเข้าถึง ระยะเวลาการเก็บรักษา และความต้องการด้านสมรรถนะ	ความถี่ในการเข้าถึง ระยะเวลาที่ต้องการเรียกคืน ความสำคัญของข้อมูล ระยะเวลาการเก็บรักษา ความพร้อมใช้งาน การกู้คืน ความมั่นคงปลอดภัย และข้อกำหนดทางกฎหมาย	จำแนกข้อมูลตามรูปแบบการใช้งาน เลือกระดับชั้นการจัดเก็บ (Storage Tiering) กำหนดนโยบายวงจรชีวิต และย้ายข้อมูลไปยังระดับชั้นที่เหมาะสมเมื่อรูปแบบการใช้งานเปลี่ยนแปลง	ลดการใช้พื้นที่จัดเก็บสมรรถนะสูงโดยไม่จำเป็น ลดทรัพยากรและค่าใช้จ่าย พร้อมรักษาความสามารถในการเข้าถึงและกู้คืนข้อมูลตามข้อกำหนด
ตำแหน่งที่เหมาะสม (Right Location)	เลือกตำแหน่งของข้อมูล การประมวลผล และบริการให้เหมาะกับผู้ใช้งาน แหล่งกำเนิดข้อมูล	ตำแหน่งผู้ใช้งานและแหล่งข้อมูล ความหน่วง ปริมาณการรับส่งข้อมูล เขตอำนาจทางกฎหมาย	วิเคราะห์การไหลของข้อมูล เลือกตำแหน่งบริการที่เหมาะสม ประมวลผลใกล้ข้อมูลหรือผู้ใช้งานเมื่อมี	ลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น ลดความหน่วงและการใช้ทรัพยากรเครือข่าย โดยยังคง

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

	การไหลของข้อมูล ข้อกำหนด และความเสี่ยง	ความมั่นคงปลอดภัย ความพร้อมใช้งาน ความต่อเนื่อง และการกู้คืน	เหตุผล ใช้การเก็บข้อมูลใกล้ผู้ใช้หรือเครือข่ายนำส่งเนื้อหา และลดการรับส่งหรือทำสำเนาข้ามพื้นที่ที่ไม่จำเป็น	ข้อกำหนดด้านกฎหมาย ความมั่นคงปลอดภัย และความต่อเนื่อง
วงจรชีวิตที่เหมาะสม (Right Lifecycle)	บริหารทรัพยากรและข้อมูลให้สอดคล้องกับความต้องการตลอดวงจรชีวิต ตั้งแต่การจัดเตรียม ใช้งาน ปรับเปลี่ยน เก็บรักษา จนถึงการยกเลิกหรือลบเมื่อหมดความจำเป็น	วัตถุประสงค์ ระยะเวลาการใช้งาน เจ้าของทรัพยากร การเปลี่ยนแปลงความต้องการ ระยะเวลาการเก็บรักษา ข้อกำหนดด้านหลักฐาน การสำรองและกู้คืน และเงื่อนไขการยกเลิก	ติดตามสถานะและการใช้ทรัพยากร กำหนด Metadata/Tag และนโยบายวงจรชีวิต ปรับเพิ่มหรือลดตามความต้องการ ย้ายหรือเก็บถาวรข้อมูล และยกเลิกทรัพยากรหรือลบข้อมูลอย่างปลอดภัยเมื่อหมดความจำเป็น	ลดทรัพยากร ข้อมูล สำเนา และค่าใช้จ่ายที่คงอยู่โดยไม่มีความจำเป็น ลดความเสี่ยงจากข้อมูลหรือทรัพยากรตกค้าง และสนับสนุนการใช้ทรัพยากรอย่างยั่งยืน

กรอบ 6 Rights (หลัก 6 ประการในการใช้ทรัพยากรคลาวด์อย่างเหมาะสม) เป็นกรอบแนวคิดที่สังเคราะห์ขึ้นสำหรับแนวทางฉบับนี้ โดยนำหลักการด้านการบริหารทรัพยากรคลาวด์ (Cloud Resource Management) วงจรชีวิตข้อมูล (Data Lifecycle) ความมั่นคงปลอดภัย (Security) ความสามารถในการรองรับและฟื้นตัวจากเหตุขัดข้อง (Resilience) และความยั่งยืน (Sustainability) มาจัดให้อยู่ในรูปแบบที่สามารถใช้ประกอบการตัดสินใจได้อย่างเป็นระบบ ทั้งนี้ กรอบ 6 Rights มิใช่ชื่อมาตรฐานหรือกรอบที่กำหนดโดย ISO/IEC, Cloud Security Alliance (CSA), OECD หรือองค์กรระหว่างประเทศหรือผู้ให้บริการคลาวด์รายใดรายหนึ่ง

การประยุกต์ใช้กรอบ 6 Rights ควรพิจารณาหลักการทั้ง 6 ด้านร่วมกัน เนื่องจากการตัดสินใจในด้านหนึ่งอาจส่งผลต่ออีกด้านหนึ่ง เช่น การเลือกประเภททรัพยากรที่เหมาะสมแต่มีขนาดเกินความจำเป็นอาจยังทำให้เกิดการใช้ทรัพยากรส่วนเกิน การเลือกระดับชั้นการจัดเก็บที่เหมาะสมแต่เก็บข้อมูลไว้นานเกินความจำเป็นอาจยังทำให้เกิดการใช้ทรัพยากรโดยไม่มีเหตุผลรองรับ หรือการเลือกตำแหน่งของบริการเพื่อให้มีความหน่วงต่ำที่สุดอาจไม่เหมาะสมหากไม่สอดคล้องกับข้อกำหนดด้านข้อมูลหรือความต่อเนื่องของบริการ

การตัดสินใจตามกรอบดังกล่าวควรพิจารณาร่วมกับระดับผลกระทบและความเสี่ยงของบริการ และอยู่ภายใต้ข้อกำหนดด้าน ความมั่นคงปลอดภัย สมรรถนะ ความพร้อมใช้งาน ความต่อเนื่อง การกู้คืน การคุ้มครองข้อมูล และการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง โดยไม่ควรปรับลดทรัพยากร ความซ้ำซ้อน การสำรองข้อมูล การบันทึกเหตุการณ์ หรือมาตรการควบคุมที่ยังมีความจำเป็น เพียงเพื่อให้ตัวชี้วัดด้านการใช้ทรัพยากร ต้นทุน หรือสิ่งแวดล้อมลดลง

ร่างสำหรับ Public Hearing ไม่ใช่ฉบับ -ห้ามใช้อ้างอิง

ดังนั้น การประยุกต์ใช้กรอบ 6 Rights ควรอยู่ภายใต้กลไกการกำกับที่ประกอบด้วย การกำหนดข้อมูลฐาน (Baseline) การติดตาม (Monitoring) การกำหนดค่าขีดแบ่งและขอบเขตควบคุม (Threshold and Guardrails) การควบคุมการเปลี่ยนแปลง (Change Control) การวัดผล (Measurement) และการทบทวนและปรับปรุงอย่างต่อเนื่อง (Continual Improvement)



รูปที่ 1 ภาพรวมกรอบการใช้ทรัพยากรคลาวด์อย่างมีประสิทธิภาพและยั่งยืน

ร่างสำหรับ PC

ขอบเขตของแนวทาง

แนวทางในข้อ 5.3 แบ่งออกเป็น 4 ส่วน ได้แก่

5.3.1 การเลือกประเภท ขนาด และรูปแบบการใช้ทรัพยากรให้เหมาะสมกับภาระงาน

ครอบคลุมการวิเคราะห์ภาระงาน การเลือกประเภทและขนาดทรัพยากร การวางแผนขีดความสามารถ การปรับทรัพยากรตามความต้องการ การกำหนดขอบเขตควบคุม ตลอดจนการบริหารทรัพยากรและโครงสร้างพื้นฐานตลอดวงจรชีวิตอย่างเป็นระบบ

5.3.2 การบริหารระดับชั้นการจัดเก็บและวงจรชีวิตข้อมูล

ครอบคลุมการเลือกระดับชั้นของพื้นที่จัดเก็บให้เหมาะสมกับคุณค่า ความถี่ในการเข้าถึง และความต้องการด้านสมรรถนะของข้อมูล การกำหนดระยะเวลาการเก็บรักษาและวงจรชีวิตข้อมูล การบริหารข้อมูลสำรอง สำเนาข้อมูล และบันทึกเหตุการณ์ ตลอดจนการย้ายระดับชั้น การลบ หรือการทำลายข้อมูลเมื่อหมดความจำเป็น โดยยังคงข้อกำหนดด้านความมั่นคงปลอดภัย การกู้คืน และกฎหมายที่เกี่ยวข้อง

5.3.3 การเลือกตำแหน่งของบริการและการลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น

ครอบคลุมการเลือกตำแหน่งของข้อมูล การประมวลผล และบริการให้เหมาะสมกับผู้ใช้งาน แหล่งข้อมูล และข้อกำหนดที่เกี่ยวข้อง การวิเคราะห์การไหลของข้อมูล การลดการรับส่งหรือทำสำเนาข้อมูลที่ไม่มีความจำเป็น การนำส่งเนื้อหาและเก็บข้อมูลใกล้ผู้ใช้งาน การประมวลผลใกล้แหล่งกำเนิดข้อมูล การลดขนาดข้อมูล และการกำหนดระดับความซ้ำซ้อนให้เหมาะสมกับความต่อเนื่องของบริการ

5.3.4 การวัด ติดตาม และปรับปรุงประสิทธิภาพการใช้ทรัพยากร

ครอบคลุมการกำหนดข้อมูลฐานและขอบเขตการวัด การติดตามการใช้ทรัพยากรและค่าใช้จ่าย การกำหนดค่าขีดแบ่งและการตรวจจับความผิดปกติ การกำหนดตัวชี้วัดและการประเมินทรัพยากรต่อหน่วยบริการ การกำหนดเป้าหมายการปรับปรุง การตรวจสอบผลกระทบหลังดำเนินการ ตลอดจนการประเมินและรายงานผลด้านสิ่งแวดล้อมเฉพาะส่วนที่มีข้อมูลและวิธีการที่สามารถตรวจสอบได้

หลักการกำกับการตัดสินใจ

การดำเนินการตามข้อ 5.3 ควรรักษาระดับความมั่นคงปลอดภัย ความพร้อมใช้งาน ความต่อเนื่อง และความสามารถในการกู้คืนที่เหมาะสมกับระดับผลกระทบและความเสี่ยงของบริการเป็นเงื่อนไขพื้นฐาน โดยเฉพาะระบบหรือข้อมูลที่มีระดับผลกระทบสูง

ในขณะเดียวกัน CSC ควรสามารถอธิบายเหตุผลของขีดความสามารถสำรอง ความซ้ำซ้อน การทำสำเนา การสำรองข้อมูล การเก็บบันทึกเหตุการณ์ หรือทรัพยากรอื่นที่จัดสรรไว้ เพื่อแยกทรัพยากรที่จำเป็นต่อความมั่นคงปลอดภัยและความสามารถในการรองรับและฟื้นตัวจากเหตุขัดข้อง (Resilience) ออกจากทรัพยากรส่วนเกินที่ไม่มีเหตุผลรองรับ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

หลักการโดยสรุปจึงเป็น **การรักษาระดับความมั่นคงปลอดภัยและความสามารถในการรองรับและฟื้นตัวจากเหตุขัดข้องเป็นเงื่อนไขกำกับ และเพิ่มประสิทธิภาพการใช้ทรัพยากรภายใต้เงื่อนไขดังกล่าว (Security and Resilience as Guardrails — Resource Efficiency as an Optimization Objective)**

หมายเหตุ: แนวทางในข้อ 5.3 เป็นแนวทางเพิ่มเติมเพื่อสนับสนุนการนำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ไปประยุกต์ใช้อย่างมีประสิทธิภาพและยั่งยืน มิใช่ข้อกำหนดขั้นต่ำเพิ่มเติมตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

5.3.1 การเลือกประเภท ขนาด และรูปแบบการใช้ทรัพยากรให้เหมาะสมกับภาระงาน

CSC ควรเลือกประเภท ขนาด จำนวน และรูปแบบการจัดสรรทรัพยากรคลาวด์ให้เหมาะสมกับลักษณะของภาระงาน ปริมาณการใช้งาน ระดับสมรรถนะที่ต้องการ ความสามารถในการยอมรับการหยุดชะงัก ระดับผลกระทบ และข้อกำหนดด้านความมั่นคงปลอดภัย โดยใช้ข้อมูลการใช้งานจริง แนวโน้มความต้องการ และข้อกำหนดของบริการเป็นพื้นฐานในการตัดสินใจ

การดำเนินการควรครอบคลุมทรัพยากรด้านการประมวลผล หน่วยความจำ พื้นที่จัดเก็บ ฐานข้อมูล เครือข่าย และบริการสนับสนุนที่เกี่ยวข้อง โดยมีเป้าหมายให้ทรัพยากรเพียงพอต่อการให้บริการและรองรับความผันผวนของภาระงานในระดับที่เหมาะสม ขณะเดียวกันควรหลีกเลี่ยงการจัดสรรทรัพยากรส่วนเกินที่ไม่มีเหตุผลรองรับ

สำหรับข้อ 5.3.1 การตัดสินใจเกี่ยวกับทรัพยากรควรพิจารณาหลักการ 3 ด้าน ได้แก่ เลือกประเภทให้เหมาะสม (Right Type) กำหนดขนาดให้เหมาะสม (Right Size) และเลือกรูปแบบการใช้ให้เหมาะสม (Right Use Case) โดยเชื่อมโยงกับการบริหารวงจรชีวิตของทรัพยากรตามความเหมาะสม

5.3.1.1 ข้อควรพิจารณาในการย้ายระบบเดิมขึ้นสู่คลาวด์และการปรับปรุงภายหลังการย้าย

การย้ายระบบหรือภาระงานเดิมขึ้นสู่บริการคลาวด์โดยยังคงสถาปัตยกรรม การกำหนดค่า และรูปแบบการจัดสรรทรัพยากรเดิมไว้เป็นส่วนใหญ่ ซึ่งมักเรียกว่า **การย้ายระบบแบบ Lift and Shift** เป็นแนวทางที่ช่วยลดความซับซ้อนและระยะเวลาในการย้ายระบบ เนื่องจากไม่จำเป็นต้องปรับเปลี่ยนระบบเดิมอย่างมีนัยสำคัญ และอาจเหมาะสมในกรณีที่องค์กรมีข้อจำกัดด้านเวลา งบประมาณ บุคลากร หรือความเสี่ยงจากการเปลี่ยนแปลงระบบ

อย่างไรก็ตาม การย้ายระบบในลักษณะดังกล่าว **มิได้ทำให้การใช้ทรัพยากรมีประสิทธิภาพขึ้นโดยอัตโนมัติ** เนื่องจากขนาดและรูปแบบการจัดสรรทรัพยากรของระบบเดิมอาจถูกออกแบบตามข้อจำกัดของโครงสร้างพื้นฐานเดิม เช่น การจัดเตรียมขีดความสามารถเผื่อไว้ล่วงหน้า การกำหนดทรัพยากรแบบคงที่ หรือการใช้สถาปัตยกรรมที่ไม่ได้ออกแบบให้สามารถปรับเพิ่มหรือลดทรัพยากรตามความต้องการ

หากนำรูปแบบดังกล่าวมาใช้บนคลาวด์โดยไม่มีการทบทวน อาจทำให้เกิด **การจัดสรรทรัพยากรเกินความจำเป็น (Over-provisioning) การคงทรัพยากรที่มีการใช้งานต่ำหรือไม่มีการใช้งาน การไม่สามารถใช้ประโยชน์จากความยืดหยุ่นของคลาวด์ได้อย่างเต็มที่ การคงข้อมูลหรือสำเนาที่ไม่มีความจำเป็น ตลอดจนค่าใช้จ่ายและ**

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การใช้ทรัพยากรที่สูงกว่าที่ควรจะเป็น นอกจากนี้ การนำสถาปัตยกรรมเดิมมาใช้โดยตรงอาจทำให้ไม่สามารถใช้รูปแบบบริการหรือกลไกของคลาวด์ที่เหมาะสมกับภาระงานได้อย่างมีประสิทธิภาพ

ดังนั้น ภายหลังการย้ายระบบ CSC ควรเก็บข้อมูลการใช้งานจริงและทบทวนความเหมาะสมของ **ประเภททรัพยากร (Right Type) ขนาดทรัพยากร (Right Size) รูปแบบการใช้ (Right Use Case) ระดับชั้น (Right Tier) ตำแหน่ง (Right Location) และวงจรชีวิต (Right Lifecycle)** รวมถึงพิจารณาการปรับสถาปัตยกรรมหรือรูปแบบบริการเพิ่มเติมเมื่อมีความเหมาะสม โดยคำนึงถึงความมั่นคงปลอดภัย สมรรถนะ ความพร้อมใช้งาน ความต่อเนื่อง การกู้คืน และข้อกำหนดที่เกี่ยวข้องร่วมด้วย

ด้วยเหตุนี้ **การย้ายระบบขึ้นสู่คลาวด์ควรถูกมองเป็นจุดเริ่มต้นของการปรับปรุงมากกว่าจุดสิ้นสุดของการใช้ทรัพยากรอย่างมีประสิทธิภาพ** และไม่ควรสรุปว่าการย้ายระบบขึ้นสู่คลาวด์เพียงอย่างเดียวทำให้เกิดการลดการใช้ทรัพยากร พลังงาน ค่าใช้จ่าย หรือผลกระทบต่อสิ่งแวดล้อม หากยังไม่มีข้อมูลและผลการวัดที่สามารถตรวจสอบได้รองรับ

5.3.1.2 การวิเคราะห์ลักษณะของภาระงานและความต้องการทรัพยากร

ก่อนเลือกหรือปรับทรัพยากร CSC ควรวิเคราะห์ลักษณะของภาระงาน (Workload Characteristics) และรูปแบบความต้องการใช้ทรัพยากร (Demand Pattern) เพื่อให้สามารถเลือกรูปแบบการจัดสรรและการปรับทรัพยากรได้เหมาะสมกับการใช้งานจริง

การวิเคราะห์ควรพิจารณาอย่างน้อยในประเด็นต่อไปนี้

1. ปริมาณการใช้งานในภาวะปกติและช่วงสูงสุด
2. แนวโน้มการเพิ่มขึ้นหรือลดลงของความต้องการ
3. ความสามารถในการคาดการณ์ช่วงเวลาที่มีการใช้งานสูง
4. ระยะเวลาและช่วงเวลาที่ภาระงานต้องทำงาน
5. ความเร่งด่วนของการประมวลผล
6. ความสามารถในการยอมรับการหยุดชะงักหรือเริ่มประมวลผลใหม่
7. ความต้องการด้านสมรรถนะและระยะเวลาตอบสนอง
8. ความต้องการด้านความพร้อมใช้งานและความต่อเนื่อง
9. ระดับผลกระทบและความสำคัญต่อภารกิจ และ
10. ข้อกำหนดด้านความมั่นคงปลอดภัย กฎหมาย สัญญา และงบประมาณ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

รูปแบบของภาระงานสามารถใช้ประกอบการเลือกแนวทางได้ ตัวอย่างเช่น

ลักษณะของภาระงาน	แนวทางที่อาจพิจารณา
ปริมาณการใช้งานค่อนข้างคงที่	การวางแผนขีดความสามารถรองรับ (Capacity Planning) และการปรับขนาดทรัพยากรให้เหมาะสม (Right-sizing)
มีแนวโน้มเพิ่มขึ้นหรือลดลงที่สามารถคาดการณ์ได้	การวางแผนขีดความสามารถร่วมกับการวิเคราะห์แนวโน้ม
เปลี่ยนแปลงตามวันหรือช่วงเวลาที่ทราบล่วงหน้า	การปรับขนาดทรัพยากรตามกำหนดเวลา (Scheduled Scaling)
เปลี่ยนแปลงตามจำนวนผู้ใช้หรือธุรกรรม	การปรับขนาดทรัพยากรโดยอัตโนมัติ (Auto Scaling)
เพิ่มขึ้นอย่างรวดเร็วและคาดการณ์ได้ยาก	การปรับขนาดโดยอัตโนมัติร่วมกับการติดตามและขอบเขตควบคุม
งานประมวลผลที่ดำเนินการเป็นรอบ	การประมวลผลแบบกลุ่ม (Batch Processing) และการกำหนดช่วงเวลาทำงาน
งานที่ไม่เร่งด่วนและสามารถเริ่มใหม่ได้	ทรัพยากรที่อาจถูกระงับหรือเรียกคืนได้ (Interruptible/Preemptible Resources)
ระบบชั่วคราวหรือใช้เฉพาะบางช่วงเวลา	จัดสรรเมื่อจำเป็นและยกเลิกหรือหยุดเมื่อหมดช่วงการใช้งาน
ระบบสำคัญที่ต้องให้บริการอย่างต่อเนื่อง	ขีดความสามารถที่เพียงพอ ขีดความสามารถสำรอง การปรับขนาด และกลไกด้านความทนทานของบริการ
มีความเสี่ยงจากคำขอจำนวนมากหรือผิดปกติ	การจำกัดอัตราการใช้งาน โควตา การติดตาม และการตรวจจับความผิดปกติ

ภาระงานหนึ่งอาจมีคุณลักษณะมากกว่าหนึ่งรูปแบบ จึงสามารถใช้แนวทางหลายประการร่วมกันได้

5.3.1.3 การเลือกประเภทและขนาดของทรัพยากร

CSC ควรเลือกประเภทของทรัพยากรให้สัมพันธ์กับลักษณะของภาระงาน โดยพิจารณาความต้องการด้านการประมวลผล หน่วยความจำ พื้นที่จัดเก็บ ปริมาณการรับส่งข้อมูล จำนวนธุรกรรม จำนวนการเชื่อมต่อ และตัวชี้วัดด้านสมรรถนะที่เกี่ยวข้อง

เมื่อเลือกประเภทแล้ว ควรกำหนดขนาดและจำนวนทรัพยากรให้สัมพันธ์กับความต้องการจริง โดยอาจจัดให้มี **ขีดความสามารถสำรอง (Capacity Headroom)** ในระดับที่เหมาะสมสำหรับรองรับความผันผวน ความผิดพลาด หรือเหตุการณ์ที่คาดการณ์ได้ตามระดับผลกระทบของระบบ

การกำหนดขนาดจึงควรพิจารณาความสัมพันธ์ระหว่าง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ความต้องการจริง + ขีดความสามารถที่จัดสรร + ขีดความสามารถสำรองที่จำเป็น

ไม่ควรกำหนดเป้าหมายให้ทรัพยากรถูกใช้งานเต็มความสามารถตลอดเวลา เนื่องจากอาจทำให้ไม่มีขีดความสามารถเพียงพอสำหรับรองรับความผันผวนหรือเหตุการณ์ผิดปกติ ขณะเดียวกันควรทบทวนทรัพยากรที่มีอัตราการใช้ประโยชน์ต่ำอย่างต่อเนื่อง เพื่อพิจารณาว่ามีการจัดสรรเกินความจำเป็นหรือไม่

การปรับขนาดทรัพยากรให้เหมาะสมควรอาศัยข้อมูลการใช้งานในช่วงเวลาที่เพียงพอ ไม่ควรพิจารณาจากค่าการใช้งาน ณ ช่วงเวลาใดช่วงเวลาหนึ่งเพียงอย่างเดียว

5.3.1.4 การเลือกรูปแบบการจัดสรรทรัพยากร

นอกจากประเภทและขนาดของทรัพยากรแล้ว CSC ควรเลือกรูปแบบการจัดสรรและการใช้ทรัพยากรให้เหมาะสมกับลักษณะของภาระงาน ระยะเวลาการใช้งาน ความสามารถในการคาดการณ์ และความสำคัญของบริการ

รูปแบบที่อาจพิจารณา ได้แก่

1) **ทรัพยากรที่จัดสรรตามความต้องการ (On-demand Resources)** เหมาะกับภาระงานที่ปริมาณหรือระยะเวลาการใช้งานยังไม่แน่นอน หรือต้องการความยืดหยุ่นในการเพิ่มและลดทรัพยากร
2) **ทรัพยากรที่มีข้อผูกพันการใช้งานล่วงหน้า (Committed-use Resources)** อาจเหมาะกับภาระงานพื้นฐานที่มีการใช้งานค่อนข้างคงที่และสามารถคาดการณ์ได้ในระยะยาว โดย CSC ควรพิจารณาปริมาณความต้องการที่เหมาะสมเพื่อหลีกเลี่ยงการผูกพันทรัพยากรมากกว่าความต้องการจริง
3) **ทรัพยากรที่อาจถูกระงับหรือเรียกคืนได้ (Interruptible/Preemptible Resources)** อาจเหมาะกับภาระงานที่ไม่เร่งด่วน สามารถหยุดและเริ่มดำเนินการใหม่ได้ เช่น งานประมวลผลแบบกลุ่ม งานวิเคราะห์ข้อมูลบางประเภท สภาพแวดล้อมทดสอบ หรืองานเบื้องหลัง หากใช้ทรัพยากรประเภทดังกล่าว ระบบควรได้รับการออกแบบให้สามารถบันทึกสถานะและดำเนินการต่อ (Checkpoint/Resume) หรือเริ่มประมวลผลใหม่ได้ตามความเหมาะสม
4) **ทรัพยากรที่กำหนดช่วงเวลาการใช้งาน** เหมาะกับระบบที่ทราบช่วงเวลาการใช้งาน เช่น ระบบทดสอบ ระบบฝึกอบรม หรือกระบวนการประมวลผลที่ทำงานเฉพาะบางช่วงเวลา การเลือกรูปแบบการจัดสรรควรพิจารณาทั้งประสิทธิภาพการใช้ทรัพยากร ความต่อเนื่องของบริการ และต้นทุนรวม ไม่ควรพิจารณาจากราคาต่อหน่วยเพียงอย่างเดียว

ทรัพยากรที่มีราคาต่อหน่วยต่ำกว่าไม่จำเป็นต้องมีประสิทธิภาพการใช้ทรัพยากรสูงกว่า หากองค์กรจัดสรรหรือผูกพันทรัพยากรไว้มากกว่าความต้องการจริง

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.3.1.5 การปรับทรัพยากรตามความต้องการ

CSC ควรพิจารณาความสามารถในการปรับทรัพยากรตามความต้องการ (Elasticity) เพื่อให้ทรัพยากรสามารถเพิ่มขึ้นเมื่อมีภาระงานเพิ่มและลดลงเมื่อความต้องการลดลง

การปรับทรัพยากรอาจดำเนินการได้หลายลักษณะ ได้แก่

- เพิ่มจำนวนทรัพยากร (Scale-out)
- ลดจำนวนทรัพยากร (Scale-in)
- เพิ่มขนาดหรือความสามารถของทรัพยากร (Scale-up)
- ลดขนาดหรือความสามารถของทรัพยากร (Scale-down)

สำหรับภาระงานที่มีรูปแบบตามช่วงเวลาที่สามารถคาดการณ์ได้ CSC อาจใช้การปรับขนาดทรัพยากรตามกำหนดเวลา ส่วนภาระงานที่เปลี่ยนแปลงตามปริมาณคำขอหรือธุรกรรม อาจพิจารณาการปรับขนาดทรัพยากรโดยอัตโนมัติ

การออกแบบควรรองรับทั้งการเพิ่มและการลดทรัพยากร เพื่อป้องกันไม่ให้ทรัพยากรที่เพิ่มขึ้นในช่วงที่มีความต้องการสูงคงอยู่ต่อเนื่องหลังความต้องการลดลงแล้ว

5.3.1.6 การติดตามและกำหนดเงื่อนไขสำหรับการปรับทรัพยากร

การปรับทรัพยากรควรอาศัยข้อมูลที่สะท้อนภาระงานจริง โดย CSC ควรกำหนดตัวชี้วัดและค่าขีดแบ่ง (Threshold) ที่เหมาะสมกับระบบ

ตัวอย่างข้อมูลที่อาจใช้ ได้แก่

- การใช้หน่วยประมวลผล
- การใช้หน่วยความจำ
- จำนวนคำขอหรือธุรกรรม
- จำนวนการเชื่อมต่อพร้อมกัน
- ความยาวของคิว
- ปริมาณข้อมูลที่ประมวลผล
- ระยะเวลาตอบสนอง
- อัตราความผิดพลาด และ
- ตัวชี้วัดเฉพาะของระบบ

ไม่ควรใช้การใช้หน่วยประมวลผลเพียงตัวเดียวเป็นเงื่อนไขสำหรับทุกภาระงาน เนื่องจากข้อจำกัดของระบบอาจเกิดจากหน่วยความจำ พื้นที่จัดเก็บ ฐานข้อมูล เครือข่าย หรือองค์ประกอบอื่น

ควรกำหนดช่วงเวลาสังเกตการณ์และระยะเวลารอก่อนปรับทรัพยากรซ้ำตามความเหมาะสม เพื่อป้องกันการเพิ่มและลดทรัพยากรถี่เกินไปจากความผันผวนระยะสั้น

ร่างสำหรับ Public Hearing ท่านใช้ - ห้ามใช้อ้างอิง

นอกจากนี้ CSC ควรพิจารณาการตรวจจับความผิดปกติ (Anomaly Detection) โดยเปรียบเทียบการใช้ทรัพยากรกับข้อมูลฐานและแนวโน้มตามปกติ เพื่อช่วยตรวจพบการใช้ทรัพยากรที่ผิดไปจากรูปแบบที่คาดหมาย

5.3.1.7 การกระจายภาระงานและตรวจสอบความพร้อมของทรัพยากร

สำหรับระบบที่ใช้ทรัพยากรหลายหน่วยร่วมกัน CSC ควรพิจารณาการกระจายภาระงาน (Load Balancing) และการตรวจสอบสถานะความพร้อม (Health Check) เพื่อให้คำขอถูกส่งไปยังทรัพยากรที่สามารถให้บริการได้

การกระจายภาระงานควรทำงานร่วมกับการปรับขนาดทรัพยากร เพื่อให้ทรัพยากรที่เพิ่มเข้ามาสามารถรับภาระงานได้อย่างเหมาะสม และทรัพยากรที่อยู่ระหว่างการยกเลิกไม่รับภาระงานใหม่

เมื่อมีการลดจำนวนทรัพยากร ควรดำเนินการอย่างเหมาะสมเพื่อหลีกเลี่ยงการยกเลิกทรัพยากรที่ยังมีธุรกรรมการเชื่อมต่อ หรืองานที่กำลังประมวลผลอยู่ โดยอาจหยุดการส่งงานใหม่ รอให้งานเดิมเสร็จสิ้น หรือถ่ายโอนภาระงานก่อนยกเลิกทรัพยากร

5.3.1.8 การกำหนดขอบเขตควบคุมการใช้ทรัพยากร

ความสามารถในการขยายทรัพยากรโดยอัตโนมัติควรอยู่ภายใต้ขอบเขตควบคุมการใช้ทรัพยากร (Resource Guardrails) เพื่อป้องกันการขยายทรัพยากรเกินระดับที่องค์กรยอมรับได้

เหตุการณ์ เช่น ความผิดพลาดของโปรแกรม การเรียกใช้บริการซ้ำโดยไม่ตั้งใจ หรือการโจมตี อาจทำให้จำนวนคำขอเพิ่มขึ้นและกระตุ้นให้ระบบเพิ่มทรัพยากรโดยอัตโนมัติ ดังนี้ **คำขอผิดปกติเพิ่มขึ้น ⟶ ภาระการประมวลผลเพิ่มขึ้น ⟶ ระบบเพิ่มทรัพยากร ⟶ การใช้ทรัพยากรและค่าใช้จ่ายเพิ่มขึ้น**

CSC จึงควรพิจารณากลไก เช่น

- จำนวนทรัพยากรขั้นต่ำและสูงสุด
- ขนาดสูงสุดของทรัพยากร
- โควตาการใช้ทรัพยากร (Resource Quota)
- การจำกัดอัตราการใช้งาน (Rate Limiting)
- ระดับค่าใช้จ่ายสำหรับการแจ้งเตือน
- การตรวจจับการใช้ทรัพยากรหรือค่าใช้จ่ายผิดปกติ
- การแจ้งเตือนผู้รับผิดชอบ และ
- การอนุมัติเมื่อจำเป็นต้องใช้ทรัพยากรเกินช่วงปกติ

ระดับค่าใช้จ่ายที่กำหนดควรใช้เพื่อแจ้งเตือน ตรวจสอบ หรือยกระดับการตัดสินใจ มากกว่าการหยุดระบบสำคัญโดยอัตโนมัติ เว้นแต่มีการประเมินผลกระทบและออกแบบมาตรการดังกล่าวไว้โดยเฉพาะ

หลักการสำคัญคือ **การปรับทรัพยากรโดยอัตโนมัติควรมีทั้งความสามารถในการขยายเพื่อรองรับภาระงานและกลไกป้องกันไม่ให้ขยายเกินขอบเขตที่องค์กรยอมรับได้**

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.3.1.9 การจัดการทรัพยากรที่ไม่มีการใช้งานหรือมีการใช้ประโยชน์ต่ำ

CSC ควรตรวจสอบทรัพยากรที่ยังถูกจัดสรรหรือเปิดใช้งานแต่ไม่มีการใช้งาน หรือมีการใช้ประโยชน์ต่ำอย่างต่อเนื่อง เพื่อพิจารณาปรับลด รวมใช้ หยุด หรือยกเลิกตามความเหมาะสม

ทรัพยากรที่ควรได้รับการทบทวนอาจรวมถึง

- ทรัพยากรประมวลผลที่ไม่มีภาระงาน
- พื้นที่จัดเก็บที่ไม่ได้เชื่อมโยงกับระบบที่ใช้งาน
- Snapshot หรือสำเนาข้อมูลที่หมดวัตถุประสงค์
- ทรัพยากรเครือข่ายที่ไม่มีการใช้งาน
- สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ การฝึกอบรม หรือการทดลอง และ
- ทรัพยากรชั่วคราวจากโครงการที่สิ้นสุดแล้ว

CSC ควรกำหนดข้อมูลกำกับทรัพยากร (Tag/Metadata) ตามความเหมาะสม เช่น เจ้าของ ระบบหรือบริการ วัตถุประสงค์ สภาพแวดล้อม ระดับความสำคัญ วันที่สร้าง และสถานะในวงจรชีวิต เพื่อสนับสนุนการติดตามและตัดสินใจเกี่ยวกับทรัพยากร

สำหรับระบบที่ไม่จำเป็นต้องทำงานตลอด 24 ชั่วโมง ควรพิจารณากำหนดช่วงเวลาเปิดและปิดทรัพยากรตามรูปแบบการใช้งาน

5.3.1.10 การกำหนดและบริหารโครงสร้างพื้นฐานอย่างเป็นระบบ

CSC ควรพิจารณาการกำหนดโครงสร้างพื้นฐานในรูปแบบรหัส (Infrastructure as Code: IaC) สำหรับระบบหรือทรัพยากรที่เหมาะสม เพื่อให้การจัดเตรียม การเปลี่ยนแปลง และการเลิกใช้ทรัพยากรสามารถดำเนินการได้อย่างสม่ำเสมอ ทำซ้ำได้ และตรวจสอบย้อนกลับได้

IaC สามารถสนับสนุนทั้งด้านความมั่นคงปลอดภัยและประสิทธิภาพการใช้ทรัพยากร เนื่องจากช่วยให้องค์กรกำหนดประเภท ขนาด จำนวน ตำแหน่ง การเชื่อมต่อ และเงื่อนไขของทรัพยากรไว้ในรูปแบบที่สามารถควบคุมและทบทวนได้ ลดความคลาดเคลื่อนจากการตั้งค่าด้วยบุคคล และช่วยให้นำรูปแบบการกำหนดทรัพยากรที่ผ่านการทบทวนแล้วกลับมาใช้ซ้ำได้

CSC ควรพิจารณาการควบคุมอย่างน้อยในประเด็นต่อไปนี้

1. จัดเก็บ IaC ภายใต้ระบบควบคุมรุ่น (Version Control)
2. กำหนดกระบวนการทบทวนและอนุมัติการเปลี่ยนแปลง
3. กำหนดสิทธิในการสร้าง ทบทวน อนุมัติ และนำการเปลี่ยนแปลงไปใช้ตามความเหมาะสม
4. ตรวจสอบข้อผิดพลาดและการกำหนดค่าที่ไม่ปลอดภัยก่อนนำไปใช้
5. ไม่จัดเก็บรหัสผ่าน กุญแจ โทเคน หรือข้อมูลลับไว้ใน IaC โดยตรง
6. เก็บหลักฐานการเปลี่ยนแปลงและการนำไปใช้งาน

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

7. กำหนดวิธีย้อนกลับหรือกู้คืนเมื่อการเปลี่ยนแปลงก่อให้เกิดผลกระทบ และ
8. ปรับปรุง IaC ให้สอดคล้องกับสถานะและข้อกำหนดของระบบ

แนวทางดังกล่าวสอดคล้องกับหลักการของ **NIST Secure Software Development Framework (SSDF), SP 800-218** ซึ่งให้ความสำคัญกับการผนวกแนวปฏิบัติด้านความมั่นคงปลอดภัยไว้ในกระบวนการพัฒนา และการใช้กระบวนการที่สามารถทำซ้ำและตรวจสอบได้

CSC อาจพิจารณาการกำหนดนโยบายในรูปแบบรหัส (Policy as Code) เพื่อให้สามารถตรวจสอบข้อกำหนดบางประการโดยอัตโนมัติก่อนหรือระหว่างการจัดเตรียมทรัพยากร เช่น

- ประเภทหรือขนาดของทรัพยากรที่อนุญาต
- ตำแหน่งที่สามารถจัดวางทรัพยากร
- การเข้ารหัส
- การเปิดเผยบริการต่อสาธารณะ
- การกำหนดเจ้าของหรือข้อมูลกำกับทรัพยากร
- โควตาและขอบเขตการใช้ทรัพยากร และ
- ข้อกำหนดด้านความมั่นคงปลอดภัยอื่นที่สามารถตรวจสอบโดยอัตโนมัติ

การใช้ IaC ควรดำเนินการร่วมกับการตรวจสอบ **ความคลาดเคลื่อนของการกำหนดค่า (Configuration Drift)** ระหว่างสถานะที่กำหนดหรือได้รับอนุมัติไว้กับทรัพยากรที่ใช้งานจริง โดยเฉพาะการเปลี่ยนแปลงที่ดำเนินการนอกกระบวนการควบคุม

เมื่อพบความคลาดเคลื่อน CSC ควรประเมินสาเหตุ ผลกระทบ และกำหนดว่าจะปรับสถานะจริงให้กลับไปสอดคล้องกับค่าที่กำหนด หรือปรับข้อกำหนดที่ได้รับอนุมัติให้สะท้อนการเปลี่ยนแปลงที่มีเหตุผลรองรับ

ดังนั้น IaC มิได้มีบทบาทเพียงการทำให้การจัดเตรียมทรัพยากรเป็นอัตโนมัติ แต่เป็นกลไกที่สามารถสนับสนุน

ความสม่ำเสมอของการกำหนดค่า ⟶ การควบคุมการเปลี่ยนแปลง ⟶ การตรวจสอบย้อนกลับ ⟶ การบังคับใช้นโยบาย ⟶ การควบคุมทรัพยากร ⟶ การเลิกใช้งานอย่างเป็นระบบ

5.3.1.11 การเพิ่มประสิทธิภาพของซอฟต์แวร์และสถาปัตยกรรม

การเพิ่มประสิทธิภาพไม่ควรจำกัดเฉพาะการปรับขนาดโครงสร้างพื้นฐาน เนื่องจากซอฟต์แวร์หรือสถาปัตยกรรมที่ไม่มีประสิทธิภาพอาจทำให้ต้องใช้ทรัพยากรเพิ่มขึ้น แม้โครงสร้างพื้นฐานได้รับการกำหนดขนาดอย่างเหมาะสมแล้ว

CSC ควรร่วมกับผู้รับผิดชอบระบบพิจารณาแนวทาง เช่น

- ลดการประมวลผลซ้ำที่ไม่มีความจำเป็น
- ปรับปรุงการเข้าถึงฐานข้อมูล

ร่างเอกสารเพื่อรับฟังความคิดเห็น (Public Hearing) เท่านั้น - ห้ามใช้อ้างอิง

- ใช้การเก็บข้อมูลชั่วคราว (Caching) เมื่อเหมาะสม
- ใช้การประมวลผลแบบไม่ประสานเวลา (Asynchronous Processing) สำหรับงานที่ไม่จำเป็นต้องตอบสนองทันที
- รวมงานที่เหมาะสมเป็นการประมวลผลแบบกลุ่ม
- ลดการสร้าง จัดเก็บ หรือรับส่งข้อมูลที่ไม่มีความจำเป็น และ
- เลือกรูปแบบสถาปัตยกรรมให้สัมพันธ์กับลักษณะของภาระงาน

การเปลี่ยนแปลงดังกล่าวควรได้รับการตรวจสอบด้านสมรรถนะ ความมั่นคงปลอดภัย ความพร้อมใช้งาน และความถูกต้องของการประมวลผลหลังดำเนินการ

5.3.1.12 การรักษาสมดุลระหว่างประสิทธิภาพ ความพร้อมใช้งาน และความมั่นคงปลอดภัย

การเพิ่มประสิทธิภาพการใช้ทรัพยากรต้องไม่ทำให้ CSC ลดความซ้ำซ้อน ขีดความสามารถสำรอง การสำรองข้อมูล ความสามารถในการกู้คืน หรือมาตรการด้านความมั่นคงปลอดภัยต่ำกว่าระดับที่จำเป็นต่อความเสี่ยงของระบบ

ระดับของทรัพยากรสำรอง ความซ้ำซ้อน และความสามารถในการปรับขนาดควรสัมพันธ์กับระดับผลกระทบความต้องการด้านความพร้อมใช้งาน ระยะเวลาเป้าหมายในการกู้คืน (Recovery Time Objective: RTO) จุดเป้าหมายในการกู้คืน (Recovery Point Objective: RPO) และข้อกำหนดด้านความมั่นคงปลอดภัย

แนวคิดนี้มีความสำคัญต่อการเชื่อมข้อ 5.3 กับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เนื่องจากประกาศของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนดการดำเนินการโดยพิจารณาระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ มิได้กำหนดให้ทุกระบบใช้มาตรการในระดับเดียวกัน

การประเมินความเหมาะสมของทรัพยากรจึงควรพิจารณาร่วมกันอย่างน้อยในมิติต่อไปนี้

ลักษณะภาระงาน + ขีดความสามารถ + การใช้ประโยชน์ + สมรรถนะ + ความพร้อมใช้งาน + ความมั่นคงปลอดภัย + ค่าใช้จ่าย

โดยมีหลักสำคัญว่า **เป้าหมายมิใช่การใช้ทรัพยากรให้เต็มความสามารถมากที่สุดหรือมีค่าใช้จ่ายต่ำที่สุด แต่เป็นการใช้ทรัพยากรในระดับที่เหมาะสมกับภารกิจ ระดับผลกระทบ และความเสี่ยง พร้อมลดทรัพยากรส่วนเกินที่ไม่มีความจำเป็น**

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง



รูปที่ 2 แนวทางการเลือกและปรับทรัพยากรคลาวด์ให้เหมาะสมกับภาระงาน

ร่างสำหรับ Public Hearing

หลักการสำคัญของข้อ 5.3.1

การเลือกและปรับทรัพยากรคลาวด์อย่างมีประสิทธิภาพมิได้หมายถึงการเลือกทรัพยากรที่มีขนาดเล็กที่สุด มีต้นทุนต่ำที่สุด หรือทำให้มีอัตราการใช้ประโยชน์สูงที่สุด แต่หมายถึง การเลือกประเภท ขนาด และรูปแบบการใช้ทรัพยากรให้เหมาะสมกับลักษณะของภาระงาน ความต้องการของบริการ ระดับผลกระทบ และความเสี่ยง พร้อมทั้งสามารถปรับเพิ่ม ปรับลด หรือยกเลิกทรัพยากรเมื่อความต้องการเปลี่ยนแปลง

การดำเนินการควรอาศัยข้อมูลการใช้งานจริง การวางแผนขีดความสามารถ การติดตาม และการกำหนดขอบเขตควบคุม รวมถึงการใช้ระบบอัตโนมัติและการกำหนดโครงสร้างพื้นฐานอย่างเป็นระบบตามความเหมาะสม เพื่อให้สามารถลดทรัพยากรส่วนเกินหรือทรัพยากรที่ไม่มีการใช้งาน โดยไม่ทำให้สมรรถนะ ความพร้อมใช้งาน ความต่อเนื่อง หรือความมั่นคงปลอดภัยต่ำกว่าระดับที่องค์กรยอมรับได้

หลักคิดสำคัญจึงเป็น “ใช้ทรัพยากรให้เหมาะกับภาระงาน และปรับเปลี่ยนตามความต้องการ ภายใต้ขอบเขตด้านความมั่นคงปลอดภัยและความต่อเนื่อง”

5.3.2 การบริหารระดับชั้นการจัดเก็บและวงจรชีวิตข้อมูล

ข้อมูลที่จัดเก็บหรือประมวลผลบนระบบคลาวด์อาจมีความสำคัญ ปริมาณ ความถี่ในการเข้าถึง ความต้องการด้านสมรรถนะ และระยะเวลาการเก็บรักษาที่แตกต่างกัน การจัดเก็บข้อมูลทุกประเภทไว้ในพื้นที่จัดเก็บที่มีระดับสมรรถนะเดียวกันตลอดอายุของข้อมูล อาจทำให้เกิดการใช้ทรัพยากรเกินความจำเป็น ขณะที่การเลือกพื้นที่จัดเก็บโดยพิจารณาจากต้นทุนต่ำที่สุดเพียงอย่างเดียวอาจส่งผลต่อความพร้อมใช้งาน ระยะเวลาในการเรียกคืนข้อมูล หรือความสามารถในการกู้คืนเมื่อเกิดเหตุการณ์

CSC จึงควรบริหารข้อมูลโดยพิจารณาร่วมกันทั้ง **คุณค่าและระดับผลกระทบของข้อมูล รูปแบบและความถี่ในการเข้าถึง ระยะเวลาการเก็บรักษา สมรรถนะที่ต้องการ ความพร้อมใช้งาน ความคงทนของข้อมูล ความสามารถในการกู้คืน ความมั่นคงปลอดภัย ข้อกำหนดทางกฎหมาย และค่าใช้จ่าย** เพื่อให้ข้อมูลได้รับการจัดเก็บในระดับที่เหมาะสมตลอดวงจรชีวิต

หลักการดังกล่าวสอดคล้องกับ **การเลือกระดับชั้นให้เหมาะสม (Right Tier)** และ **การบริหารวงจรชีวิตให้เหมาะสม (Right Lifecycle)** ตามกรอบ 6 Rights ของแนวทางฉบับนี้

ในด้านการกำกับดูแลข้อมูลบนระบบคลาวด์ ISO/IEC 22624:2020 กำหนดกรอบการจัดการข้อมูลตามอนุกรมวิธานสำหรับบริการคลาวด์ (Taxonomy Based Data Handling for Cloud Services) ครอบคลุมประเด็นที่เกี่ยวข้องกับการใช้ การจัดการ การกำกับดูแล ตำแหน่ง และการเคลื่อนย้ายข้อมูล ขณะที่ ISO/IEC 19944-1:2020 กำหนดแนวคิดเกี่ยวกับข้อมูล การไหลของข้อมูล และการใช้ข้อมูลในบริการคลาวด์และแพลตฟอร์มแบบกระจาย

นอกจากนี้ Cloud Security Alliance (CSA) ภายใต้ Cloud Controls Matrix (CCM) ให้ความสำคัญกับการบริหารข้อมูลตลอดวงจรชีวิต ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การเก็บรักษา การจัดเก็บระยะยาว จนถึงการลบหรือทำลายข้อมูล โดยการเก็บรักษาและการลบข้อมูลควรสัมพันธ์กับความต้องการขององค์กรและข้อกำหนดทางกฎหมายหรือกฎระเบียบที่เกี่ยวข้อง

ดังนั้น การเพิ่มประสิทธิภาพด้านพื้นที่จัดเก็บตามข้อ 5.3.2 จึงไม่ใช่เพียงการลดปริมาณข้อมูลหรือค่าใช้จ่าย แต่เป็นการบริหารให้**ข้อมูลที่จำเป็นอยู่ในระดับชั้นที่เหมาะสม ในระยะเวลาที่เหมาะสม และได้รับการลบหรือทำลายเมื่อหมดความจำเป็น โดยยังคงรักษาข้อกำหนดด้านความมั่นคงปลอดภัย ความพร้อมใช้งาน การกู้คืน และกฎหมาย**

5.3.2.1 การจำแนกข้อมูลและเลือกระดับชั้นการจัดเก็บ

ก่อนกำหนดระดับชั้นของพื้นที่จัดเก็บ CSC ควรวิเคราะห์ลักษณะและความต้องการของข้อมูล เพื่อให้สามารถเลือกระดับสมรรถนะของพื้นที่จัดเก็บได้เหมาะสมกับการใช้งานจริง

การพิจารณาควรครอบคลุมอย่างน้อย

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

1. ประเภทและวัตถุประสงค์ของข้อมูล
2. ระดับความสำคัญหรือระดับผลกระทบ
3. ความถี่และรูปแบบการเข้าถึง
4. ปริมาณข้อมูลและแนวโน้มการเพิ่มขึ้น
5. สมรรถนะที่ต้องการในการอ่านและเขียนข้อมูล
6. ระยะเวลาในการเรียกคืนข้อมูลที่ยอมรับได้
7. ระยะเวลาที่ต้องเก็บรักษา
8. ความต้องการด้านความพร้อมใช้งานและความคงทนของข้อมูล
9. ความต้องการด้านการสำรองและกู้คืน
10. ข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล
11. ข้อกำหนดทางกฎหมาย กฎระเบียบ สัญญา และการตรวจสอบ และ
12. ค่าใช้จ่ายในการจัดเก็บ เรียกคืน และรับส่งข้อมูล

CSC ควรใช้ข้อมูลดังกล่าวประกอบการจัดระดับชั้นพื้นที่จัดเก็บ (Storage Tiering) โดยในเชิงหน้าที่อาจจำแนกได้ดังนี้

ลักษณะของข้อมูล	แนวทางการจัดเก็บ
มีการเข้าถึงบ่อยและต้องการการตอบสนองรวดเร็ว	ระดับชั้นสำหรับข้อมูลที่มีการเข้าถึงบ่อย (Frequently Accessed Data Storage)
มีการเข้าถึงเป็นครั้งคราวและสามารถยอมรับข้อจำกัดบางประการในการเรียกคืน	ระดับชั้นสำหรับข้อมูลที่มีการเข้าถึงไม่บ่อย (Infrequently Accessed Data Storage)
มีการเข้าถึงต่ำมากและสามารถยอมรับระยะเวลาในการเรียกคืนที่เพิ่มขึ้น	ระดับชั้นสำหรับข้อมูลที่มีการเข้าถึงต่ำ (Low-access Data Storage)
ต้องเก็บรักษาเป็นระยะเวลานานและไม่ได้ใช้ในการปฏิบัติงานตามปกติ	ระดับชั้นสำหรับการเก็บรักษาระยะยาว (Archival Storage)
ครบกำหนดการเก็บรักษาและไม่มีความจำเป็นต้องเก็บต่อ	การลบหรือทำลายข้อมูลตามกระบวนการที่กำหนด

หมายเหตุ: การจำแนกข้างต้นเป็นการอธิบายระดับชั้นตามลักษณะการใช้งานและความต้องการของข้อมูล มิใช่ชื่อประเภทผลิตภัณฑ์หรือบริการของ CSP รายใดรายหนึ่ง ชื่อเรียก คุณลักษณะ ระยะเวลาในการเรียกคืน และเงื่อนไขของแต่ละระดับชั้นอาจแตกต่างกันระหว่างผู้ให้บริการ

ข้อมูลแต่ละประเภทไม่จำเป็นต้องผ่านทุกระดับชั้นตามลำดับ และไม่จำเป็นต้องเริ่มต้นจากระดับชั้นที่มีสมรรถนะสูงที่สุด หากสามารถกำหนดระดับที่เหมาะสมกับวัตถุประสงค์ได้ตั้งแต่เริ่มต้น

ตัวอย่างเช่น ข้อมูลที่ต้องเก็บรักษาเป็นเวลา 10 ปี แต่อาจถูกเรียกใช้งานเป็นประจำเฉพาะในช่วง 2 ปีแรก ไม่จำเป็นต้องจัดเก็บในระดับสมรรถนะสูงตลอด 10 ปี หากสามารถเปลี่ยนไปยังระดับชั้นสำหรับการเก็บรักษาระยะยาวโดยยังคงตอบสนองข้อกำหนดด้านการเรียกคืน ความมั่นคงปลอดภัย และกฎหมายได้

ร่างสำหรับ Public Hearing ชั่วคราน - ห้ามใช้อ้างอิง

5.3.2.2 การกำหนดและบริหารวงจรชีวิตข้อมูล

CSC ควรกำหนดวงจรชีวิตข้อมูล (Data Lifecycle) ตั้งแต่การสร้างหรือได้รับข้อมูล การใช้งาน การจัดเก็บ การเปลี่ยนระดับชั้น การเก็บรักษาระยะยาว จนถึงการลบหรือทำลายเมื่อหมดความจำเป็น

วงจรดังกล่าวสามารถอธิบายโดยสรุปได้เป็น **สร้างหรือได้รับข้อมูล ⟶ ใช้งาน ⟶ จัดเก็บ ⟶ ทบทวน ⟶ เปลี่ยนระดับชั้น ⟶ เก็บรักษาระยะยาว ⟶ ครบกำหนดการเก็บรักษา ⟶ ลบหรือทำลาย**

การเปลี่ยนระดับชั้นหรือสถานะของข้อมูลอาจพิจารณาจาก

- ระยะเวลานับจากการสร้างหรือแก้ไขข้อมูล
- ระยะเวลานับจากการเข้าถึงครั้งล่าสุด
- ความถี่ในการเข้าถึง
- ประเภทและระดับผลกระทบของข้อมูล
- คุณค่าของข้อมูลต่อภารกิจ
- ระยะเวลาการเก็บรักษา
- ความต้องการด้านการกู้คืน
- ความจำเป็นด้านการตรวจสอบหรือพิสูจน์หลักฐาน และ
- ข้อกำหนดทางกฎหมายหรือสัญญา

เมื่อเหมาะสม CSC ควรพิจารณากำหนด **นโยบายวงจรชีวิต (Lifecycle Policy)** เพื่อให้การเปลี่ยนระดับชั้นการเก็บรักษา หรือการลบข้อมูลสามารถดำเนินการอย่างสม่ำเสมอและเป็นอัตโนมัติ

กลไกอัตโนมัติควรได้รับการกำหนดเงื่อนไขและทดสอบอย่างเหมาะสม เพื่อป้องกันการย้ายหรือลบข้อมูลที่ยังมีความจำเป็น โดยเฉพาะข้อมูลที่อยู่ภายใต้ข้อกำหนดการเก็บรักษา การระงับการทำลายข้อมูลเพื่อวัตถุประสงค์ทางกฎหมาย (Legal Hold) การตรวจสอบ การสืบสวนเหตุการณ์ หรือการเก็บรักษาหลักฐาน

หลักการบริหารตลอดวงจรชีวิตดังกล่าวยังสอดคล้องกับ ISO/IEC TS 20125-1:2026 ซึ่งให้ความสำคัญกับการลดผลกระทบด้านสิ่งแวดล้อมของบริการดิจิทัลตั้งแต่การกำหนดความต้องการ การออกแบบ การดำเนินงาน การบำรุงรักษา จนถึงการสิ้นสุดการใช้งาน มิใช่พิจารณาเฉพาะช่วงการดำเนินงาน

5.3.2.3 การกำหนดระยะเวลาการเก็บรักษาและการจัดการข้อมูลที่หมดความจำเป็น

CSC ควรกำหนดระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period) ให้สัมพันธ์กับวัตถุประสงค์ของข้อมูล ภารกิจ กฎหมาย กฎระเบียบ สัญญา ความจำเป็นในการตรวจสอบ การกู้คืน และการเก็บรักษาหลักฐาน

การที่พื้นที่จัดเก็บบนคลาวด์สามารถขยายได้ง่ายไม่ควรเป็นเหตุให้เก็บข้อมูลไว้โดยไม่มีกำหนด หากไม่มีวัตถุประสงค์หรือข้อกำหนดรองรับการเก็บรักษา

CSC ควรทบทวนข้อมูลที่อาจไม่มีความจำเป็น เช่น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- ข้อมูลที่ครบกำหนดการเก็บรักษา
- ข้อมูลซ้ำซ้อน
- ข้อมูลชั่วคราวจากการประมวลผล
- ไฟล์หรือชุดข้อมูลที่ไม่มีเจ้าของหรือวัตถุประสงค์ชัดเจน
- สำเนาที่หมดวัตถุประสงค์ และ
- ข้อมูลที่เกิดจากระบบหรือบริการที่เลิกใช้งานแล้ว

เมื่อข้อมูลครบกำหนดและไม่มีเหตุผลรองรับการเก็บรักษาต่อ ควรดำเนินการลบหรือทำลายตามกระบวนการที่กำหนด รวมถึงพิจารณาสำเนาที่เกี่ยวข้องตามความเหมาะสม

อย่างไรก็ตาม การลดข้อมูลต้องไม่กระทบต่อข้อกำหนดด้านการเก็บรักษาตามกฎหมาย การระงับการทำลายข้อมูล การตรวจสอบ การสืบสวนเหตุการณ์ หรือการเก็บรักษาหลักฐาน

การบริหารข้อมูลตามหลักดังกล่าวสามารถสนับสนุนทั้ง **การลดข้อมูลที่ไม่จำเป็น (Data Minimization) การลดพื้นที่ความเสี่ยงที่ต้องควบคุม และการเพิ่มประสิทธิภาพการใช้ทรัพยากร** ไปพร้อมกัน

5.3.2.4 การบริหารข้อมูลสำรอง Snapshot และสำเนาข้อมูล

การสำรองข้อมูล (Backup) การสร้าง Snapshot และการทำสำเนาข้อมูล (Replication) มีความสำคัญต่อความพร้อมใช้งาน ความต่อเนื่อง และความสามารถในการฟื้นคืนบริการ แต่หากไม่มีการกำหนดขอบเขตและวงจรชีวิตที่เหมาะสม อาจทำให้มีสำเนาข้อมูลสะสมเป็นจำนวนมาก

CSC ควรกำหนดแนวทางการสำรองและทำสำเนาข้อมูลให้สัมพันธ์กับ

1. ระดับผลกระทบของข้อมูลและระบบ
2. ความสำคัญต่อภารกิจ
3. ระยะเวลาเป้าหมายในการกู้คืน (Recovery Time Objective: RTO)
4. จุดเป้าหมายในการกู้คืน (Recovery Point Objective: RPO)
5. ความเสี่ยงจากการสูญหาย ถูกทำลาย หรือถูกแก้ไขข้อมูล
6. ระยะเวลาการเก็บรักษาข้อมูลสำรอง
7. ความต้องการด้านความสามารถในการฟื้นคืนจากเหตุการณ์ทางไซเบอร์
8. ข้อกำหนดทางกฎหมายและการตรวจสอบ และ
9. ทรัพยากรที่ใช้ในการจัดเก็บ รับส่ง และเรียกคืนข้อมูล

CSC ควรทบทวนจำนวนสำเนา ความถี่ในการสำรอง ระยะเวลาการเก็บรักษา และระดับชั้นของพื้นที่จัดเก็บเพื่อระบุ Backup หรือ Snapshot ที่หมดวัตถุประสงค์หรือเก็บรักษาเกินความจำเป็น

ตัวอย่างเช่น Snapshot ที่สร้างขึ้นก่อนการเปลี่ยนแปลงระบบเพื่อใช้สำหรับการย้อนกลับระยะสั้น ควรมีวัตถุประสงค์ เจ้าของ และระยะเวลาการเก็บรักษาที่ชัดเจน เพื่อป้องกันไม่ให้ทรัพยากรชั่วคราวดังกล่าวกลายเป็นสำเนาข้อมูลที่ถูกเก็บไว้โดยไม่มีกำหนด

ร่างเอกสารเพื่อรับฟังความคิดเห็นสาธารณะ Public Hearing ร่างนี้ ห้ามใช้อ้างอิง

อย่างไรก็ตาม **การเพิ่มประสิทธิภาพการใช้พื้นที่จัดเก็บต้องไม่ใช้เป็นเหตุผลในการลดจำนวนสำเนา ระยะเวลาการเก็บรักษา หรือความสามารถในการกู้คืนให้ต่ำกว่าระดับที่จำเป็นต่อผลกระทบและความเสี่ยงของระบบ**

หลักการนี้สอดคล้องกับโครงสร้างของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ซึ่งกำหนดมาตรการตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

5.3.2.5 การบริหารบันทึกเหตุการณ์และข้อมูลสำหรับการติดตามระบบ

บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Logs) และข้อมูลสำหรับการติดตามระบบ (Telemetry) มีความสำคัญต่อการตรวจจับ วิเคราะห์ ตอบสนอง และสืบสวนเหตุการณ์ แต่การจัดเก็บข้อมูลดังกล่าวในระดับความละเอียดสูงเป็นระยะเวลานานโดยไม่มีการประเมินความจำเป็น อาจทำให้ปริมาณข้อมูลและทรัพยากรที่ใช้เพิ่มขึ้นอย่างต่อเนื่อง

CSC ควรกำหนดอย่างน้อย

- ประเภทของบันทึกเหตุการณ์และข้อมูลติดตามที่จำเป็น
- ระดับรายละเอียดและความถี่ในการเก็บข้อมูล
- ระยะเวลาการเก็บรักษา
- ความสามารถในการค้นหาและวิเคราะห์
- ระยะเวลาในการเรียกคืน
- ความถูกต้องและความครบถ้วน
- การคุ้มครองความสมบูรณ์ของข้อมูล
- ระดับชั้นของพื้นที่จัดเก็บ และ
- เงื่อนไขการเปลี่ยนระดับชั้นหรือลบข้อมูล

ข้อมูลที่จำเป็นต่อการตรวจจับและตอบสนองเหตุการณ์ในปัจจุบันอาจจำเป็นต้องอยู่ในพื้นที่ที่สามารถค้นหาและวิเคราะห์ได้รวดเร็ว ขณะที่ข้อมูลที่พ้นช่วงการใช้งานเชิงปฏิบัติการแต่ยังต้องเก็บเพื่อการตรวจสอบ การพิสูจน์หลักฐาน หรือกฎหมาย อาจย้ายไปยังระดับชั้นสำหรับการเก็บรักษาระยะยาวได้ หากยังคงรักษาความถูกต้อง ความครบถ้วน ความสามารถในการเรียกคืน และคุณค่าของข้อมูลในฐานะหลักฐาน

การลดความละเอียด ปริมาณ หรือระยะเวลาการเก็บบันทึกเหตุการณ์ต้องไม่ทำให้ความสามารถในการตรวจจับ วิเคราะห์ ตอบสนอง สืบสวน หรือพิสูจน์เหตุการณ์ต่ำกว่าระดับที่องค์กรกำหนด

นอกจากนี้ CSC ควรคำนึงว่า **กระบวนการติดตามระบบเองก็สร้างข้อมูลและใช้ทรัพยากร** จึงควรกำหนดระดับรายละเอียดและระยะเวลาการเก็บข้อมูลให้เพียงพอต่อวัตถุประสงค์ด้านการปฏิบัติงานและความมั่นคงปลอดภัย โดยไม่เก็บข้อมูลในระดับที่ละเอียดหรือยาวนานเกินความจำเป็นโดยไม่มีเหตุผลรองรับ

ร่างเอกสารเพื่อ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

5.3.2.6 การติดตามการเติบโตของข้อมูล

CSC ควรติดตามปริมาณและอัตราการเพิ่มขึ้นของข้อมูล (Data Growth) เพื่อให้สามารถแยกการเพิ่มขึ้นที่สัมพันธ์กับการเติบโตของบริการออกจากการเพิ่มขึ้นที่อาจเกิดจากความไม่มีประสิทธิภาพหรือความผิดปกติ

การเพิ่มขึ้นของข้อมูลอาจเกิดจาก

- จำนวนผู้ใช้งานหรือธุรกรรมเพิ่มขึ้น
- การสร้างข้อมูลซ้ำ
- การสร้าง Snapshot หรือ Backup โดยไม่มีนโยบายวงจรชีวิต
- การตั้งค่าบันทึกเหตุการณ์ละเอียดเกินความจำเป็น
- กระบวนการประมวลผลที่สร้างข้อมูลชั่วคราวแต่ไม่มีการลบ
- การทำสำเนาข้อมูลเกินความจำเป็น
- ความผิดพลาดของระบบหรือโปรแกรม หรือ
- เหตุการณ์ด้านความมั่นคงปลอดภัย

CSC ควรกำหนดข้อมูลฐานและค่าขีดแบ่งตามความเหมาะสม เพื่อช่วยตรวจพบกรณีที่ปริมาณข้อมูลหรืออัตราการเติบโตผิดไปจากแนวโน้มที่คาดหมาย

กระบวนการสามารถสรุปได้เป็น **กำหนดข้อมูลฐาน → ติดตาม → ตรวจพบการเติบโตผิดปกติ → วิเคราะห์สาเหตุ → ปรับปรุงหรือแก้ไข → วัดผล**

การเพิ่มขึ้นของปริมาณข้อมูลไม่ควรถูกตีความว่าเป็นความไม่มีประสิทธิภาพโดยอัตโนมัติ หากการเพิ่มขึ้นนั้นสัมพันธ์กับปริมาณบริการหรือความต้องการทางธุรกิจที่เพิ่มขึ้นอย่างมีเหตุผล

5.3.2.7 การจัดการข้อมูลและทรัพยากรเมื่อสิ้นสุดการใช้งาน

เมื่อข้อมูล ระบบ หรือบริการสิ้นสุดการใช้งาน CSC ควรกำหนดกระบวนการเลิกใช้งาน (Decommissioning) เพื่อให้ข้อมูลและทรัพยากรที่เกี่ยวข้องได้รับการจัดการอย่างครบถ้วน และไม่เหลือทรัพยากรที่ไม่มีความจำเป็นหรือข้อมูลที่ขาดการกำกับดูแล

กระบวนการควรพิจารณาอย่างน้อย

1. ยืนยันเจ้าของและการอนุมัติการเลิกใช้งาน
2. ระบุข้อมูลที่ยังต้องเก็บรักษา ส่งคืน หรือเคลื่อนย้าย
3. ตรวจสอบระยะเวลาการเก็บรักษาและการระงับการทำลายข้อมูล
4. ย้ายหรือจัดเก็บข้อมูลที่ยังมีความจำเป็นในระดับชั้นที่เหมาะสม
5. ลบหรือทำลายข้อมูลที่หมดความจำเป็น
6. ตรวจสอบ Backup, Snapshot และสำเนาที่เกี่ยวข้อง
7. ยกเลิกทรัพยากรด้านการประมวลผล พื้นที่จัดเก็บ และเครือข่ายที่หมดความจำเป็น

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

8. ยกเลิกบัญชี สิทธิ กุญแจ โทเคน และการเชื่อมต่อที่เกี่ยวข้อง
9. ตรวจสอบว่ามีทรัพยากรที่ยังคงก่อให้เกิดค่าใช้จ่ายหรือไม่ และ
10. เก็บหลักฐานการเลิกใช้งานตามความเหมาะสม

การดำเนินการดังกล่าวสะท้อนหลัก **การบริหารวงจรชีวิตให้เหมาะสม (Right Lifecycle)** เนื่องจากประสิทธิภาพการใช้ทรัพยากรไม่ได้สิ้นสุดเมื่อระบบหยุดให้บริการ แต่รวมถึงการจัดการข้อมูลและทรัพยากรที่เหลืออยู่หลังสิ้นสุดการใช้งานด้วย

แนวคิดการพิจารณาตลอดวงจรชีวิตยังสอดคล้องกับ OECD ซึ่งเสนอให้พิจารณาผลกระทบด้านสิ่งแวดล้อมของเทคโนโลยีดิจิทัลตลอดวงจรชีวิต และให้ความสำคัญกับการวัดผลอย่างมีขอบเขตและวิธีการที่ชัดเจน มากกว่าการสรุปผลประโยชน์ด้านสิ่งแวดล้อมจากการใช้เทคโนโลยีเพียงอย่างเดียว

หลักการสำคัญของข้อ 5.3.2

การบริหารพื้นที่จัดเก็บอย่างมีประสิทธิภาพและยั่งยืนมิได้หมายถึงการนำข้อมูลทั้งหมดไปจัดเก็บในระดับชั้นที่มีต้นทุนต่ำที่สุด การลดจำนวนสำเนาให้เหลือน้อยที่สุด หรือการลบข้อมูลให้ได้มากที่สุด แต่หมายถึง **การจัดเก็บข้อมูลในระดับชั้นที่เหมาะสมกับคุณค่า รูปแบบการเข้าถึง ระยะเวลาการเก็บรักษา ระดับผลกระทบ และข้อกำหนดที่เกี่ยวข้อง พร้อมปรับเปลี่ยนระดับชั้นหรือสิ้นสุดการเก็บรักษาเมื่อความต้องการเปลี่ยนแปลง โดยไม่ลดทอนความมั่นคงปลอดภัย ความพร้อมใช้งาน และความสามารถในการกู้คืนที่จำเป็น**

ผลจากการดำเนินการสามารถแสดงในรูปของข้อมูลที่ตรวจสอบได้ เช่น ปริมาณข้อมูลที่เปลี่ยนไปยังระดับชั้นที่เหมาะสม ปริมาณข้อมูลที่ครบกำหนดและได้รับการจัดการ สัดส่วนข้อมูลที่อยู่ภายใต้นโยบายวงจรชีวิต หรือจำนวน Snapshot ที่หมดความจำเป็นและได้รับการยกเลิก

การแปลงผลดังกล่าวไปเป็นปริมาณพลังงาน น้ำ หรือการปล่อยก๊าซเรือนกระจกที่ลดลง ควรดำเนินการเฉพาะเมื่อมีข้อมูล ขอบเขต และวิธีการคำนวณที่น่าเชื่อถือรองรับ ซึ่งสอดคล้องกับแนวทางของ OECD ที่ให้ความสำคัญกับการวัดผลกระทบด้านสิ่งแวดล้อมของเทคโนโลยีดิจิทัลอย่างมีหลักฐานและคำนึงถึงวงจรชีวิต

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง



รูปที่ 3 แนวทางการบริหารระดับชั้นการจัดเก็บและวงจรชีวิตข้อมูล

ร่างสำหรับ Public Hearing

5.3.3 การเลือกตำแหน่งของบริการและการลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น

ตำแหน่งของข้อมูล ภาระงาน และองค์ประกอบของบริการคลาวด์มีผลต่อความหน่วงของการสื่อสาร ปริมาณการรับส่งข้อมูล ความพร้อมใช้งาน ความต่อเนื่องของบริการ เขตอำนาจทางกฎหมาย ต้นทุน และการใช้ทรัพยากรของโครงสร้างพื้นฐานดิจิทัล ดังนั้น การเลือกตำแหน่งของข้อมูลหรือบริการไม่ควรพิจารณาจากปัจจัยด้านใดด้านหนึ่งโดยลำพัง แต่ควรพิจารณาความเหมาะสมโดยรวมตามลักษณะของข้อมูล ระบบ ผู้ใช้งาน ภารกิจ และข้อกำหนดที่เกี่ยวข้อง

หลักการดังกล่าวสอดคล้องกับ **การเลือกตำแหน่งให้เหมาะสม (Right Location)** ตามกรอบ 6 Rights โดยมีเป้าหมายให้ข้อมูล การประมวลผล และการให้บริการอยู่ในตำแหน่งที่เหมาะสมกับแหล่งกำเนิดข้อมูล ผู้ใช้งาน รูปแบบการประมวลผล ระดับผลกระทบ และข้อกำหนดด้านความมั่นคงปลอดภัยและกฎหมาย ตลอดจนลดการเคลื่อนย้ายหรือทำสำเนาข้อมูลที่ไม่มีความจำเป็น

ISO/IEC 22624:2020 กำหนดกรอบสำหรับการจัดการข้อมูลในสภาพแวดล้อมคลาวด์ โดยครอบคลุมประเด็นเกี่ยวกับตำแหน่งทางภูมิศาสตร์ของข้อมูล (Data Geolocation) การไหลของข้อมูลข้ามพรมแดน (Cross-border Data Flow) การเข้าถึงข้อมูล การเคลื่อนย้ายข้อมูล และการนำข้อมูลไปใช้ รวมถึงข้อมูลขณะจัดเก็บและขณะรับส่ง ซึ่งเหมาะสำหรับใช้เป็นฐานอ้างอิงในการพิจารณาตำแหน่งและการเคลื่อนย้ายข้อมูลในบริการคลาวด์ และมาตรฐานดังกล่าวได้รับการทบทวนและยืนยันให้ยังคงใช้อยู่ในปี 2025

ดังนั้น การพิจารณาตำแหน่งในข้อ 5.3.3 จึงมิใช่เพียงการเลือกพื้นที่ที่ใกล้ผู้ใช้งานที่สุดหรือมีต้นทุนต่ำที่สุด แต่ควรพิจารณาร่วมกันระหว่าง **ความมั่นคงปลอดภัย ข้อกำหนดทางกฎหมาย ความต่อเนื่อง สมรรถนะ ต้นทุน และประสิทธิภาพการใช้ทรัพยากร**

5.3.3.1 การเลือกตำแหน่งของข้อมูลและภาระงาน

CSC ควรพิจารณาตำแหน่งของข้อมูล การประมวลผล และองค์ประกอบของบริการโดยคำนึงถึงอย่างน้อย

1. ตำแหน่งของผู้ใช้งานหลักและแหล่งกำเนิดข้อมูล
2. ปริมาณและทิศทางของการรับส่งข้อมูล
3. ระดับความหน่วง (Latency) ที่บริการสามารถยอมรับได้
4. ระดับผลกระทบและความอ่อนไหวของข้อมูล
5. ข้อกำหนดด้านสถานที่จัดเก็บหรือประมวลผลข้อมูล
6. เขตอำนาจทางกฎหมายที่เกี่ยวข้อง
7. ความต้องการด้านความพร้อมใช้งานและความต่อเนื่อง
8. ความสามารถในการสำรองและกู้คืน
9. ความสามารถในการเคลื่อนย้ายข้อมูลและบริการ
10. ค่าใช้จ่ายในการรับส่งหรือเรียกคืนข้อมูล และ
11. ประสิทธิภาพการใช้ทรัพยากรและผลกระทบด้านสิ่งแวดล้อม ในกรณีที่มีข้อมูลเพียงพอสำหรับการประเมิน

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้งานอย่างอื่น

การวางข้อมูลหรือภาระงานให้ใกล้กับผู้ใช้งานหรือแหล่งข้อมูลหลักอาจช่วยลดความหน่วงและลดการรับส่งข้อมูลผ่านเครือข่ายที่ไม่มีความจำเป็น อย่างไรก็ตาม ไม่ควรสรุปว่าตำแหน่งที่อยู่ใกล้ที่สุดหรือตั้งอยู่ภายในประเทศย่อมมีผลกระทบด้านสิ่งแวดล้อมต่ำที่สุด เนื่องจากผลดังกล่าวยังขึ้นอยู่กับประสิทธิภาพของศูนย์ข้อมูล แหล่งพลังงาน รูปแบบสถาปัตยกรรม และองค์ประกอบอื่นของโครงสร้างพื้นฐานดิจิทัล

ดังนั้น เป้าหมายของการเลือกตำแหน่งจึงควรเป็น **ความเหมาะสมของตำแหน่งโดยรวม (Location Appropriateness)** มากกว่าการกำหนดตำแหน่งเดียวให้กับทุกระบบ

5.3.3.2 การวิเคราะห์การไหลของข้อมูล

CSC ควรทำความเข้าใจเส้นทางการไหลของข้อมูล (Data Flow) ตั้งแต่แหล่งกำเนิด การจัดเก็บ การประมวลผล การรับส่ง การสำรอง ไปจนถึงการเข้าถึงจากผู้ใช้งานหรือระบบอื่น เพื่อให้สามารถระบุได้ว่าการเคลื่อนย้ายข้อมูลแต่ละรายการมีความจำเป็นหรือสามารถลดลงได้หรือไม่

การวิเคราะห์ควรพิจารณาอย่างน้อยว่า

- ข้อมูลมีต้นทางและปลายทางอยู่ที่ใด
- ข้อมูลถูกส่งระหว่างบริการหรือพื้นที่ใดบ้าง
- การรับส่งเกิดขึ้นบ่อยเพียงใด
- ปริมาณข้อมูลในแต่ละเส้นทางเป็นเท่าใด
- มีการทำสำเนาหรือจำลองข้อมูลหรือไม่
- การเคลื่อนย้ายดังกล่าวมีวัตถุประสงค์ด้านภารกิจ ความพร้อมใช้งาน การสำรอง หรือกฎหมายหรือไม่
- สามารถประมวลผลข้อมูล ณ ตำแหน่งเดิมแทนการเคลื่อนย้ายได้หรือไม่ และ
- มีการเคลื่อนย้ายข้อมูลข้ามประเทศหรือเขตอำนาจทางกฎหมายหรือไม่

ISO/IEC 22624:2020 สนับสนุนการพิจารณาในลักษณะดังกล่าวโดยครอบคลุมทั้งตำแหน่งของข้อมูล การไหลข้ามพรมแดน การเข้าถึง และการเคลื่อนย้ายข้อมูลในบริการคลาวด์

5.3.3.3 การลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น

CSC ควรพิจารณาลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น (Unnecessary Data Movement) โดยไม่กระทบต่อความพร้อมใช้งาน การสำรอง การกู้คืน การตรวจสอบ หรือข้อกำหนดทางกฎหมาย

แนวทางที่อาจพิจารณา ได้แก่

- ประมวลผลข้อมูลใกล้แหล่งกำเนิดหรือแหล่งจัดเก็บ
- ส่งเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์ของบริการ
- ลดการทำสำเนาข้อมูลระหว่างพื้นที่โดยไม่มีเหตุผลรองรับ
- ใช้การเก็บข้อมูลชั่วคราว (Caching) เมื่อสามารถลดการเรียกข้อมูลซ้ำได้
- ใช้การบีบอัดข้อมูล (Compression) เมื่อเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

- เลือกรูปแบบข้อมูลที่เหมาะสมกับการรับส่งและประมวลผล
- รวมข้อมูล (Aggregation) ก่อนรับส่งเมื่อไม่จำเป็นต้องส่งข้อมูลต้นฉบับทั้งหมด และ
- ทบทวนการรับส่งข้อมูลข้ามพื้นที่หรือข้ามประเทศที่เกิดขึ้นเป็นประจำ

การลดการเคลื่อนย้ายข้อมูลไม่ควรถูกกำหนดเป็นเป้าหมายโดยตัวมันเอง แต่ควรพิจารณาว่าการเคลื่อนย้ายข้อมูลดังกล่าวสร้างคุณค่าหรือจำเป็นต่อความมั่นคงปลอดภัย ความต่อเนื่อง หรือภารกิจขององค์กรหรือไม่

5.3.3.4 การใช้เครือข่ายนำส่งเนื้อหาและการเก็บข้อมูลใกล้ผู้ใช้งาน

สำหรับบริการที่มีการส่งเนื้อหาหรือข้อมูลเดิมซ้ำไปยังผู้ใช้งานจำนวนมาก CSC ควรพิจารณาการใช้เครือข่ายนำส่งเนื้อหา (Content Delivery Network: CDN) หรือการเก็บสำเนาข้อมูลใกล้ผู้ใช้งาน (Local Caching) เมื่อเหมาะสมกับลักษณะของข้อมูลและบริการ

แนวทางดังกล่าวสามารถช่วย

- ลดความหน่วงของการให้บริการ
- ลดจำนวนครั้งที่ต้องเรียกข้อมูลจากระบบต้นทาง
- ลดภาระของระบบต้นทาง
- ลดปริมาณข้อมูลที่ต้องรับส่งผ่านเครือข่ายระยะไกลซ้ำหลายครั้ง และ
- เพิ่มความสามารถในการรองรับผู้ใช้งานจำนวนมาก

อย่างไรก็ตาม การใช้ CDN หรือ Caching ควรพิจารณาร่วมกับความอ่อนไหวของข้อมูล การควบคุมการเข้าถึง ตำแหน่งที่ข้อมูลอาจถูกทำสำเนา ความเป็นปัจจุบันของข้อมูล และข้อกำหนดด้านเขตอำนาจทางกฎหมาย

CSC ควรกำหนดระยะเวลาที่ข้อมูลสามารถคงอยู่ในหน่วยความจำชั่วคราว (Cache Lifetime) และเงื่อนไขในการปรับปรุงหรือยกเลิกข้อมูลใน Cache เมื่อข้อมูลต้นทางเปลี่ยนแปลง เพื่อป้องกันทั้งการเรียกข้อมูลต้นทางบ่อยเกินความจำเป็นและการให้บริการข้อมูลที่ล้าสมัย

เป้าหมายจึงเป็นการรักษาสมดุลระหว่าง **ความเป็นปัจจุบันของข้อมูล + สมรรถนะ + ความมั่นคงปลอดภัย + ประสิทธิภาพการใช้ทรัพยากร**

5.3.3.5 การประมวลผลใกล้แหล่งกำเนิดข้อมูล

สำหรับระบบที่สร้างข้อมูลจำนวนมากจากอุปกรณ์ปลายทางหรือแหล่งข้อมูลที่กระจายตัว CSC อาจพิจารณาการประมวลผลใกล้แหล่งกำเนิดข้อมูล (Edge Processing) เพื่อลดปริมาณข้อมูลที่ต้องรับส่งไปยังระบบส่วนกลาง เมื่อเหมาะสมกับลักษณะของบริการ

การดำเนินการอาจประกอบด้วย

- การคัดกรองข้อมูล
- การรวมข้อมูล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- การประมวลผลเบื้องต้น
- การตรวจหาเหตุการณ์หรือเงื่อนไขที่สนใจ
- การส่งเฉพาะผลลัพธ์หรือข้อมูลที่จำเป็น

ตัวอย่างเช่น หากอุปกรณ์ตรวจวัดสร้างข้อมูลอย่างต่อเนื่อง แต่ระบบส่วนกลางต้องการเพียงค่าผิดปกติหรือข้อมูลสรุป การประมวลผลใกล้แหล่งข้อมูลอาจช่วยลดปริมาณข้อมูลที่ต้องส่งเข้าสู่ระบบส่วนกลางได้

อย่างไรก็ตาม การเพิ่มองค์ประกอบประมวลผลบริเวณปลายทางทำให้เกิดองค์ประกอบที่ต้องได้รับการรักษาความมั่นคงปลอดภัยเพิ่มเติม จึงควรพิจารณาการควบคุมสิทธิ การปรับปรุงซอฟต์แวร์ การติดตามสถานะ ความถูกต้องของข้อมูล และการบริหารอุปกรณ์ปลายทางร่วมด้วย

ITU-T มีมาตรฐานด้านการออกแบบการประหยัดพลังงานของศูนย์ข้อมูลคลาวด์และเอดจ์ โดยให้ความสำคัญกับการประสานการออกแบบของ Cloud และ Edge Data Centers เพื่อเพิ่มประสิทธิภาพด้านพลังงาน ซึ่งสะท้อนว่าการจัดวางการประมวลผลระหว่างส่วนกลางและส่วนปลายเป็นหนึ่งในองค์ประกอบของประสิทธิภาพโครงสร้างพื้นฐานดิจิทัล

5.3.3.6 การจัดวางการประมวลผลให้ใกล้กับข้อมูล

สำหรับภาระงานที่ต้องประมวลผลข้อมูลปริมาณมาก CSC ควรพิจารณาการจัดวางการประมวลผลให้ใกล้กับตำแหน่งที่ข้อมูลถูกจัดเก็บ (Data Locality) เมื่อสามารถลดการเคลื่อนย้ายข้อมูลขนาดใหญ่ได้อย่างมีนัยสำคัญ

หลักการดังกล่าวมีประโยชน์กับภาระงาน เช่น

- การวิเคราะห์ข้อมูลจำนวนมาก
- การประมวลผลข้อมูลแบบกลุ่ม
- การสร้างดัชนีหรือค้นหาข้อมูล
- การประมวลผลภาพหรือสื่อขนาดใหญ่
- การประมวลผลชุดข้อมูลเดิมซ้ำหลายครั้ง

อย่างไรก็ตาม การเลือกตำแหน่งของการประมวลผลต้องพิจารณาร่วมกับข้อกำหนดด้านตำแหน่งของข้อมูล เขตอำนาจทางกฎหมาย การควบคุมการเข้าถึง ความพร้อมใช้งาน และการกู้คืน

ดังนั้น หลักการ Data Locality มิได้หมายความว่า “ต้องนำการประมวลผลไปอยู่ใกล้ข้อมูลเสมอ” แต่หมายถึงการนำระยะทางและปริมาณการเคลื่อนย้ายข้อมูลมาเป็นปัจจัยหนึ่งในการตัดสินใจด้านสถาปัตยกรรม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามอ้างอิง

5.3.3.7 การลดขนาดข้อมูลในการจัดเก็บและรับส่ง

CSC ควรพิจารณาเทคนิคที่ช่วยลดปริมาณข้อมูลที่ต้องจัดเก็บหรือรับส่ง โดยไม่ทำให้สูญเสียคุณค่าหรือสาระที่จำเป็นต่อภารกิจ

แนวทางอาจประกอบด้วย

- การบีบอัดข้อมูล (Compression)
- การรวมข้อมูล (Aggregation)
- การลดข้อมูลซ้ำซ้อน (Deduplication)
- การเลือกรูปแบบข้อมูลที่มีประสิทธิภาพ
- การส่งเฉพาะข้อมูลที่มีการเปลี่ยนแปลง
- การเลือกส่งเฉพาะข้อมูลที่จำเป็น และ
- การลดความละเอียดของข้อมูลในกรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูลต้นฉบับเต็มรูปแบบ

การลดข้อมูลต้องไม่กระทบต่อความถูกต้อง ความครบถ้วน คุณภาพของข้อมูล ความสามารถในการตรวจสอบย้อนกลับ หรือความสามารถในการใช้ข้อมูลเป็นหลักฐาน

ในกรณีข้อมูลที่มีความสำคัญต่อการพิสูจน์เหตุการณ์หรือการตรวจสอบ ไม่ควรลดรายละเอียดหรือแปลงรูปแบบจนทำให้ข้อมูลสูญเสียคุณสมบัติที่จำเป็นต่อวัตถุประสงค์ดังกล่าว

5.3.3.8 การควบคุมปริมาณคำขอและการใช้งานที่ผิดปกติ

CSC ควรพิจารณาการจำกัดอัตราการใช้งาน (Rate Limiting) โควตาการใช้บริการ (Service Quota) หรือกลไกควบคุมอื่นตามความเหมาะสม เพื่อป้องกันการใช้ทรัพยากรเกินความจำเป็นอันเกิดจาก

- ความผิดพลาดของโปรแกรม
- การเรียกใช้บริการซ้ำโดยไม่ตั้งใจ
- การตั้งค่าที่ไม่เหมาะสม
- กระบวนการอัตโนมัติที่ทำงานผิดปกติ
- รูปแบบการใช้งานที่ผิดปกติ หรือ
- เหตุการณ์ด้านความมั่นคงปลอดภัยที่ก่อให้เกิดคำขอจำนวนมาก

กลไกดังกล่าวควรทำงานร่วมกับการติดตาม การแจ้งเตือน และกระบวนการตอบสนองเหตุการณ์ เพื่อให้สามารถแยกการเพิ่มขึ้นของภาระงานตามปกติออกจากเหตุการณ์ผิดปกติ

ประเด็นนี้ควรเชื่อมโยงกับการปรับขนาดทรัพยากรโดยอัตโนมัติตามข้อ 5.3.1 เนื่องจากหากระบบเพิ่มทรัพยากรตามจำนวนคำขอโดยไม่มีขอบเขตควบคุม เหตุการณ์ผิดปกติอาจทำให้ระบบเพิ่มทรัพยากรอย่างต่อเนื่อง ทั้งที่คำขอดังกล่าวไม่ได้เกิดจากความต้องการใช้งานที่แท้จริง

ร่างเอกสารเพื่อ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

หลักการสำคัญคือ **กลไกปรับขนาดใช้เพื่อรองรับความต้องการที่แท้จริง ขณะที่การจำกัดอัตราการใช้งานโควตา และขอบเขตควบคุมช่วยป้องกันไม่ให้ความยืดหยุ่นของคลาวด์ขยายผลจากความผิดปกติโดยไม่มีขอบเขต**

5.3.3.9 การกำหนดระดับการทำสำเนาและความซ้ำซ้อนตามความจำเป็น

การทำสำเนาข้อมูลหรือกระจายระบบไปยังหลายตำแหน่งสามารถเพิ่มความพร้อมใช้งานและความสามารถในการกู้คืน แต่ในขณะเดียวกันทำให้เกิดการใช้พื้นที่จัดเก็บ การรับส่งข้อมูล และทรัพยากรประมวลผลเพิ่มขึ้น

CSC ควรกำหนดระดับการทำสำเนาและความซ้ำซ้อน (Redundancy) ให้สัมพันธ์กับ

1. ระดับผลกระทบของระบบ
2. ความต้องการด้านความพร้อมใช้งาน
3. ระยะเวลาเป้าหมายในการกู้คืน (RTO)
4. จุดเป้าหมายในการกู้คืน (RPO)
5. ความเสี่ยงจากการสูญเสียพื้นที่ให้บริการ
6. ความต้องการด้านความสามารถในการฟื้นคืนจากเหตุการณ์ทางไซเบอร์
7. ข้อกำหนดด้านตำแหน่งข้อมูลและกฎหมาย และ
8. ทรัพยากรและค่าใช้จ่ายที่เกิดจากการทำสำเนา

ไม่ควรกำหนดให้ทุกระบบใช้ระดับการทำสำเนาหรือความซ้ำซ้อนสูงสุดในลักษณะเดียวกัน หากระดับผลกระทบและความต้องการของบริการแตกต่างกัน

หลักการคือ **ระดับความซ้ำซ้อนควรเพียงพอต่อความต้องการด้านความพร้อมใช้งานและความสามารถในการฟื้นคืน แต่ไม่ควรสูงเกินความจำเป็นโดยไม่มีเหตุผลรองรับ**

5.3.3.10 ความสัมพันธ์กับตำแหน่งข้อมูลและเขตอำนาจทางกฎหมาย

การเพิ่มประสิทธิภาพด้านตำแหน่งและการเคลื่อนย้ายข้อมูลต้องไม่ทำให้การจัดเก็บหรือประมวลผลข้อมูลขัดต่อข้อกำหนดด้านอธิปไตยข้อมูล เขตอำนาจทางกฎหมาย หรือการโอนข้อมูลข้ามประเทศ

CSC ควรสามารถระบุได้อย่างน้อยว่า

- ข้อมูลถูกจัดเก็บหรือประมวลผลที่ใด
- ข้อมูลสำรองหรือสำเนาสามารถอยู่ที่ใด
- ข้อมูลอาจถูกส่งข้ามประเทศหรือไม่
- บุคลากรจากตำแหน่งใดสามารถเข้าถึงข้อมูล
- CSP หรือผู้ให้บริการช่วงสามารถเคลื่อนย้ายข้อมูลหรือไม่ และ
- CSC สามารถเรียกคืนหรือเคลื่อนย้ายข้อมูลของตนได้อย่างไร

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ISO/IEC 22624:2020 ครอบคลุมโดยตรงถึงตำแหน่งข้อมูล การไหลข้ามพรมแดน การเข้าถึง และการเคลื่อนย้ายข้อมูล จึงควรเป็นแหล่งอ้างอิงหลักของประเด็นนี้

รายละเอียดเชิงข้อกำหนดด้านอธิปไตยข้อมูลและกฎหมายควรเชื่อมโยงกับข้อ 5.1 ของแนวทางฉบับนี้ เพื่อหลีกเลี่ยงการกำหนดข้อกำหนดซ้ำในข้อ 5.3

5.3.3.11 การพิจารณาประสิทธิภาพและผลด้านสิ่งแวดล้อมของตำแหน่งบริการ

ตำแหน่งของศูนย์ข้อมูลและโครงสร้างพื้นฐานที่ใช้ให้บริการอาจมีผลต่อประสิทธิภาพด้านพลังงาน การใช้น้ำ การปล่อยก๊าซเรือนกระจก และผลกระทบด้านสิ่งแวดล้อมอื่น เนื่องจากแต่ละพื้นที่อาจมีสภาพภูมิอากาศ แหล่งพลังงาน ระบบไฟฟ้า เทคโนโลยีระบายความร้อน และประสิทธิภาพของโครงสร้างพื้นฐานแตกต่างกัน

ITU-T L.1312 ซึ่งได้รับอนุมัติในปี 2026 กำหนดกรอบหลายมิติสำหรับประเมินผลการดำเนินงานด้านสิ่งแวดล้อมของศูนย์ข้อมูลตลอดวงจรชีวิต โดยครอบคลุมประสิทธิภาพพลังงาน ประสิทธิภาพการใช้ทรัพยากร การปล่อยก๊าซเรือนกระจก และผลกระทบด้านสิ่งแวดล้อม ซึ่งสนับสนุนแนวคิดว่าการประเมินศูนย์ข้อมูลไม่ควรพิจารณาตัวชี้วัดด้านพลังงานเพียงค่าเดียว

ดังนั้น หาก CSC มีข้อมูลที่เชื่อถือได้เกี่ยวกับประสิทธิภาพด้านพลังงาน การใช้ทรัพยากร แหล่งพลังงาน หรือผลกระทบด้านสิ่งแวดล้อมของพื้นที่ให้บริการ อาจนำข้อมูลดังกล่าวมาใช้เป็นปัจจัยประกอบการตัดสินใจได้

อย่างไรก็ตาม ไม่ควรเลือกพื้นที่ให้บริการโดยพิจารณาปัจจัยด้านสิ่งแวดล้อมเพียงอย่างเดียว หากขัดกับข้อกำหนดด้านกฎหมาย ความมั่นคงปลอดภัย ความต่อเนื่อง หรือภารกิจ

ในเชิงหลักการ อาจพิจารณาตามลำดับดังนี้ **ข้อกำหนดด้านข้อมูลและกฎหมาย ⟶ ความมั่นคงปลอดภัยและระดับผลกระทบ ⟶ ความพร้อมใช้งานและความต่อเนื่อง ⟶ สมรรถนะและตำแหน่งของผู้ใช้งาน/ข้อมูล ⟶ ต้นทุนและการเคลื่อนย้ายข้อมูล ⟶ ประสิทธิภาพการใช้ทรัพยากรและผลด้านสิ่งแวดล้อม**

ลำดับดังกล่าวมิได้หมายความว่าปัจจัยแต่ละด้านต้องมีน้ำหนักเท่ากัน แต่มีวัตถุประสงค์เพื่อให้มั่นใจว่า การพิจารณาด้านความยั่งยืน (Sustainability) ไม่ถูกนำมาใช้แทนข้อกำหนดพื้นฐานด้านความมั่นคงปลอดภัย (Security) และการปฏิบัติตามข้อกำหนด (Compliance)

หลักการสำคัญของข้อ 5.3.3

การเลือกตำแหน่งและการบริหารการเคลื่อนย้ายข้อมูลอย่างมีประสิทธิภาพมิได้หมายถึงการเก็บข้อมูลไว้ในพื้นที่เดียว การลดการทำสำเนาให้เหลือน้อยที่สุด หรือการเลือกพื้นที่ที่ใกล้ผู้ใช้งานที่สุดเสมอไป แต่หมายถึง **การจัดวางข้อมูล การประมวลผล และการนำส่งบริการในตำแหน่งที่เหมาะสมกับภารกิจ ผู้ใช้งาน ข้อกำหนดความเสี่ยง และรูปแบบการรับส่งข้อมูล พร้อมลดการเคลื่อนย้ายและการทำสำเนาที่ไม่มีความจำเป็น**

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing ร่างนี้ ยังไม่ใช่ฉบับจริง

ผลจากการดำเนินการอาจแสดงได้จากข้อมูลที่ตรวจสอบได้ เช่น ปริมาณการรับส่งข้อมูลที่ลดลง ความหน่วงที่ดีขึ้น ปริมาณข้อมูลที่ไม่ต้องส่งกลับไปยังระบบต้นทาง ปริมาณข้อมูลที่ได้รับการประมวลผลหรือรวมก่อนรับส่ง หรือจำนวนเส้นทางการทำสำเนาที่ได้รับการทบทวน

การลดปริมาณการรับส่งข้อมูลไม่ควรถูกแปลงเป็นปริมาณพลังงานหรือการปล่อยก๊าซเรือนกระจกที่ลดลงโดยตรง เว้นแต่มีข้อมูล ขอบเขต และวิธีการคำนวณที่สามารถตรวจสอบได้รองรับ



รูปที่ 4 แนวทางการเลือกตำแหน่งและลดการเคลื่อนย้ายข้อมูลที่ไม่จำเป็น

5.3.4 การวัด ติดตาม และปรับปรุงประสิทธิภาพการใช้ทรัพยากร

การใช้ทรัพยากรคลาวด์อย่างมีประสิทธิภาพและยั่งยืนควรสามารถวัด ติดตาม และประเมินผลได้อย่างเป็นระบบ เพื่อให้องค์กรสามารถทราบได้ว่าการปรับปรุงที่ดำเนินการทำให้การใช้ทรัพยากรมีความเหมาะสมมากขึ้นเพียงใด และส่งผลกระทบต่อสมรรถนะ ความพร้อมใช้งาน ความต่อเนื่อง ความมั่นคงปลอดภัย ค่าใช้จ่าย หรือภารกิจขององค์กรหรือไม่

การประเมินไม่ควรพิจารณาจากการลดจำนวนทรัพยากรหรือลดค่าใช้จ่ายเพียงอย่างเดียว เนื่องจากการใช้ทรัพยากรที่เพิ่มขึ้นอาจเกิดจากการขยายตัวของบริการ จำนวนผู้ใช้งาน หรือปริมาณธุรกรรมที่เพิ่มขึ้น ขณะที่การใช้ทรัพยากรที่ลดลงอาจเกิดจากการลดระดับบริการหรือขีดความสามารถรองรับจนไม่เพียงพอต่อภารกิจ

ร่างสำหรับ PU

ดังนั้น การประเมินควรพิจารณาร่วมกันอย่างน้อย 3 มิติ ได้แก่

1. ปริมาณทรัพยากรที่ใช้
2. ปริมาณงานหรือผลลัพธ์ของบริการ
3. ระดับคุณภาพและข้อกำหนดที่ต้องรักษา เช่น สมรรถนะ ความพร้อมใช้งาน ความต่อเนื่อง และความมั่นคงปลอดภัย

แนวคิดดังกล่าวสอดคล้องกับมาตรฐานในกลุ่ม ISO/IEC 30134 ซึ่งกำหนดหลักการและตัวชี้วัดสำหรับประสิทธิผลและประสิทธิภาพการใช้ทรัพยากรของศูนย์ข้อมูล โดยให้ความสำคัญกับการกำหนดขอบเขต วิธีการวัด และเงื่อนไขของตัวชี้วัดอย่างชัดเจน เพื่อให้ผลที่ได้สามารถตีความและเปรียบเทียบได้อย่างเหมาะสม

สำหรับ CSC ที่ใช้บริการคลาวด์สาธารณะ การวัดควรเน้นตัวชี้วัดที่อยู่ภายใต้การควบคุมหรือสามารถเข้าถึงข้อมูลได้จริง เช่น จำนวนทรัพยากรที่จัดสรร ปริมาณข้อมูลที่จัดเก็บ ปริมาณการรับส่งข้อมูล ระยะเวลาที่ทรัพยากรถูกเปิดใช้งาน รูปแบบการใช้บริการ และค่าใช้จ่าย โดยไม่จำเป็นต้องเข้าถึงข้อมูลการดำเนินงานภายในของศูนย์ข้อมูลของ CSP

5.3.4.1 การกำหนดข้อมูลฐานและขอบเขตการวัด

CSC ควรกำหนดข้อมูลฐาน (Baseline) ก่อนดำเนินการปรับปรุง เพื่อให้สามารถเปรียบเทียบผลก่อนและหลังการดำเนินการได้อย่างมีความหมาย

ข้อมูลฐานควรครอบคลุมตามความเหมาะสม ได้แก่

1. ระบบ บริการ หรือภาระงานที่อยู่ในขอบเขต
2. ช่วงเวลาที่ใช้เป็นข้อมูลฐาน
3. จำนวนและประเภทของทรัพยากรที่จัดสรร
4. การใช้หน่วยประมวลผล หน่วยความจำ และทรัพยากรที่เกี่ยวข้อง
5. ปริมาณและระดับชั้นของพื้นที่จัดเก็บ
6. ปริมาณการรับส่งข้อมูล
7. จำนวนผู้ใช้งาน ธุรกรรม หรือหน่วยบริการ
8. ระดับสมรรถนะและความพร้อมใช้งาน
9. ทรัพยากรที่ไม่มีการใช้งานหรือมีการใช้ประโยชน์ต่ำ
10. ค่าใช้จ่ายที่เกี่ยวข้องกับการใช้ทรัพยากร และ
11. ข้อกำหนดหรือข้อจำกัดที่อาจมีผลต่อการปรับปรุง

ข้อมูลฐานควรใช้ช่วงเวลาที่สะท้อนรูปแบบการใช้งานตามปกติของระบบ และควรพิจารณาช่วงที่มีการใช้งานสูงหรือมีความผันผวนตามฤดูกาล หากมีผลต่อการตัดสินใจ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้งานจริง

หากมีการเปลี่ยนแปลงขอบเขตของระบบอย่างมีนัยสำคัญ เช่น จำนวนผู้ใช้งานเพิ่มขึ้นมาก มีการรวมระบบหรือเปลี่ยนสถาปัตยกรรม ควรระบุข้อจำกัดในการเปรียบเทียบกับข้อมูลฐานเดิม หรือกำหนดข้อมูลฐานใหม่ตามความเหมาะสม

5.3.4.2 การติดตามการใช้ทรัพยากร

CSC ควรกำหนดการติดตามการใช้ทรัพยากร (Resource Monitoring) ในระดับที่เหมาะสมกับความสำคัญของระบบ เพื่อสนับสนุนการวางแผนขีดความสามารถรองรับ การปรับขนาด การตรวจจับทรัพยากรส่วนเกิน และการระบุรูปแบบการใช้งานที่ผิดปกติ

ข้อมูลที่อาจนำมาใช้ ได้แก่

- การใช้หน่วยประมวลผล
- การใช้หน่วยความจำ
- ปริมาณพื้นที่จัดเก็บและอัตราการเพิ่มขึ้น
- ปริมาณการรับส่งข้อมูล
- จำนวนคำขอหรือธุรกรรม
- จำนวนผู้ใช้งานพร้อมกัน
- ความยาวของคิว
- ระยะเวลาตอบสนอง
- อัตราความผิดพลาด
- จำนวนทรัพยากรที่เปิดใช้งาน
- ระยะเวลาที่ทรัพยากรถูกจัดสรร
- ค่าใช้จ่าย และ
- ตัวชี้วัดเฉพาะของภาระงาน

การติดตามควรสัมพันธ์กับวัตถุประสงค์ของระบบ ไม่จำเป็นต้องเก็บข้อมูลทุกประเภทด้วยความละเอียดสูงตลอดเวลา หากข้อมูลดังกล่าวไม่จำเป็นต่อการตัดสินใจ การตรวจสอบ หรือการรักษาความมั่นคงปลอดภัย

หลักการนี้ควรเชื่อมโยงกับข้อ 5.3.2 โดยเฉพาะการบริหารบันทึกเหตุการณ์และข้อมูลสำหรับการติดตามระบบ เนื่องจากกระบวนการติดตามเองก็สร้างข้อมูลและใช้พื้นที่จัดเก็บ จึงควรกำหนดระดับรายละเอียดและระยะเวลาการเก็บรักษาให้เหมาะสมกับวัตถุประสงค์

5.3.4.3 การกำหนดค่าขีดแบ่งและการตรวจจับความผิดปกติ

CSC ควรกำหนดค่าขีดแบ่ง (Threshold) หรือเงื่อนไขสำหรับการแจ้งเตือน การทบทวน หรือการปรับทรัพยากร โดยอ้างอิงจากข้อมูลฐาน รูปแบบการใช้งาน และระดับบริการที่กำหนด

ค่าขีดแบ่งอาจใช้สำหรับ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

- แจ้งเตือนเมื่อทรัพยากรใกล้ถึงขีดจำกัด
- เพิ่มหรือลดขีดความสามารถรองรับ
- ตรวจพบการเติบโตของข้อมูลที่ผิดปกติ
- ตรวจพบปริมาณการรับส่งข้อมูลที่สูงผิดปกติ
- แจ้งเตือนค่าใช้จ่าย
- ตรวจพบทรัพยากรที่ไม่มีการใช้งาน หรือ
- ตรวจพบการใช้ทรัพยากรต่ำหรือสูงกว่าช่วงที่คาดหมาย

ไม่ควรกำหนดค่าขีดแบ่งเดียวกันสำหรับทุกระบบ เนื่องจากภาระงานแต่ละประเภทมีลักษณะและข้อจำกัดแตกต่างกัน

นอกจากค่าขีดแบ่งแล้ว CSC ควรพิจารณาการตรวจจับความผิดปกติ (Anomaly Detection) โดยเปรียบเทียบพฤติกรรมปัจจุบันกับข้อมูลฐานและแนวโน้มการใช้งานตามปกติ เพื่อให้สามารถตรวจพบความผิดปกติได้ก่อนที่จะถึงค่าขีดแบ่งที่กำหนด

ตัวอย่างเช่น หากระบบหนึ่งมีการใช้หน่วยประมวลผลตามปกติอยู่ที่ประมาณร้อยละ 20 การเพิ่มขึ้นเป็นร้อยละ 60 อย่างต่อเนื่องอาจเป็นเหตุให้ต้องตรวจสอบ แม้ยังไม่ถึงค่าขีดแบ่งที่กำหนดไว้ที่ร้อยละ 80

ดังนั้น การติดตามที่มีประสิทธิผลควรพิจารณาร่วมกันระหว่าง **ข้อมูลฐาน (Baseline) + แนวโน้ม (Trend) + ค่าขีดแบ่ง (Threshold) + การตรวจจับความผิดปกติ (Anomaly Detection)**

5.3.4.4 การกำหนดตัวชี้วัดประสิทธิภาพการใช้ทรัพยากร

CSC ควรเลือกตัวชี้วัดที่สัมพันธ์กับลักษณะของระบบและสามารถเก็บข้อมูลได้จริง โดยไม่จำเป็นต้องใช้ตัวชี้วัดทุกประเภทกับทุกระบบ

ตัวชี้วัดสามารถแบ่งออกเป็น 4 กลุ่ม ดังนี้

1) ตัวชี้วัดด้านการจัดสรรและการใช้ทรัพยากร

ใช้ประเมินว่าทรัพยากรที่จัดสรรมีความสัมพันธ์กับการใช้งานจริงเพียงใด เช่น อัตราการใช้ทรัพยากร จำนวนทรัพยากรที่ไม่มีการใช้งาน ขีดความสามารถส่วนเกิน และระยะเวลาที่ทรัพยากรถูกเปิดใช้งานโดยไม่มีภาระงาน

2) ตัวชี้วัดด้านข้อมูลและพื้นที่จัดเก็บ

ใช้ประเมินประสิทธิผลของการจัดระดับชั้นพื้นที่จัดเก็บและการบริหารวงจรชีวิตข้อมูล เช่น ปริมาณข้อมูลที่เปลี่ยนระดับชั้น ปริมาณข้อมูลที่ครบกำหนดและได้รับการลบ สัดส่วนข้อมูลภายใต้นโยบายวงจรชีวิต และปริมาณ Snapshot หรือ Backup ที่หมดความจำเป็น

3) ตัวชี้วัดด้านเครือข่ายและการเคลื่อนย้ายข้อมูล

ร่างเอกสารเพื่อรับฟังความคิดเห็น (Public Hearing) เท่านั้น - ห้ามใช้อ้างอิง

ใช้ประเมินประสิทธิภาพของการเลือกตำแหน่งและการลดการเคลื่อนย้ายข้อมูล เช่น ปริมาณการรับส่งข้อมูลข้ามพื้นที่ ปริมาณข้อมูลที่ลดลงจากการใช้ Cache หรือ CDN และปริมาณข้อมูลที่ลดลงจากการประมวลผลใกล้แหล่งข้อมูล

4) ตัวชี้วัดประสิทธิภาพต่อหน่วยผลลัพธ์

ใช้เปรียบเทียบทรัพยากรที่ใช้กับปริมาณงานหรือผลลัพธ์ของบริการ เช่น ทรัพยากรประมวลผลต่อธุรกรรม พื้นที่จัดเก็บต่อผู้ใช้ หรือปริมาณการรับส่งข้อมูลต่อหน่วยบริการ

กลุ่มที่ 4 มีความสำคัญ เพราะช่วยแยกกรณีที่ทรัพยากรเพิ่มขึ้นเนื่องจากบริการเติบโตออกจากกรณีที่ทรัพยากรเพิ่มขึ้นจากความไม่มีประสิทธิภาพ

5.3.4.5 ตัวอย่างตัวชี้วัด

ตารางต่อไปนี้เป็นตัวอย่างสำหรับเลือกใช้ตามความเหมาะสม มิใช่ข้อกำหนดให้ทุกระบบต้องใช้ตัวชี้วัดทั้งหมด

ประเด็น	ตัวชี้วัดตัวอย่าง	วิธีการวัดตัวอย่าง
การปรับขนาด	**อัตราความครอบคลุมของการทบทวนขนาดทรัพยากร (Right-sizing Coverage)**	ทรัพยากรที่ได้รับการทบทวน ÷ ทรัพยากรในขอบเขต × 100
การปรับขนาด	**อัตราการดำเนินการปรับขนาด**	ทรัพยากรที่ได้รับการปรับ ÷ ทรัพยากรที่พบว่าไม่เหมาะสม × 100
ทรัพยากรที่ไม่ได้ใช้งาน	**การลดทรัพยากรที่ไม่มีการใช้งาน**	จำนวนทรัพยากรที่ยกเลิก รวมใช้ หยุด หรือปรับลด
ระยะเวลาที่ไม่ได้ใช้	**ระยะเวลาที่ทรัพยากรถูกจัดสรรแต่ไม่มีการใช้งาน (Idle Runtime)**	จำนวนชั่วโมงต่อรอบการวัด
การปรับขนาดอัตโนมัติ	**อัตราความครอบคลุมของนโยบายการปรับขนาด**	ภาระงานที่มีนโยบายปรับขนาด ÷ ภาระงานที่เหมาะสม × 100
ขอบเขตควบคุม	**อัตราความครอบคลุมของขอบเขตการขยายทรัพยากร**	ระบบที่กำหนดค่าต่ำสุด/สูงสุดหรือโควตา ÷ ระบบที่ปรับขนาดอัตโนมัติ × 100
พื้นที่จัดเก็บ	**อัตราความครอบคลุมของการจัดระดับชั้นพื้นที่จัดเก็บ**	ข้อมูลที่จัดอยู่ในระดับชั้นที่เหมาะสม ÷ ข้อมูลในขอบเขต × 100
พื้นที่จัดเก็บ	**ปริมาณข้อมูลที่ได้รับการปรับระดับชั้น**	ปริมาณข้อมูลที่ย้ายไปยังระดับชั้นที่เหมาะสม (GB/TB)
วงจรชีวิตข้อมูล	**อัตราความครอบคลุมของนโยบายวงจรชีวิต**	ข้อมูลภายใต้นโยบายวงจรชีวิต ÷ ข้อมูลที่เหมาะสม × 100

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

การลดข้อมูล	**ปริมาณข้อมูลที่หมดความจำเป็นและได้รับการจัดการ**	ปริมาณข้อมูลที่ลบหรือทำลายตามหลักเกณฑ์ (GB/TB)
ข้อมูลสำรอง	**ประสิทธิภาพการใช้พื้นที่สำหรับข้อมูลสำรอง**	เปรียบเทียบปริมาณพื้นที่ก่อนและหลังการทบทวน โดยยังบรรลุ RTO/RPO
บันทึกเหตุการณ์	**อัตราความครอบคลุมของการบริหารวงจรชีวิต Log**	ปริมาณ Log ที่มี Retention/Tiering เหมาะสม ÷ Log ในขอบเขต × 100
เครือข่าย	**ปริมาณการรับส่งข้อมูลที่ลดลง**	GB/TB ก่อนและหลังการปรับปรุง
CDN/Cache	**การลด Traffic จากระบบต้นทาง**	ปริมาณ Traffic ต้นทางก่อนและหลังการใช้ Cache/CDN
Edge	**การลดข้อมูลก่อนรับส่ง**	ปริมาณข้อมูลต้นฉบับเทียบกับข้อมูลหลังคัดกรองหรือรวม
ตำแหน่ง	**อัตราความครอบคลุมของการทบทวนตำแหน่งภาระงาน**	ภาระงานที่ได้รับการทบทวนตำแหน่ง ÷ ภาระงานในขอบเขต × 100
ค่าใช้จ่าย	**ค่าใช้จ่ายของทรัพยากรที่ไม่มีการใช้งาน**	ค่าใช้จ่ายจริงของทรัพยากรที่ได้รับการยืนยันว่าไม่มีการใช้งาน
ค่าใช้จ่ายผิดปกติ	**อัตราการทบทวนเหตุการณ์ค่าใช้จ่ายผิดปกติ**	เหตุการณ์ที่ได้รับการตรวจสอบ ÷ เหตุการณ์แจ้งเตือนทั้งหมด × 100
การเลิกใช้งาน	**อัตราการเลิกใช้งานทรัพยากรครบถ้วน**	ระบบที่เลิกใช้แล้วไม่มีทรัพยากรคงค้าง ÷ ระบบที่เลิกใช้ทั้งหมด × 100
ประสิทธิภาพโดยรวม	**ความเข้มข้นของการใช้ทรัพยากร (Resource Intensity)**	ทรัพยากรที่ใช้ ÷ หน่วยผลลัพธ์ของบริการ

ร่างสำหรับ Public Hearing เท่านั้น ห้ามนำไปใช้อ้างอิง

5.3.4.6 การประเมินทรัพยากรต่อหน่วยบริการ

การพิจารณาปริมาณทรัพยากรรวมเพียงอย่างเดียวอาจทำให้การประเมินคลาดเคลื่อนได้ เนื่องจากระบบที่มีผู้ใช้งานหรือธุรกรรมเพิ่มขึ้นย่อมมีแนวโน้มใช้ทรัพยากรเพิ่มขึ้น

ในกรณีที่สามารถกำหนดหน่วยผลลัพธ์ของบริการได้ CSC ควรพิจารณา **ความเข้มข้นของการใช้ทรัพยากร (Resource Intensity)** เพื่อประเมินว่าทรัพยากรที่ใช้ต่อหน่วยบริการเพิ่มขึ้นหรือลดลง

ตัวอย่างเช่น

ความเข้มข้นของการใช้ทรัพยากรประมวลผล = ชั่วโมงการประมวลผล ÷ จำนวนธุรกรรม

ความเข้มข้นของการใช้พื้นที่จัดเก็บ = ปริมาณพื้นที่จัดเก็บ ÷ จำนวนหน่วยบริการ

ความเข้มข้นของการรับส่งข้อมูล = ปริมาณข้อมูลที่รับส่ง ÷ จำนวนธุรกรรม

ค่าใช้จ่ายต่อหน่วยบริการ = ค่าใช้จ่ายของทรัพยากร ÷ จำนวนหน่วยบริการ

ตัวอย่างเช่น หากพื้นที่จัดเก็บเพิ่มจาก 100 TB เป็น 120 TB แต่จำนวนธุรกรรมเพิ่มจาก 1 ล้านรายการเป็น 2 ล้านรายการ การพิจารณาเฉพาะพื้นที่จัดเก็บรวมอาจแสดงว่าทรัพยากรเพิ่มขึ้น แต่พื้นที่จัดเก็บต่อธุรกรรมลดลง ซึ่งสะท้อนว่าประสิทธิภาพต่อหน่วยบริการดีขึ้น

ดังนั้น การประเมินควรพิจารณาทั้ง **ปริมาณทรัพยากรรวม (Absolute Resource Consumption) และความเข้มข้นของการใช้ทรัพยากร (Resource Intensity)** ร่วมกัน

5.3.4.7 การติดตามค่าใช้จ่ายในฐานะตัวบ่งชี้การใช้ทรัพยากร

ค่าใช้จ่ายสามารถใช้เป็นสัญญาณหนึ่งในการตรวจพบทรัพยากรที่ไม่มีการใช้งาน การขยายทรัพยากรผิดปกติ หรือการใช้บริการที่เปลี่ยนแปลงจากรูปแบบปกติได้ แต่ไม่ควรใช้ค่าใช้จ่ายเป็นตัวชี้วัดประสิทธิภาพเพียงตัวเดียว

ค่าใช้จ่ายที่เพิ่มขึ้นอาจเกิดจากปัจจัยที่เหมาะสม เช่น

- จำนวนผู้ใช้งานเพิ่มขึ้น
- ปริมาณธุรกรรมเพิ่มขึ้น
- มีการเพิ่มระดับความพร้อมใช้งาน
- เพิ่มมาตรการด้านความมั่นคงปลอดภัย
- เพิ่มความสามารถสำรองเพื่อรองรับความเสี่ยง หรือ
- ขยายบริการตามภารกิจ

ขณะเดียวกัน ค่าใช้จ่ายที่เพิ่มขึ้นอาจเกิดจาก

- ทรัพยากรที่ไม่มีการใช้งาน
- การปรับขนาดโดยอัตโนมัติที่ไม่มีขอบเขตควบคุม
- การเก็บข้อมูลเกินความจำเป็น
- การรับส่งข้อมูลผิดปกติ
- การสร้างทรัพยากรซ้ำ หรือ
- ข้อผิดพลาดในการตั้งค่า

ดังนั้น CSC ควรพิจารณาค่าใช้จ่ายร่วมกับข้อมูลด้านภาระงาน การใช้ทรัพยากร ขีดความสามารถ และผลลัพธ์ของบริการ

ร่างเอกสาร Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

CSC ควรกำหนดระดับค่าใช้จ่ายสำหรับการแจ้งเตือน (Cost Threshold) และอาจกำหนดงบประมาณหรือขอบเขตค่าใช้จ่ายสำหรับระบบหรือหน่วยงานตามความเหมาะสม เพื่อช่วยตรวจพบการใช้ทรัพยากรที่เปลี่ยนแปลงผิดปกติ

อย่างไรก็ตาม **การถึงระดับค่าใช้จ่ายที่กำหนดควรเป็นเหตุให้มีการแจ้งเตือน ตรวจสอบ หรือยกระดับการตัดสินใจ มิควรเป็นเหตุให้ระบบสำคัญถูกหยุดโดยอัตโนมัติ เว้นแต่ได้มีการประเมินผลกระทบและกำหนดมาตรการดังกล่าวไว้ล่วงหน้า**

5.3.4.8 การกำหนดเป้าหมายการปรับปรุง

CSC ควรกำหนดเป้าหมายการปรับปรุงโดยอ้างอิงจากข้อมูลฐาน ลักษณะของระบบ และศักยภาพในการปรับปรุงจริง

ไม่ควรกำหนดค่าเป้าหมายเดียวกันสำหรับทุกระบบ เช่น กำหนดให้ทุกระบบต้องลดทรัพยากรหรือค่าใช้จ่ายในอัตราร้อยละเดียวกัน เนื่องจากบางระบบอาจได้รับการปรับให้เหมาะสมอยู่แล้ว ขณะที่บางระบบจำเป็นต้องรักษาขีดความสามารถสำรองหรือความซ้ำซ้อนในระดับสูงด้วยเหตุผลด้านความพร้อมใช้งานหรือความมั่นคงปลอดภัย

ตัวอย่างเป้าหมาย ได้แก่

- เพิ่มสัดส่วนทรัพยากรที่ได้รับการทบทวนขนาด
- ลดทรัพยากรที่ไม่มีการใช้งาน
- ลดระยะเวลาที่ทรัพยากรถูกเปิดใช้งานโดยไม่มีภาระงาน
- เพิ่มอัตราความครอบคลุมของการจัดระดับชั้นพื้นที่จัดเก็บ
- เพิ่มอัตราความครอบคลุมของนโยบายวงจรชีวิตข้อมูล
- ลดการรับส่งข้อมูลที่ไม่มีความจำเป็น
- ลดความเข้มข้นของการใช้ทรัพยากรต่อหน่วยบริการ
- ลดค่าใช้จ่ายจากทรัพยากรที่ไม่มีการใช้งาน และ
- เพิ่มอัตราการเลิกใช้งานระบบหรือทรัพยากรอย่างครบถ้วน

เป้าหมายควรสามารถวัดได้ มีผู้รับผิดชอบ และกำหนดช่วงเวลาทบทวนอย่างเหมาะสม

5.3.4.9 การตรวจสอบผลกระทบหลังการปรับปรุง

หลังการปรับปรุง CSC ควรตรวจสอบว่าการเพิ่มประสิทธิภาพไม่ได้ก่อให้เกิดผลกระทบที่ไม่ยอมรับได้ต่อบริการ

การตรวจสอบควรครอบคลุมอย่างน้อย

- สมรรถนะ
- ความพร้อมใช้งาน
- ความต่อเนื่อง

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้อ้างอิง

- RTO และ RPO
- ความมั่นคงปลอดภัย
- ความสามารถในการตรวจจับและตอบสนองเหตุการณ์
- การปฏิบัติตามกฎหมายและสัญญา และ
- ประสบการณ์ของผู้ใช้งานตามความเหมาะสม

ตัวอย่างเช่น การลดขนาดทรัพยากรอาจทำให้อัตราการใช้หน่วยประมวลผลสูงขึ้นและดูเหมือนว่ามีประสิทธิภาพมากขึ้น แต่หากทำให้ระยะเวลาตอบสนองสูงกว่าระดับที่กำหนด การดำเนินการดังกล่าวไม่ควรถูกถือว่าเป็นการปรับปรุงที่ประสบผลสำเร็จ

ดังนั้น ผลการปรับปรุงควรพิจารณาทั้ง **ผลด้านประสิทธิภาพการใช้ทรัพยากร + ผลกระทบต่อคุณภาพและความมั่นคงของบริการ**

5.3.4.10 การประเมินตัวชี้วัดระดับศูนย์ข้อมูล

ในกรณีที่ CSC สามารถเข้าถึงข้อมูลที่น่าเชื่อถือจาก CSP หรือศูนย์ข้อมูล อาจนำตัวชี้วัดระดับโครงสร้างพื้นฐานมาใช้ประกอบการประเมินได้

มาตรฐาน ISO/IEC 30134 series กำหนดตัวชี้วัดสำคัญสำหรับศูนย์ข้อมูล เช่น ประสิทธิผลการใช้พลังงาน (Power Usage Effectiveness: PUE) และตัวชี้วัดด้านประสิทธิภาพทรัพยากรอื่นตามขอบเขตของมาตรฐานแต่ละส่วน

ตัวชี้วัดดังกล่าวเหมาะสำหรับการประเมินประสิทธิภาพระดับศูนย์ข้อมูล แต่ไม่ได้สะท้อนประสิทธิภาพของภาระงานของ CSC โดยตรงในทุกกรณี

ดังนั้น สำหรับ CSC ที่ใช้บริการคลาวด์สาธารณะ **ไม่ควรกำหนด PUE หรือ KPI ระดับศูนย์ข้อมูลเป็นตัวชี้วัดบังคับ หาก CSC ไม่สามารถเข้าถึงหรือควบคุมข้อมูลที่จำเป็นต่อการวัดได้**

หาก CSP เปิดเผยข้อมูลดังกล่าว CSC อาจนำมาใช้เป็นข้อมูลประกอบ โดยควรพิจารณาขอบเขต พื้นที่ ช่วงเวลา และวิธีการวัดของข้อมูลให้ชัดเจนก่อนเปรียบเทียบ

5.3.4.11 การประเมินและรายงานผลประโยชน์ด้านสิ่งแวดล้อม

ผลจากการดำเนินการตามข้อ 5.3 สามารถใช้แสดง **การเพิ่มประสิทธิภาพการใช้ทรัพยากร** ซึ่งเป็นปัจจัยหนึ่งที่สามารถสนับสนุนการลดผลกระทบด้านสิ่งแวดล้อมของบริการดิจิทัล

OECD Digital Economy Outlook 2024 ชี้ว่าผลกระทบของเทคโนโลยีดิจิทัลต่อสิ่งแวดล้อมเกิดขึ้นทั้งจากอุปกรณ์ โครงสร้างพื้นฐาน พลังงาน และรูปแบบการนำเทคโนโลยีไปใช้ และการประเมินผลกระทบสุทธิมีความซับซ้อน จึงควรใช้ข้อมูลและวิธีการวัดที่เหมาะสมในการแสดงผล ไม่ควรสรุปผลจากการเปลี่ยนแปลงทางเทคโนโลยีเพียงอย่างเดียว

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

นอกจากนี้ แนวทางของ OECD ในเรื่องเทคโนโลยีดิจิทัลและสิ่งแวดล้อมให้ความสำคัญกับการใช้วิธีการวัดที่สามารถเปรียบเทียบและตรวจสอบได้ รวมถึงการพิจารณาผลกระทบตลอดวงจรชีวิต ซึ่งสอดคล้องกับแนวคิดของ ISO/IEC TS 20125-1:2026 สำหรับการออกแบบบริการดิจิทัลโดยคำนึงถึงผลกระทบด้านสิ่งแวดล้อมตลอดช่วงของวงจรชีวิต

การรายงานควรแยกให้ชัดเจนระหว่าง **ผลด้านประสิทธิภาพการใช้ทรัพยากรที่สามารถวัดได้โดยตรง** กับ **ผลด้านสิ่งแวดล้อมที่ต้องอาศัยข้อมูลหรือวิธีการคำนวณเพิ่มเติม**

ผลด้านประสิทธิภาพการใช้ทรัพยากรที่สามารถรายงานได้โดยตรง

ตัวอย่างเช่น

- จำนวนทรัพยากรที่ไม่มีการใช้งานที่ได้รับการยกเลิก
- จำนวนชั่วโมงที่ลดลงจากการปิดทรัพยากรเมื่อไม่มีการใช้งาน
- จำนวนทรัพยากรที่ได้รับการปรับขนาด
- ปริมาณข้อมูลที่ได้รับการปรับระดับชั้น
- ปริมาณข้อมูลที่ครบกำหนดและได้รับการลบ
- ปริมาณ Traffic จากระบบต้นทางที่ลดลง
- ปริมาณการรับส่งข้อมูลข้ามพื้นที่ที่ลดลง
- ความเข้มข้นของการใช้ทรัพยากรที่ลดลง และ
- ค่าใช้จ่ายของทรัพยากรที่ไม่มีการใช้งานที่ลดลง

ผลด้านสิ่งแวดล้อมที่ควรมีข้อมูลเพิ่มเติม

ตัวอย่างเช่น

- การใช้พลังงานที่ลดลง
- การใช้น้ำที่ลดลง
- การปล่อยก๊าซเรือนกระจกที่ลดลง
- ผลกระทบต่อสิ่งแวดล้อมตลอดวงจรชีวิตที่ลดลง

การกล่าวอ้างผลในกลุ่มหลังควรอาศัยข้อมูลหรือวิธีการประเมินที่เชื่อถือได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

การกล่าวอ้างผลด้านการลดการใช้พลังงาน การลดการใช้น้ำ การลดการปล่อยก๊าซเรือนกระจก หรือผลประโยชน์ด้านสิ่งแวดล้อมอื่น ควรกำหนดขอบเขต ข้อมูลฐาน วิธีการวัดหรือคำนวณ แหล่งข้อมูล สมมติฐาน และช่วงเวลาที่ใช้เปรียบเทียบอย่างชัดเจนและสามารถตรวจสอบได้ หากไม่มีข้อมูลที่เพียงพอ ควรรายงานผล

ในรูปของประสิทธิภาพการใช้ทรัพยากรที่วัดได้ โดยไม่แปลงผลดังกล่าวเป็นผลด้านสิ่งแวดล้อมโดยไม่มีวิธีการที่เชื่อถือได้รองรับ

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ตัวอย่างการแสดงผลก่อนและหลังการปรับปรุง

รายการ	ข้อมูลฐาน	หลังปรับปรุง	ผลที่เกิดขึ้น
ทรัพยากรประมวลผลที่ไม่มีการใช้งาน	180 รายการ	25 รายการ	ลดลง 155 รายการ
ระยะเวลาเปิดใช้งานระบบทดสอบ	168 ชั่วโมง/สัปดาห์	60 ชั่วโมง/สัปดาห์	ลดลง 108 ชั่วโมง/สัปดาห์
ข้อมูลบนพื้นที่จัดเก็บระดับสมรรถนะสูง	500 TB	200 TB	ปรับระดับชั้น 300 TB
ข้อมูลที่ครบกำหนดการเก็บรักษา	70 TB	5 TB	ลดลง 65 TB
การรับส่งข้อมูลข้ามพื้นที่	500 TB/เดือน	320 TB/เดือน	ลดลง 180 TB/เดือน
Traffic จากระบบต้นทาง	400 TB/เดือน	210 TB/เดือน	ลดลง 190 TB/เดือน
พื้นที่จัดเก็บต่อ 1,000 ธุรกรรม	85 GB	62 GB	ลดลงประมาณ 27%
ทรัพยากรที่เลิกใช้แล้วแต่ยังมีค่าใช้จ่าย	45 รายการ	3 รายการ	ลดลง 42 รายการ

หมายเหตุ: ตัวเลขในตารางเป็นเพียงตัวอย่างเพื่ออธิบายวิธีการรายงาน มิใช่ค่าเป้าหมายหรือเกณฑ์มาตรฐาน

5.3.4.12 การทบทวนและปรับปรุงอย่างต่อเนื่อง

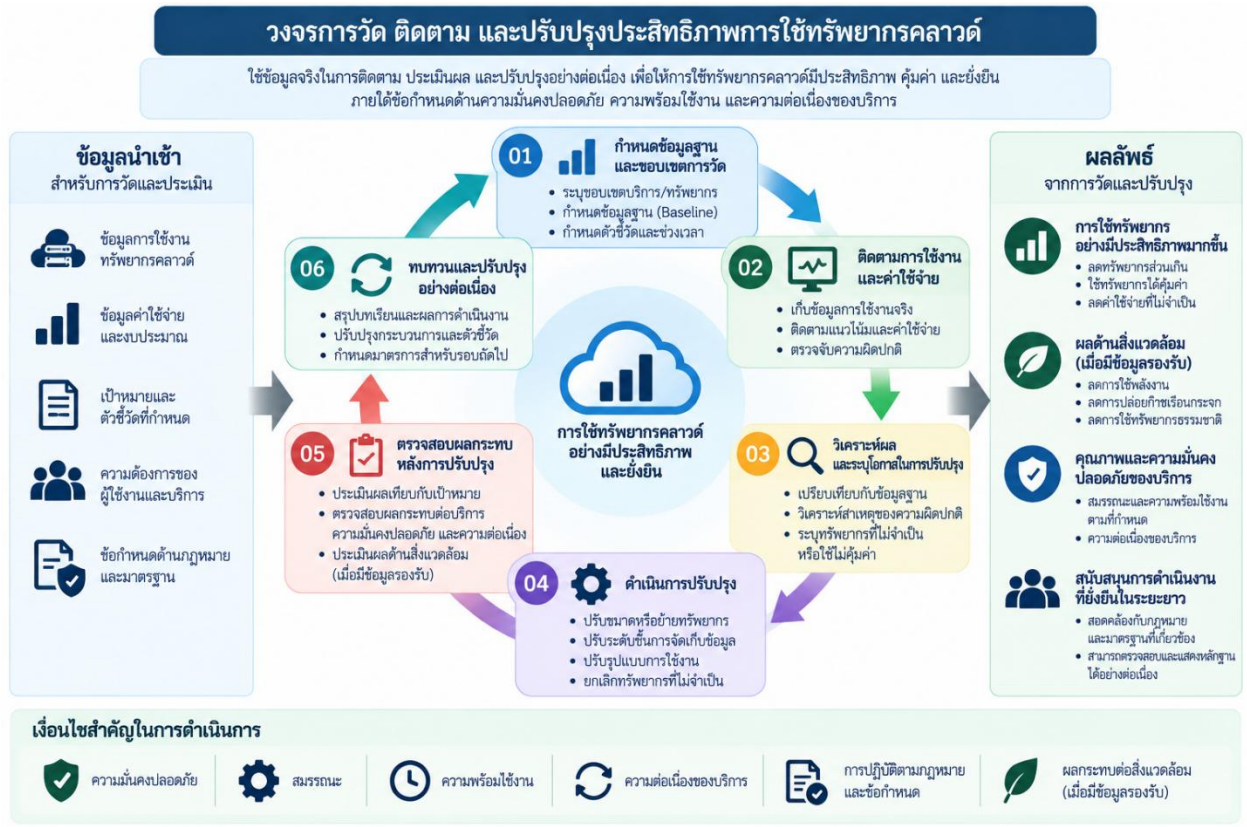
การบริหารทรัพยากรคลาวด์ควรได้รับการทบทวนอย่างต่อเนื่อง เนื่องจากปริมาณงาน พฤติกรรมผู้ใช้งาน ปริมาณข้อมูล สถาปัตยกรรม เทคโนโลยี และข้อกำหนดขององค์กรสามารถเปลี่ยนแปลงได้

CSC ควรกำหนดให้มีการทบทวนเป็นระยะ และทบทวนเพิ่มเติมเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น

- จำนวนผู้ใช้งานหรือธุรกรรมเปลี่ยนแปลงมาก
- มีการเพิ่มหรือลดบริการ
- มีการเปลี่ยนแปลงสถาปัตยกรรม
- มีการย้ายระบบหรือข้อมูล
- RTO หรือ RPO เปลี่ยนแปลง
- พบความผิดปกติของทรัพยากรหรือค่าใช้จ่าย
- ปริมาณข้อมูลเพิ่มขึ้นผิดปกติ
- มีการเปลี่ยนแปลงกฎหมายหรือข้อกำหนด และ
- มีเทคโนโลยีหรือรูปแบบบริการที่สามารถตอบสนองความต้องการได้อย่างมีประสิทธิภาพมากขึ้น

ผลจากการทบทวนควรนำกลับไปประเมินกรอบ 6 Rights อีกครั้ง ได้แก่ **เลือกประเภทให้เหมาะสม ⟶ กำหนดขนาดให้เหมาะสม ⟶ เลือกรูปแบบการใช้ให้เหมาะสม ⟶ เลือกระดับชั้นให้เหมาะสม ⟶ เลือกตำแหน่งให้เหมาะสม ⟶ บริหารวงจรชีวิตให้เหมาะสม** เพื่อสนับสนุนการปรับปรุงอย่างต่อเนื่อง

ร่างเพื่อการประชาพิจารณ์ Public Hearing เท่านั้น - ห้ามนำไปอ้างอิง



รูปที่ 5 วงจรการวัดและปรับปรุงประสิทธิภาพการใช้ทรัพยากรคลาวด์

การใช้ทรัพยากรคลาวด์อย่างมีประสิทธิภาพและยั่งยืนมิได้หมายถึงการใช้ทรัพยากรให้น้อยที่สุด เลือกบริการที่มีราคาต่ำที่สุด หรือปรับลดความซ้ำซ้อนของระบบให้มากที่สุด แต่หมายถึงการเลือกประเภท ขนาด รูปแบบการใช้ ระดับชั้น ตำแหน่ง และวงจรชีวิตของทรัพยากรให้สอดคล้องกับลักษณะของภาระงาน ข้อมูล ภารกิจ ระดับผลกระทบ และความเสี่ยง พร้อมทั้งติดตาม วัดผล และปรับเปลี่ยนทรัพยากรเมื่อความต้องการเปลี่ยนแปลง โดยไม่ลดทอนระดับความมั่นคงปลอดภัย ความพร้อมใช้งาน และความต่อเนื่องที่จำเป็น

การประยุกต์กรอบ 6 Rights ร่วมกับการกำหนดข้อมูลฐาน การติดตาม การปรับขนาด ขอบเขตควบคุม การจัดระดับชั้นข้อมูล การลดการเคลื่อนย้ายข้อมูล และการบริหารวงจรชีวิต ช่วยให้องค์กรสามารถเชื่อมโยงความมั่นคงปลอดภัยของระบบคลาวด์กับประสิทธิภาพการใช้ทรัพยากร ประสิทธิภาพด้านต้นทุน และผลประโยชน์ด้านสิ่งแวดล้อมที่สามารถวัดและตรวจสอบได้อย่างเป็นระบบ

ร่างสำหรับ Public Hearing

หลักการสำคัญของข้อ 5.3.4

การประเมินประสิทธิภาพการใช้ทรัพยากรไม่ควรพิจารณาจากปริมาณทรัพยากรหรือค่าใช้จ่ายที่ลดลงเพียงอย่างเดียว เนื่องจากการใช้ทรัพยากรที่เพิ่มขึ้นอาจเกิดจากการเพิ่มขึ้นของผู้ใช้งาน ธุรกรรม หรือภารกิจ ขณะที่การใช้ทรัพยากรที่ลดลงอาจเกิดจากการลดระดับสมรรถนะหรือความพร้อมใช้งานของบริการ

CSC จึงควรกำหนดข้อมูลฐาน ขอบเขต และช่วงเวลาการวัดที่เหมาะสม และพิจารณาความสัมพันธ์ระหว่างทรัพยากรที่ใช้ ผลงานหรือหน่วยบริการที่เกิดขึ้น และคุณภาพของบริการ รวมถึงติดตามแนวโน้ม ความผิดปกติ ค่าใช้จ่าย และผลกระทบหลังการปรับปรุง เพื่อให้สามารถแสดงได้ว่าการเปลี่ยนแปลงทำให้การใช้ทรัพยากรมีประสิทธิภาพขึ้นจริง โดยไม่ลดทอนความมั่นคงปลอดภัย ความพร้อมใช้งาน ความต่อเนื่อง หรือการปฏิบัติตามข้อกำหนด

ผลด้านสิ่งแวดล้อมควรรายงานจากข้อมูลที่สามารถตรวจสอบได้ หากมีการแปลงผลการลดทรัพยากรไปเป็นการลดพลังงาน น้ำ หรือการปล่อยก๊าซเรือนกระจก ควรระบุข้อมูลฐาน ขอบเขต วิธีการคำนวณ แหล่งข้อมูล สมมติฐาน และช่วงเวลาที่ใช้เปรียบเทียบอย่างชัดเจน

หลักคิดสำคัญจึงเป็น “วัดจากข้อมูลฐาน เปรียบเทียบกับผลลัพธ์ของบริการ ตรวจสอบผลกระทบ และปรับปรุงอย่างต่อเนื่อง โดยกล่าวอ้างผลด้านสิ่งแวดล้อมเฉพาะส่วนที่สามารถพิสูจน์ได้”

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

สรุปแนวคิดของข้อ 5.3

โดยสรุป การใช้ทรัพยากรคลาวด์อย่างมีประสิทธิภาพและยั่งยืนมิได้หมายถึงการใช้ทรัพยากรให้น้อยที่สุด แต่เป็นการเลือกประเภท ขนาด รูปแบบการใช้ ระดับชั้น ตำแหน่ง และวงจรชีวิตของทรัพยากรให้เหมาะสมกับภารกิจ ลักษณะของภาระงาน ระดับผลกระทบ และความเสี่ยง โดยใช้กรอบ 6 Rights เป็นเครื่องมือประกอบการตัดสินใจ และรักษาความมั่นคงปลอดภัย ความพร้อมใช้งาน ความต่อเนื่อง และความสามารถในการกู้คืนเป็นเงื่อนไขกำกับ

CSC ควรกำหนดข้อมูลฐาน ตัวชี้วัด และหลักฐานที่สามารถตรวจสอบได้ เพื่อแสดงผลของการปรับปรุง เช่น การลดทรัพยากรที่ไม่มีการใช้งาน การปรับขนาดทรัพยากรให้เหมาะสม การย้ายข้อมูลไปยังระดับชั้นการจัดเก็บที่เหมาะสม การลดข้อมูลที่หมดความจำเป็น และการลดการรับส่งข้อมูลที่ไม่จำเป็น พร้อมนำผลการวัดกลับมาทบทวนและปรับปรุงการตัดสินใจอย่างต่อเนื่อง

ในกรณีที่นำผลดังกล่าวไปกล่าวอ้างเป็นผลด้านการลดการใช้พลังงาน การใช้น้ำ การปล่อยก๊าซเรือนกระจก หรือผลประโยชน์ด้านสิ่งแวดล้อมอื่น ควรมีข้อมูลฐาน ขอบเขต วิธีการวัดหรือคำนวณ แหล่งข้อมูล สมมติฐาน และช่วงเวลาที่ใช้เปรียบเทียบอย่างชัดเจนและสามารถตรวจสอบได้ เพื่อให้ผลด้านสิ่งแวดล้อมที่รายงานสามารถพิสูจน์และตรวจสอบย้อนกลับได้

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามนำไปใช้งานอื่น

เอกสารอ้างอิงหลักสำหรับข้อ 5.3

ลำดับ	เอกสารอ้างอิง	ประเด็นที่ใช้รองรับ
1	**ISO/IEC TS 20125-1:2026, Information technology — Digital services ecodesign — Part 1: Ecopractices for life cycle stages**	Sustainability ของบริการดิจิทัลตลอดวงจรชีวิต ตั้งแต่ Requirements ถึง End-of-life
2	**ISO/IEC TS 20000-16:2025, Information technology — Service management — Part 16: Guidance on sustainability within a service management system based on ISO/IEC 20000-1**	การบูรณาการ Sustainability กับการบริหารบริการเทคโนโลยีสารสนเทศ
3	**ISO/IEC 22624:2020, Information technology — Cloud computing — Taxonomy based data handling for cloud services**	Data Geolocation, Cross-border Flow, Data Access, Portability, Data Management และ Governance
4	**ISO/IEC 19944-1:2020, Cloud computing and distributed platforms — Data flow, data categories and data use — Part 1: Fundamentals**	ประเภทและการไหลของข้อมูลในระบบคลาวด์
5	**ISO/IEC 30134-1:2016, Information technology — Data centres — Key performance indicators — Part 1: Overview and general requirements**	หลักการและเงื่อนไขทั่วไปของ KPI ด้านประสิทธิภาพทรัพยากรศูนย์ข้อมูล
6	**Cloud Security Alliance, Cloud Controls Matrix (CCM) v4.1**	Cloud Security และ Data Security & Privacy Lifecycle Management ที่เป็นกลางต่อผู้ให้บริการ
7	**OECD Digital Economy Outlook 2024 (Volume 2), Digital Technologies and the Environment**	Environmental Footprint ของเทคโนโลยีดิจิทัล การใช้พลังงานของ Data Centre และความซับซ้อนของการวัดผล

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

8	**OECD Recommendation of the Council on Digital Technologies and the Environment, OECD/LEGAL/0380, amended 2025**	หลักนโยบายสากลเกี่ยวกับเทคโนโลยีดิจิทัลและสิ่งแวดล้อม
9	**ITU-T L.1312:2026, Guidelines on multi-dimensional environmental metrics and management for data centres**	การประเมิน Energy Efficiency, Resource Efficiency, GHG และ Environmental Impact แบบหลายมิติ
10	**ISO/IEC 27001:2022 และ ISO/IEC 27002:2022**	ใช้เป็นฐานด้าน Security, Backup, Logging, Redundancy, Continuity และการควบคุมที่ต้องไม่ถูกลดทอนจากการเพิ่ม Resource Efficiency

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ภาคผนวก

ภาคผนวก ก (ประกอบหัวข้อ 5.2.4)

แนวทางการคัดเลือกผู้ให้บริการคลาวด์ด้านการเข้ารหัสและการจัดการกุญแจ (Guidelines for Cloud Provider Selection: Cryptography and Key Management)

1. หลักการและวัตถุประสงค์

ภาคผนวกนี้จัดทำขึ้นเพื่อเป็นแนวทางเพิ่มเติมสำหรับหน่วยงานในการประเมินและคัดเลือกผู้ให้บริการคลาวด์ด้านความสามารถในการเข้ารหัสและการบริหารจัดการกุญแจเข้ารหัส โดยมุ่งสนับสนุนการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) และการปฏิบัติตามข้อกำหนดด้านกฎหมาย มาตรฐาน และการกำกับดูแลที่เกี่ยวข้อง

ทั้งนี้ หน่วยงานควรพิจารณาให้สอดคล้องกับประเภทข้อมูล ระดับผลกระทบของระบบสารสนเทศ ผลการประเมินความเสี่ยง และบริบทเฉพาะของหน่วยงาน

2. แนวทางการพิจารณาเบื้องต้น

ก่อนดำเนินการคัดเลือกผู้ให้บริการ หน่วยงานควรพิจารณาประเด็นต่อไปนี้

1. ประเภทและระดับชั้นของข้อมูลที่จัดเก็บหรือประมวลผลบนระบบคลาวด์
2. ระดับผลกระทบของระบบสารสนเทศหรือภารกิจที่เกี่ยวข้อง
3. ข้อกำหนดทางกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง
4. ความต้องการด้านการควบคุมกุญแจเข้ารหัส
5. ความจำเป็นในการเคลื่อนย้ายข้อมูลหรือเปลี่ยนผู้ให้บริการในอนาคต
6. ระยะเวลาการคุ้มครองข้อมูลและความต้องการด้านการปกป้องระยะยาว

3. ตัวอย่างรายการประเมินผู้ให้บริการคลาวด์ด้านการเข้ารหัสและการจัดการกุญแจ

ประเด็นการประเมิน	รายละเอียดที่ควรพิจารณา	ผลการประเมิน	หลักฐานอ้างอิง
การเข้ารหัสข้อมูลขณะจัดเก็บ (Encryption at Rest)	รองรับการเข้ารหัสข้อมูลที่จัดเก็บหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Product Documentation / Security Whitepaper / Service Guide
การเข้ารหัสข้อมูลขณะรับส่ง (Encryption in Transit)	รองรับ TLS ตามมาตรฐานปัจจุบันหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Security Whitepaper / Technical Documentation
มาตรฐานอัลกอริทึม (Cryptographic Standard Support)	รองรับอัลกอริทึมที่ได้รับการยอมรับในระดับสากลหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Cryptographic Standard Documentation / Product Documentation

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

Customer Managed Key	ผู้ใช้บริการสามารถบริหารจัดการกุญแจได้ด้วยตนเองหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Service Documentation / Product Feature Guide
Bring Your Own Key (BYOK)	รองรับการนำกุญแจจากภายนอกเข้ามาใช้งานหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Technical Documentation / Key Management Guide
Hold Your Own Key (HYOK)	รองรับการจัดเก็บกุญแจไว้นอกระบบผู้ให้บริการหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Technical Documentation / Architecture Guide
Key Management Service (KMS)	มีบริการบริหารจัดการกุญแจหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Service Documentation
Hardware Security Module (HSM)	รองรับการใช้งาน HSM หรือไม่	☐ รองรับ ☐ ไม่รองรับ	Compliance Report / Technical Guide / Product Documentation
Key Rotation	รองรับการหมุนเวียนกุญแจหรือไม่	☐ อัตโนมัติ ☐ กำหนดเอง ☐ ไม่รองรับ	Key Management Documentation
Key Lifecycle Management	รองรับการสร้าง จัดเก็บ หมุนเวียน เพิกถอน และทำลายกุญแจหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Key Lifecycle Documentation
Audit Logging	มีการบันทึกกิจกรรมด้านการเข้ารหัสหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Audit Guide / Logging Documentation
Monitoring Capability	มี Dashboard หรือการแจ้งเตือนกิจกรรมที่เกี่ยวข้องหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Monitoring Guide / Product Documentation
Key Lifecycle Transparency	เปิดเผยกระบวนการจัดการกุญแจหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Public Documentation / Service Description
Vendor Lock-in	สามารถนำข้อมูลหรือกุญแจออกได้หรือไม่	☐ รองรับ ☐ ไม่รองรับ	Migration Guide / Exit Plan Documentation
Data Portability	รองรับการย้ายข้อมูลและองค์ประกอบด้านการเข้ารหัสหรือไม่	☐ รองรับ ☐ ไม่รองรับ	Data Migration Documentation

ร่างสำหรับ Public Hearing เท่านั้น – ห้ามใช้งานจริง

Crypto-Agility	รองรับการเปลี่ยนอัลกอริทึมหรือมาตรฐานได้หรือไม่	☐ รองรับ ☐ ไม่รองรับ	Product Roadmap / Architecture Documentation
Post-Quantum Cryptography Readiness	มีแนวทางหรือแผนรองรับ PQC หรือไม่	☐ มี ☐ ไม่มี	Product Roadmap / PQC Statement / Technical Whitepaper
Hybrid Cryptography Support	รองรับการใช้งานแบบ Hybrid ระหว่างอัลกอริทึมเดิมและ PQC หรือไม่	☐ รองรับ ☐ ไม่รองรับ	Technical Whitepaper
Compliance and Certification	มีการรับรองมาตรฐานที่เกี่ยวข้องหรือไม่	☐ มี ☐ ไม่มี	ISO/IEC 27001 / ISO/IEC 27017 / ISO/IEC 27018 / SOC Report
Shared Responsibility Transparency	มีการระบุขอบเขตความรับผิดชอบระหว่างผู้ใช้และผู้ให้บริการชัดเจนหรือไม่	☐ มี ☐ ไม่มี	Shared Responsibility Matrix

ตัวอย่างสรุปผลการประเมิน

ระดับผลการประเมิน	**เกณฑ์ตัวอย่าง**
ผ่าน (Pass)	รองรับข้อกำหนดสำคัญทั้งหมด
ผ่านแบบมีเงื่อนไข (Conditional Pass)	มีข้อจำกัดบางประการแต่สามารถกำหนดมาตรการชดเชยได้
ไม่ผ่าน (Fail)	ไม่รองรับข้อกำหนดสำคัญหรือมีความเสี่ยงสูง
ต้องขอข้อมูลเพิ่มเติม	ข้อมูลไม่เพียงพอต่อการประเมิน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

4. ตัวอย่างคำถามสำหรับใช้ในการประเมินผู้ให้บริการ

หน่วยงานอาจใช้คำถามต่อไปนี้ประกอบการประเมินหรือขอข้อมูลเพิ่มเติมจากผู้ให้บริการ

1. ผู้ให้บริการใช้มาตรฐานการเข้ารหัสใดในการปกป้องข้อมูล
2. ผู้ใช้บริการสามารถควบคุมกุญแจเข้ารหัสด้วยตนเองได้หรือไม่
3. ผู้ให้บริการมีการหมุนเวียนกุญแจอัตโนมัติหรือไม่
4. มีการใช้ระบบบริหารจัดการกุญแจ (KMS) หรืออุปกรณ์ HSM หรือไม่
5. ผู้ใช้บริการสามารถตรวจสอบกิจกรรมด้านการเข้ารหัสย้อนหลังได้หรือไม่
6. ผู้ให้บริการมีแผนการยุติอัลกอริทึมที่ล้าสมัยอย่างไร
7. ผู้ให้บริการมีแนวทางรองรับความคล่องตัวทางรหัสลับ (Crypto-Agility) หรือไม่

8. ผู้ให้บริการมีแผนรองรับการเปลี่ยนผ่านสู่ Post-Quantum Cryptography หรือไม่
9. หากย้ายผู้ให้บริการในอนาคต สามารถนำกุญแจหรือข้อมูลออกได้หรือไม่

หมายเหตุ

รายการในภาคผนวกนี้เป็นแนวทางเบื้องต้น หน่วยงานอาจเพิ่มเติม ปรับเปลี่ยน หรือกำหนดเกณฑ์การประเมินอื่นเพิ่มเติมให้เหมาะสมกับประเภทข้อมูล ระดับความเสี่ยง ภารกิจ และข้อกำหนดเฉพาะของหน่วยงาน

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

ภาคผนวก ข (ประกอบหัวข้อ 5.2.8)

แบบตรวจสอบข้อกำหนดและความสามารถด้านความมั่นคงปลอดภัยของบริการคลาวด์ (Cloud Service Security Requirements and Capability Assessment Checklist)

1. วัตถุประสงค์

แบบตรวจสอบนี้จัดทำขึ้นเพื่อสนับสนุนการประเมินการปฏิบัติตามข้อ 5.2.8 โดยช่วยให้หน่วยงานสามารถตรวจสอบว่า

- ได้กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยที่เหมาะสม
- ได้รับข้อมูลจาก CSP อย่างเพียงพอ
- ได้ประเมินความสามารถของบริการเทียบกับข้อกำหนด
- ได้พิจารณาช่องว่างและความเสี่ยงที่เกี่ยวข้อง
- ได้พิจารณาข้อมูลเกี่ยวกับการพัฒนาที่ปลอดภัยของ CSP

แบบตรวจสอบนี้ไม่ใช้แทนการประเมินรายละเอียดของมาตรการควบคุมด้านความมั่นคงปลอดภัยในแต่ละหมวดของประกาศ

2. วิธีใช้แบบตรวจสอบ

ให้ผู้ประเมินพิจารณารายการตรวจสอบตามลักษณะของบริการและขอบเขตความรับผิดชอบ โดยสามารถระบุผลเป็น

ใช่ — มีการดำเนินการหรือมีหลักฐานเพียงพอ

ไม่ใช่ — ยังไม่มีการดำเนินการหรือหลักฐานไม่เพียงพอ

N/A — ไม่เกี่ยวข้องหรือไม่สามารถนำมาประยุกต์ใช้กับบริการนั้นได้

การสรุปผลการประเมินโดยรวมควรพิจารณาจากสาระสำคัญของข้อกำหนด ระดับของช่องว่าง และความเสี่ยงที่เกี่ยวข้อง โดยไม่ควรพิจารณาจากจำนวนรายการที่ตอบ “ใช่” หรือ “ไม่ใช่” เพียงอย่างเดียว ทั้งนี้ รายการที่ระบุ N/A ควรมีเหตุผลประกอบตามความเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น ห้ามใช้อ้างอิง

3. แบบตรวจสอบ

ส่วน ก การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ — 5.2.8.1

ลำดับ	รายการตรวจสอบ	ใช่	ไม่ใช่	N/A	หลักฐาน/หมายเหตุ
1	มีการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบหรือบริการคลาวด์ก่อนการเลือกใช้หรือใช้งานหรือไม่	☐	☐	☐	
2	การกำหนดข้อกำหนดได้พิจารณาความสำคัญของข้อมูล ระบบ ผลกระทบ และความเสี่ยงที่เกี่ยวข้องหรือไม่	☐	☐	☐	
3	มีการพิจารณาข้อกำหนดด้านกฎหมาย กฎ ระเบียบ ข้อบังคับ สัญญา หรือข้อกำหนดอื่นที่เกี่ยวข้องหรือไม่	☐	☐	☐	
4	CSC ได้รับข้อมูลเกี่ยวกับความสามารถด้านความมั่นคงปลอดภัยของบริการจาก CSP ในระดับที่เพียงพอต่อการประเมินหรือไม่	☐	☐	☐	
5	มีการประเมินความสามารถของบริการเทียบกับข้อกำหนดด้านความมั่นคงปลอดภัยของหน่วยงานหรือไม่	☐	☐	☐	
6	หากพบข้อกำหนดที่บริการไม่สามารถตอบสนองได้ครบถ้วน มีการพิจารณาช่องว่างและมาตรการเพิ่มเติมหรือมาตรการทดแทนตามความเหมาะสมหรือไม่	☐	☐	☐	
7	มีการพิจารณาความเสี่ยงที่เหลืออยู่ก่อนการตัดสินใจเลือกใช้หรือใช้งานบริการตามความเหมาะสมหรือไม่	☐	☐	☐	
8	CSP ให้ข้อมูลที่เพียงพอต่อการประเมิน โดยคำนึงถึงการป้องกันข้อมูลที่มีความอ่อนไหวด้านความมั่นคงปลอดภัยหรือไม่	☐	☐	☐	

ส่วน ข นโยบายการพัฒนาที่ปลอดภัย — 5.2.8.2

ลำดับ	รายการตรวจสอบ	ใช่	ไม่ใช่	N/A	หลักฐาน/หมายเหตุ
9	CSC ได้ขอหรือรวบรวมข้อมูลเกี่ยวกับขั้นตอนหรือวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของ CSP หรือไม่	☐	☐	☐	
10	ข้อมูลหรือหลักฐานที่ได้รับจาก CSP เพียงพอให้ CSC พิจารณาความเหมาะสมของกระบวนการพัฒนาที่ปลอดภัยตามความเสี่ยงของบริการหรือไม่	☐	☐	☐	

ร่างเอกสารเพื่อรับฟังความคิดเห็น Public Hearing เท่านั้น - ห้ามใช้อ้างอิง

11	CSP ได้ให้ข้อมูลเกี่ยวกับขั้นตอนหรือวิธีปฏิบัติในการพัฒนาที่ปลอดภัย ในขอบเขตที่สอดคล้องกับนโยบายการเปิดเผยข้อมูลของตนหรือไม่	☐	☐	☐	
12	ในกรณีที่ CSC พัฒนา ปรับแต่ง หรือเชื่อมต่อระบบภายใต้ความรับผิดชอบของตน มีการนำหลักการพัฒนาที่ปลอดภัยมาประยุกต์ใช้ตามระดับความเสี่ยงหรือไม่	☐	☐	☐	
13	ในกรณีที่ข้อมูลจาก CSP มีข้อจำกัดหรือไม่เพียงพอ CSC ได้พิจารณาความเสี่ยงหรือดำเนินการเพิ่มเติมตามความเหมาะสมหรือไม่	☐	☐	☐	

4. สรุปผลการประเมิน

รายการ	**ผลการพิจารณา**
บริการ/ระบบที่ประเมิน	
CSP	
ผู้ประเมิน	
วันที่ประเมิน	
ผลการประเมินโดยรวม	☐ สอดคล้อง ☐ สอดคล้องบางส่วน ☐ ไม่สอดคล้อง
พบช่องว่างที่ต้องดำเนินการเพิ่มเติม	☐ ไม่มี ☐ มี
ต้องประเมินความเสี่ยงเพิ่มเติม	☐ ไม่ต้อง ☐ ต้อง
เอกสาร/หลักฐานอ้างอิง	
หมายเหตุ/การดำเนินการเพิ่มเติม	

หมายเหตุ: ผลการประเมินตามแบบตรวจสอบนี้ใช้เพื่อสนับสนุนการพิจารณาความเหมาะสมด้านความมั่นคงปลอดภัยของบริการคลาวด์ตามข้อ 5.2.8 โดยควรพิจารณาร่วมกับผลการประเมินความเสี่ยง ข้อกำหนดของหน่วยงาน และข้อกำหนดอื่นที่เกี่ยวข้องตามความเหมาะสม

ร่างสำหรับ Public Hearing เท่านั้น - ห้ามใช้อ้างอิง