Cloud Security Standard for Practitioner | Day 1

การอบรมตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

25-27 พฤษภาคม 2569

THAILAND CLOUD SECURITY ASSURANCE PROGRAM

เอกสารประกอบ Cloud Practitioner Training – Day 1,2,3

https://dg.th/tngd3lfakv

หลักสูตรสำหรับผู้ปฏิบัติงาน

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

	Day 1	Day 2	Day 3
	กฎหมายไซเบอร์และมาตรฐานระบบคลาวด์ของประเทศไทย	มาตรฐานสากลด้านความมั่นคงปลอดภัยและการจัดการข้อมูลส่วนบุคคล ในบริบทของบริการคลาวด์	มาตรฐานสากลด้านความมั่นคงปลอดภัยและการจัดการข้อมูลส่วนบุคคล ในบริบทของบริการคลาวด์ (ต่อ)
Morning	• กฎหมายและกรอบกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ • มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	• ISO/IEC 27001 และระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) • ISO/IEC 27017 : การรักษาความปลอดภัยของข้อมูลในบริการคลาวด์	• ISO/IEC 27701 และระบบการบริหารความเป็นส่วนตัว (PIMS) • CSA STAR (Security, Trust, Assurance and Risk) : มาตรฐานความปลอดภัยสำหรับผู้ให้บริการคลาวด์
Afternoon	• ข้อกำหนดขั้นต่ำตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	• ISO/IEC 27018 : การคุ้มครองข้อมูลส่วนบุคคลในบริการคลาวด์ • ISO/IEC 27017 และ ISO/IEC 27018 : การประยุกต์ใช้งาน	• การเชื่อมโยงและเปรียบเทียบมาตรฐาน (Mapping) • สรุปประเด็นสำคัญ (Key Takeaways) • แบบทดสอบหลังการอบรม (Post-test)

ช่วงที่ 1

กฎหมายและกรอบกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

กฎหมายไซเบอร์และมาตรฐานระบบคลาวด์ของประเทศไทย

- **กฎหมายและกรอบกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์**
  - พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562: โครงสร้าง หลักการ และความสำคัญ
  - บทบาทและหน้าที่ของหน่วยงานกำกับดูแล (กมช. และ สกมช.)
  - ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
  - ประกาศ สกมช. เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย พ.ศ. 2567

ภาพรวมการรักษาความมั่นคงปลอดภัยระบบคลาวด์

คุณลักษณะสำคัญ 5 ประการของระบบคลาวด์ (NIST SP 800-145)

NIST SP 800-145 The NIST Definition of Cloud Computing

นิยามคลาวด์ตาม NIST SP 800-145

ระบบคลาวด์ คือ แบบจำลองการประมวลผลที่อนุญาตให้ผู้ใช้เข้าถึงทรัพยากร IT (เครือข่าย, เซิร์ฟเวอร์, สตอเรจ, แอป) ผ่านอินเทอร์เน็ตได้สะดวก คล่องตัว และตามความต้องการ

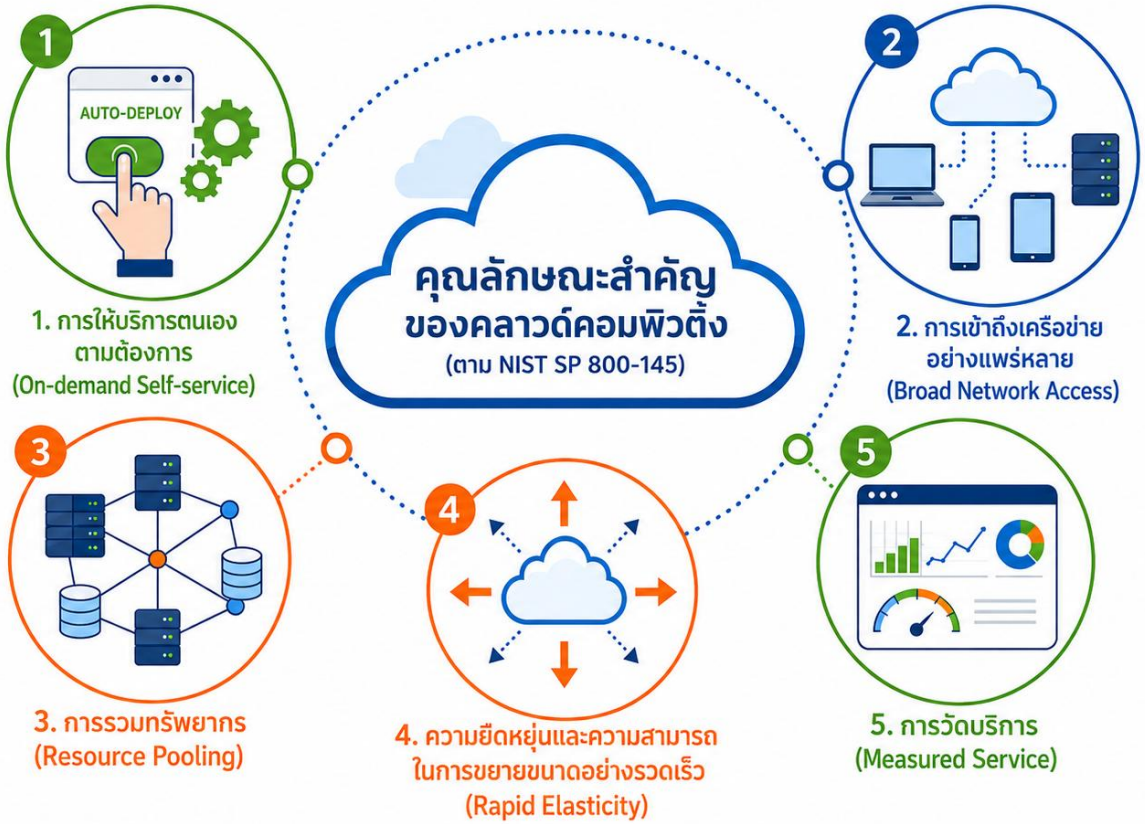
01 **On-demand Self-service**
ให้บริการตนเองตามต้องการ

02 **Broad Network Access**
เข้าถึงเครือข่ายอย่างแพร่หลาย

03 **Resource Pooling**
การรวมทรัพยากร

04 **Rapid Elasticity**
ยืดหยุ่นและขยายขนาดได้รวดเร็ว

05 **Measured Service**
วัดการให้บริการได้



หลักการพื้นฐานความมั่นคงปลอดภัยสารสนเทศ — CIA Triad

Confidentiality / Integrity / Availability — 3 มิติที่ต้องปกป้องพร้อมกัน

C — Confidentiality

การรักษาความลับ

ป้องกันมิให้ข้อมูลถูกเข้าถึงโดยผู้ไม่ได้รับอนุญาต

ภัยคุกคาม: Phishing, Data Leakage

I — Integrity

ความถูกต้องครบถ้วน

ป้องกันการเปลี่ยนแปลง/ทำลายข้อมูลโดยไม่ได้รับอนุญาต

ภัยคุกคาม: Data Tampering, Ransomware

A — Availability

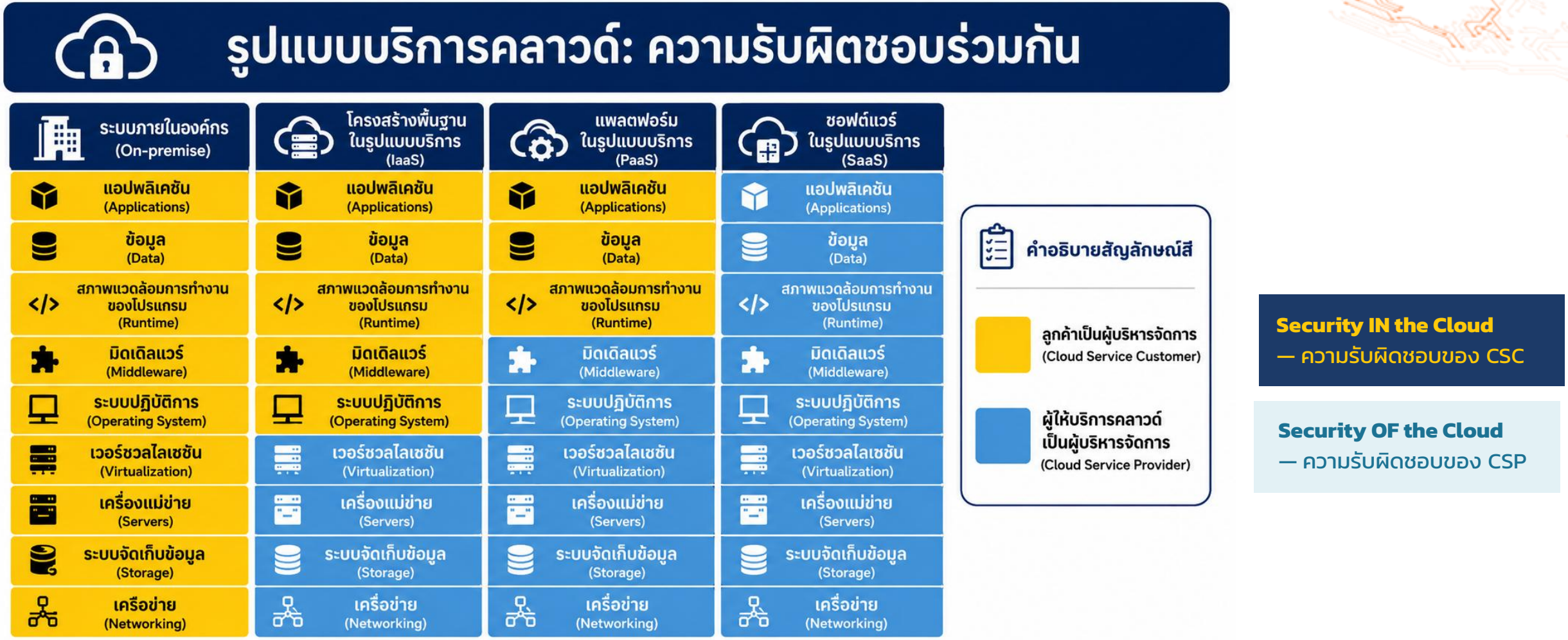
ความพร้อมใช้งาน

ระบบและข้อมูลสามารถเข้าถึงและใช้งานได้เมื่อต้องการ

ภัยคุกคาม: DDoS, System Outage

รูปแบบบริการคลาวด์และความรับผิดชอบร่วม (Shared Responsibility)

IaaS / PaaS / SaaS — ขอบเขตความรับผิดชอบของ CSP และ CSC แตกต่างกันตามรูปแบบ



Security IN the Cloud
— ความรับผิดชอบของ CSC

Security OF the Cloud
— ความรับผิดชอบของ CSP

รูปแบบการให้บริการ (Deployment Models) ตาม NIST SP 800-145

Public / Private / Hybrid / Community Cloud

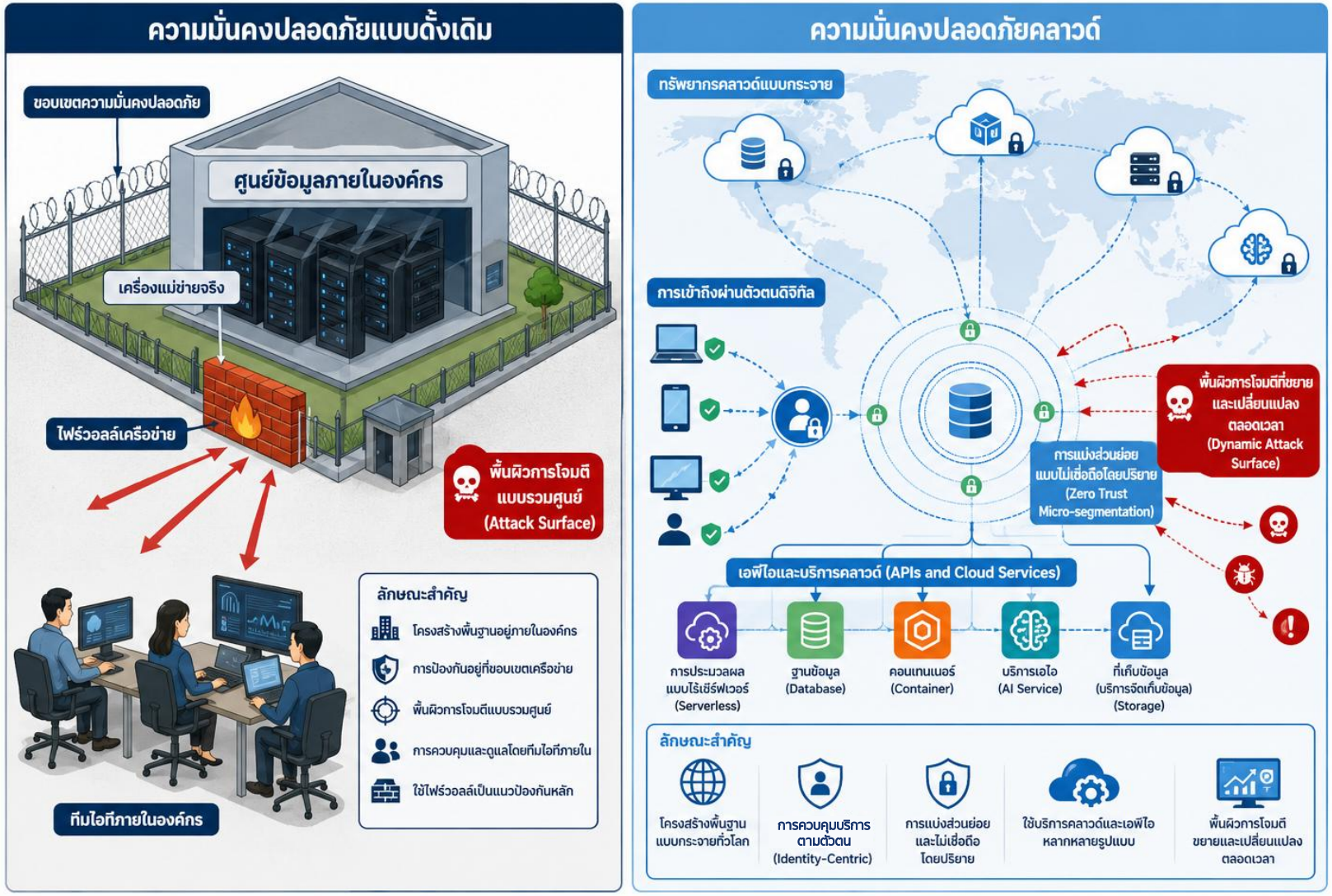
รูปแบบ (EN)	ภาษาไทย	คำอธิบาย	หมายเหตุ
Public Cloud	คลาวด์สาธารณะ	CSP ให้บริการสาธารณะหลายองค์กรร่วมกัน บนโครงสร้างพื้นฐานเดียวกัน	
Private Cloud	คลาวด์ส่วนตัว	ให้บริการเฉพาะองค์กรเดียว อาจตั้งใน data center ของหน่วยงานเอง	อยู่นอกขอบเขตของมาตรฐานคลาวด์ฯ
Hybrid Cloud	คลาวด์ผสม	ผสมระหว่าง Public และ Private โดยข้อมูลและแอปสามารถโยกย้ายข้ามได้	
Community Cloud	คลาวด์ชุมชน	ให้บริการกลุ่มองค์กรที่มีภารกิจหรือข้อกำหนดเหมือนกัน	

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ.2567

"คลาวด์สาธารณะ หมายความว่า รูปแบบการใช้คลาวด์ที่บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ใด ๆ และทรัพยากรถูกควบคุมโดยผู้ให้บริการคลาวด์"

การเปลี่ยนกระบวนทัศน์ — จาก Perimeter Defense สู่ Zero Trust

ความมั่นคงปลอดภัยคลาวด์ เทียบกับ ความมั่นคงปลอดภัยแบบดั้งเดิม: การเปลี่ยนกระบวนทัศน์



Zero Trust

ไม่ไว้วางใจสิ่งใดโดยปริยาย ตรวจสอบสิทธิ์ทุกครั้ง, Microsegmentation

Identity-Centric

IAM กลายเป็นแนวรับหลัก แทนการพึ่งขอบเขตเครือข่าย (Perimeter)

Encryption Everywhere

เข้ารหัสทั้ง At-rest และ In-transit เพราะข้อมูลอยู่นอกการควบคุม

Continuous Visibility

บันทึก ตรวจสอบ และวิเคราะห์เหตุการณ์ตลอดเวลา ผ่าน SIEM/SOC

ภัยคุกคามทางไซเบอร์ต่อระบบคลาวด์ — 8 ประเภทหลัก

Misconfiguration เป็นสาเหตุอันดับ 1 ของการรั่วไหลข้อมูลในคลาวด์

01 **Misconfiguration**
แนวทางรับมือ: CSPM + Config Review

02 **Account Takeover**
แนวทางรับมือ: MFA + UBA

03 **Supply Chain Attack**
แนวทางรับมือ: SBOM + Code Signing

04 **Insider Threat**
แนวทางรับมือ: Least Privilege + Audit Log

05 **DDoS Attack**
แนวทางรับมือ: CDN + DDoS Protection

06 **Cloud Ransomware**
แนวทางรับมือ: Immutable / Air-gap Backup

07 **Cryptojacking**
แนวทางรับมือ: CPU/GPU Anomaly Detection

08 **API Attack**
แนวทางรับมือ: API Gateway + Rate Limiting

ความเสี่ยงเชิงกลยุทธ์เพิ่มเติม — มากกว่าภัยคุกคามทางเทคนิค

Vendor Lock-in / Data Sovereignty / Compliance / Availability — ต้องประเมินคู่ขนาน

01

Vendor Lock-in

การพึ่งพาผู้ให้บริการรายเดียว

ทำให้ยากต่อการโยกย้ายในอนาคต — ต้องวางแผน Exit Strategy และใช้สถาปัตยกรรมที่ไม่ผูกขาด

02

Data Sovereignty

อธิปไตยของข้อมูล

ข้อมูลที่ประมวลผลในต่างประเทศอาจอยู่ภายใต้กฎหมายต่างประเทศ ซึ่งอาจขัดแย้งกับกฎหมายไทย

03

Compliance

การปฏิบัติตามกฎหมาย

สัญญาบริการต้องสอดคล้องกับ PDPA และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

04

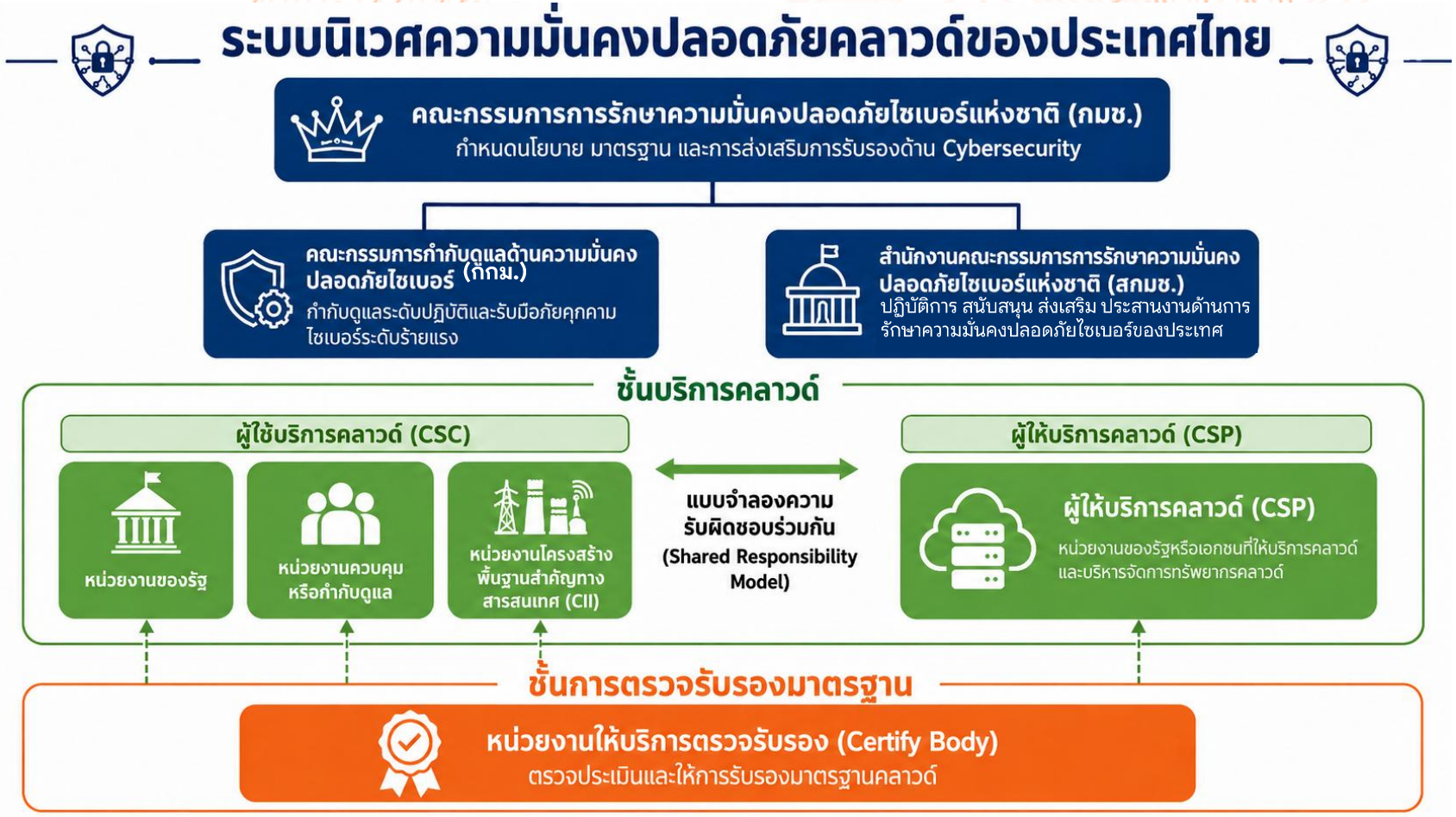
Availability

ความพร้อมใช้งานขึ้นกับเครือข่าย

ขึ้นอยู่กับเครือข่ายอินเทอร์เน็ตและบริการของ CSP — กรณีขัดข้องอาจกระทบภารกิจหลัก

ระบบนิเวศความมั่นคงปลอดภัยคลาวด์ของประเทศไทย

กลุ่มผู้มีบทบาทหลักภายใต้ระบบนิเวศความมั่นคงปลอดภัยคลาวด์ของไทย



1 **กมช.**
นโยบาย/มาตรฐานระดับชาติ

2 **กกม. / สกมช.**
กำกับดูแล / กำหนดหลักเกณฑ์

3 **CSC ↔ CSP**
ทำงานภายใต้ Shared Responsibility

4 **Certify Body**
ตรวจประเมินและออกใบรับรองมาตรฐาน

กรอบกฎหมาย — ประกาศ 7 ฉบับที่เกี่ยวข้องกับมาตรฐานคลาวด์ พ.ศ. 2567

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ฐานอำนาจของประกาศและมาตรฐานทั้งหมดด้านความมั่นคงปลอดภัยไซเบอร์

ประกาศ กมช. เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็น CII ฯ พ.ศ. 2568

- กำหนดหลักเกณฑ์ในการระบุหน่วยงานที่ถือว่า (CII)
- มอบหมายหน่วยงานควบคุมหรือกำกับดูแลในแต่ละภาคส่วน

ประกาศ กมช. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ พ.ศ. 2564

- กรอบมาตรฐานหลักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ใช้กับ หน่วยงานของรัฐ (GOV), หน่วยงานควบคุมหรือกำกับดูแล (Regulator), CII

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

- กำหนดวิธีการประเมินระดับผลกระทบใน 3 ด้าน (CIA) แบ่งเป็น 3 ระดับ (ต่ำ/กลาง/สูง)
- มาตรฐานคลาวด์ฯ ใช้ระดับผลกระทบนี้เป็นพื้นฐานในการระบุข้อกำหนดขั้นต่ำ

ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

- กำหนดมาตรการควบคุมขั้นต่ำสำหรับข้อมูลและระบบสารสนเทศแบบทั่วไป (ไม่เฉพาะระบบคลาวด์) ตามระดับผลกระทบที่ประเมินได้

ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

- กำหนดแนวทางในการพัฒนาและส่งเสริมผู้ให้บริการด้านความมั่นคงปลอดภัย
- รวมถึงการรับรองผู้ให้บริการคลาวด์ (CSP) ขึ้นทะเบียนหน่วยตรวจรับรอง (CAB)

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

- ระบุข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์
- ครอบคลุมทั้งฝั่งผู้ให้บริการ (CSP) และผู้ใช้บริการ (CSC)

ประกาศ สกมช. เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลในไทย พ.ศ. 2567

- แนวปฏิบัติสำหรับการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลตั้งอยู่ในประเทศไทย
- ขยายความนโยบายอธิปไตยของข้อมูล (Data Sovereignty/Data Localization)

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

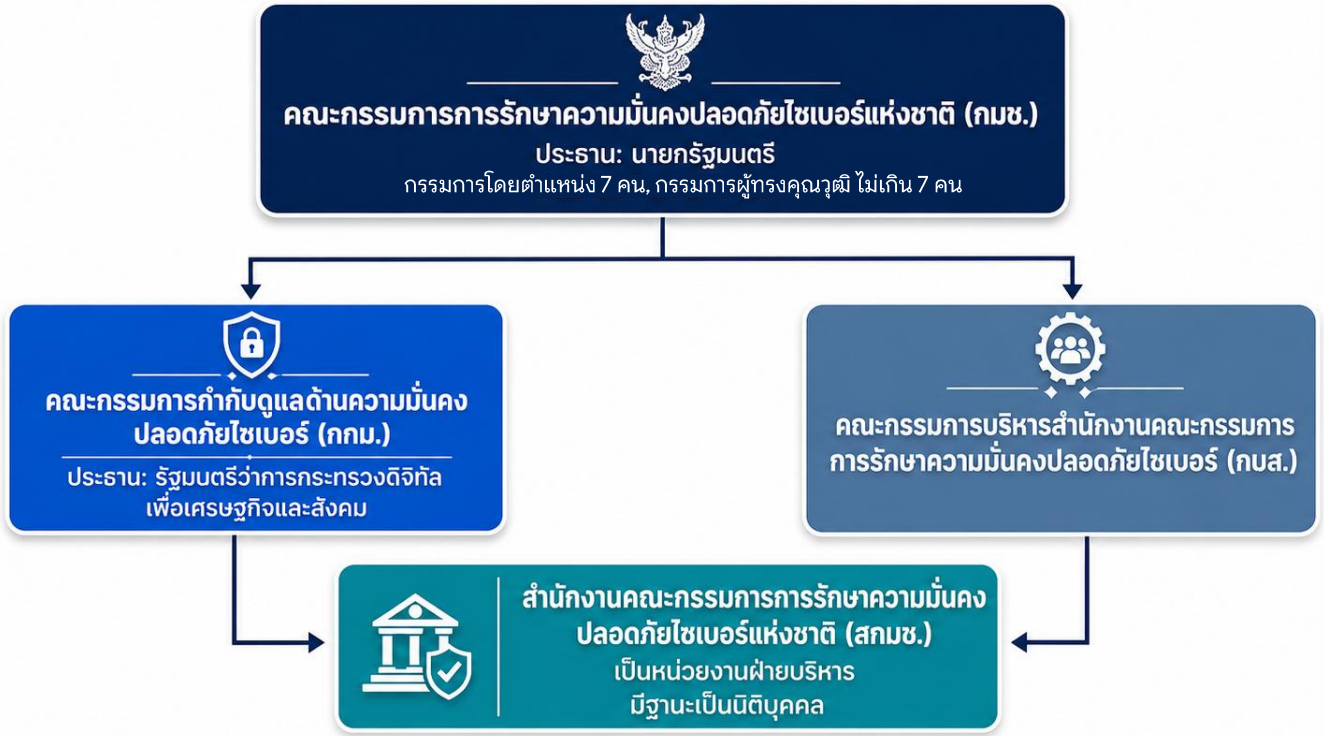
โครงสร้าง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

กฎหมายหลักด้านความมั่นคงปลอดภัยไซเบอร์ของไทย

หมวด 1	หมวด 2	หมวด 3	หมวด 4	หมวด 5
คณะกรรมการ	**สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ**	**สำนักงาน สกมช.**	**การรักษาความมั่นคงปลอดภัยไซเบอร์**	**บทกำหนดโทษ**
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.), คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)	จัดตั้ง สกมช., กำหนดอำนาจหน้าที่, คณะกรรมการบริหาร สกมช.	หน่วยงานปฏิบัติของรัฐในฐานะนิติบุคคล	นโยบายและแผนฯ, การบริหารจัดการ, โครงสร้างพื้นฐานสำคัญทางสารสนเทศ, การรับมือกับภัยคุกคามไซเบอร์	โทษทางอาญาและทางปกครอง

บทบาทของหน่วยงานกำกับดูแล — กมช. (NCSC) และ สกมช. (NCSA)

โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของไทย



กมช. — คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นายกรัฐมนตรีเป็นประธาน

- กำหนดนโยบายและแผนระดับชาติ
- ออกประกาศและกำหนดมาตรฐาน
- กำหนดหลักเกณฑ์การกำหนดลักษณะหน่วยงาน CII
- กำหนดลักษณะของภัยคุกคามทางไซเบอร์

สกมช. — สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล • ฝ่ายเลขานุการ กมช.

- ปฏิบัติงานหลักด้านความมั่นคงปลอดภัยไซเบอร์
- ขับเคลื่อนภารกิจตามนโยบายของ กมช.
- ออกแนวทางเสริมตามอำนาจสำนักงาน

หน่วยงานในระบบกำกับดูแล — 3 ประเภท

หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงาน CII

01

หน่วยงานของรัฐ

Government Agencies

ส่วนราชการ องค์กรปกครองส่วนท้องถิ่น รัฐวิสาหกิจ และหน่วยงานอิสระของรัฐ ที่ใช้ข้อมูลหรือระบบสารสนเทศของรัฐ

หน้าที่หลัก

ปฏิบัติตามมาตรฐานขั้นต่ำที่ กมช. กำหนด ตามระดับผลกระทบที่ประเมินได้

02

Regulator

หน่วยงานควบคุมหรือกำกับดูแล

หน่วยงานของรัฐที่ได้รับมอบหมายให้ควบคุมหรือกำกับดูแลหน่วยงาน CII ในภาคส่วนใดภาคส่วนหนึ่ง

หน้าที่หลัก

ออกหลักเกณฑ์เฉพาะภาคส่วน เช่น ภาคการเงิน (ธปท., ก.ล.ต.), สาธารณสุข, พลังงาน

03

CII

Critical Information Infrastructure

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ — กระทบความมั่นคงของรัฐและการบริการสาธารณะอย่างมีนัยสำคัญ

หน้าที่หลัก

ปฏิบัติตามมาตรฐานขั้นสูง รายงานภัยคุกคามต่อ สกมช. และฝึกซ้อมรับมือเหตุ

หน่วยงาน CII — 7 ภาคส่วนสำคัญทางสารสนเทศของประเทศ

หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568

01	**ความมั่นคงของรัฐ**	*National Security*
02	**บริการภาครัฐที่สำคัญ**	*Critical Government Services*
03	**การเงินการธนาคาร**	*Banking & Finance*
04	**เทคโนโลยีสารสนเทศและโทรคมนาคม**	*ICT & Telecom*
05	**การขนส่งและโลจิสติกส์**	*Transport & Logistics*
06	**พลังงานและสาธารณูปโภค**	*Energy & Utilities*
07	**สาธารณสุข**	*Public Health*

โครงสร้างความสัมพันธ์ของกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ และระบบคลาวด์ของ สกมช.

กฎหมายแม่

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- ตั้ง 3 คณะกรรมการ: กมช. / กกม. / คณะกรรมการบริหาร สกมช.
- ตั้งสำนักงาน สกมช. เป็นหน่วยปฏิบัติ

ให้อำนาจออกประกาศ

กฎหมายฉบับรอง

ฝั่งผู้ใช้บริการคลาวด์ ได้แก่ GOV, CII, Regulator

ประกาศ กมช. เรื่อง ประมวลแนวทางปฏิบัติฯ พ.ศ.2564 [มาตรา 13, 54]
→ “กรอบใหญ่” สำหรับ GOV, CII, Regulator

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะฯ พ.ศ.2566 [มาตรา 9]
→ “วิธีจำแนกประเภท” ข้อมูล/ระบบสารสนเทศ

ใช้ระบุข้อกำหนดขั้นต่ำ

ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบฯ พ.ศ. 2566 [มาตรา 9]
→ “กำหนดพื้นฐานที่ต้องทำ”

ฝั่งผู้ให้บริการคลาวด์ ต่อ GOV, CII, Regulator

ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 [มาตรา9]
→ กำหนด “มาตรฐาน และการรับรอง” ฝั่งผู้ให้บริการ

ให้อำนาจ ออกประกาศ

ใช้ระบุข้อกำหนดขั้นต่ำ

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 [มาตรา 9]
→ กำหนด “พื้นฐานที่ต้องทำ” เฉพาะสำหรับระบบคลาวด์

เพิ่มเติม แนวทางปฏิบัติ

กำหนดหลักเกณฑ์สำหรับการตรวจรับรองระบบคลาวด์

ประกาศ สกมช.

ประกาศ สกมช. เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลในไทย พ.ศ. 2567

ประกาศอื่น ของ สกมช. ที่เกี่ยวกับหลักเกณฑ์และข้อกำหนดเกี่ยวกับการรับรองบริการคลาวด์

GOV : หน่วยงานของรัฐ

CII : หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Regulator : หน่วยงานควบคุมหรือกำกับดูแล

ที่มาของสองมาตรฐานคลาวด์ภายใต้นโยบาย Cloud First

ทำไมหน่วยงานรัฐต้องเข้าใจทั้งมาตรฐานความมั่นคงปลอดภัย และแนวทางการใช้คลาวด์

นโยบายการใช้คลาวด์เป็นหลัก

(Cloud First Policy)

คณะรัฐมนตรีแถลงต่อรัฐสภา 11 ก.ย. 2566 ให้หน่วยงานรัฐพิจารณาใช้บริการคลาวด์เป็นทางเลือกแรก (First Choice) แทนการจัดซื้ออุปกรณ์และซอฟต์แวร์แบบเดิม (On-Premise)

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ — กำหนดข้อกำหนดขั้นต่ำเชิงความปลอดภัย

(ร่าง) มรด. 9-2 : 2568

มาตรฐานว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลักของ สพร. — เน้นการเลือกและบริหารจัดการคลาวด์ให้คุ้มค่า

ลำดับเหตุการณ์สำคัญ

11 ก.ย. 2566
ครม. แถลงนโยบาย Cloud First

พ.ศ. 2567
ประกาศ กมช. มาตรฐานคลาวด์

1 ก.ค. 2567
ตั้งคณะกรรมการเฉพาะด้านฯ มอบหมาย สพร.

ธ.ค. 2568
เปิดรับฟังความเห็น (ร่าง) มรด. 9-2

จุดมุ่งหมาย และกลุ่มเป้าหมายที่แตกต่างกัน

สองมาตรฐานออกแบบมาเพื่อภารกิจคนละด้าน จึงต้องใช้ประกอบกัน

(ร่าง) มรด. 9-2 : 2568 • สพร.	มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
จุดมุ่งหมาย	
เลือกใช้และบริหารจัดการคลาวด์ กำหนดแนวทางเลือกใช้คลาวด์ให้เหมาะกับระดับชั้นข้อมูลและภารกิจ ปกป้องข้อมูลสำคัญของรัฐ และเน้นความคุ้มค่าในการบริหารทรัพยากร	**ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัย** กำหนดข้อกำหนดขั้นต่ำสำหรับการใช้งานและให้บริการระบบคลาวด์ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ
กลุ่มเป้าหมาย	
หน่วยงานของรัฐทั้งหมด บังคับใช้กับหน่วยงานของรัฐ แต่ไม่ครอบคลุม CSP ที่เป็นเอกชนซึ่งให้บริการคลาวด์แก่หน่วยงานของรัฐ	**ครอบคลุมทั้งระบบนิเวศ** หน่วยงานของรัฐ • หน่วยงานควบคุม/กำกับดูแล • หน่วยงาน CII • และ CSP ของหน่วยงานเหล่านี้

การจัดประเภทข้อมูล สู่การเลือกประเภทคลาวด์

(ร่าง) มรด. 9-2 ผูกประเภทข้อมูลกับชนิดคลาวด์ตามระดับชั้นความลับ

ระดับความอ่อนไหวของข้อมูลสูงขึ้น → ยิ่งต้องการการควบคุมและอธิปไตยของข้อมูล (Data Sovereignty) มากขึ้น

Official Data 1

ข้อมูลที่เปิดเผยได้

ชั้นเผยแพร่ภายในองค์กร / เปิดเผย

Public Cloud

Protected Data 2

ข้อมูลที่ต้องได้รับความคุ้มครอง

ชั้นลับ / ลับมาก

Public Cloud ที่มีมาตรการสูง (VPC)

Highly Protected Data 3

ข้อมูลที่ต้องคุ้มครองสูงสุด

ชั้นลับที่สุด (ข้อมูลความมั่นคง)

Sovereign Cloud

เกณฑ์จำแนก : ประเมินค่าเฉลี่ย CIA (Confidentiality • Integrity • Availability)

ตั้งแต่ 3 คะแนนขึ้นไป จัดเป็นชั้นลับที่สุด • หากต่ำกว่า 3 ให้ประเมินความเสี่ยง (โอกาสเกิด × ผลกระทบ)

ประเด็นเรื่องที่ตั้งศูนย์ข้อมูล

Data Localization

(ร่าง) มรด. 9-2 : 2568

ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงที่สุดต่อรัฐ ซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก

บังคับ Sovereign Cloud เฉพาะข้อมูล Highly Protected (ชั้นลับที่สุด) เท่านั้น

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 + ประกาศ สกมช. เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลในไทย พ.ศ. 2567

- หากข้อมูลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยของประเทศในระดับสูง ต้องตั้งศูนย์ข้อมูลหลักในประเทศไทย
- ตั้งศูนย์ข้อมูลสำรองในไทย หรือภูมิภาคเอเชียตะวันออกเฉียงใต้ รวมสิงคโปร์และฮ่องกง

วิเคราะห์ความแตกต่าง : หัวข้อความรับผิดชอบ 11 ด้าน

(ร่าง) มรด. 9-2 ไม่ได้ระบุชัดเจนในบางประเด็นด้านความปลอดภัย เทียบกับ มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

✓ **Cryptography**
ของ สกมช. ลงลึกความเป็นเจ้าของกุญแจ (Key)

✓ **Configuration**
ของ สกมช. เจาะจงแยก Dev/Test/Prod

✓ **Identity & Access**
ของ สกมช. มีข้อกำหนด Privileged Access, Secrets

✓ **Physical Security**
ของ สกมช. มีข้อกำหนด Secure Disposal

✗ **Data Center Location**
ไม่ได้ระบุชัดเรื่อง Data Localization ที่ตั้งศูนย์ข้อมูล

✗ **Event Logging**
ไม่ได้ระบุชัดเรื่อง Log Protection & Retention

✗ **Data Backup**
ไม่ได้ระบุชัดเรื่อง ความรับผิดชอบการสำรอง/กู้คืน

✗ **Supply Chain / Supplier**
ไม่ได้ระบุชัดเรื่อง การกำกับผู้รับจ้างช่วง

✗ **Incident Management**
ไม่ได้ระบุชัดเรื่อง การรายงาน/ตอบสนองเหตุ

✗ **Vulnerability Mgmt**
ไม่ได้ระบุชัดเรื่อง การจัดการช่องโหว่ทางเทคนิค

✗ **Independent Review**
ไม่ได้ระบุชัดเรื่อง การตรวจสอบความเป็นอิสระ (Audit)

ทั้งสองมีหัวข้อนี้

(ร่าง) มรด. 9-2 ยังไม่ได้ระบุชัดเจน

บทสรุป : ทั้งสองมาตรฐานต้องเดินไปด้วยกัน

ความคุ้มค่าจาก สพร. + ความมั่นคงปลอดภัยจาก กมช. = คลาวด์ภาครัฐที่ยั่งยืน

1

ใช้ประกอบกัน

(ร่าง) มรด. 9-2 ช่วยเลือกคลาวด์ให้คุ้มค่า ส่วนประกาศ กมช. กำหนดความปลอดภัยขั้นต่ำ — ต้องอ้างอิงซึ่งกันและกัน

2

ปิดช่องว่าง

อยู่ระหว่างกระบวนการทบทวนร่วมกันเพื่อให้แน่ใจว่ากฎเกณฑ์มีความสมบูรณ์และไม่ขัดแย้งกัน

มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล และระบบสารสนเทศ พ.ศ. 2566

แนวทางการพิจารณาผลกระทบแก่ข้อมูลหรือระบบสารสนเทศ

ด้านทรัพย์สินและชื่อเสียง

ผลกระทบต่อมูลค่าความเสียหายทางการเงิน ทรัพย์สิน หรือต่อชื่อเสียงของหน่วยงาน

ด้านบุคคล

ผลกระทบต่อจำนวนผู้ใช้บริการของหน่วยงาน บุคลากร หรือประชาชน

ที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด

ด้านการดำเนินงาน

ผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน

ด้านความมั่นคง

ผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

เกณฑ์การประเมินระดับผลกระทบ
(The Impact Assessment)

	การรักษาความลับ (การเปิดเผยข้อมูลทั้งหมดหรือบางส่วนโดยไม่ได้รับอนุญาต)	การรักษาความถูกต้องครบถ้วน (การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต)	การรักษาสภาพพร้อมใช้งาน (หน่วยงานไม่สามารถเข้าถึงหรือใช้งานข้อมูลหรือระบบได้)
 ผลกระทบต่ำ	อาจส่งผลกระทบต่อการดำเนินงาน หรือ ทรัพย์สิน (หรือ ชื่อเสียง)* ของหน่วยงานหรือบุคคล **เพียงเล็กน้อยหรือจำกัด**		
 ผลกระทบปานกลาง	อาจส่งผลกระทบต่อการดำเนินงาน หรือ ทรัพย์สิน (หรือ ชื่อเสียง)* ของหน่วยงานหรือบุคคล **ร้ายแรง**		
 ผลกระทบสูง	อาจส่งผลกระทบต่อการดำเนินงาน หรือ ทรัพย์สิน (หรือ ชื่อเสียง)* ของหน่วยงานหรือบุคคล **ร้ายแรงมาก**		

หมายเหตุ * ผลกระทบด้านชื่อเสียง พิจารณาเฉพาะการประเมินตามวัตถุประสงค์ด้านการรักษาความลับ

การจัดระดับผลกระทบด้านการรักษาความลับ โดยพิจารณาจากคุณสมบัติของข้อมูล

-- ชั้นความลับของข้อมูล อิงตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

ข้อควรระวังสำคัญ:
หากระบบจัดเก็บข้อมูลส่วนบุคคล (PDPA) ระบบนั้นจะต้องถูกจัดจัดให้อยู่ในระดับผลกระทบปานกลาง (Medium) เป็นอย่างน้อยเสมอ

อิงจาก ข้อ ๔ ในประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

การประเมินผลกระทบตามหลัก CIA Triad และ "High Water Mark"

ประเมินทั้ง 3 มิติ — และใช้ระดับสูงสุดเป็นระดับโดยรวมของข้อมูล/ระบบ

Confidentiality	Integrity	Availability
ความลับ	ความถูกต้อง	พร้อมใช้งาน
กลาง	ต่ำ	สูง
ตัวอย่างระดับที่ประเมินได้	*ตัวอย่างระดับที่ประเมินได้*	*ตัวอย่างระดับที่ประเมินได้*

ระดับโดยรวม

ระดับสูง

ขั้นตอนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

กระบวนการ 6 ขั้นตอน — ตั้งแต่ระบุข้อมูล/ระบบ ไปจนถึงทบทวน

01	02	03	04	05	06
Inventory	Classify	Assess CIA	High Water Mark	Document	Review
ระบุข้อมูล/ระบบ	**จัดประเภทข้อมูล**	**ประเมิน 3 มิติ**	**ใช้ระดับสูงสุด**	**จัดทำเอกสาร**	**ทบทวน**
รวบรวมบัญชีข้อมูลและระบบสารสนเทศของหน่วยงาน	พิจารณาว่าเป็นข้อมูลทั่วไป ลับ หรือข้อมูลส่วนบุคคล	ประเมินผลกระทบด้าน C, I, A ของแต่ละข้อมูล/ระบบ	เลือกระดับสูงสุดเป็นระดับโดยรวม	บันทึกผลพร้อมเหตุผล	ทบทวนทุก 3 ปีเป็นอย่างน้อย หรือ เมื่อข้อมูล ระบบ หน้าที่ของหน่วยงานมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ผลลัพธ์ที่ได้

บัญชีข้อมูล/ระบบสารสนเทศที่ระบุระดับผลกระทบ (Low/Moderate/High) ครบถ้วน — เป็นพื้นฐานการเลือกมาตรการควบคุมและการคัดเลือกผู้ให้บริการคลาวด์

“หน่วยงานอาจดำเนินการกำหนดประเภทข้อมูลตามหลักเกณฑ์ของหน่วยงาน”

ตัวอย่างหลักเกณฑ์ของหน่วยงาน ในการพิจารณาผลกระทบ 4 ด้าน × 3 ระดับ

มิติ / ระดับ	ระดับต่ำ	ระดับกลาง	ระดับสูง
1. การเงิน / ทรัพย์สิน / ชื่อเสียง	< 1 ล้านบาท หรือชื่อเสียงเฉพาะภายในหน่วยงาน	1–100 ล้านบาท หรือชื่อเสียงระดับสาธารณะภายในประเทศ	> 100 ล้านบาท หรือชื่อเสียงระดับนานาชาติ
2. การดำเนินงาน / บุคลากร / ประชาชน	กระทบ < 100 ราย หรือบริการลดลงเล็กน้อย	กระทบ 100–10,000 ราย หรือบริการหยุด 1–24 ชม.	กระทบ > 10,000 ราย หรือบริการหยุด > 24 ชม. หรือกระทบชีวิต
3. ภารกิจของหน่วยงาน	ภารกิจรองหรือสนับสนุน ดำเนินงานต่อได้	ภารกิจหลักบางส่วนหยุดชะงัก แต่ดำเนินงานทดแทนได้	ภารกิจหลักหยุดทั้งหมด ปฏิบัติหน้าที่ตามกฎหมายไม่ได้
4. ความมั่นคง / ความสงบเรียบร้อย	ไม่กระทบความมั่นคงหรือความสงบเรียบร้อย	กระทบความมั่นคงระดับท้องถิ่นหรือเฉพาะภาคส่วน	กระทบความมั่นคงของรัฐ เศรษฐกิจ การทหาร เป็นวงกว้าง

ตัวอย่าง Information Asset Register — องค์ประกอบ 9 หมวด

ใช้เป็นเครื่องมือหลักในการติดตามและบริหารทรัพย์สินสารสนเทศของหน่วยงาน

ข้อมูลพื้นฐาน 1

Asset ID • ชื่อ • ประเภท • คำอธิบาย

เจ้าของและผู้ดูแล 2

Data Owner • Custodian • Users

คุณลักษณะการจำแนก 3

C / I / A และระดับชั้นรวม

ตำแหน่งและบริการ 4

Location • Cloud Provider • Service Tier

ข้อมูลที่เกี่ยวข้อง 5

Data Types • Laws & Regulations

ความสำคัญต่อภารกิจ 6

Mission Criticality • Impact if down

ความเสี่ยงและภัยคุกคาม 7

Top Threats • Residual Risk

มาตรการควบคุม 8

Controls Applied

วันที่และผู้รับผิดชอบ 9

Classified On • Approved By • Next Review

กฎหมายไซเบอร์และมาตรฐานระบบคลาวด์ของประเทศไทย

- **มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567**
  - ความเสี่ยงจากการใช้บริการคลาวด์
  - กรอบแนว เหตุผลความจำเป็นและวัตถุประสงค์ของมาตรฐาน
  - ฐานอำนาจ ขอบเขต และโครงสร้างของมาตรฐาน
  - ความเชื่อมโยงกับการคุ้มครองข้อมูลส่วนบุคคลและมาตรฐานสากล
  - กระบวนการตรวจรับรองมาตรฐาน

เหตุผลความจำเป็นและวัตถุประสงค์ของมาตรฐานคลาวด์ พ.ศ. 2567

ทำไมประเทศไทยต้องมีมาตรฐานเฉพาะสำหรับระบบคลาวด์?

01

Adoption เร่งตัว

การใช้คลาวด์ของหน่วยงานของรัฐและ CII ขยายตัวอย่างรวดเร็ว แต่ยังไม่มีมาตรฐานเฉพาะของไทย

02

ภัยคุกคามเฉพาะคลาวด์

Misconfiguration, API Attack, Account Takeover — ภัยที่ระบบ on-premise แบบเดิมไม่ครอบคลุม

03

อธิปไตยของข้อมูล

ข้อมูลของรัฐ/CII ที่ประมวลผลในต่างประเทศ ต้องมีกรอบกำกับชัดเจน

04

เชื่อมโยงสากล

สอดคล้องกับ ISO/IEC 27017, ISO/IEC 27018 เพื่อให้เปรียบเทียบกับมาตรฐานสากลได้

ฐานอำนาจและขอบเขตการบังคับใช้

ออกตามอำนาจ พ.ร.บ. ไซเบอร์ พ.ศ. 2562 — ใช้กับทั้ง CSP และ CSC

ฐานอำนาจ (Legal Basis)

- อำนาจ กมช. ตามมาตรา 9 (4) ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
- ใช้ร่วมกับประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

ใครต้องปฏิบัติ (Who)

- **ผู้ใช้บริการคลาวด์ (CSC)** ได้แก่ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และ CII
- **ผู้ให้บริการคลาวด์ (CSP)** ทั้งในและต่างประเทศ ที่ให้บริการกับ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และ CII

ครอบคลุมอะไร (What)

- ทุก service model — IaaS, PaaS, SaaS
- สำหรับบริการคลาวด์สาธารณะ (ไม่รวม Private Cloud)
- ข้อกำหนดขั้นต่ำ ตามระดับผลกระทบ Low/Moderate/High

โครงสร้างของมาตรฐาน ฯ

ข้อกำหนดขั้นต่ำตามระดับผลกระทบ

		ต่ำ	กลาง	สูง
Governance	5.1.1 นโยบายด้านความมั่นคงปลอดภัย	✓	✓	✓
	5.1.2 โครงสร้างองค์กร	✓	✓	✓
	5.1.3 การปฏิบัติตามกฎระเบียบ		✓	✓
Operations	5.2.1 การบริหารทรัพยากรมนุษย์	✓	✓	✓
	5.2.2 การจัดการทรัพย์สิน	✓	✓	✓
	5.2.3 การควบคุมการเข้าถึง	✓	✓	✓
	5.2.4 การเข้ารหัส	✓	✓	✓
	5.2.5 ความปลอดภัยทางกายภาพ			✓
	5.2.6 ความมั่นคงปลอดภัยการปฏิบัติการ			✓
	5.2.7 ความมั่นคงปลอดภัยเครือข่าย		✓	✓
	5.2.8 การจัดหา พัฒนา บำรุงรักษา	✓	✓	✓
	5.2.9 การจัดการผู้ให้บริการภายนอก	✓	✓	✓
	5.2.10 การจัดการเหตุภัยคุกคาม		✓	✓

ข้อกำหนดการตรวจรับรอง (Certification Requirements by Impact Level)

	ผลกระทบระดับต่ำ (Low)	กลาง (Medium)	สูง (High)
ผู้ใช้บริการ (CSC)	 ประเมินตนเอง (Self-assessment) พร้อมขออนุมัติจากผู้บริหารสูงสุด	 รับรองโดยหน่วยงานกำกับดูแล (Attestation) หรือ หน่วยงานตรวจรับรอง (Certify Body)	 รับรองโดยหน่วยงานตรวจรับรอง (Certify Body) เท่านั้น
ผู้ให้บริการ (CSP) [ต้องใช้ Certify Body ทั้งหมด]	รับรองโดย Certify Body + ISO/IEC 27001 + CSA STAR Level 1/CCM Lite	รับรองโดย Certify Body + CSA STAR Level 2/CCM + ISO/IEC 27701	รับรองโดย Certify Body + ISO/IEC 27017 หรือ CSA STAR Level 2/CCM + ISO/IEC 27018 + ISO/IEC 27701

ความเชื่อมโยงกับมาตรฐานสากล — ISO/IEC Family

27017 + 27018 เป็นรากฐานของข้อกำหนดในมาตรฐานคลาวด์

ISO/IEC 27002 ISMS	**แนวทางปฏิบัติมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ**	ฐานของระบบบริหารด้านความมั่นคงปลอดภัยข้อมูล ตาม ISO 27017:2015 และ ISO 27018:2019 (now v.2025)
ISO/IEC 27017:2015 Cloud Controls	**แนวทางปฏิบัติมาตรการควบคุมด้านความมั่นคงปลอดภัยบนบริการคลาวด์** (ส่วนเสริมจาก ISO/IEC 27002)	ข้อกำหนดเฉพาะสำหรับบริการคลาวด์ ครอบคลุม CSP และ CSC
ISO/IEC 27018:2019 PII in Public Cloud	**แนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ใน Public Cloud** (ส่วนเสริมจาก ISO/IEC 27002)	ข้อกำหนดเฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลบนบริการคลาวด์

กรอบเวลาการบังคับใช้และสิ่งที่ต้องดำเนินการ (Enforcement Timeline & Next Steps)

การรายงานผล (Reporting Requirement):
เมื่อหน่วยงานดำเนินการประเมินและปรับปรุงตามข้อกำหนดแล้วเสร็จ ต้องจัดส่งผลสรุปรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน 30 วัน

ความเชื่อมโยงกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

เมื่อระบบคลาวด์ประมวลผลข้อมูลส่วนบุคคล — มาตรฐานคลาวด์ + PDPA ต้องบังคับใช้ร่วมกัน

บทบาทตาม PDPA

Data Controller
CSC — ผู้ใช้บริการคลาวด์

ผู้ควบคุมข้อมูล — ตัดสินใจวัตถุประสงค์/วิธีประมวลผล

Data Processor
CSP — ผู้ให้บริการคลาวด์

ผู้ประมวลผลข้อมูลตามคำสั่งของ Controller

DPO
Data Protection Officer

ทั้ง CSC และ CSP ต้องมี DPO ตามเงื่อนไขกฎหมาย

Data Subject
เจ้าของข้อมูล

มีสิทธิ์เข้าถึง แก้ไข ลบ และคัดค้านการประมวลผล

หน้าที่ที่ต้องร่วมกันปฏิบัติ

- สัญญา DPA (Data Processing Agreement) ระหว่าง CSC–CSP
- การกำหนดมาตรการเชิงเทคนิคและกระบวนการที่เหมาะสม
- การบันทึกกิจกรรมการประมวลผล (RoPA — Record of Processing)
- การประเมิน DPIA สำหรับการประมวลผลความเสี่ยงสูง
- การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง
- การโอนข้อมูลข้ามชายแดน (Cross-border Data Transfer)

ประเด็นสำคัญที่ต้องจดจำ — Key Takeaways

5 ข้อสรุปที่ผู้บริหารและทีมงานควรนำกลับไปขับเคลื่อนในองค์กร

01	**มาตรฐานคลาวด์ พ.ศ. 2567 เป็นเรื่องสำคัญ** เป็นส่วนหนึ่งของระบบนิเวศกฎหมายที่อิงตาม พ.ร.บ. ฯ พ.ศ. 2562	Takeaway #1
02	**ต้องใช้ร่วมกับมาตรฐานการกำหนดคุณลักษณะฯ พ.ศ. 2566** เริ่มจากประเมิน CIA และระดับผลกระทบของข้อมูล/ระบบเสมอ	Takeaway #2
03	**ระดับมาตรการขึ้นกับ "ระดับผลกระทบ"** ต่ำ/กลาง/สูง — แตกต่างกันไปตามแต่ละหน่วยงาน	Takeaway #3
04	**ทุกฝ่ายมีความรับผิดชอบ "ร่วมกัน"** CSP รับผิดชอบ Security of the Cloud / CSC รับผิดชอบ Security in the Cloud	Takeaway #4
05	**ตรวจรับรองโดย CB ที่ขึ้นทะเบียนกับ สกมช.** ใบรับรองอายุ 3 ปี + ตรวจติดตามทุกปี (ตรวจรับรองในปีที่ 1 และการตรวจติดตามในปีที่ 2, 3)	Takeaway #5

บทสรุป — เส้นทางสู่ระบบคลาวด์ที่มั่นคงปลอดภัยของประเทศไทย

การเชื่อมโยง 4 เสาหลัก: กฎหมาย / มาตรฐาน / ความรับผิดชอบร่วม / การตรวจรับรอง

01

กฎหมาย

Legal Framework

พ.ร.บ. ฯ พ.ศ. 2562 + ประกาศ 7 ฉบับ

02

มาตรฐาน

Standards

มาตรฐานคลาวด์ พ.ศ. 2567

03

ความรับผิดชอบ

Shared Responsibility

CSP — Security OF / CSC — Security IN

04

การตรวจรับรอง

Certification

ใบรับรอง 3 ปี + Surveillance ทุกปี

Call to Action

เริ่มต้นวันนี้ — ประเมิน CIA ของระบบที่ใช้คลาวด์ • คุยกับ CSP เรื่องความสอดคล้องมาตรฐาน • ยกระดับการตั้งค่าและการอบรมทีม • วางแผน Roadmap สู่การตรวจรับรอง

กฎหมายไซเบอร์และมาตรฐานระบบคลาวด์ของประเทศไทย

- **ข้อกำหนดขั้นต่ำตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (ส่วนที่ 1)**
  - นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)
  - โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)
  - การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)
  - การบริหารทรัพยากรมนุษย์ (Human Resource Security)
  - การจัดการทรัพย์สิน (Asset Management)
  - การควบคุมการเข้าถึง (Access Control)

5.1 การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

Cloud Security Governance

5.1 การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

5.1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Policies

ข้อกำหนดสำหรับ

CSC | CSP

ข้อกำหนดตามมาตรฐาน ฯ : ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

CSC – Cloud Service Customer

ก) CSC ต้องกำหนด**นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อ**ของ CSC นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของ CSC ต้อง**สอดคล้องกับระดับความเสี่ยง**ที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ขององค์กร

ข) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับการประมวลผลบนคลาวด์ CSC **ต้องคำนึงถึง**สิ่งต่อไปนี้

- **ข้อมูลที่จัดเก็บ**ในสภาพแวดล้อมการประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงและการจัดการโดย CSP
- **ทรัพย์สินขององค์กร**อาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชัน
- **กระบวนการ**ต่าง ๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย
- **ผู้ใช้บริการคลาวด์** (Cloud Service Users) และบริบทที่ใช้บริการคลาวด์
- **ผู้ดูแลระบบ**บริการคลาวด์ของ CSC ที่ได้รับสิทธิพิเศษในการเข้าถึง
- **ตำแหน่งทางภูมิศาสตร์**ขององค์กรของ CSP และประเทศที่ CSP สามารถจัดเก็บข้อมูล CSC ได้ (แม้จะเป็นการชั่วคราว)

CSP – Cloud Service Provider

ก) CSP ต้องเพิ่ม**นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์** โดยคำนึงถึงสิ่งต่อไปนี้

- **ข้อกำหนดขั้นต่ำ**ด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์
- **ความเสี่ยงจากบุคคลภายใน**ที่ได้รับอนุญาต
- การเช่าหลายรายและ**การแยก CSC** (รวมถึงการจำลองเสมือน)
- การเข้าถึง**ทรัพย์สินของ CSC** โดยเจ้าหน้าที่ของ CSP
- ขั้นตอน**การควบคุมการเข้าถึง** เช่น การยืนยันตัวตน ที่เข้มงวดสำหรับการเข้าถึงบริการคลาวด์ของผู้ดูแลระบบ
- **การสื่อสารกับ CSC ระหว่างการจัดการการเปลี่ยนแปลง**
- ความปลอดภัยของ**การจำลองเสมือน**
- การเข้าถึงและปกป้อง**ข้อมูลของ CSC**
- การจัดการวงจรชีวิตของ**บัญชี CSC**
- การ**สื่อสารกรณีเกิดเหตุ**ละเมิดและแนวทางการแบ่งปันข้อมูลเพื่อช่วยในการสืบสวนและนิติเวช

ข้อกำหนดตามมาตรฐาน ฯ : ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

CSC – Cloud Service Customer

ค) **นโยบายคุ้มครองข้อมูลส่วนบุคคล**ของ CSC ต้องระบุข้อความเกี่ยวกับข้อตกลงทาง**สัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ และ CSC**

ง) ข้อตกลงทางสัญญาต้อง**กำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง (Sub-contractors) และ CSC** อย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaS หรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกันขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS

CSP – Cloud Service Provider

-

ทำไมข้อกำหนดนี้สำคัญ | Why This Matters

6 ความเสี่ยงที่เกิดขึ้นจริงเมื่อองค์กรไม่มีนโยบายเฉพาะการประมวลผลบนคลาวด์

Policy Gap

ความเสี่ยง: สูง

ไม่มีนโยบายเฉพาะคลาวด์ → พนักงานนำข้อมูลขึ้น Shadow IT, เกิด Data Leakage

Compliance Failure

ความเสี่ยง: สูงมาก

ขัด PDPA ม.37/39, พ.ร.บ. ไซเบอร์ ม.44

Vendor Mismanagement

ความเสี่ยง: สูง

นโยบายไม่ระบุ Shared Responsibility → บังคับ CSP ตามสัญญาเมื่อเกิดเหตุไม่ได้

Audit Failure

ความเสี่ยง: สูง

ไม่มี Policy ที่อนุมัติเป็นทางการ → ตรวจประเมินไม่ผ่านมาตรฐาน ISO 27001/27017/27018 รวมถึง

CII Risk

ความเสี่ยง: สูงมาก

หน่วยงาน CII ไม่มีประมวลแนวทางปฏิบัติ → ขัดกับ พ.ร.บ. ไซเบอร์ ม.44

Privacy Breach

ความเสี่ยง: สูงมาก

ไม่มี Data Processing Agreement → CSC รับผิดเต็มตาม PDPA

★ สถิติสำคัญ

99% ของความล้มเหลวด้านความปลอดภัยในคลาวด์ถึงปี 2025 มาจาก Customer Misconfiguration (Gartner)

USD 4.44M ค่าใช้จ่ายเฉลี่ยต่อเหตุ Breach (IBM Cost of Breach 2024) | **30%** ขององค์กรเท่านั้นที่มีนโยบายครอบคลุม Multi-cloud (CSA)

ถอดรหัสข้อกำหนดสำหรับ CSP | ผู้ให้บริการคลาวด์

10 ประเด็นที่ CSP ต้องระบุในนโยบาย

01 Baseline Security Requirements
ข้อกำหนดขั้นต่ำในการออกแบบและพัฒนาบริการคลาวด์

02 Insider Risk
ความเสี่ยงจากเจ้าหน้าที่ของ CSP ที่ได้รับอนุญาตเข้าถึงข้อมูล CSC

03 Multi-tenancy & Isolation
การแบ่งแยกผู้ใช้แต่ละราย รวมถึง Virtualization

04 Staff Access to CSC Assets
แนวทางและเงื่อนไขที่พนักงาน CSP เข้าถึงทรัพย์สิน CSC

05 Strong Authentication
MFA / PAM สำหรับ Privileged Access ของผู้ดูแลระบบ

06 Change Management Comm.
สื่อสารกับ CSC เมื่อมีการเปลี่ยนแปลงระบบ

07 Virtualization Security
มาตรการความปลอดภัยที่ระดับ Hypervisor

08 Customer Data Protection
เข้าถึงและปกป้องข้อมูล CSC ทั้ง At-rest, In-transit, In-use

09 Account Lifecycle Mgmt
Onboarding → Operation → Termination → Destruction

10 Breach Communication
การสื่อสารและแบ่งปันข้อมูลกรณีเกิดเหตุละเมิด + Forensics

Mindset Shift | On-premise vs Cloud — สิ่งที่นโยบายต้องครอบคลุมเปลี่ยนไปอย่างไร

9 มิติเปรียบเทียบ — จุดที่ผู้เขียนนโยบายต้องปรับมุมมองเมื่อย้ายจาก On-prem ไป Cloud

มิติเปรียบเทียบ	On-premise (เดิม)	Cloud Computing (ปัจจุบัน)
ขอบเขตและเครื่องมือ	Hardware/Software อยู่ในองค์กร — CMDB, SCCM, AD	Asset กระจายใน CSP หลายราย — ใช้ IAM, CSPM, CASB
Lifecycle ของนโยบาย	ปรับตามรอบภายใน วงจรช้าและคงที่	ปรับเมื่อ CSP เพิ่ม Service / Sub-processor — Trigger-based
ผู้ที่เกี่ยวข้อง	องค์กร + Vendor ที่ทำสัญญาตรง	CSC + CSP + Sub-CSP + DC Operator + MSSP — Supply Chain
การตรวจสอบหลักฐาน	เข้าตรวจ Site, ดู Server, สัมภาษณ์	ตรวจผ่าน SOC 2, ISO Cert, Trust Center — ไม่ได้เข้า DC
ความเสี่ยงเฉพาะ	Insider Threat, ลาออก, ความเสียหายทางกายภาพ	Misconfiguration, Multi-tenant, Data Residency, CSP Insider
ความรับผิดชอบ	อยู่ในองค์กร — Top Mgmt สั่งการตรง	Shared Responsibility — ต้องใช้สัญญา/SLA เป็นเครื่องมือ
Automation Capability	จำกัด — Manual Process, Script	สูง — Policy as Code, IaC, SCP, Azure Policy, Org Policy
Compliance Reporting	องค์กรจัดทำเอง	CSP มี Trust Center — CSC Map กลับเอง
Documentation Format	เอกสารกระดาษ / PDF	Machine-readable — OSCAL, JSON Policy, Compliance as Code

หลักการพื้นฐาน | Process & Technical Foundations

5 หลักการสำคัญในการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับคลาวด์

01 Risk-based	02 Comprehensive	03 Approved & Documented	04 Communicated	05 Reviewed
สอดคล้องกับ Risk Assessment และ Risk Appetite ที่อนุมัติแล้ว ไม่ใช่ Copy-paste จากต้นแบบ	ครอบคลุมประเด็นเฉพาะคลาวด์ 6 ข้อ (CSC) หรือ 10 ข้อ (CSP) ตามข้อกำหนด — ไม่ตกหล่น	อนุมัติเป็นทางการโดยผู้บริหารระดับสูง	เผยแพร่ให้พนักงาน คู่สัญญา และผู้เกี่ยวข้องในรูปแบบที่เข้าถึงง่าย — Awareness Training	ทบทวนตามรอบ + เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น เปลี่ยน CSP, Service ใหม่, Incident, กฎหมายใหม่

องค์ประกอบของนโยบายที่ดี (10 ส่วน)

1. Purpose & Scope	2. Definitions	3. References (ISO/PDPA/สกมช.)	4. Policy Statements	5. Roles & Responsibilities
6. Risk Management	7. Cloud-specific Considerations	8. Privacy Considerations	9. Exception Process	10. Review & Approval

Implementation Steps : 8 ขั้นตอนสำหรับ CSC

STEP 01	ประเมินบริบทและความเสี่ยงคลาวด์
STEP 02	กำหนดโครงสร้างนโยบาย (Architecture)
STEP 03	ร่างเนื้อหานโยบายเฉพาะคลาวด์
STEP 04	ร่างนโยบายคุ้มครองข้อมูลส่วนบุคคล
STEP 05	Stakeholder Consultation (Legal, HR, Procurement)
STEP 06	อนุมัติและประกาศใช้ (Top Management Approval)
STEP 07	เผยแพร่ ฝึกอบรม และบังคับใช้ทางเทคนิค
STEP 08	ทบทวน วัดผล และปรับปรุง

⚠ Top Pitfall: ใช้ Risk Assessment เก่าก่อนย้ายขึ้นคลาวด์ — ความเสี่ยงเปลี่ยนแล้ว เช่น Shared Tenancy, Data Residency ต้องประเมินใหม่

⚠ Top Pitfall: เผยแพร่บน Intranet แล้วถือว่าจบ — ไม่บังคับใช้ทาง Technical ไม่มี Awareness — กลายเป็นนโบบายแค่ในกระดาษ

Implementation Steps : 8 ขั้นตอนสำหรับ CSP

01 Gap Analysis เทียบกับมาตรฐานคลาวด์ฯ	**02** ร่างนโยบาย Cloud Service Provision (10 ประเด็น)	**03** Privacy Policy + Sub-processor Disclosure	**04** Cross-functional Alignment (Operation, Engineering, Legal)
05 Top Management Approval + Internal Training	**06** เผยแพร่ต่อ CSC ผ่าน Trust Center / Compliance Portal	**07** บังคับใช้ + Monitor (Internal Policy as Code, SIEM)	**08** ทบทวน + Change Notification ให้ CSC ล่วงหน้า 30 วัน

🌐 จุดที่แตกต่างจาก CSC — "Disclosure-driven Implementation"

- **Service Description Document** — เผยแพร่ว่า Service แต่ละตัวอยู่ใน IaaS/PaaS/SaaS Model ใด พร้อม Shared Responsibility
- **Sub-processor Register** — เปิดเผยรายชื่อ Country, Purpose, Safeguards (เช่น Stripe = Payment, Mailgun = Email)
- **Compliance Report** — SOC 2 Type II, ISO 27001/27017/27018, ISAE 3402 — ดาวน์โหลดได้จาก Trust Portal
- **Change Notification** — แจ้ง CSC ล่วงหน้า 30 วันก่อนเปลี่ยน Sub-processor, Region หรือ Service Deprecation

Common Pitfalls | ข้อผิดพลาดที่พบบ่อยในการ Implement

1	**Copy-paste Policy**	นำ Template ของบริษัทอื่นมาใช้โดยไม่ปรับ Risk Appetite	2	**ไม่ครอบคลุม Cloud-specific**	เขียนเหมือน On-prem ไม่มี Multi-tenancy, Sub-processor, Data Residency
3	**ไม่อนุมัติอย่างเป็นทางการ**	อนุมัติแค่ระดับ Manager — ขัด ISO 27001:2022 ข้อ 5.2	4	**Paper Policy**	เขียนสวยแต่ไม่มี Technical Enforcement ไม่มี Compliance Audit
5	**ขาด Exception Process**	ทีมเลี่ยง Policy โดยไม่มีบันทึก	6	**Annual Rubber-stamp**	ทบทวนแบบเปลี่ยนแค่วันที่อนุมัติ
7	**ไม่ผูกกับ Risk Assessment**	Policy ไม่สะท้อนผล Risk Assessment ปัจจุบัน	8	**ภาษาอังกฤษเท่านั้น**	พนักงาน Operation ไทยไม่เข้าใจ
9	**Policy-Code Drift**	Policy as Code เก่า ไม่ Update ตาม Document → เกิด Gap	10	**Inconsistent Enforcement**	บางทีม Enforce บางทีมไม่

5.1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

5.1.2.1 บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

Organization of Information Security

ข้อกำหนดสำหรับ

CSC | CSP

ทำไมข้อกำหนดนี้สำคัญ | Why This Matters

6 ความเสี่ยงที่เกิดขึ้นจริงเมื่อองค์กรไม่มีการแบ่งบทบาทและความรับผิดชอบอย่างชัดเจน

Responsibility Gap — สูง

ทั้งสองฝ่ายเข้าใจว่าอีกฝ่ายเป็นผู้ทำ Patch หรือ Backup สุดท้ายไม่มีใครทำ

Responsibility Overlap — ปานกลาง

ทั้งสองฝ่ายเปลี่ยน Config โดยไม่ประสานกัน เกิด Configuration Drift

Incident Response ล่าช้า — สูง

ไม่รู้จะติดต่อใครก่อน — MTTR ยาวขึ้น ความเสียหายเพิ่ม

ไม่ปฏิบัติตาม PDPA — สูงมาก

ตอบ DSR / แจ้งเหตุละเมิดต่อ สคส. ใน 72 ชม. ไม่ทันเวลา

Vendor Lock-in — ปานกลาง

ไม่มี Contract Owner ทำให้พึ่งพา CSP เกินจำเป็น

ละเลย Shared Resp. — สูง

CSC คาดหวังว่า CSP 'ปลอดภัยอยู่แล้ว' จึงไม่ตั้งค่าควบคุมระดับ App/Data

การกำหนดบทบาทชัดเจน = ลดความเสียหาย + ปกป้องชื่อเสียงองค์กร + ปฏิบัติตามกฎหมายทันเวลา

ถอดรหัสข้อกำหนดสำหรับ CSC | ผู้ใช้บริการคลาวด์

ข้อกำหนดสำหรับ Cloud Service Customer

ตัวบทต้นฉบับ ข้อ 5.1.2.1	ตีความเป็นภาษาที่อ่านง่าย
ก) CSC **ตกลง**กับผู้ให้บริการคลาวด์เกี่ยวกับการ**แบ่งบทบาทหน้าที่และความรับผิดชอบ**ด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และ**ยืนยันว่า CSC สามารถทำหน้าที่และความรับผิดชอบ**ที่จัดสรรได้ ต้อง**ระบุบทบาทและความรับผิดชอบ**ด้านความมั่นคงปลอดภัยสารสนเทศ**ของทั้งสองฝ่ายไว้ในข้อตกลง**	1) ตกลงกับ CSP เป็นเอกสารว่าใครรับผิดชอบอะไร 2) ตรวจสอบตนเองว่ามีความสามารถ บุคลากร และทรัพยากรเพียงพอที่จะทำตามบทบาทที่ได้รับ 3) ระบุบทบาททั้งของฝ่ายตนและของ CSP ไว้ในข้อตกลง เช่น สัญญา, SLA, Service Description Document, หรือ Acceptable Use Policy
ข) CSC ต้อง**ระบุและจัดการความสัมพันธ์**กับส่วนงานที่**เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของ CSP**	1) CSC ต้องรู้ว่า CSP มีช่องทาง Customer Support แบบใด และต้องบริหารความสัมพันธ์เหล่านี้อย่างเป็นทางการ เช่น มีการประชุมรายเดือน, มีการรายงานเชิงบริหาร, มีช่องทางสำรองในกรณีฉุกเฉิน

ถอดรหัสข้อกำหนดสำหรับ CSP | ผู้ให้บริการคลาวด์

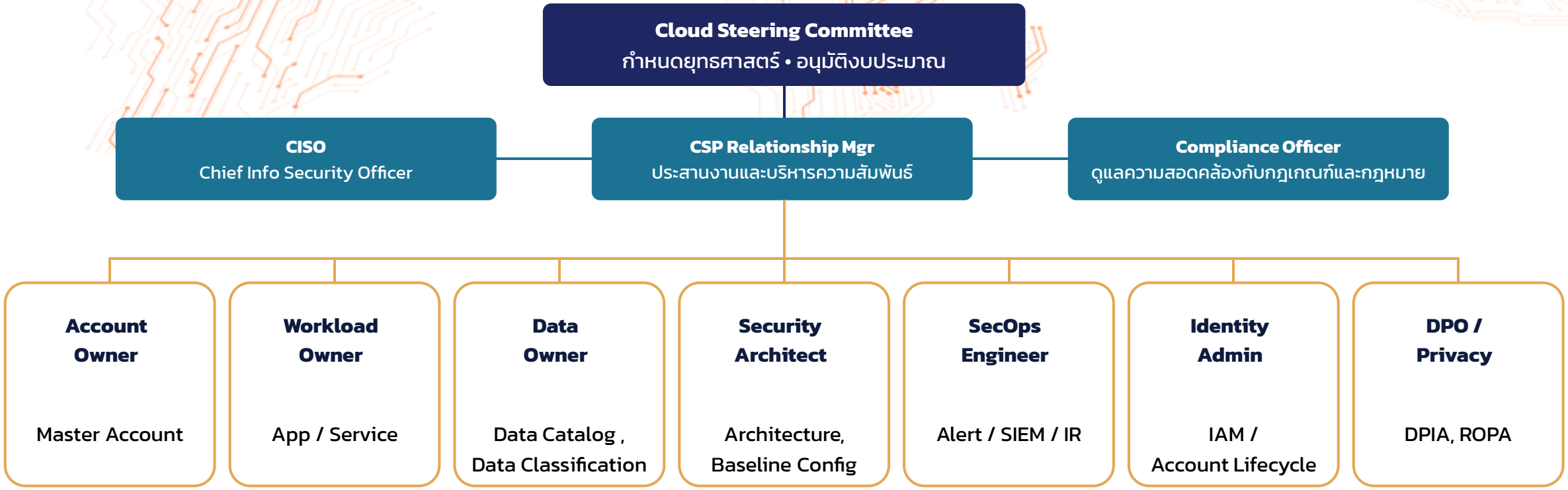
ข้อกำหนดสำหรับ Cloud Service Provider

ตัวบทต้นฉบับ ข้อ 5.1.2.1	ตีความเป็นภาษาที่อ่านง่าย
ก) CSP ต้อง**ตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบ**ด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับ CSC, ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก	1) ทำ Shared Responsibility Matrix ที่ครอบคลุมแต่ละ Stake-holder และต้อง "บันทึก" ไว้เป็นเอกสารทางการคือ • กับ CSC แต่ละราย/แต่ละ Service Model • กับ Sub-CSP หรือ CSP รายอื่นที่ตน Resell/Integrate • กับ Supplier หรือผู้ให้บริการภายนอก เช่น Data Center Operator, MSSP, Hardware Vendor
ข) CSP ต้อง**แต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล** เพื่อประสานงานกับ CSC	1) ต้องมีบุคคลหรือทีมที่ทำหน้าที่ DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

โครงสร้างบทบาทด้านความมั่นคงปลอดภัยของ CSC

ตัวอย่าง Organization Chart ด้าน Cloud Security

Governance → Management → Operational



โครงสร้างบทบาทด้านความมั่นคงปลอดภัยของ CSC

ตัวอย่างบทบาทและหน้าที่ของบุคลากรฝั่ง CSP

CSP Responsibilities

ผู้ให้บริการคลาวด์

- จัดทำ Shared Responsibility Matrix
- ตกลงบทบาทกับ Sub-CSP / Supplier
- แต่งตั้ง DPO ตาม PDPA ม.41
- เปิด Trust Center / Compliance Portal
- ให้เครื่องมือ (IAM, Audit Log, SOC2)
- แจ้งการเปลี่ยนแปลงล่วงหน้า

CSP TAM – Technical Account Manager

ผู้จัดการลูกค้าด้านเทคนิคของ CSP

- Responsible: เจรจา Matrix, ตอบสนอง Incident
- Consult: ระบุขอบเขต Service Model

CSP DPO – Data Protection Officer

DPO / เจ้าหน้าที่ประสานงานด้าน Privacy

- Accountable: แต่งตั้ง DPO/เจ้าหน้าที่ประสานงานด้าน Privacy

Procurement (CSC-side, cross-functional)

ฝ่ายจัดซื้อจัดจ้าง

- Responsible: เจรจาและร่าง Shared Responsibility Matrix
- Consult: ระบุขอบเขต / Informed: Annual Review

Shared Responsibility | การแบ่งความรับผิดชอบตามรูปแบบบริการ

องค์ประกอบแต่ละ Layer เปรียบเทียบ IaaS / PaaS / SaaS

องค์ประกอบแต่ละชั้นของบริการคลาวด์	IaaS	PaaS	SaaS
Data Classification & Acceptable Use	CSC	CSC	CSC
Identity & Access Management	CSC	CSC	CSC
Application Security	CSC	Shared	CSP
OS Patching & Hardening	CSC	CSP	CSP
Virtualization / Hypervisor	CSP	CSP	CSP
Physical Facility	CSP	CSP	CSP
Multi-tenancy & Isolation	CSP	CSP	CSP
Privacy & PDPA Compliance	Shared	Shared	Shared
Breach Notification	Shared	Shared	Shared
Change & Maintenance Comm.	CSP	CSP	CSP

CSC = รับผิดชอบหลัก

CSP = รับผิดชอบหลัก

Shared = ร่วมรับผิดชอบ

Implementation Steps : 8 ขั้นตอนสำหรับ CSC & CSP

CSC – 8 ขั้นตอน

1. สำรวจและจัดทำ Cloud Service Inventory
2. ขอและทบทวน Shared Responsibility Matrix จาก CSP
3. ระบุและมอบหมายบทบาทภายในของ CSC
4. ทำสัญญา/ข้อตกลงให้ครอบคลุมบทบาท
5. แต่งตั้ง DPO / ผู้ประสานงานด้าน Privacy ของ CSC
6. สร้างช่องทางสื่อสารและ Escalation Matrix
7. ทบทวนและซ้อมการสื่อสารกับ CSP
8. การทบทวน ปรับปรุงและเก็บหลักฐาน

CSP – 8 ขั้นตอน

1. จัดทำ Service Catalog และ Service Description
2. จัดทำ Shared Responsibility Matrix แบบละเอียด
3. ตกลงบทบาทกับ Sub-CSP และ Supplier
4. แต่งตั้งและเปิดเผย DPO
5. สร้าง Customer Support และ Care Function
6. จัดเตรียมเครื่องมือให้ CSC ปฏิบัติตามบทบาท
7. สื่อสารและ Onboarding CSC
8. การทบทวนและการสื่อสารการเปลี่ยนแปลง

5.1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

5.1.2.2 การติดต่อกับเจ้าหน้าที่

Contact with Authorities

ข้อกำหนดสำหรับ

CSC | CSP

ข้อกำหนดตามมาตรฐาน ฯ : ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

CSC – Cloud Service Customer

ก) CSC ต้อง**ระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการ**ร่วมกันระหว่าง CSC และ CSP

CSP – Cloud Service Provider

ก) CSP ควร**แจ้งให้ CSC ทราบถึงที่ตั้งทางภูมิศาสตร์**ขององค์กรที่เป็นเจ้าของ **CSP** และประเทศที่ **CSP** สามารถจัดเก็บข้อมูล CSC ได้

เจ้าหน้าที่ในบริบทคลาวด์หมายถึงใคร

ครอบคลุมเจ้าหน้าที่ 6 กลุ่มหลัก ทั้งในประเทศและประเทศที่ Region ของ CSP ตั้งอยู่

Governance → Management → Operational

01 Regulator

หน่วยงานกำกับดูแล

สกมช. (NCSA), สคส. (PDPC), ธปท., ก.ล.ต., กสทช.
— แจ้งเหตุ/ส่งรายงานเป็นภาคบังคับ

02 CERT/CSIRT

ทีมตอบสนองเหตุ

ThaiCERT (ETDA), Sector CERT
— แลกเปลี่ยน IoC, Technical Support, Threat Intel

03 Law Enforcement

บังคับใช้กฎหมาย

ตำรวจไซเบอร์ (กก.5 บก.สอท.), DSI
— ร้องทุกข์ ยื่นพยานหลักฐาน สอบสวน

04 Sector Regulator

ผู้กำกับรายอุตสาหกรรม

BoT, SEC, OIC, HSA
— Sectoral Notification ตาม Sectoral Rule

05 Emergency Service

บริการฉุกเฉิน

199 (ดับเพลิง), 1669 (EMS), 1784 (ปภ.)
— เหตุฉุกเฉินทางกายภาพ

06 Foreign Authority

หน่วยงานต่างประเทศ

PDPC สิงคโปร์, NACSA มาเลเซีย ฯลฯ
— ผ่าน CSP เป็นช่องทาง

FOCUS สกมช. (NCSA) + ThaiCERT คือสองหน่วยงานหลักบริบทของกฎหมายไซเบอร์ที่ต้องถูกระบุ พร้อมช่องทางติดต่อประสานงาน

CSC vs CSP: ใครต้องทำอะไร

บทบาทหน้าที่ของทั้งสองฝ่ายที่ต้องสอดประสานกัน

CSC — Cloud Service Customer

ระบุหน่วยงานที่เกี่ยวข้องและจัดเตรียมช่องทาง

- จัดทำรายการและช่องทางติดต่อเจ้าหน้าที่ ครอบคลุมทุก Jurisdiction
- กำหนด Trigger Events และ Threshold ของแต่ละหน่วยงาน
- แต่งตั้งผู้ประสานงานหลักภายใน
- ทำสัญญาให้ CSP เปิดเผยที่ตั้งทางภูมิศาสตร์
- ทบทวนรายปี + Tabletop Exercise ≥ 1 ครั้ง/ปี
- เก็บ Audit Trail การประสานงานทุกครั้ง

CSP — Cloud Service Provider

เปิดเผยที่ตั้งทางภูมิศาสตร์และสนับสนุน CSC

- แจ้งที่ตั้งของ Legal Entity ของ CSP
- เปิดเผยรายการประเทศที่จัดเก็บข้อมูล (Region/AZ)
- เปิดเผย Sub-processor List พร้อม Location
- Trust Center / Annual Transparency Report
- แจ้งล่วงหน้าเมื่อมีการเปลี่ยน Region/Sub-processor
- Customer Hotline สำหรับการการประสานงานกับเจ้าหน้าที่

หลักการ Operational Responsibility แบ่งระหว่าง CSC/CSP แต่ Legal Accountability ยังคงอยู่ที่ CSC ในฐานะ PII Controller

7 องค์ประกอบที่ควรระบุในทะเบียนหน่วยงาน

01 Authority Identification

ระบุหน่วยงานครบทุกประเภท ทั้งในและต่างประเทศ

02 Register / Mapping

ทะเบียนเอกสารควบคุม ระบุภารกิจ ช่องทาง กรอบเวลา

03 Trigger Event Mapping

เกณฑ์ Trigger ของแต่ละหน่วยงาน — Severity × Affected

04 Internal Liaison

Primary + Backup พร้อม Escalation Path

05 Communication Channels

หลายช่องทาง + Out-of-band fallback

06 Periodic Validation

ทบทวนรายปี + Tabletop Exercise

07 Documentation & Audit Trail

เก็บหลักฐานการประสานงาน เก็บ Acknowledgement

การติดต่อกับเจ้าหน้าที่

ต้องแจ้งใคร ภายในเมื่อไหร่

ตัวอย่าง Matrix สำหรับตัดสินใจในเวลาวิกฤต

Trigger Event	หน่วยงานที่ต้องแจ้ง	กรอบเวลา	อ้างอิง
Data Breach (PII)	สคส. (PDPC)	**72 ชั่วโมง**	*PDPA ม.37(4)*
Cyber Incident — GOV, CII	สกมช. (NCSA)	**โดยเร็ว**	*พ.ร.บ.ไซเบอร์ ม.57-58*
Technical Support / IoC	ThaiCERT	-	-
Cybercrime (ต้องคดี)	บก.สอท.	**ตามแต่กรณี**	*ป.วิ.อาญา*
Financial Sector	ธปท. / ก.ล.ต. / คปภ.	**Sectoral Rule**	*Sector Guideline*
Physical Emergency	199 / 1669 / 1784	**ทันที**	*BCM Procedure*

5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

5.1.3.1 การระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา

Identification of Applicable Legislation and Contractual Requirements

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสข้อกำหนดสำหรับ CSC | ผู้ใช้บริการคลาวด์

ข้อกำหนดสำหรับ Cloud Service Customer

ตัวบทมาตรฐาน	อธิบายเป็นภาษาที่อ่านง่าย
ก) CSC ต้องพิจารณาประเด็นที่ว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของ**เขตอำนาจศาล**ที่ควบคุม CSP นอกเหนือจากกฎหมายที่ควบคุม CSC	อย่าคิดว่าใช้คลาวด์แล้วต้องดูเฉพาะกฎหมายไทย — ต้องดูกฎหมายของประเทศที่ CSP จดทะเบียนและประเทศที่ตั้ง Data Center ด้วย
ข) CSC ต้อง**ขอหลักฐาน**ว่า CSP ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับ CSC โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก	ห้าม "เชื่อใจ" CSP โดยไม่มีหลักฐาน — ต้องขอใบรับรอง ISO 27001/27017/27018, SOC 2 Type II, ISAE 3402 จากผู้ตรวจสอบภายนอกที่เป็นกลาง

ถอดรหัสข้อกำหนดสำหรับ CSP | ผู้ให้บริการคลาวด์

ข้อกำหนดสำหรับ Cloud Service Provider

ตัวบทมาตรฐาน	อธิบายเป็นภาษาที่อ่านง่าย
(ก) CSP ต้อง**แจ้งให้ CSC ทราบถึงเขตอำนาจศาล**ทางกฎหมายที่ควบคุมบริการคลาวด์	CSP ต้องเปิดเผยชัดเจน (ลายลักษณ์อักษร) ว่าบริการอยู่ภายใต้กฎหมายของประเทศใด — จดทะเบียน, HQ, Data Center
(ข) CSP ต้อง**ระบุข้อกำหนดทางกฎหมาย**ที่เกี่ยวข้อง**ของตนเอง** (เช่น เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลส่วนบุคคล) และต้องให้ข้อมูลนี้แก่ CSC เมื่อได้รับการร้องขอ	CSP ต้องจัดทำ "ทะเบียนกฎหมาย" ของตนเอง เช่น Export Control, Lawful Access, Data Localization — พร้อมส่ง CSC
(ค) CSP ต้อง**แสดงหลักฐาน**ให้ CSC ทราบถึง**การปฏิบัติตามกฎหมาย**ที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา	CSP ต้องมี "หลักฐานที่เป็นปัจจุบัน" — ใบรับรองที่ยังไม่หมดอายุ, Audit Reports ฉบับล่าสุด, จดหมายรับรอง

ข้อ 5.1.3.1 เป็น “ประตูแรก” ของ Cloud Compliance

Control อื่นในหมวด 5.1.3 — IP, Records, Crypto, Privacy — จะทำงานไม่ได้เลยถ้ายังไม่รู้ว่ามีกฎหมายอะไรบังคับใช้

01 Multi-Jurisdiction Reality

ข้อมูลอยู่ในประเทศ A, CSP จดทะเบียนประเทศ B, Region อยู่ประเทศ C — ทั้งหมดมีกฎหมายตัวเอง รวม CLOUD Act, GDPR, PDPA

02 PDPA มาตรา 28 บังคับ

การโอนข้อมูลส่วนบุคคลไปต่างประเทศต้องมี “มาตรการคุ้มครองที่เหมาะสม” — ค่าปรับสูงสุด 5 ล้านบาทต่อกรณี

03 หลักเกณฑ์ของ สตง. และกระทรวงการคลัง

หน่วยงานของรัฐต้องกำหนดวัตถุประสงค์ของการควบคุมภายใน ซึ่งรวมถึงด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ (Compliance) รวมถึงการประเมินความเสี่ยงที่อาจทำให้ไม่บรรลุวัตถุประสงค์ ตามมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561

04 Reliance Model

Auditor ของ CSC อาจไม่ได้รับอนุญาตให้เข้า Data Center ของ CSP โดยตรง — ต้องอ้างใบรับรอง ISO/SOC ของ Third-party

MINDSET SHIFT → Compliance ในคลาวด์ คือการ “จัดการกฎหมายของหลายประเทศพร้อมกัน” ไม่ใช่แค่กฎหมายไทย

ภูมิทัศน์กฎหมายและหน่วยงานกำกับของไทย

ตัวอย่างกฎหมายที่เกี่ยวข้องในประเทศไทย

PDPA — พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562

- ม.28 การโอนข้อมูลไปต่างประเทศ
- ม.37, 39, 40 หน้าที่ PII Controller, PII Processor
- ม.41 DPO

Cyber Act — พ.ร.บ. ไซเบอร์ฯ 2562

- ม.49 หลักเกณฑ์ระบุ CII
- ม.56–58 แจ้งเหตุภัยคุกคาม
- ม.44–45 บริหารความเสี่ยง

ETA — พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ 2544

- ม.25, 26, 35 มาตรฐานความมั่นคงปลอดภัยสำหรับธุรกรรมรัฐ

BOT — ประกาศ ธปท. (Outsourcing & Cloud)

- ประเมินความเสี่ยง public cloud และการใช้ CSP ในต่างประเทศ
- ข้อกำหนดกรณีใช้งาน CSP ในต่างประเทศ

SEC / OIC — ก.ล.ต. + คปภ. แนวปฏิบัติคลาวด์

- ก.ล.ต.: Cloud Computing Practice (Governance, Due Diligence, Engage, Operate, Monitor & Exit)
- คปภ: รวมอยู่ในหลักเกณฑ์ IT Risk

PDPC — หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

- ประเทศปลายทางมีมาตรฐานด้าน Privacy
- เนื้อหาขั้นต่ำของ DPA ระหว่าง Controller–Processor

DGA — (ร่าง) CLOUD USAGE STANDARD

- ครอบคลุม Cloud lifecycle (เลือก → ย้าย → ใ → จ่าย → ออก)
- อ้างอิงมาตรฐานคลาวด์ของ สกมช. ในด้านความปลอดภัย

Computer CrimeAct — พ.ร.บ. อาชญากรรมคอมพิวเตอร์ฯ

- ผู้ให้บริการต้องเก็บ Log
- และให้ความร่วมมือกับเจ้าหน้าที่

CSC vs CSP: ใครต้องทำอะไร

Closed Loop: CSP เปิดเผย → CSC พิจารณา → CSC ขอหลักฐาน → CSP ส่งหลักฐาน → ทบทวนต่อเนื่อง

CSC • ผู้ใช้บริการคลาวด์

พิจารณา → ขอหลักฐาน → จัดการตามทะเบียน

01 พิจารณากฎหมายของเขตอำนาจศาลที่ควบคุม CSP เพิ่มเติมจากกฎหมายของ CSC เอง

02 ขอหลักฐานการปฏิบัติตามกฎเกณฑ์จาก CSP ในรูปแบบ Third-party Certification

03 จัดทำ Legal & Contractual Register ระบุกฎหมาย + มาตรา + Owner + Review Cycle

04 ทบทวนทะเบียนและหลักฐานอย่างน้อยปีละครั้ง หรือเมื่อมี Trigger สำคัญ

05 CII เพิ่ม: ระบุภาระ พ.ร.บ. ไซเบอร์ฯ มาตรา 56–58 ในสัญญา CSP

CSP • ผู้ให้บริการคลาวด์

เปิดเผย → ระบุของตน → พิสูจน์ด้วยหลักฐาน

01 เปิดเผยเขตอำนาจศาลที่ควบคุมบริการ (HQ, Region, Sub-processor) เป็นลายลักษณ์อักษร

02 จัดทำ CSP's own Legal Register รวมถึง Export Control + Lawful Access

03 ส่งมอบหลักฐานปัจจุบัน ISO 27001/27017/27018, SOC 2 Type II, CSA STAR

04 Trust Center + Transparency Report เผยแพร่ผ่านช่องทางที่ลูกค้าเข้าถึงได้

05 แจ้งล่วงหน้า 30–60 วัน เมื่อเพิ่ม Sub-processor หรือเปลี่ยน Region

DUAL-JURISDICTION → CSP "เปิดเผย" แต่ CSC ต้อง "พิจารณา" ว่าสอดคล้องกับธุรกิจของตน — ไม่ทำคือรับผิดเต็ม

Shared Responsibility | การแบ่งความรับผิดชอบตามรูปแบบบริการ

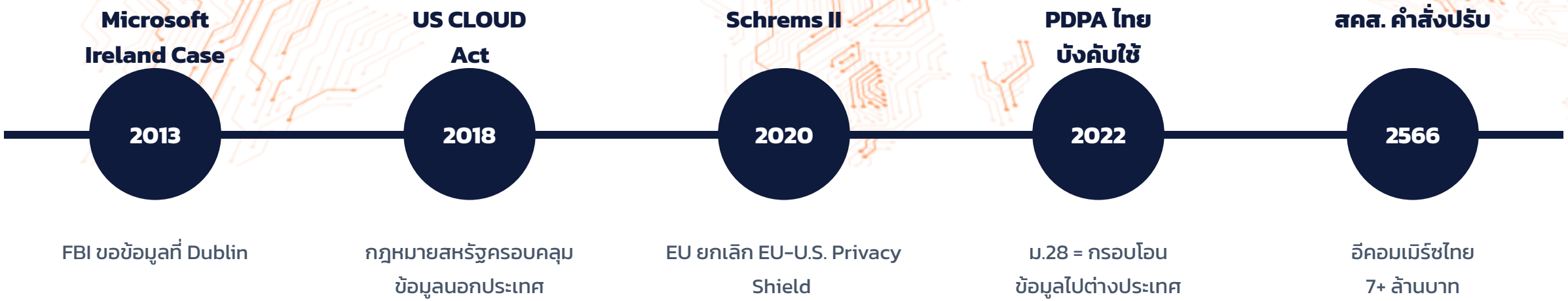
การแบ่งความรับผิดชอบ เปรียบเทียบ IaaS / PaaS / SaaS

กิจกรรมตามข้อ 5.1.3.1	IaaS	PaaS	SaaS
ระบุกฎหมายที่บังคับใช้กับการดำเนินธุรกิจของ CSC	CSC	CSC	CSC
ระบุกฎหมายของเขตอำนาจศาลที่ควบคุมบริการคลาวด์	Shared	Shared	Shared
ทำสัญญาบริการและ DPA ที่ครอบคลุมเขตอำนาจศาล	Shared	Shared	Shared
จัดทำทะเบียนกฎหมายของระบบสารสนเทศของผู้ใช้บริการ (CSC)	CSC	CSC	CSC
จัดทำทะเบียนกฎหมายของบริการคลาวด์ (CSP)	CSP	CSP	CSP
ขอ/ส่งหลักฐาน Compliance (Certs, Audit Reports)	Shared	Shared	Shared
แจ้งการเปลี่ยน Sub-processor / Data Center	CSP	CSP	CSP
ตอบสนอง Government Access Request	Shared	Shared	Shared

CSC = ผู้ใช้บริการ CSP = ผู้ให้บริการ แบ่งร่วม (Shared)

Historical Context | เหตุการณ์ที่ผลักดันให้ข้อ 5.1.3.1 สำคัญ

กรณีศึกษาจากเหตุการณ์จริง



★ **Key Takeaway: ทุกเหตุการณ์ผลักดันให้องค์กรต้องระบุ "เขตอำนาจศาลของ CSP" ตั้งแต่เริ่มต้น**

— ไม่ใช่หลังจากเกิดเหตุ เพราะตอนนั้นมักจะสายเกินไป

5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

5.1.3.2 สิทธิในทรัพย์สินทางปัญญา

Intellectual Property Rights

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC)

ข้อกำหนด 5.1.3.2 สำหรับ CSC

ตัวบทมาตรฐาน

ก) การติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์ในบริการคลาวด์อาจทำให้เกิดการละเมิดเงื่อนไขการอนุญาตให้ใช้สิทธิสำหรับซอฟต์แวร์ได้ CSC ต้อง**มีขั้นตอนในการระบุข้อกำหนดในการให้สิทธิการใช้งานเฉพาะระบบคลาวด์**ก่อนที่จะอนุญาตให้ติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในบริการคลาวด์ และต้องให้ความสนใจเป็นพิเศษกับกรณีที่บริการคลาวด์มีความยืดหยุ่นและสามารถปรับขนาดได้ และสามารถใช้งานซอฟต์แวร์บนระบบหรือแกนประมวลผลได้มากกว่าที่อนุญาตโดยเงื่อนไขการอนุญาตให้ใช้สิทธิ

01 กระบวนการที่เป็นทางการ

ต้องมี Pre-deployment License Review เป็นกระบวนการอย่างเป็นทางการ ไม่ใช่แค่ "เข้าใจกัน" — มีผู้รับผิดชอบ ผู้อนุมัติ แบบฟอร์มอนุมัติ

02 เงื่อนไขเฉพาะคลาวด์

พิจารณาสิทธิ์การใช้งาน BYOL, Per-vCPU / Per-Core / Per-Instance, Region restriction, Geo-restriction, Cloud Environment ที่ได้รับอนุญาต ก่อนติดตั้งทุกครั้ง

03 เฝ้าระวัง Auto-scaling

Auto-scaling Group, Kubernetes HPA, Serverless Concurrency อาจรัน Workload เกิน License Cap โดยอัตโนมัติ — ต้องจำกัด + แจ้งเตือน + ตรวจสอบอย่างสม่ำเสมอ

ความแตกต่างจาก On-premise ที่ต้องตระหนัก

- 1 Container Image อาจมี > 100 Open-source Componentห แต่ละชั้นมี License ต่างกัน
- BYOL ไม่ใช่ทางออกอัตโนมัติ — Vendor หลายรายมีเงื่อนไขเฉพาะ Public Cloud
- Cross-region Replicate อาจกระทบ License Geo-restriction และ Compliance

8 ความเสี่ยงด้านสิทธิในทรัพย์สินทางปัญญาบนคลาวด์

หากไม่จัดการ องค์กรอาจเผชิญความเสี่ยงครอบคลุมทั้งกฎหมาย การเงิน ชื่อเสียง และการดำเนินงาน

1 

Auto-scaling Over-use

เมื่อ Auto-scaling Group หรือ Kubernetes HPA ขยาย Pod/Instance, vCPU และ RAM อาจเกิน License Cap

2 

BYOL Misuse

ใช้ On-prem License บน Cloud โดยไม่ตรวจ

3 

Shadow SaaS

พนักงานสมัครใช้งานเอง — ไม่มี SLA, DPA

4 

Container License

สัญญาอนุญาตซอฟต์แวร์แบบโอเพนซอร์ส (AGPL/GPL) ใน Image อาจต้องเปิด Source Code ทั้งหมด

5 

AI/ML Model License

Foundation Model (Llama, Mistral) มี Acceptable Use Policy ห้ามใช้บางกรณี

6 

Customer Data IPR

CSP บางรายเก็บสิทธิ์ใช้ Customer Content เพื่อ Train AI Model

7 

Copy Right Complaint

CSP ที่ไม่มีกระบวนการตอบสนองข้อร้องเรียน — เสี่ยงถูกฟ้องฐานสนับสนุนการละเมิด

8 

Cross-border Transfer

ข้อมูลที่มี IPR ถูกย้ายข้ามประเทศโดยไม่ทำ Data Transfer Agreement

ถอดรหัสตัวบทมาตรฐาน — ผู้ให้บริการคลาวด์ (CSP)

ข้อกำหนด 5.1.3.2 สำหรับ CSP และกระบวนการรับเรื่องร้องเรียน

ตัวบทมาตรฐาน

ก) ผู้ให้บริการคลาวด์ต้องกำหนด**กระบวนการในการตอบสนองต่อการร้องเรียนเรื่องสิทธิในทรัพย์สิน”**

ตัวอย่างกระบวนการ

รับเรื่อง	ตรวจสอบความครบถ้วน	ตรวจสอบความถูกต้อง	ดำเนินการ	แจ้งผล	ปิดเรื่อง + Log
1	2	3	4	5	6
รับเรื่องร้องเรียน	ตรวจความครบถ้วนของแบบฟอร์ม	ตรวจความถูกต้อง โดยที่ปรึกษาด้านกฎหมาย	ดำเนินการ Takedown หรือ Maintain	แจ้งผลให้ผู้ร้องและผู้ถูกร้อง พร้อมเปิดโอกาสให้โต้แย้ง	ปิดเรื่อง พร้อมเก็บบันทึกเป็นหลักฐาน
SLA: ≤ 24 ชม.	SLA: ≤ 1 วัน	SLA: 3 วัน	SLA: 5–14 วัน	SLA: 1 วัน	SLA: ต่อเนื่อง

Shared Responsibility | การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบ เปรียบเทียบ IaaS / PaaS / SaaS

มิติของ License/IPR	IaaS	PaaS	SaaS
OS License	CSC (BYOL หรือ Pay-as-you-go)	CSP รวมในบริการ — CSC ตรวจสอบ	CSP จัดการ
Middleware / Database	CSC ทั้งหมด	CSP จัดเตรียม / CSC ตรวจเงื่อนไข	CSP ทั้งหมด
Application Software	CSC ทั้งหมด ตรวจ License Terms	CSC สำหรับแอปที่ติดตั้งเอง	CSP จัดการ + CSC อ่าน EULA
Container / Open Source	CSC รับผิดชอบทั้งหมด	CSC รับผิดชอบ Image ที่ Deploy	CSP รับผิดชอบ
Customer Content	CSC เป็นเจ้าของ	CSC เป็นเจ้าของ	CSC เป็นเจ้าของ
IPR Complaint Handling	CSP-Infra / CSC-Workload	CSP หลัก / CSC ระดับเนื้อหา	CSP รับผิดชอบหลัก
License Monitoring	CSC ใช้ Cloud-native + 3rd Party	ร่วมกัน — CSP ให้ Usage Data	CSP จัดเตรียม Report

Legend & Key Insight

CSC รับผิดชอบ | CSP รับผิดชอบ | ร่วมกัน (Shared)

PaaS คือจุดเสี่ยงสุด — แบ่งความรับผิดชอบไม่ชัดเจน ต้องระบุในสัญญา MSA/SLA ทุกครั้ง

ความท้าทายเชิงเทคนิคสำหรับผู้ใช้บริการคลาวด์ (CSC)

ความท้าทาย และรูปแบบสถาปัตยกรรมการจัดการ

ความท้าทายเชิงเทคนิค

- **Container Multi-layer License**
  1 Image อาจมี > 100 Open-source Component
- **Serverless / FaaS**
  ไม่มี OS/Instance ชัดเจน แต่ Runtime/Library ยังต้องตรวจ
- **Ephemeral Workload**
  Container เกิด-ดับเร็ว Snapshot Audit ไม่เพียงพอ
- **Multi-cloud Tagging**
  แต่ละ CSP มี License Manager + Tag Scheme ต่างกัน
- **AI/ML Model License**
  Llama Acceptable Use Policy, Mistral License — เงื่อนไขเฉพาะ
- **Data Sovereignty + Geo-restriction**
  บาง License จำกัด Region ที่ใช้งานได้
- **Copyleft Cascading**
  Library 1 ตัว อาจดึง Dependency อื่นเข้ามาด้วย

Pattern 1 — Centralized + Distributed

Central License Authority + per-account Cloud-native enforcement

ใช้ Policy-as-Code (OPA, AWS Config, Azure Policy) บังคับใช้ License Rule ก่อน Deploy

✓เหมาะกับ: องค์กรใหญ่ Multi-cloud, หลาย BU

Pattern 2 — Shift-Left in CI/CD

ฝัง License Check ใน Pipeline ด้วย SCA Tool (Snyk, Black Duck)

Container Scan ทุก Build + Block Deploy เมื่อพบ License ที่ไม่อนุมัติ + Generate SBOM อัตโนมัติ

✓เหมาะกับ: องค์กร DevOps/DevSecOps Mature

Pattern 3 — Tag-based Cloud-native

ใช้ Cloud Tag (Owner, License-Pool) เป็น Primary Allocation Key

เชื่อม Tag กับ License Inventory + Daily Automated Reconciliation + Real-time Dashboard

✓เหมาะกับ: Cloud-native, Containerized, Serverless

5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

5.1.3.3 การปกป้องบันทึกข้อมูล

Protection of Records

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สื่อสารระหว่าง CSC และ CSP

ผู้ใช้บริการต้อง “ขอข้อมูล” ผู้ให้บริการต้อง “ให้ข้อมูล” การปกป้องบันทึก

CSC — ผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ขอข้อมูลจาก CSP เกี่ยวกับการปกป้องบันทึกข้อมูล**ที่รวบรวมและจัดเก็บโดย CSP ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของ CSC

สิ่งที่ CSC ต้องทำ

1) ระบุประเภท "บันทึกข้อมูล (Records)” ที่ฝากกับ CSP: *Audit Logs, Meeting Records, Transaction Logs, CRM / ERP Records, Risk Assessment Report*

2) ขอเอกสารทางการจาก CSP — Service Description, Whitepaper, SOC 2 Report

3) ตรวจสอบว่าเงื่อนไข CSP เพียงพอกับ PDPA / พ.ร.บ. ไซเบอร์ / ข้อกำหนดขององค์กร

4) ทบทวนปีละครั้ง หรือเมื่อ CSP เปลี่ยนนโยบาย/บริการ

5) เก็บหลักฐานการขอ–การได้รับ เพื่อให้ Auditor ของ สกมช. ตรวจสอบได้

CSP — ผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลแก่ CSC เกี่ยวกับการปกป้องบันทึกข้อมูล**ที่รวบรวมและจัดเก็บโดย CSP ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของ CSC

สิ่งที่ CSP ต้องทำ

1) จัดทำ Service Description / Security Whitepaper / Trust Center ที่ระบุประเภท ระยะเวลา และมาตรการปกป้องบันทึก

2) เผยแพร่ผ่าน Customer Portal / Trust Center / เอกสารแนบ Master Service Agreement อย่างเป็นระบบ

3) แยกชัด Built-in (อัตโนมัติ) vs. Optional (ลูกค้าเปิด + จ่ายเพิ่ม)

4) แจ้งล่วงหน้าเมื่อมี Material Change Notification

5) พิสูจน์ได้ด้วยการตรวจรับรอง ISO 27001/27017/27018, SOC 2 Type II

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
จัดประเภท & เจ้าของบันทึก	CSC	CSC	CSC
นโยบายระยะเวลาเก็บ (Retention)	CSC	Shared	Shared
ปกป้องโครงสร้างพื้นฐาน/ฮาร์ดแวร์	CSP	CSP	CSP
เข้ารหัสบันทึก (at-rest/in-transit)	Shared	Shared	CSP
ควบคุมการเข้าถึง (IAM)	Shared	Shared	Shared
รักษาความถูกต้อง / Immutability	Shared	Shared	CSP
สำรอง & กู้คืนบันทึก	Shared	Shared	CSP
ส่งออก/เข้าถึงบันทึกของ CSC	Shared	Shared	Shared
เปิดเผยนโยบายปกป้องบันทึก	CSP	CSP	CSP
ลบบันทึกอย่างปลอดภัย	Shared	Shared	CSP
จัดทำบันทึกประมวลผล PII (RoPA)	CSC	Shared	Shared

CSC = ผู้ใช้บริการ CSP = ผู้ให้บริการ แบ่งร่วม (Shared)

5 Mindset Shifts: จาก On-Premise สู่ Cloud

การจัดการ Records บนคลาวด์ ต้องคิดต่างจาก On-prem — เพราะ Storage / Tools / Control อยู่ในมือ CSP

01

บันทึกอยู่ในมือ “คนอื่น”

CSC ไม่ครอบครอง Physical Storage — ต้องอาศัยสัญญา + การตรวจรับรอง (ISO 27001/27017/27018, SOC 2)

02

เปิด/ปิด Log ไม่ใช่อัตโนมัติ

CSP บางรายเปิด Default บางรายต้อง enable เอง เช่น VPC Flow Log, S3 Server Access Log

03

Default Retention มักสั้นเกิน

ต้องตั้งใหม่ ≥ 90 วันสำหรับ Traffic Data (พ.ร.บ. คอม. ม.26) หรือ ≥ 2 ปีตามสัญญา

04

ลบไม่ใช่หายไปทันที

CSP เก็บใน Soft-delete 7-90 วัน — สำคัญต่อ Right-to-Erasure ของ PDPA

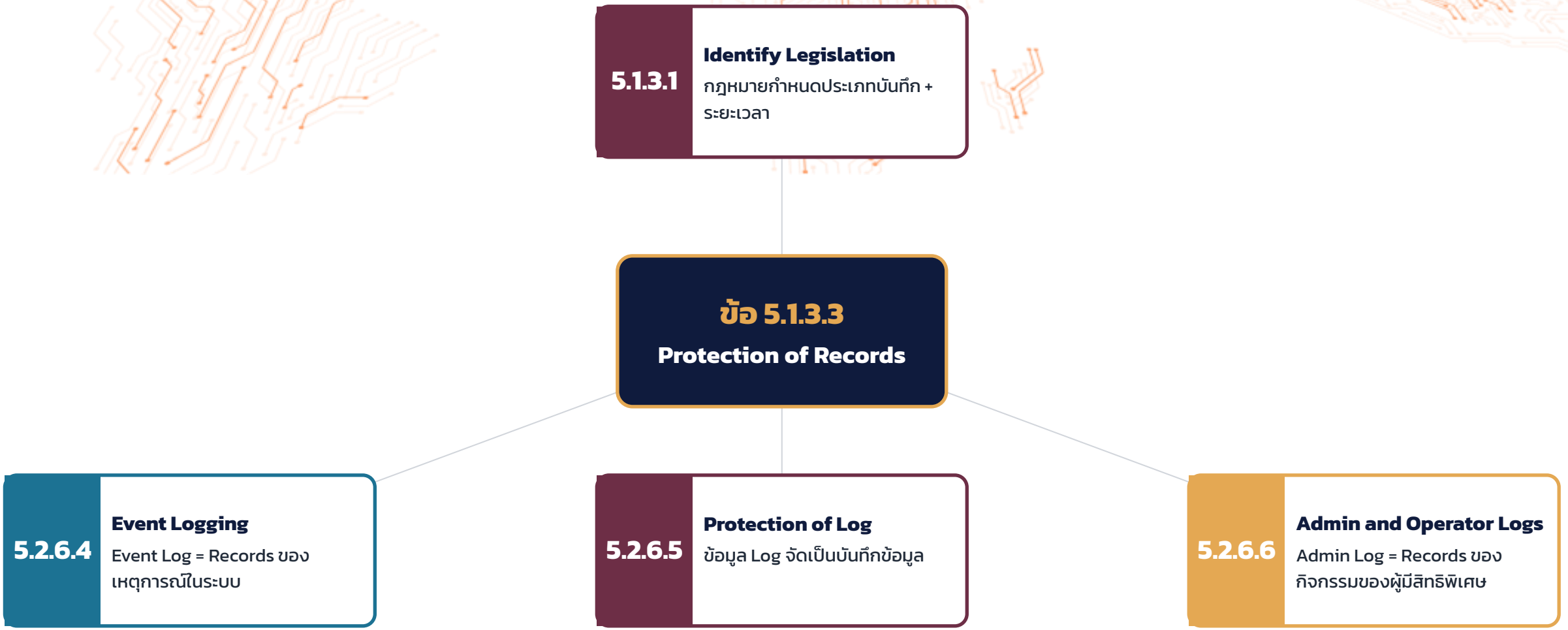
05

Multi-tenancy = Log อาจปนกัน

ต้อง Verify ว่า Log Isolation มีจริง — ขอ Architecture Diagram จาก CSP เป็นหลักฐาน

ความเชื่อมโยงของข้อกำหนด 5.1.3.3 กับข้อกำหนดอื่น

ข้อกำหนดนี้เชื่อมโยงกับห่วงโซ่ Compliance หลายข้อ — ต้องวางแผนแบบ Integrated ไม่ใช่ Siloed



วงจรชีวิตของบันทึก — Records Lifecycle Management

ตั้งแต่ Creation จนถึง Disposal — ทุกระยะมีมาตรการปกป้องที่เหมาะสม

1 Creation
ระบุประเภท เจ้าของ ระยะเวลาตั้งแต่สร้าง

2 Classification
จำแนกตามความสำคัญและกฎหมาย

3 Storage
เข้ารหัส + Access Control + Versioning

4 Access / Use
Authn + Authz + Audit Log ทุก Access

5 Maintenance
Backup + Cross-region + Integrity Check

6 Retention
เก็บครบตามกฎหมาย / สัญญา / ธุรกิจ

7 Disposal
ลบ Primary + Backup + Replica + Evidence

ระยะเวลาขั้นต่ำตามกฎหมายไทย

ประเภทบันทึก	กฎหมาย	ระยะเวลาขั้นต่ำ
Traffic Log	พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 / พ.ศ. 2560	90 วัน
Financial Transaction	พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 22 + กฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า พ.ศ. 2563	5 ปี
KYC documents (ข้อมูลการแสดงตน)	พ.ร.บ. ปปง. พ.ศ. 2542 มาตรา 20, 22 + กฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า พ.ศ. 2563	5 ปี หลังปิดบัญชี
CDD documents (การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า)	กฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า พ.ศ. 2563 + ประกาศสำนักงาน ปปง.	10 ปี หลังปิดบัญชี
เอกสารบัญชี/งบการเงิน	พ.ร.บ. การบัญชี พ.ศ. 2543 มาตรา 14	5 ปี (ขยายได้ถึง 7 ปี)
เอกสารภาษี (ใบกำกับภาษี, รายงานภาษีซื้อ-ขาย)	ประมวลรัษฎากร มาตรา 87/3	10 ปี หลังปิดบัญชี
เอกสารทั่วไปที่อาจถูกเรียกตรวจ	ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 193/30-31	อายุความ 10 ปี

5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

5.1.3.4 กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล

Regulation of Cryptographic Controls

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ฝั่ง CSC

ข้อกำหนด 5.1.3.4 · ผู้ใช้บริการคลาวด์ (Cloud Service Customer)

ตัวบทมาตรฐาน

ก) CSC ต้อง**ตรวจสอบ**ให้แน่ใจว่า**ชุดของมาตรการควบคุมการเข้ารหัสข้อมูล**ที่ใช้กับการใช้บริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

ถอดรหัสเป็นภาษาที่อ่านง่าย

1. **Identify**
   จัดทำรายการ Cryptographic Controls ทั้งหมดที่ใช้ในบริการคลาวด์ — รวม Storage, TLS, Application-layer
2. **Map**
   จับคู่ Controls กับข้อกำหนดในสัญญา / กฎหมาย / มาตรฐาน (CSA, DPA, PDPA, สกมช., PCI DSS)
3. **Verify**
   ระบุช่องว่าง (Gap) ระหว่างสิ่งที่มีกับสิ่งที่บังคับ และวางแผน Remediation
4. **Maintain**
   ทบทวนเป็นระยะ หรือเมื่อมีการเปลี่ยนแปลงสำคัญ พร้อมเก็บหลักฐานสำหรับ Auditor

Key Takeaway: CSC ต้องพิสูจน์ได้ว่าการเข้ารหัสที่ใช้สอดคล้องกับ PDPA, สกมช., สัญญา และมาตรฐานที่อ้างอิง — ไม่ใช่แค่ "เปิด Encryption"

ถอดรหัสตัวบทมาตรฐาน — ฝั่ง CSP

ข้อกำหนด 5.1.3.4 · ผู้ให้บริการคลาวด์ (Cloud Service Provider)

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้คำอธิบายกับ CSC เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล**ที่ดำเนินการโดย CSP เพื่อใช้ในการทบทวนการปฏิบัติตามข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้อง

ถอดรหัสเป็นภาษาที่อ่านง่าย

D — Document
จัดทำ Cryptographic Controls Description ต่อ Service — Data at Rest / in Transit / in Use

A — Specify
ระบุอัลกอริทึม, ความยาวกุญแจ, โหมด, ใบรับรอง FIPS 140-2/140-3

L — Disclose
เปิดเผยข้อจำกัด — Export Control (EAR/ITAR), US CLOUD Act, Region availability

P — Publish
เปิดเผยผ่าน Trust Center / Compliance Portal และอัปเดตเมื่อมีการเปลี่ยนแปลง

Key Takeaway: CSP เป็น "Source of Truth" เกี่ยวกับ Cryptographic Controls — CSC พึ่งพาเอกสารนี้ในการ Audit

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

ใครรับผิดชอบส่วนใด ใน IaaS · PaaS · SaaS

CSP ผู้ให้บริการรับผิดชอบทั้งหมด | CSC ผู้ใช้บริการรับผิดชอบทั้งหมด | SHARED ต้องตกลงกันชัดเจนในสัญญา

รายการความรับผิดชอบ	IaaS	PaaS	SaaS
Encryption Physical / Hypervisor / Disk	CSP	CSP	CSP
Encryption Data at Rest (Object/Block)	SHARED	SHARED	CSP
Encryption Data in Transit (TLS)	SHARED	SHARED	CSP
Application / Field-level Encryption	CSC	CSC	CSC*
Key Management — KEK (Master Key)	SHARED	SHARED	CSP
Key Management — DEK (Data Key)	CSP	CSP	CSP
เปิดเผย Cryptographic Controls Description	CSP	CSP	CSP
ตรวจสอบ Compliance vs สัญญา/กฎหมาย	CSC	CSC	CSC
Cryptographic Inventory (CBOM)	CSC	CSC	CSC

** SaaS — Application/Field-level Encryption ขึ้นกับ Feature ที่ SaaS เปิดให้ใช้ (เช่น Customer Key, Field Encryption, Tokenization)*

5.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

5.1.3.5 การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ

Independent Review of Information Security

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ฝั่ง CSC

ข้อกำหนด 5.1.3.5 · ผู้ใช้บริการคลาวด์ (Cloud Service Customer)

ตัวบทมาตรฐาน

ก) CSC ต้อง**ขอหลักฐาน**ที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ และ**มีความสอดคล้องกับที่ CSP กล่าวอ้าง** ทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย

ถอดรหัสเป็นภาษาที่อ่านง่าย

ขอ หลักฐาน เอกสาร จาก CSP เพื่อยืนยันว่ามาตรการที่ CSP กล่าวอ้างถูกนำไปปฏิบัติจริง

- ใบรับรองมาตรฐาน — ISO/IEC 27017, 27018, 27701, 27001
- รายงาน Third-party Audit — SOC 2 Type II, CSA STAR, Penetration Test
- Bridge Letter ระหว่างรอบ Audit เพื่อปิดช่องว่างของหลักฐาน
- ตรวจสอบ Validity Period, Audit Scope, Region/Service Coverage และ Sub-processor List
- ทบทวนซ้ำเป็นประจำ — อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมี Material Change
- จัดทำ Internal Review สำหรับส่วนที่ CSC รับผิดชอบเอง (Configuration, IAM, Encryption Key)

*Bridge Letter — คือ จดหมายที่เชื่อมโยง “ช่องว่าง” ระหว่างวันที่รายงานของผู้ให้บริการ และสิ้นปีของผู้ใช้บริการ (เช่น สิ้นปีปฏิทินหรือปีงบประมาณ) จดหมายฉบับนี้เป็นเครื่องมือใช้แทนการให้ลูกค้ารอรายงานการตรวจสอบ (SOC) ฉบับถัดไป ซึ่งอาจต้องรออีก 12 เดือน

Trust, but verify อย่าเชื่อแค่คำพูด — ต้องขอ ‘ใบรับรอง’ หรือ ‘รายงานการตรวจ’ จากบุคคลที่สามที่อิสระมาตรวจสอบ

ถอดรหัสตัวบทมาตรฐาน — ฝั่ง CSP

ข้อกำหนด 5.1.3.5 · ผู้ให้บริการคลาวด์ (Cloud Service Provider)

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้หลักฐาน**ที่เป็นเอกสารแก่ CSC เพื่อยืนยันข้อเรียกร้องของ CSP ใน**การนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้**

ข) ในกรณีที่การตรวจสอบโดย CSC แต่ละรายการไม่สามารถกระทำได้หรืออาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้

CSP ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและขั้นตอนของ CSP

ทั้งนี้ CSP ต้องแสดงหลักฐานดังกล่าวให้กับผู้ที่คาดว่าจะเป็น CSC ก่อนเข้าทำสัญญา โดยปกติแล้วการตรวจสอบอิสระที่เกี่ยวข้องตามที่ CSP เลือก ควรเป็นวิธีการที่เป็นที่ยอมรับเพื่อตอบสนองความต้องการของ CSC ในการตรวจสอบการดำเนินงานของ CSP หากมีความโปร่งใสเพียงพอ

เมื่อการตรวจสอบที่เป็นอิสระไม่สามารถทำได้ CSP ต้องทำการประเมินตนเอง และเปิดเผยกระบวนการและผลลัพธ์ต่อ CSC

ถอดรหัสเป็นภาษาที่อ่านง่าย

จัดทำ และ ให้หลักฐานเอกสารแก่ลูกค้า เพื่อยืนยันการนำมาตรการความมั่นคงปลอดภัยฯ ไปปฏิบัติ

- Independent Audit Report จาก Third-party — เปิดเผยก่อนทำสัญญา
- กรณี Independent Audit ทำไม่ได้ → ต้องจัดทำ Self-assessment ที่ตรวจสอบได้
- Trust Center / Compliance Portal สำหรับเข้าถึงเอกสาร
- เปิดเผย Audit Scope, Service Boundaries, Sub-processor List, Excluded Components
- แจ้งลูกค้าเมื่อมีการเปลี่ยนแปลงที่สำคัญ ใน Scope, Service Description หรือ Compliance Status
- ทบทวน ISMS ภายในอย่างน้อยปีละ 1 ครั้ง โดยทีมที่อิสระจากฝ่ายปฏิบัติการ

Independent Review = การยืนยันมาตรการความมั่นคงปลอดภัยฯ โดยบุคคลที่สาม ที่ปราศจากผลประโยชน์ทับซ้อน

ส่วนที่ 2

5.2 การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

Cloud Infrastructure Security and Operation

5.2.1 การบริหารทรัพยากรมนุษย์ (Human Resource Security)

5.2.1.1 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรม

Information Security Awareness, Education and Training

ข้อกำหนดสำหรับ

CSC | CSP

ข้อกำหนดตามมาตรฐาน ฯ : ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

CSC – Cloud Service Customer

ก) CSC ต้อง**เพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้** การศึกษาและการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และ**ผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง**

- มาตรฐานและขั้นตอนการใช้บริการคลาวด์
- ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น
- ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์
- การคุ้มครองข้อมูลส่วนบุคคล
- ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง

ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการ**ฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ** (Business Units)

CSP – Cloud Service Provider

ก) CSP ต้อง**สร้างความตระหนักรู้**ด้านความมั่นคงปลอดภัยสารสนเทศและด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษา และการฝึกอบรม**แก่พนักงาน รวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกัน**เกี่ยวกับ**การจัดการข้อมูลของ CSC** และ**ข้อมูลที่ได้จากบริการคลาวด์**อย่างเหมาะสม โดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อ CSC หรืออยู่ภายใต้ข้อจำกัดเฉพาะ รวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึงและใช้งานโดย CSP

ถอดรหัสตัวบทมาตรฐาน — ภาระของผู้ใช้บริการคลาวด์ (CSC)

5 หัวข้อบังคับที่ต้องเพิ่มในโปรแกรมอบรม + กลุ่มเป้าหมายตั้งแต่ผู้บริหารถึงผู้ใช้งาน

CSC ต้องเพิ่ม 5 หัวข้อเหล่านี้เข้าในโปรแกรมอบรมที่มีอยู่ — และจัดให้กับทุกกลุ่มเป้าหมาย

01

มาตรฐานและขั้นตอนการใช้บริการคลาวด์

นโยบาย Cloud Usage,
ขั้นตอนขอใช้ Account,
แนวทาง Multi-cloud

02

ความเสี่ยงด้านความปลอดภัยและวิธีจัดการ

Account Hijacking,
API Key Leak,
Misconfiguration

03

ความเสี่ยงด้านสภาพแวดล้อมและเครือข่าย

VPC peering,
Public IP,
Cloud Network Identity

04

การคุ้มครองข้อมูลส่วนบุคคล

Data Classification,
Cross-border Transfer,
Data Subject Rights (PDPA)

05

ข้อพิจารณาทางกฎหมายและข้อบังคับ

พ.ร.บ. ไซเบอร์, PDPA,
ประกาศ สกมช.,
กฎเฉพาะอุตสาหกรรม

กลุ่มเป้าหมายของ CSC — ต้องครอบคลุมทุกระดับ

ผู้บริหารระดับสูง	ผู้จัดการสายธุรกิจ	ผู้ดูแลระบบคลาวด์	Developer / DevOps	ผู้ประกอบบริการคลาวด์ (Integrator)	ผู้ใช้งานทั่วไป
Cloud Strategy & Compliance	Risk, Cost, Vendor Lock-in	IAM Deep-dive + Hands-on Lab	Secure-by-Design, IaC, Secrets Management	Cross-system Risk, Data Flow	Phishing, BYOD, Reporting

ถอดรหัสตัวบทมาตรฐาน — ภาระของผู้ให้บริการคลาวด์ (CSP)

การจัดการข้อมูลลูกค้า ความลับ ข้อจำกัดด้านกฎระเบียบ และ Supply Chain

3 ภาระหลักที่ CSP ต้องสร้างความตระหนักรู้แก่พนักงานและผู้รับจ้าง

1 Appropriate Handling
การจัดการข้อมูลลูกค้าอย่างเหมาะสม

ครอบคลุมทั้ง Customer Data (ลูกค้านำมาเก็บ) และ Cloud Service Derived Data (Log, Metric, Usage Pattern) ห้ามใช้ผิดวัตถุประสงค์

2 Confidentiality Protection
การปกป้องข้อมูลที่เป็นความลับ

ข้อมูลลูกค้าอาจมีระดับความลับสูง เช่น ข้อมูลทางการเงิน ข้อมูลสุขภาพ หรือข้อมูลที่ถูกกำกับโดยกฎหมายเฉพาะ

3 Regulatory Constraints
ข้อจำกัดด้านกฎระเบียบ

ห้ามใช้ข้อมูลลูกค้าฝึก AI ของตน ห้ามถ่ายโอนข้อมูลออกนอกประเทศโดยไม่ได้รับอนุญาต ต้องผ่าน Data Access Approval Workflow

จุดที่ต้องระวัง

Supply Chain Awareness

CSP ต้อง "กำหนดให้ผู้รับจ้างทำเช่นเดียวกัน" — Subcontractor ทั้งห่วงโซ่ต้องผ่านการอบรม ไม่ใช่แค่พนักงานของ CSP เอง

แนวปฏิบัติที่ดี:

- Code of Conduct + Data Handling Policy ครอบคลุม Derived Data
- Onboarding เสร็จก่อนอนุญาตให้เข้าถึงระบบงานจริง
- Subcontractor Attestation + Audit Right
- Customer Data Access Approval Workflow + Notification
- Phishing / Vishing Drill รายไตรมาส โดยเฉพาะทีม Help Desk
- Insider Threat Awareness — DLP/UBA Integration

องค์ประกอบโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรม

องค์ประกอบของโปรแกรมที่ดี + วงจร Assess → Plan → Deliver → Measure → Improve

8 องค์ประกอบของกระบวนการที่ดี (Building Blocks)

01
Policy & Charter
นโยบายและ Charter ลงนามโดยผู้บริหาร

02
Stakeholder Map
CISO, HR, Legal, Cloud Ops, BU, ผู้รับจ้าง

03
Needs Analysis
Gap ของแต่ละบทบาท Admin vs User

04
Curriculum Design
Foundation / Practitioner / Specialist

05
Delivery Channels
E-learning, Workshop, Tabletop

06
Assessment
Quiz + Phishing Simulation Behavior

07
Records & Reporting
Audit Trail + KPI ต่อผู้บริหาร

08
Continuous Improve
ทบทวนตามภัยใหม่ ฟีเจอร์ใหม่

วงจรชีวิต PDCA (Lifecycle)

1 Assess
Risk + Skill Gap Analysis

2 Plan
Training Plan + Curriculum Catalog

3 Deliver
อบรม + Workshop + Phishing

4 Measure
KPI Dashboard + Phishing %

5 Improve
ปรับเนื้อหาตามภัยใหม่

5.2.2 การจัดการทรัพย์สิน (Asset Management)

5.2.2.1 ทะเบียนทรัพย์สิน

Inventory of Assets

ข้อกำหนดสำหรับ

CSC CSP

ถอดรหัสมาตรฐานสำหรับผู้ใช้บริการคลาวด์ (CSC)

CSC ต้องบันทึกทรัพย์สินคลาวด์ + ระบุสถานที่จัดเก็บ + เชื่อมเข้ากับกระบวนการอื่นขององค์กร

> ก) **ทะเบียนทรัพย์สินของ CSC ต้องคำนึงถึงข้อมูลและทรัพย์สิน** ที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของ CSP
>
> — ข้อกำหนด 5.2.2.1 ทะเบียนทรัพย์สิน

สิ่งที่ CSC ต้องทำ 3 ประการ

01 ขยายขอบเขต Inventory

ครอบคลุม Cloud Asset ทุกชั้น — Data, VM, Container, Database, Storage, Backup, Image, Service Account, Secret, API Key

02 ระบุ Location เชิงตรรกะ

CSP (AWS / Azure / GCP / NIPA / INET ...), Region (ap-southeast-1 ...), Account / Subscription / Project ID, Service Type

03 เชื่อมโยงเข้ากระบวนการอื่น

Data Classification, ROPA (PDPA), Risk Register, Change Management, Incident Response Playbook — ใช้ Inventory เดียวกัน

ถอดรหัสมาตรฐานสำหรับผู้ให้บริการคลาวด์ (CSP)

ข้อกำหนด 5.2.2.1 ทะเบียนทรัพย์สิน

ก) **ทะเบียนทรัพย์สินของ CSP** ต้องระบุอย่างชัดเจนในเรื่อง
- **ข้อมูลของ CSC**
- **ข้อมูลที่เกิดจากการใช้บริการคลาวด์**

TYPE 1 — Cloud Service Customer Data

ข้อมูลที่ลูกค้านำเข้ามาเก็บ/ประมวลผล

- ฐานข้อมูลลูกค้า, ไฟล์เอกสาร, ภาพ, วิดีโอ
- ข้อมูล Application และ Source Code (ที่ CSC อัปโหลด)
- Backup และ Snapshot ที่ลูกค้าสร้าง

บทบาทตาม PDPA

CSP = Data Processor / CSC = Data Controller

หน้าที่ของ CSP

- บันทึกประเภทและสถานที่จัดเก็บในทะเบียนของตน
- ไม่ใช้ข้อมูลเกินวัตถุประสงค์ตาม DPA
- เปิด API ให้ CSC ดึง Inventory ของข้อมูลตนได้

TYPE 2 — Cloud Service Derived Data

ข้อมูลที่ระบบสร้างขึ้นจากการใช้บริการ

- Resource Utilization Log, Audit Log, API Call Log
- Billing Metric, Performance Telemetry
- Crash Dump, Error Log, Cookie / Session, IP Log

ข้อควรระวัง

หาก Log/Telemetry สามารถระบุตัวบุคคลได้ → ถือเป็นข้อมูลส่วนบุคคล CSP ต้องจัดการตามกฎหมาย PDPA

หน้าที่ของ CSP

- เปิดเผยประเภท Derived Data ทั้งหมดให้ CSC ทราบ
- ระบุ Retention Period และสถานที่จัดเก็บ
- ระบุในสัญญา MSA/DPA อย่างชัดเจน

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

ใครต้องบันทึกอะไรในทะเบียน — แม้ความรับผิดชอบทางเทคนิคของ CSP เพิ่มขึ้นจาก IaaS → SaaS แต่ CSC ยังต้องบันทึกข้อมูลของตนเสมอ

ทรัพย์สิน / Layer	IaaS	PaaS	SaaS
Customer Data (ข้อมูลที่ลูกค้านำเข้า)	CSC	CSC	CSC
Derived Data (Log, Telemetry)	CSP	CSP	CSP
Application & Source Code	CSC	CSC + CSP	CSP (CSC config)
Database / Schema	CSC	CSC	CSP schema / CSC content
Middleware / Runtime	CSC	CSP	CSP
OS / Container Image	CSC	CSP	CSP
Virtualization / Hypervisor	CSP	CSP	CSP
Physical HW / Facility	CSP	CSP	CSP
Identity & Service Account	CSC	CSC	CSC
API Key / Secret / Certificate	CSC	CSC	CSC
Backup & Snapshot	CSC	Shared	CSP (CSC แจ้ง)
Network / DNS / LB	CSC	Shared	CSP
Compliance Asset (Cert/Report)	CSC + CSP เผยแพร่	CSC + CSP เผยแพร่	CSC + CSP เผยแพร่

CSC บันทึกในทะเบียนของตน

Shared / Both

CSP บันทึก (เปิดเผยให้ CSC)

วงจรชีวิตของทรัพย์สินคลาวด์ (Cloud Asset Lifecycle)

ทะเบียนต้องรองรับ 6 ขั้นตอน — ทุกการเปลี่ยนแปลงต้องสะท้อนใน Inventory โดยอัตโนมัติ

01 PLAN
วางแผน
Owner ลงทะเบียน Use Case, Data Classification, Region ก่อนสร้าง

02 PROVISION
สร้าง
สร้างผ่าน IaC/Console พร้อม Tag ครบ — Inventory Update อัตโนมัติผ่าน Event

03 OPERATE
ใช้งาน
Update Tag เมื่อเปลี่ยน Classification / Compliance Scope

04 CHANGE
เปลี่ยนแปลง
เปลี่ยน Config, ย้าย Region, ขยาย Capacity — บันทึก Change Log

05 REVIEW
ทบทวน
Owner ยืนยันรายปีว่ายังจำเป็น และ Owner ยังถูกต้อง

06 DECOMMISSION
ปลด
Secure Wipe + Mark เป็น Decommissioned (ไม่ลบ Record เพื่อ Audit Trail)

หลักการสำคัญของ Lifecycle ในคลาวด์

- **Event-driven, not Poll-based**
  Ephemeral resource (Container/Function) อยู่ไม่นาน — ต้อง subscribe กับ Cloud Event
- **Tag at Provision**
  บังคับ Tag ตอนสร้าง ไม่ใช่ตามไป Backfill — บังคับด้วย Policy-as-Code
- **Decommission ≠ Delete Record**
  เก็บ Record ไว้พร้อม Audit Trail เพื่อใช้ในการ Investigation ภายหลัง

อ้างอิง: ISO/IEC 27002:2022 §5.9 | NIST SP 800-53 CM-8 (System Component Inventory) | CSA CCM v4.1 DCS-06

ตัวอย่าง Schema ของ Cloud Asset Inventory

ทุก Asset ควรระบุ Metadata — เพื่อบังคับใช้ผ่าน Tagging Policy ตั้งแต่ Provision

IDENTITY & TYPE

Field	Type	Req	ตัวอย่าง
AssetId	UUID	Yes	*asset-7f3a-9c12*
AssetName	String	Yes	*prod-customer-db-01*
AssetType	Enum	Yes	*Database / VM / Storage*
CSP	Enum	Yes	*AWS / Azure / GCP / NIPA*
Region	String	Yes	*ap-southeast-1*
AccountId	String	Yes	*123456789012*
ServiceType	String	Yes	*Amazon RDS PostgreSQL*
Environment	Enum	Yes	*Prod / Stg / Dev / Sandbox*
Status	Enum	Yes	*Active / Decommissioned*

OWNERSHIP & CONTEXT

Field	Type	Req	ตัวอย่าง
OwnerEmail	Email	Yes	*somchai.t@org.go.th*
BackupOwnerEmail	Email	Yes	*somying.s@org.go.th*
BusinessUnit	String	Yes	*Customer Service*
CostCenter	String	Yes	*CC-1042*
DataClassification	Enum	Yes	*Public / PII / Secret*
ComplianceTags	Array	Cond.	*["PDPA","CII"]*
DataResidency	String	Yes	*TH-only / ASEAN*
ProjectCode	String	Yes	*PRJ-2026-018*
LastReviewedDate	Date	Auto	*2026-04-01*

TIP: บังคับ Mandatory Tags ทั้ง 8 ตัว (Owner, BackupOwner, Environment, DataClassification, CostCenter, BusinessUnit, DataResidency, ProjectCode) ผ่าน AWS SCP / Azure Policy / GCP Org Policy — Resource ที่ขาด Tag จะถูก Block ตั้งแต่ Provision

5.2.2 การจัดการทรัพย์สิน (Asset Management)

5.2.2.2 การบ่งชี้ข้อมูล

Labelling of Information

ข้อกำหนดสำหรับ

CSC CSP

ถอดรหัสตัวบทมาตรฐาน — สิ่งที่ CSC ต้องทำ vs สิ่งที่ CSP ต้องทำ

ข้อกำหนด 5.2.2.2 — ภาระหน้าที่ของ เจ้าของข้อมูล และ เจ้าของเครื่องมือ

ผู้ใช้บริการคลาวด์ (CSC) — เจ้าของข้อมูล

ตัวบทมาตรฐาน

ก) CSC **ต้องบ่งชี้ข้อมูลและทรัพย์สิน**ขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร

01 ต้องมี Procedure ที่เป็นทางการ
ไม่ใช่ทำตามใจชอบของแต่ละบุคคล

02 บ่งชี้ทั้ง Information และ Associated Assets
Database, Object Storage, Container Image, Volume

03 ครอบคลุมข้อมูลที่ Stored และ In-use
ไม่ใช่เฉพาะข้อมูลที่สร้างใหม่

04 ใช้มาตรฐานเดียวกัน On-prem + Cloud
หลีกเลี่ยงสองมาตรฐานในองค์กร

ผู้ให้บริการคลาวด์ (CSP) — เจ้าของเครื่องมือ

ตัวบทมาตรฐาน

ก) CSP ต้องจัดทำเอกสารและ**เปิดเผยฟังก์ชัน**การทำงานของบริการใด ๆ ที่ CSC สามารถนำไปใช้เพื่อ**การบ่งชี้ข้อมูลและทรัพย์สิน**ที่เกี่ยวข้องได้

01 เปิดเผย Functionality ของบริการ
ไม่ใช่หน้าที่ติดป้ายให้ลูกค้า — แต่ให้เครื่องมือ

02 เอกสารต้องเข้าถึงได้
เพื่อให้ลูกค้านำไปใช้งาน รวมถึงประเมินในขั้นตอนการจัดหา

03 ครอบคลุม Built-in + Integration
รวม Third-party Tool ที่ Integrate ได้

04 เปิดเผย Limitations อย่างชัดเจน
Tag Limit, Character Set, Inheritance Behaviour

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

ระดับการควบคุมเปลี่ยนตามรูปแบบบริการ — ต้องเข้าใจขอบเขตก่อนวางแผน Control

กิจกรรม	IaaS	PaaS	SaaS
กำหนด Classification Scheme & ระดับชั้น	CSC	CSC	CSC
ติดป้ายลงข้อมูล/ทรัพย์สิน	CSC	CSC	CSC
จัดเตรียมฟังก์ชัน Tagging/Labelling	CSP	CSP	CSP
เอกสาร & เปิดเผย Functionality	CSP	CSP	CSP
บังคับใช้ Label ใน DLP/Access Control	CSC	Shared	Shared
รักษา Label ข้อมูลตลอด Lifecycle	CSC	Shared	CSP
จัดทำ Audit Evidence	Shared	Shared	CSP

CSC — ลูกค้ารับผิดชอบหลัก CSP — ผู้ให้บริการรับผิดชอบหลัก Shared — ร่วมรับผิดชอบ

องค์ประกอบของกระบวนการบ่งชี้ข้อมูลที่มีประสิทธิภาพ

Process Perspective — Policy, Procedure, Tools, People, Measure & Improve

01 Policy & Standards

- Classification Scheme
- Label Naming Convention
- Reclassification Trigger
- Review Cycle

02 Procedures

- Initial Labelling
- Re-labelling Workflow
- Misclassification Handling
- Exception Process

03 Tools & Technology

- Auto/Manual Classify
- DLP, IRM, CASB
- ABAC Engine
- Monitoring Tool

04 People & Awareness

- Training ทุกคน
- Specialized: DevOps, DBA
- KPI สะท้อนการปฏิบัติ
- Data Owner Cert

05 Measure & Improve

- Coverage %
- Misclassification Rate
- Mean Time to Reclassify
- Annual Review

เชื่อมโยงกับ: Classification (Input) → Labelling → Media Handling → Access Control (ABAC) → Cryptography → Incident Response

Label ต้องเดินทางไปกับข้อมูลตลอด Data Lifecycle

ตั้งแต่ Create → Store → Use → Share → Archive → Destroy — Label ห้ามหาย

1	2	3	4	5	6
Create	**Store**	**Use**	**Share**	**Archive**	**Destroy**
Tag-on-Create Default Label	คงสภาพใน Metadata Object Tag, DB Column	บังคับใช้ Label ใน Access Policy	ส่งต่อพร้อมข้อมูล ผ่าน API / Email	คงสภาพ Label Adjust ตาม Retention	ทำลายตามมาตรฐาน บันทึก Evidence

KPI ที่นิยมใช้วัด — ติดตามให้ Label "อยู่ครบ อยู่ถูก"

Label Coverage Rate: **>95%**

Misclassification Rate: **<2%**

Time to Label: **<24 ชม.**

Policy Violation Detection: **Real-time**

6 ระดับของ Label บนคลาวด์ — เลือก Layer ที่เหมาะกับข้อมูล

Resource → Object → File → Database Column → Network/Traffic → Container/Workload

	LABEL TYPE	ขอบเขตการใช้งาน	ตัวอย่างเทคโนโลยี
L1	**Resource-level Tag**	VM, Storage Bucket, Database Instance	*Resource Tags — Key-Value Pair*
L2	**Object-level Tag**	Object Storage / ไฟล์	*Object Tagging, Custom Metadata*
L3	**File / Document Sensitivity Label**	Label ฝังในไฟล์ — คงอยู่แม้ย้าย	*Purview Sensitivity Label, Google Drive Labels, Adobe IRM*
L4	**Database Column-level Tag**	ระดับคอลัมน์/ตารางใน DB	*Data Catalog, AWS Glue / Azure Purview / GCP Data Catalog*
L5	**Network / Traffic Tag**	Traffic ระหว่างบริการ	*Service Mesh Labels (Istio, Linkerd), VPC Tags*
L6	**Container / Workload Label**	Pod / Workload Level	*Kubernetes Labels & Annotations*

เครื่องมือสำคัญในตลาด (Vendor-neutral) — รู้จัก 8 หมวด

เลือกใช้ตามขนาดและ Maturity ขององค์กร — เริ่มจาก Native Tag ไปจนถึง Persistent Label

01 Cloud-Native Tagging

Key-Value Tag บน Resource ของทุก Hyperscaler

เช่น: *ข้อจำกัด: Cardinality / Character Set*

02 Data Classification & Discovery

สแกนและจัดประเภทอัตโนมัติ

เช่น: *AWS Macie, MS Purview, GCP DLP, BigID, Spirion*

03 Information Rights Management (IRM)

ฝัง Label ในไฟล์ บังคับ Persistent Policy

เช่น: *MS Purview / Azure IP, Adobe DRM*

04 CASB — Cloud Access Security Broker

บังคับใช้ Label เมื่อแชร์ข้ามคลาวด์

เช่น: *Netskope, Zscaler, MS Defender for Cloud Apps*

05 DLP — Data Loss Prevention

ตรวจจับการเคลื่อนย้ายข้อมูลผิด Policy

เช่น: *ใช้ Label เป็น Trigger หลัก*

06 CSPM — Cloud Security Posture Mgmt

ตรวจหา Resource ที่ขาด Tag / Tag ผิด

เช่น: *Wiz, Prisma Cloud, Lacework, Defender for Cloud*

07 Data Catalog & Governance

เก็บ Label เป็น Single Source of Truth

เช่น: *Collibra, Alation, Cloud Data Catalogs*

08 Policy-as-Code

บังคับ Tag-on-Create ผ่าน CI/CD

เช่น: *Open Policy Agent, AWS SCP, Azure Policy*

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.1 การควบคุมเข้าถึงเครือข่ายและบริการเครือข่าย

Access to Networks and Network Services

ข้อกำหนดสำหรับ

CSC -

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.3.1 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) **นโยบายการควบคุมการเข้าถึง**ของ CSC สำหรับการใช้บริการเครือข่าย ต้อง**ระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์**ตามแต่ละบริการที่ใช้งาน

01

นโยบายเป็นลายลักษณ์อักษร

จัดทำเอกสาร Network Access Control Policy ที่อนุมัติโดยผู้บริหารระดับสูง ครอบคลุมการใช้บริการเครือข่ายของทุก Cloud Service ที่องค์กรใช้งาน

02

ข้อกำหนดรายบริการ (Per-Service)

พิจารณาข้อกำหนดเฉพาะสำหรับแต่ละบริการ — นโยบายที่กว้างเกินไปอาจไม่ตอบโจทย์

03

ระบุเงื่อนไขผู้ใช้งาน

ใคร / เข้าถึงจาก Network ใด / ผ่าน Protocol อะไร / ต้องมี MFA หรือไม่ / ต้องผ่าน VPN หรือ Bastion หรือ ZTNA หรือไม่

บทบาท CSP: แม้ข้อ 5.2.3.1 จะเป็น CSC-Only แต่ CSP ต้องจัดเตรียม NSG, IAM, MFA, VPN, Private Endpoint และเอกสาร Service Description เพื่อสนับสนุน CSC

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSC และ CSP ในรูปแบบบริการ IaaS / PaaS / SaaS

องค์ประกอบ	IaaS	PaaS	SaaS
Physical / Backbone Network	CSP	CSP	CSP
VPC / VNet Design	CSC	CSC*	CSP
Security Group / Firewall Rule	CSC	CSC	CSP
Web Application Firewall (WAF)	CSC	CSC*	CSP
Identity & Access (Network-related)	CSC	CSC	CSC
Network Access Policy & Docs	CSC	CSC	CSC
Network Monitoring / Flow Logs	CSC	CSC	CSC*
DDoS Protection (Baseline)	CSP	CSP	CSP

คำอธิบายสัญลักษณ์

- **CSP** ความรับผิดชอบของผู้ให้บริการ
- **CSC** ความรับผิดชอบของผู้ใช้บริการ
- **CSC*** บางส่วน / ขึ้นกับบริการ

Key Note

Policy & Identity เป็นของ CSC เสมอ

ไม่ว่า IaaS / PaaS / SaaS — การกำหนดและบังคับใช้ Network Access Policy รวมถึง Identity ที่เข้าถึงเครือข่าย เป็นความรับผิดชอบของ CSC ทุกครั้ง CSP เพียงจัดเตรียมเครื่องมือและ Default-Secure Configuration ให้

องค์ประกอบของการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

Policy → Standards → Architecture → Implementation → Monitoring → Review

01
Policy
นโยบายอนุมัติโดยผู้บริหาร ครอบคลุมทุก Cloud Service ทบทวนปีละ 1 ครั้ง

02
Standards & Procedures
Naming, Tagging, Default Deny Rule, Allowed Ports + ขั้นตอนปฏิบัติ

03
Architecture
Network Design รองรับ Segmentation, Private Endpoint, Landing Zone

04
Implementation
บังคับใช้ผ่าน NSG, Firewall, IAM Policy, Conditional Access, Service Endpoint

05
Monitoring & Detection
Flow Logs, Access Logs, Configuration Drift, Alert การละเมิดนโยบาย

06
Review & Improvement
Quarterly Access Review, Policy Review, Internal Audit, Lesson Learned

Continuous Loop วงจร 6 องค์ประกอบนี้ไม่ใช่เส้นตรง — ผลจาก Review ต้อง Feedback กลับเข้า Policy / Standards / Architecture เพื่อปรับปรุงต่อเนื่อง (Plan-Do-Check-Act)

Technology Stack — เครื่องมือเชิงเทคนิคที่จำเป็น

รู้จัก 11 ประเภทเทคโนโลยีหลักที่ใช้บังคับใช้นโยบาย

01 VPC / VNet

เครือข่ายส่วนตัวเชิง Logical

02 Subnet & Routing

แบ่ง Public/Private + Route Table

03 Security Group / NACL

Inbound/Outbound ระดับ Instance

04 Web Application Firewall

ป้องกัน L7 — SQLi, XSS

05 DDoS Protection

ป้องกัน L3/4 และ L7

06 Private / Service Endpoint

PaaS โดยไม่ผ่าน Internet

07 VPN / Direct Connect

เชื่อม On-prem กับ Cloud

08 Bastion / Jump Server

จุดเข้าถึงกลางสำหรับ Admin

09 Zero Trust Network Access

พิสูจน์ตัวตนทุกครั้ง

10 SASE

Network + Security รวมกัน

11 CSPM

ตรวจ Misconfiguration อัตโนมัติ

หลักการ Defense in Depth

เลือกใช้ผสมกันหลายชั้น — ไม่มีเครื่องมือใดป้องกันได้ครบทุก Vector

Protocols การสื่อสารอย่างปลอดภัย

TLS, IPsec, SSH, SAML, OAuth, FIDO2 และกรอบ Zero Trust

มาตรฐานและ Protocol

TLS 1.2 / TLS 1.3

การเข้ารหัสข้อมูลระหว่างส่ง บังคับใช้เป็นค่าเริ่มต้น ปิด Cipher ที่ล้าสมัย เช่น TLS 1.0/1.1, RC4, 3DES

IPsec / IKEv2

เข้ารหัสสำหรับ Site-to-Site VPN ระหว่าง On-prem กับ Cloud — Encryption + Integrity + Authentication

SSH (Protocol 2)

เข้าถึง Server ระยะไกล ใช้ Key-based Authentication เท่านั้น ห้าม Password Authentication

SAML 2.0 / OAuth 2.0 / OpenID Connect

Identity Federation สำหรับ SSO ข้ามระบบ — แนะนำ OIDC สำหรับ Modern Application

FIDO2 / WebAuthn

MFA สมัยใหม่ที่ทนทานต่อ Phishing — ใช้ Hardware Token เช่น YubiKey หรือ Platform Authenticator

กรอบแนวคิดอ้างอิง

Zero Trust Architecture

NIST SP 800-207

Never trust, always verify — ตรวจสอบสิทธิ์ทุกครั้งก่อนให้เข้าถึง ไม่ตั้งสมมติฐานว่า Network ภายในปลอดภัย

เปรียบเทียบ On-premise vs Cloud — เปลี่ยน Mindset

ผู้ปฏิบัติงานต้องปรับวิธีคิดในการควบคุมการเข้าถึงเครือข่าย

มิติเปรียบเทียบ	On-premise (Traditional)	Cloud (Modern)
ขอบเขตและเครื่องมือ	Firewall ขอบเขต, Layer 3/4 ACL, VLAN, Physical NIC, IDS/IPS	SDN, Security Group, Private Endpoint, Service Mesh, Identity-based
Lifecycle	ผ่าน Change Process หลายวัน บังคับโดยทีม Network	เปลี่ยนทันที (Self-service) ผ่าน API/Console/IaC — เสี่ยง Drift
ผู้เกี่ยวข้อง	ทีม Network + ทีม Security ภายใน	หลายฝ่าย: AppOwner, DevOps, Architect, Security, CSP, Sub-CSP
Evidence	Firewall Config, Switch Config, IDS Log, Manual Snapshot	IaC Repository, Cloud Config Snapshot, Flow Logs, SIEM
Trust Model	Active Directory + Network Location (inside is trusted)	Identity-based / Zero Trust — Never trust, always verify
Segmentation	VLAN, Physical, IP/Subnet-based	Logical — VPC, Subnet, Security Group, Tag-based Microsegmentation

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.2 การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้

User Registration and Deregistration

ข้อกำหนดสำหรับ

CSC CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.3.2 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) **ขั้นตอนการลงทะเบียนและยกเลิก**การลงทะเบียนสำหรับผู้ใช้ **ต้องครอบคลุมถึงสถานการณ์**ที่การควบคุม**การเข้าถึงของผู้ใช้ถูกคุกคาม** เช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่น ๆ (ยกตัวอย่างเช่น จากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม

ตีความและสิ่งที่ CSC ต้องจัดเตรียม · 4 ภารกิจหลัก

01 Written Procedure

จัดทำขั้นตอน (Procedure) เป็นลายลักษณ์อักษรครอบคลุมทุกบริการคลาวด์ที่องค์กรใช้

02 Cover Normal + Special Case

ครอบคลุมทั้ง Joiner-Mover-Leaver และกรณี Credential / ข้อมูลทะเบียนถูกคุกคาม

03 Define Triggers

ระบุ Trigger ที่ต้องเพิกถอน/รีเซ็ต เช่น รหัสผ่านรั่ว, ตกเป็นเหยื่อฟิชชิง, อุปกรณ์หาย, ลาออกฉุกเฉิน, พบการเข้าถึงที่ผิดปกติ

04 Internal SLA

กำหนด SLA เพิกถอน/รีเซ็ตในแต่ละสถานการณ์ — เช่น ภายใน 1 ชั่วโมงสำหรับกรณีถูกคุกคาม

หลักการ: CSC คือเจ้าของกระบวนการและสิทธิ์ผู้ใช้ของตน — ไม่ว่าจะใช้ IaaS / PaaS / SaaS ก็ตาม

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.2 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) เพื่อจัดการการเข้าถึงบริการคลาวด์โดยผู้ใช้งานของ CSC CSP ต้อง**จัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิก**การลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้แก่ CSC

ตีความและสิ่งที่ CSP ต้องจัดเตรียม · 4 ภารกิจหลัก

01 Working Function

จัดเตรียมฟังก์ชันที่ใช้งานได้จริงสำหรับ CSC — UI Console, CLI, API, SAML / OIDC / Cross-domain Identity Management (SCIM)

02 Self-service Support

รองรับการบริหารแบบ Self-service โดย CSC ไม่ต้องร้องขอผ่าน Ticket ของ CSP ในงานปกติ

03 Specifications & Docs

จัดทำข้อกำหนดและคู่มือการใช้งาน อธิบายขั้นตอน ข้อจำกัด ความสามารถ และ Best Practice

04 Audit Log Provision

จัดเตรียม Audit Log ที่ CSC ดึงไปใช้เป็นหลักฐานการตรวจสอบและการสอบสวนเหตุการณ์ได้

หลักการ: CSP ต้องส่งมอบ "เครื่องมือ" และ "คู่มือ" — แต่ CSC ยังเป็นเจ้าของผู้ใช้และสิทธิ์ของตนเสมอ

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

ตารางความรับผิดชอบในการลงทะเบียน/ยกเลิกการลงทะเบียนผู้ใช้ ตามรูปแบบบริการคลาวด์ทั้ง 3 รูปแบบ

กิจกรรม / Layer	IaaS	PaaS	SaaS
IAM Console / Engine (ระบบจัดการ Identity)	CSP	CSP	CSP
การสร้าง/อนุมัติบัญชีผู้ใช้ของ CSC	CSC	CSC	CSC
การกำหนด Role / Permission ของผู้ใช้	CSC	CSC	CSC
การลงทะเบียนผู้ใช้ภายในของ CSP (Privileged Admin)	CSP	CSP	CSP
Identity Federation (SAML / OIDC / SCIM)	Shared	Shared	Shared
การยกเลิก / เพิกถอนบัญชีผู้ใช้ของ CSC	CSC	CSC	CSC
Password Reset / Credential Rotation (Self-service)	Shared	Shared	Shared
Audit Log ของกิจกรรม IAM	Shared*	Shared*	Shared*
Credential Compromise Response (ผู้ใช้ของ CSC)	CSC	CSC	CSC
Credential Compromise Response (ผู้ใช้ของ CSP เอง)	CSP	CSP	CSP
Service Account / API Key Lifecycle	CSC	Shared	Shared

* CSP จัดเตรียม / CSC ใช้

CSC รับผิดชอบหลัก

CSP รับผิดชอบหลัก

Shared / ร่วมรับผิดชอบ

7 องค์ประกอบของกระบวนการลงทะเบียน/ยกเลิกผู้ใช้

ส่วนประกอบที่ต้องมีครบในกระบวนการลงทะเบียน/ยกเลิกผู้ใช้สำหรับระบบคลาวด์

01 Request Channel

ITSM Ticket / IGA Portal — ไม่รับคำขอนอกช่องทาง

02 Approval Workflow

Business Owner อนุมัติเฉพาะสิทธิ์ที่จำเป็น (Least Privilege)

03 Identity Verification

พิสูจน์ตัวตนของผู้ขอ และผู้อนุมัติ — เน้น Privileged Account

04 Provisioning Engine

สร้าง/แก้ไข/ลบ Account อัตโนมัติผ่าน SCIM และ API

05 Lifecycle Triggers

Event-driven จาก HR (Onboard / Offboard), AD Group Change Event, หรือ Contract Expiry Date

06 Compromise Playbook

ขั้นตอนเฉพาะสำหรับ Credential รั่ว/ถูกขโมย พร้อม SLA สั้น

07 Continuous Monitoring

ทบทวนสิทธิ์ตามรอบ + เฝ้าระวังการใช้งานผิดปกติอย่างต่อเนื่อง

เทคโนโลยีที่สนับสนุน User Lifecycle Management ในระบบคลาวด์

ตัวอย่าง Solution ที่นิยมในตลาดสำหรับแต่ละประเภทเทคโนโลยี

ประเภทเครื่องมือ	ตัวอย่างในตลาด (Vendor-Neutral)	บทบาทใน 5.2.3.2
Cloud-native IAM	AWS IAM, Azure Entra ID, GCP IAM, Alibaba RAM, Huawei IAM, OCI IAM	*สร้าง/ลบ Account ในระดับ Tenant*
Enterprise IdP	Microsoft Entra ID, Okta, Ping Identity, ForgeRock, JumpCloud, Google Cloud Identity	*Authoritative Source ของ Identity ฝั่ง CSC*
IGA Platform (Identity Governance & Admin)	SailPoint, Saviynt, One Identity, Omada, Microsoft Entra ID Governance, Oracle IGA	*Workflow, Approval, Lifecycle, Access Review*
PAM (Privileged Access Management)	CyberArk, BeyondTrust, Delinea, HashiCorp Boundary, Cloud-native PAM	*บริหาร Privileged Account — Vault* + Just-in-Time Access
CIEM (Cloud Infra Entitlement Management)	Wiz, Orca, Permiso, Sonrai, CrowdStrike Falcon Cloud Security	*วิเคราะห์ Over-privileged และ misconfigured permissions*
Secrets Management	HashiCorp Vault, AWS Secrets Manager, Azure Key Vault, GCP Secret Manager, CyberArk Conjur	*Credential ของ Service Account / API Key*
ITSM / Workflow	ServiceNow, Jira Service Management, Freshservice, ManageEngine	*ช่องทางร้องขอ + เก็บหลักฐาน Approval*
SIEM / Cloud SIEM	Splunk, Microsoft Sentinel, IBM QRadar, Elastic, Chronicle, Sumo Logic	*เก็บและวิเคราะห์ IAM Audit Log*

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.3 การจัดสรรการเข้าถึงของผู้ใช้

User Access Provisioning

ข้อกำหนดสำหรับ	
-	CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.3 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**จัดเตรียมฟังก์ชันสำหรับการจัดการสิทธิการเข้าถึง**ของ CSC รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้

01

Lifecycle Coverage

ฟังก์ชันครอบคลุมทุกขั้น Grant → Modify → Revoke → Review เข้าถึงได้ผ่าน UI, API และ CLI

02

Identity Types

ฟังก์ชันรองรับ Human User, Service Account, API Key, Federated Identity และ Workload Identity

03

Specifications

เผยแพร่ Documentation, API Reference, Best Practices, Limitations และ Known Issues

ข้อกำหนดนี้บังคับ CSP โดยตรง — CSC คือ "ผู้บริโภคของฟังก์ชัน" ที่ CSP จัดเตรียม

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

องค์ประกอบของ Provisioning Function	IaaS	PaaS	SaaS
ฟังก์ชัน Grant / Revoke (Engine)	CSP	CSP	CSP
UI / API / CLI สำหรับเรียกใช้ฟังก์ชัน	CSP	CSP	CSP
Documentation ของฟังก์ชัน	CSP	CSP	CSP
Audit Log (CSP จัดเตรียม / CSC ใช้)	Shared	Shared	Shared
ออกแบบ Role / Permission Model ภายใน	CSC	CSC	CSC
เรียกใช้ฟังก์ชันเพื่อ Grant ผู้ใช้จริง	CSC	CSC	CSC
Federation / SCIM Integration	Shared	Shared	Shared
Hardening ของฟังก์ชันเอง	CSP	CSP	CSP
Backup / DR ของระบบ Provisioning	CSP	CSP	CSP
กำหนด Approval Workflow ภายใน	CSC	CSC	CSC
ปฏิบัติตามคู่มือของ CSP	CSC	CSC	CSC
SLA (Availability, Latency)	CSP	CSP	CSP

CSP CSC Shared

มาตรฐานสำคัญที่เกี่ยวข้อง — RFC, OASIS และ NIST

เครื่องมือใดก็ตามต้องสอดคล้องกับมาตรฐานเหล่านี้ จึงจะใช้งานข้ามระบบได้

มาตรฐาน	แหล่งอ้างอิง	หน้าที่หลัก
SCIM 2.0	*RFC 7642 / 7643 / 7644*	Provisioning Protocol สำหรับ Identity Lifecycle — REST/JSON Standard
SAML 2.0	*OASIS Standard 2005*	Markup Language สำหรับ Authentication / Authorization ระหว่างองค์กร
OpenID Connect 1.0	*OIDF (บน OAuth 2.0)*	Identity Layer ทันสมัยกว่า SAML — ใช้ทั่วในแอป Modern Web/Mobile
OAuth 2.0	*RFC 6749*	Framework สำหรับ Delegated Authorization — Access Token, Refresh Token
JWT	*RFC 7519*	JSON Web Token — รูปแบบส่งข้อมูล Identity / Claims อย่างปลอดภัย
XACML 3.0	*OASIS Standard*	Policy แบบ ABAC — กำหนดกฎการเข้าถึงเชิงคุณลักษณะ
OID4VC	*OpenID for Verifiable Credentials*	Decentralized Identity — มาตรฐานใหม่ที่ผู้ใช้ถือ Credential เอง
NIST SP 800-63-3	*U.S. NIST*	Digital Identity Guidelines — IAL, AAL, FAL

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.4 การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ

Management of Privileged Access Rights

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.4 ในบริบทของบริการคลาวด์

ผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ใช้เทคนิคการยืนยันตัวตนที่เพียงพอ** (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของ CSC ให้มีความสามารถในการจัดการบริการคลาวด์ที่**สอดคล้องตามความเสี่ยง**ที่ระบุไว้

ใคร	พิสูจน์ตัวตนผู้ดูแลระบบ Cloud ของตนเอง — พนักงานที่เข้า Console / API
อะไร	ใช้ MFA เป็นมาตรฐาน + กลไกป้องกัน MFA Fatigue, Phishing-resistant
เมื่อไหร่	ทุกครั้งที่เข้าถึงทรัพยากร Production และ Privileged Role
อย่างไร	Risk-based Authentication: บัญชี Prod ใช้ Hardware Token, Dev อาจใช้ TOTP

ผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**มีเทคนิคการยืนยันตัวตนที่เพียงพอ** (เช่น การยืนยันตัวตนแบบหลายปัจจัย) **สำหรับ**การตรวจสอบสิทธิของ**ผู้ดูแลระบบบริการคลาวด์ของ CSC** ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

ใคร	จัดเตรียม MFA / IdP ของ Platform + ดูแลพนักงานของ CSP เอง
อะไร	รองรับ MFA หลายรูปแบบ: TOTP, WebAuthn/FIDO2, Push + Number Matching
เมื่อไหร่	เปิดเผย Log และ API เพื่อให้ลูกค้านำเข้า SIEM ได้แบบ Real-time
อย่างไร	Just-in-Time, Customer Lockbox, Session Recording สำหรับพนักงาน CSP

หัวใจสำคัญ : ทั้ง CSC และ CSP ต้องใช้ MFA + กลไกป้องกันการ Bypass — ห้ามมีบัญชี Privileged ที่ไม่มี MFA

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

ประเด็นความรับผิดชอบ	IaaS	PaaS	SaaS
จัดเตรียมเครื่องมือ MFA / IdP ของ Platform	CSP	CSP	CSP
เปิดใช้งาน MFA บัญชี Cloud Admin ของลูกค้า	CSC	CSC	CSC
กำหนด Policy / Conditional Access ระดับ Tenant	CSC	CSC	Shared
จัดการ Privileged ระดับ OS (Root, Administrator)	CSC	CSP	CSP
จัดการ Privileged ระดับ Platform (DB, Cluster)	CSC	Shared	CSP
จัดการ Privileged ของพนักงาน CSP เอง	CSP	CSP	CSP
Audit Log ของ Privileged Action	Shared	Shared	Shared *
ทบทวนสิทธิ (Access Review) ตามรอบ	CSC	CSC	CSC
กำหนดและบริหาร Break-glass Account	CSC	CSC	Shared

* CSP ลงมือ / CSC รับทราบ

CSC รับผิดชอบหลัก

CSP รับผิดชอบหลัก

Shared / ร่วมรับผิดชอบ

6 หลักการพื้นฐานของ Privileged Access

หลักการสากลที่ทุกองค์กรต้อง Apply ไม่ว่าจะใช้ Cloud เจ้าใด

1 Least Privilege

ให้สิทธิเท่าที่จำเป็นในช่วงเวลาจำกัด ลด Blast Radius

2 Separation of Duties

แยกผู้ขอสิทธิ ผู้อนุมัติ และผู้ตรวจสอบ ไม่ให้รวมในคนเดียว

3 Need-to-Know

เข้าถึงเฉพาะข้อมูลที่จำเป็นต่อบทบาทเท่านั้น

4 Zero Trust

ไม่ไว้วางใจการเข้าถึงโดยอัตโนมัติ ตรวจสอบทุกครั้ง

5 Just-in- Time (JIT)

ให้สิทธิ Privileged เป็นช่วงเวลา ไม่ใช่ถาวร

6 Auditability

ทุก Privileged Action ต้อง Trace ย้อนหลังได้ ไม่แก้ไขได้

มาตรฐานและ Protocol การยืนยันตัวตน

เลือก MFA และ Protocol ให้สอดคล้องกับระดับความเสี่ยงของ Workload

NIST SP 800-63B — เลือก Authenticator Assurance Level ให้สอดคล้องกับความเสี่ยง

AAL1 — **Single-factor หรือ Memorized Secret**

เหมาะกับ: Workload ความเสี่ยงต่ำมาก

AAL2 — **MFA — TOTP, Push with Number Matching**

เหมาะกับ: Workload ทั่วไป / PII ระดับกลาง

AAL3 — **Phishing-resistant FIDO2 / Hardware Token**

เหมาะกับ: CII, PII ระดับสูง ระบบการเงิน

Protocols และมาตรฐานสากลที่เกี่ยวข้อง

FIDO2 / WebAuthn	การยืนยันตัวตนแบบ Phishing-resistant ด้วย Hardware Token / Platform Authenticator
OAuth 2.0 / OIDC	โปรโตคอลมอบสิทธิและยืนยันตัวตนแบบรวมศูนย์ — เหมาะกับ API/Cloud Console
SAML 2.0	โปรโตคอลรวมศูนย์ตัวตนระดับ Enterprise — มาตรฐาน Federation ของลูกค้ากับ CSP

5 ความท้าทายเชิงเทคนิคและทางออก

ปัญหาที่ผู้ปฏิบัติงานพบจริงในระบบคลาวด์ พร้อมมาตรการรับมือ

เทคโนโลยี / สถานการณ์	ความท้าทาย (Challenge)	ทางออก (Mitigation)
Service Account / Workload Identity	✗ ไม่สามารถ MFA แบบบุคคลได้	✓ ใช้ Short-lived Credential ผ่าน OIDC Federation / IAM Role
Break-glass Account	✗ หากออกแบบไม่ดีจะกลายเป็น Backdoor	✓ Sealed Process + Alert ทุกการใช้งาน + ทดสอบปีละครั้ง
MFA Fatigue / Push Bombing	✗ ผู้ใช้กดยอมรับโดยไม่ตั้งใจ	✓ ผู้ใช้กรอกตัวเลข OTP ในหน้า Sign-in + Geographic Verification + Phishing-resistant
Multi-cloud / Multi-tenant	✗ Identity และ Policy กระจาย	✓ ใช้ Federation จาก Enterprise IdP เป็น Single Source of Truth
Legacy Application	✗ ใช้ Basic Auth ไม่รองรับ MFA สมัยใหม่	✓ PAM Broker / Jump Server คั่นกลาง + Compensating Controls

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.5 การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้

Management of Secret Authentication Information of Users

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.5 ในบริบทของบริการคลาวด์

CSC — ผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ตรวจสอบว่า**กระบวนการจัดการของ CSP สำหรับ**การจัดสรรข้อมูลการตรวจสอบความลับ** (Secret Authentication Information) เช่น รหัสผ่าน **เป็นไปตามข้อกำหนด**ของ CSC

1. **ทบทวนเอกสาร/นโยบายของ CSP**
   ตรวจสอบว่ากระบวนการจัดสรร Credential ของ CSP ปลอดภัยและเข้มงวดเพียงพอ
2. **เปรียบเทียบกับนโยบายภายในของ CSC**
   หากไม่สอดคล้อง ต้องเจรจาหรือใช้ Configuration Option เพื่อบังคับให้ตรงกัน
3. **บังคับ MFA สำหรับ Administrator ทุกบัญชี**
   Root, Owner, Global Admin, Billing Admin ต้องมี MFA และพิจารณาขยายถึง End User ที่เข้าถึงข้อมูลสำคัญ
4. **ตรวจสอบและเก็บหลักฐานเป็นระยะ**
   เก็บ Audit Log และทบทวน Configuration อย่างน้อยรายไตรมาส

CSP — ผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ** (Secret Authentication Information) ของ CSC รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าวสำหรับการตรวจสอบสิทธิผู้ใช้งาน

1. **จัดทำเอกสารกระบวนการให้ละเอียดและเปิดเผย**
   ครอบคลุม Onboarding, Activation, Reset, Rotation, Decommission พร้อมเผยแพร่ใน Trust Portal
2. **จัดเตรียมเครื่องมือ Secure-by-Default**
   Password Policy Engine, MFA, Federation, Secret Manager, API Key Management
3. **แจ้งให้ CSC ทราบล่วงหน้าเมื่อเปลี่ยนกระบวนการ**
   พร้อมกำหนดระยะเวลาเปลี่ยนผ่านที่เพียงพอ ≥ 90 วันสำหรับการเปลี่ยนแปลงสำคัญ

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

ใครรับผิดชอบส่วนใดใน IaaS, PaaS, SaaS

องค์ประกอบ	IaaS	PaaS	SaaS
Password Policy ของ Console	CSC	CSC	CSC + CSP
MFA ของ Administrator	CSC	CSC	CSC (เปิดฟีเจอร์)
Credential ใน Guest OS / VM	CSC	–	–
จัดเก็บ Secret / API Key	CSC + CSP (Secret Manager)	CSC	CSP
Rotate Credential	CSC	CSC + CSP	CSP + CSC
ส่ง Password ครั้งแรก	CSC	CSC	CSP
Helpdesk Reset	CSC	CSC	CSP + CSC (Verify)

CSC รับผิดชอบ | CSP รับผิดชอบ | ร่วมกัน (Shared) | ไม่เกี่ยวข้อง

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.6 การจำกัดการเข้าถึงข้อมูล

Information Access Restriction

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — มุมมองผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.3.6 ในบริบทผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

"

ก) CSC ต้อง**ตรวจสอบ**ให้แน่ใจ**ว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบาย**การควบคุมการเข้าถึงและปฏิบัติตามข้อจำกัดดังกล่าว ซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูล CSC ที่เก็บไว้ในบริการ

ตีความ: CSC ต้องทำ 4 ภารกิจหลัก

1. **Access Control Policy**
   นโยบายต้องครอบคลุมข้อมูลบนคลาวด์ทุกประเภท — Public / Internal / Confidential และ PII
2. **แปลงนโยบาย → Configuration**
   บังคับใช้ด้วยกลไก CSP จริง: IAM Role, Bucket Policy, DB Permission, Key Policy
3. **ตรวจสอบการเข้าถึงจริง**
   ผู้ใช้/ระบบเข้าถึงได้เฉพาะที่นโยบายอนุญาต — ใช้ IAM Analyzer/Access Advisor
4. **ทบทวนสิทธิ์ + เก็บหลักฐาน**
   Periodic Access Review พร้อมหลักฐานที่ Sign-off พร้อมตรวจ

ถอดรหัสตัวบทมาตรฐาน — มุมมองผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.6 ในบริบทผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

"

ก) CSP ต้อง**ให้การควบคุมการเข้าถึง**ที่อนุญาตให้กับ CSC **เพื่อจำกัดการเข้าถึง**บริการต่าง ๆ บนระบบคลาวด์ และข้อมูล CSC ที่เก็บไว้ในบริการ

ตีความ: CSP ต้องทำ 4 ภารกิจหลัก

A **Implement กลไก Access Control ที่หลากหลาย**

Identity, Role, Resource Policy, Network ACL ครบทุกระดับ

B **Service Description + Documentation**

เอกสารที่ CSC อ่านแล้วตั้งค่าเองได้ — Whitepaper, API Docs, Hardening Guide

C **บังคับใช้ Tenant Isolation**

ลูกค้า A ไม่สามารถเข้าถึงข้อมูลลูกค้า B ได้ ไม่ว่าโดยตั้งใจหรือผิดพลาด

D **Audit Log**

Log การเข้าถึงข้อมูลที่ CSC ดึงไปวิเคราะห์ได้

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
Access Control Policy (เนื้อหานโยบาย)	CSC	CSC	CSC
IAM / Identity Provider Configuration	CSC	CSC	CSC
การกำหนด Role และ Permission	CSC	CSC	CSC
Resource Policy (Bucket/DB Policy)	CSC	CSC	Shared
Network ACL / Firewall / Security Group	CSC	Shared	CSP
Encryption at Rest (Key Management)	Shared	Shared	CSP
Field/Row-level Security ภายในแอป	CSC	CSC	Shared
Tenant Isolation	CSP	CSP	CSP
MFA / SSO / Conditional Access	CSC	CSC	CSC
Audit Log การเข้าถึงข้อมูล	Shared	Shared	Shared
Periodic Access Review + Revocation	CSC	CSC	CSC
ออกแบบกลไก Platform + ประกาศเปลี่ยนแปลง	CSP	CSP	CSP

CSC รับผิดชอบหลัก CSP รับผิดชอบหลัก Shared / ร่วมรับผิดชอบ

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.7 การใช้โปรแกรมอรรถประโยชน์พิเศษ

Use of Privilege Utility Programs

ข้อกำหนดสำหรับ

CSC | CSP

เมื่อเครื่องมือดูแลระบบกลายเป็นอาวุธของผู้โจมตี

ภัยคุกคามจาก Privileged Utility — สถิติที่น่าสนใจ

Living-off-the-Land (LOTL) — ผู้โจมตีใช้ Utility ที่ติดมากับ OS/Cloud อยู่แล้ว ทำให้ตรวจจับยากและซ่อนตัวได้นาน

82%	+277%	84%
Malware-free Intrusion — อาศัย Tool ในระบบเพื่อกลมกลืนกับกิจกรรมปกติ	การเพิ่มขึ้นของการใช้เครื่องมือ Remote Monitoring and Management (RMM) ในการโจมตี	84% ของการโจมตีครั้งใหญ่ (เหตุการณ์ที่มีความรุนแรงสูง) เกี่ยวข้องกับการใช้ไบนารี Living-off-the-Land
CrowdStrike Global Threat 2026	*Huntress 2026 Cyber Threat Report*	*Bitdefender Labs 2025*

ทำไม Utility Program จึงเป็นเป้าโจมตีอันดับต้น?

เครื่องมือบริการจัดการคลาวด์ที่มักจะถูกนำมาใช้ในการโจมตี และมักจะรอดการตรวจจับไปได้ ตัวอย่างเช่น

- Infrastructure-as-Code tools (e.g. Terraform, Pulumi)
- Kubectl สำหรับจัดการ Kubernetes clusters
- Systems Manager / Session Manager
- CloudShell / Cloud CLI
- Microsoft Graph API
- Entra ID (Azure AD)

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.7 ในบริบทของบริการคลาวด์

CSC — Cloud Service Customer (ผู้ใช้บริการ)

ตัวบทมาตรฐาน

ก) หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ CSC **ต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้**ในสภาพแวดล้อมการประมวลผลบนคลาวด์ และตรวจสอบให้มั่นใจว่าโปรแกรมเหล่านั้น ไม่รบกวนการควบคุมของบริการคลาวด์

จัดทำ	"บัญชี Approved Utility List" — CLI, DB Client, IaC, File Transfer, Forensic/Backup
ประเมิน	เครื่องมือต้อง "ไม่ขัดแย้ง" กับมาตรการ CSP เช่น ไม่ปิด CloudTrail/Audit Log
บันทึก	Audit Trail เชื่อมโยง User → Action ผ่าน Bastion/PAM, SIEM, EDR/MDR
ทบทวน	Process Review เป็นรอบ + Onboarding/Offboarding เมื่อทีมหรือเครื่องมือเปลี่ยน

CSP — Cloud Service Provider (ผู้ให้บริการ)

ตัวบทมาตรฐาน

ก) CSP ต้อง**ระบุข้อกำหนดสำหรับโปรแกรม**อรรถประโยชน์ใด ๆ ที่ใช้ในบริการคลาวด์ CSP ต้องตรวจสอบให้มั่นใจว่าการใช้โปรแกรมอรรถประโยชน์ใด ๆ ที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการรักษาความปลอดภัยนั้น**จำกัดเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น** และต้อง**มีการทบทวนและตรวจสอบการใช้**โปรแกรมดังกล่าวอย่างสม่ำเสมอ

กำหนด	นโยบาย + Utility List ของ Operator/SRE/Support พร้อมระดับสิทธิ์และขอบเขต Tenant
ควบคุม	Hypervisor Console, Storage Admin, Network ACL Override ต้องผ่าน Just-In-Time Approval
บันทึก	Tamper-evident Logging + Customer Notification / Transparency Log
รับรอง	Independent Audit รายไตรมาส + SOC 2 Type II / ISO 27001 / 27017 Attestation

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
Approved Utility Policy ภายในองค์กร	CSC	CSC	CSC
Privileged Utility ของ Operator CSP บน Hypervisor / Control Plane	CSP	CSP	CSP
OS-level Utility (sudo, PsExec, Diagnostic Tools)	CSC	Shared	CSP
Database Admin Utility (mysqldump, pg_dump)	CSC	Shared	CSP
Cloud CLI / SDK (aws, gcloud, az, kubectl)	CSC	CSC	CSC
Bastion / PAM / Privileged Workstation	CSC	Shared	Shared
Logging การเรียก Utility ของผู้ใช้ CSC	CSC	Shared	CSP
Allow-/Block-listing ระดับ Application	CSC	Shared	CSP
Attestation / รายงานตรวจสอบให้ CSC	CSP	CSP	CSP

CSC CSP Shared

ประเภทของ Privileged Utility ที่พบบนคลาวด์

Utility บนคลาวด์ไม่ใช่แค่ .exe — รวม Cloud Shell, IaC, AI Copilot, SaaS Integration และอื่น ๆ

OS-level Tools

High

sudo · runas · PsExec
Diagnostic · Sysinternals

Cloud CLI / Shell

High

aws · gcloud · az · kubectl
Cloud Shell · Console

Config Mgmt / IaC

High

Terraform · Pulumi · Ansible
Helm · Kustomize

Database Admin

High

psql · mysql · mongosh
ETL · Dump Tools

File Transfer / Storage

High

rclone · mc · s3 sync
gsutil · azcopy

Forensic / Recovery

Medium

Memory Dump · Disk Imaging
Live Response · Snapshots

DevOps Agents

High

Pipeline Agents · GitOps
Secret Injection Sidecars

AI Copilots / Agents

New

Cloud AI Assistants
IDE Copilots · Agents

เทคโนโลยีและเครื่องมือสำหรับควบคุม

ตัวอย่างเทคโนโลยีที่นำมาประกอบให้การควบคุม Privileged Utility ทำได้จริงในระดับองค์กร

Identity & Access

PAM · Bastion · JIT/JEA · MFA · Conditional Access
IdP/SSO · Privileged Workstation

Runtime Control

Allow-listing · Code Signing
AppLocker · WDAC · SELinux · AppArmor · eBPF

Audit & Detection

Cloud-native Audit · SIEM
EDR/MDR · CWPP · UEBA

Secret & Crypto

Secrets Manager · Vault
KMS · HSM · BYOK · Customer Lockbox

Policy & Compliance

Policy-as-Code (OPA/Rego, Cedar, Sentinel)
CSPM · Continuous Compliance · SBOM

10 Checks ก่อนใช้ Privileged Utility

ตัวอย่างรายการตรวจสอบรายขั้น ก่อนเรียก Privileged Utility ใน Production

01 INVENTORY
Utility อยู่ใน Approved List

02 ACCESS PATH
ใช้ผ่าน Bastion / PAM แล้ว

03 IDENTITY
Identity ผ่าน MFA + Conditional Access

04 PRIVILEGE
สิทธิ์เป็น JEA + JIT (มีเวลาหมดอายุ)

05 LOGGING
Log ของ Utility เปิดและส่ง SIEM

06 AUDIT
Session Recording ทำงาน

07 APPROVAL
มี Approval ใน ITSM พร้อม Reason Code

08 INTEGRITY
Hash / Signature ตรงกับ Allow List

09 OWNER
Workload Owner รับทราบ + พร้อมตรวจสอบ

10 RECOVERY
แผน Rollback / Revert ชัดเจน

ปัญหาที่พบบ่อย

Approved List ทำครั้งเดียวแล้วลืม · Allow-list กว้างเกินไป · เปิด Log แต่ Retention เพียง 30 วัน · บังคับ Bastion เฉพาะ Production · ลืม Non-human Identity

5.2.3 การควบคุมการเข้าถึง (Access Control)

5.2.3.8 ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย

Secure Log-on Procedures

ข้อกำหนดสำหรับ

CSC | CSP

ภาพรวม: Secure Log-on Procedure ในระบบคลาวด์

ประตูตรวจชั้นแรกของระบบสารสนเทศ — "Identity is the new perimeter"

เป้าหมายหลัก: รับประกันว่า "เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และต้องเป็นบุคคลที่อ้างว่าเป็นจริง ๆ" จึงจะเข้าใช้งานระบบคลาวด์ได้ โดยขั้นตอนพิสูจน์ตัวตนต้องไม่เปิดเผยข้อมูลที่ช่วยผู้บุกรุก และต้องมีกลไกตรวจจับ ตอบสนอง และป้องกันการโจมตีที่พบบ่อย

Auth Z — Authenticate before Authorize

ยืนยันตัวตนทุกครั้งก่อนระบบให้สิทธิ์ใด ๆ — ไม่มีข้อยกเว้น

MIN — Minimal Disclosure

หน้า Log-on ห้ามเผยชื่อบัญชี ชื่อระบบ หรือ Banner ที่ช่วยผู้บุกรุก

RES — Resistance to Common Attacks

ทนต่อ Brute-force, Credential Stuffing, Phishing, MFA Fatigue, MITM

AUD — Auditability

ทุก Event Log-on (สำเร็จ/ล้มเหลว) ต้องบันทึก พร้อม Timestamp + Source IP

RPP — Risk-Proportionate

ระดับความเข้มต้องสมดุลกับความเสี่ยง — บัญชี Privileged เข้มกว่าทั่วไป

TRP — Transparency to Users

ผู้ใช้เห็นเวลา Log-on ล่าสุด ความพยายามที่ล้มเหลว เพื่อตรวจจับเองได้

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.3.8 ในบริบทบริการคลาวด์

CSC — ผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของ **CSC ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ**

1 กำหนดเป็นนโยบาย

Information Security / Access Control Policy ระบุชัดเจนว่าการเข้าสู่ระบบทุกประเภทต้องผ่านกระบวนการที่ปลอดภัย

2 บังคับใช้ทุกกลุ่มผู้ใช้

พนักงาน ลูกจ้าง คู่ค้า ผู้รับจ้าง Admin, Privileged และ Non-human Identity ทุกประเภท

3 ครอบคลุมบัญชีทุกระดับ

Cloud Console, Application, Database, OS, Service Account, API Key, Token — ไม่ใช่แค่ User ทั่วไป

4 กำกับและตรวจสอบ

Access Review, Audit Log Review และรายงานการละเมิดนโยบายเป็นประจำ

CSP — ผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) ในกรณีที่จำเป็น CSP ต้อง**จัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย**สำหรับบัญชีใด ๆ ที่ CSC ร้องขอสำหรับผู้ใช้ที่อยู่ภายใต้การควบคุมของ CSC

1 จัดเตรียม Capability

Cloud IAM, MFA, Federation (SAML/OIDC), Adaptive Auth, Account Lockout, Audit Logging — เป็นฟีเจอร์ในบริการ

2 ตอบสนองคำร้อง CSC

ผ่าน Service Portal, Support Ticket หรือ API ภายใน SLA ที่ตกลงไว้

3 เปิดเผยข้อมูล (Disclosure)

Service Description ระบุฟีเจอร์ มาตรฐานที่รองรับ (SAML 2.0, OIDC, SCIM, FIDO2), Default vs Optional

4 บำรุงรักษาต่อเนื่อง

ติดตามภัยคุกคามใหม่ ปรับปรุงฟีเจอร์ Authentication อย่างทันท่วงที (FIDO2, Passkey, Device Trust)

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
จัดเตรียมฟีเจอร์ MFA / SSO / Federation	CSP	CSP	CSP
ตั้งค่าระดับ Tenant (Enable MFA / Conditional Access)	CSC	CSC	CSC
กำหนด Password Policy ระดับ OS / DB / Middleware	CSC	Shared	CSP
Account Lockout / Rate Limiting	Shared	Shared	Shared
แสดง Warning Banner / Login Notification	CSC	Shared	Shared
ไม่เปิดเผยข้อมูลก่อน Log-on (Username Existence)	Shared	Shared	CSP
จัดเก็บ Authentication Log + Export	Shared	Shared	Shared
Re-authenticate / Step-up เมื่อทำงาน Sensitive	CSC	Shared	Shared

CSC = ผู้ใช้บริการ CSP = ผู้ให้บริการ Shared

ตัวอย่าง Authentication Standard ตามระดับความเสี่ยง

บัญชี Critical ต้องเข้มกว่า Standard — แต่ละ Tier มาตรฐานต่างกันชัดเจน

Tier	ประเภทระบบ	Auth Mechanism	Password Policy	Session
TIER 0 CRITICAL	Cloud Root/Admin, ระบบ CII, ระบบที่มี PII > 5,000 รายการ	FIDO2 / Hardware Token (Phishing-resistant MFA บังคับ)	Password >= 16 ตัว, ตรวจ Compromised, ไม่หมดอายุถ้าใช้ Token	<= 1 ชม., Re-auth ทุก Privileged Action
TIER 1 IMPORTANT	ระบบสารสนเทศหลัก, SaaS ที่มีข้อมูล Confidential	MFA — Time-based OTP / Push with Number Match	Password >= 12 ตัว, ตรวจ Compromised, เปลี่ยนทุก 365 วันถ้าไม่มี MFA	<= 8 ชม.
TIER 2 STANDARD	ระบบสนับสนุนการทำงาน, Internal Tool	MFA แนะนำ, อย่างน้อย SSO ผ่าน Enterprise IdP	Password >= 10 ตัว	<= 24 ชม.

💡 *แนวทาง: อ้างอิง NIST SP 800-63B — เน้น Length (>= 12-16 ตัว) มากกว่า Complexity, ตรวจกับ Compromised Password List ทุกครั้ง*

ข้อผิดพลาดที่พบบ่อย & SIEM Detection Rules ที่จำเป็น

เรียนรู้จากสิ่งที่คนอื่นพลาด + Detection Rule ขั้นต่ำ 9 ประเภท

❌ Common Pitfalls (อย่าทำ)	✓ SIEM Detection Rules ที่ควรมี
✗ เปิด MFA เฉพาะ Admin — ไม่บังคับ User ทั่วไป	✓ Brute-force / Password Spraying (>10 Fail / 5 นาที)
✗ ใช้ SMS OTP เป็น MFA หลัก (NIST ลดเป็น Restricted)	✓ Impossible Travel (2 ตำแหน่งภายในเวลาที่เป็นไปไม่ได้)
✗ ลืม Legacy Auth: POP3 / IMAP / SMTP Basic Auth	✓ Anomalous Sign-in Time (Admin นอกเวลาทำงาน)
✗ Service Account / API Key ไม่มี MFA หรือ Rotation	✓ MFA Fatigue (>5 Prompt / 5 นาที ไม่ Approve)
✗ Token Lifetime ยาวเกินไป (Access > 1 วัน)	✓ New Country Sign-in (ประเทศที่ User ไม่เคยใช้)
✗ Banner ไม่มีผลทางกฎหมาย — ไม่อ้าง พ.ร.บ. คอมฯ	✓ Risky IP (Tor, Botnet, Malware-linked)
✗ ระบบ Reveal User Existence: Password ผิด vs User ไม่มี	✓ Token Theft Indicator (Refresh จาก IP/Device ใหม่)
✗ เก็บเฉพาะ Successful Sign-in — ตรวจไม่พบ Brute-force	✓ Service Account Used by Human (Interactive Sign-in)
✗ Break-glass Account ใน Wiki แทน Vault	✓ Privileged from Untrusted Device (Admin จากเครื่องนอก)

กฎหมายไซเบอร์และมาตรฐานระบบคลาวด์ของประเทศไทย

- **ข้อกำหนดขั้นต่ำตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (ส่วนที่ 2)**
  - การเข้ารหัส (Cryptography)
  - การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)
  - การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)
  - การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)
  - การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)
  - การจัดการผู้ให้บริการภายนอก (Supplier Relationships)
  - การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

5.2.4 การเข้ารหัส (Cryptography)

5.2.4.1 นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส

Policy on the Use of Cryptographic Controls

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — CSC ทำอะไร, CSP ทำอะไร

ISO/IEC 27017:2015 ข้อ 10.1.1 ในภาษาที่อ่านง่าย

CSC — ผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้องใช้**มาตรการควบคุมการเข้ารหัส**สำหรับการใช้บริการระบบคลาวด์ที่**มีความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยง**ที่ได้ระบุไว้ ไม่ว่า CSC หรือ CSP จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม

ข) เมื่อ CSP นำเสนอการเข้ารหัสใดๆ CSC ต้อง**ตรวจสอบข้อมูลที่ CSP จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัส**ดังนี้หรือไม่
- ปฏิบัติตามข้อกำหนดด้านนโยบายของ CSC
- เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่นๆ ที่ใช้โดย CSC
- ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์

1. **มีนโยบายการเข้ารหัสของตนเอง**
   ไม่พึ่งพานโยบายของ CSP เพียงอย่างเดียว — ต้องมี Cryptographic Policy ที่ลงนามโดยผู้บริหาร
2. **ประเมินความเสี่ยงและจำแนกข้อมูล**
   เลือกระดับการเข้ารหัส "ได้สัดส่วนกับความเสี่ยง" ตาม Data Classification
3. **ตรวจสอบ Encryption ของ CSP 3 มิติ**
   ก) ตรงกับนโยบายภายใน ข) เข้ากับ Crypto อื่นที่ใช้ ค) ครอบคลุม Data at Rest + in Transit
4. **การ Verify ต้องเป็นเชิงเทคนิค**
   ไม่ใช่แค่อ่านเอกสาร — ต้องเป็นการประเมินที่บันทึกเป็นหลักฐาน Audit ได้

CSP — ผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลแก่ CSC เกี่ยวกับการเข้ารหัส**เพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคลที่ CSP ประมวลผล นอกจากนี้ CSP ต้อง**ให้ข้อมูลแก่ CSC เกี่ยวกับความสามารถ**ใดๆ ที่ CSP มอบให้ซึ่งสามารถช่วย CSC ในการใช้**การเข้ารหัส**ดังกล่าว

1. **เปิดเผยข้อมูล Encryption ของตน**
   ระบุ Algorithm, Key Length, ผู้จัดการกุญแจ, ผ่าน FIPS 140 หรือไม่ — ครบถ้วนใน Trust Center
2. **จัดเตรียมเครื่องมือให้ CSC ใช้**
   KMS, HSM Service, Encryption SDK, TLS Config — ใช้ Secure-by-Default
3. **ให้ข้อมูลครบเพื่อให้ CSC ตัดสินใจ**
   รวมถึง Limitations เช่น "บริการนี้ไม่รองรับ CMK" หรือ "Algorithm นี้รองรับเฉพาะ Region X"
4. **ความโปร่งใส = หลักฐาน Audit**
   ไม่ใช่แค่ "มีบริการเข้ารหัส" แต่ต้องสื่อสารและเอกสารชัดเจน (Transparency)

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

องค์ประกอบของการเข้ารหัส	IaaS	PaaS	SaaS
นโยบายการเข้ารหัส	CSC	CSC	CSC
เลือก Algorithm / Key Length	CSC	CSC+CSP	CSP (Verify)
Encryption at Rest (Storage)	CSC+CSP	CSP (BYOK)	CSP
Encryption in Transit (External)	CSC+CSP	CSP (Config)	CSP
Encryption in Transit (East-West)	CSC (mTLS)	CSP	CSP
Customer-Managed Key (CMK/BYOK)	CSC	CSC*	CSP*
Key Rotation Schedule	CSC/CSP	CSP+CSC	CSP
Cryptographic Audit Log	CSP/CSC review	CSP/CSC review	CSP (CSC ขอ)
Verify CSP Encryption Compliance	CSC	CSC	CSC

CSC รับผิดชอบหลัก

CSP รับผิดชอบหลัก

รับผิดชอบร่วม
— ระบุใน DPA/MSA

นโยบายการเข้ารหัสไม่อยู่โดดเดี่ยว — เชื่อมโยง 8 ข้อกำหนด

ความสัมพันธ์กับข้อกำหนดอื่นในมาตรฐาน

5.1.1

นโยบายความมั่นคงปลอดภัย

Cryptographic Policy เป็นนโยบายลูก (Subordinate) ต้องสอดคล้องนโยบายแม่

5.1.2.1

บทบาทและความรับผิดชอบ

RACI ของ Crypto ต้อง Map กับ Role Register — Key Custodian ต้องชัด

5.1.3.4

กฎระเบียบ Crypto

คู่กัน — 5.1.3.4 เน้น Legal, 5.2.4.1 เน้น Technical Implementation

5.2.2.2

การบ่งชี้ข้อมูล

Data Classification เป็น Input หลัก — เลือกระดับการเข้ารหัสตาม Class

5.2.3.5

การจัดการ Secret

Cryptographic Key เป็น Secret พิเศษ — เก็บใน HSM / Vault / KMS

5.2.4.2

การจัดการกุญแจ

หมวดเดียวกัน — 5.2.4.1 = "นโยบาย", 5.2.4.2 = "การปฏิบัติ" Key Lifecycle

5.4

Operations Security

Backup ต้อง Encrypt / Log ต้องมี Integrity / Cryptographic Audit แยก

5.5

Communications Security

TLS, IPSec, VPN — บังคับนโยบายการเข้ารหัสกับ Network Layer

7 เสาหลักของกระบวนการ Cryptographic Controls

Process Foundation สำหรับการบริหารจัดการการเข้ารหัสในคลาวด์

Governance

นโยบาย + Steering Committee + Decision Authority สำหรับ Algorithm และ Exception

Risk-based Approach

เลือกระดับ Encryption ตาม Classification และ Risk — ไม่ใช่ "AES-256 ทุกอย่าง"

Cryptographic Inventory

ทะเบียน: ระบบใช้ Algorithm อะไร, Key Length, ที่เก็บกุญแจ, Rotation

Key Lifecycle Mgmt

Generation → Distribution → Storage → Use → Rotation → Archive → Destruction

Separation of Duties

ผู้ใช้กุญแจ ≠ ผู้จัดการกุญแจ ≠ ผู้ตรวจสอบ — ป้องกัน Insider Threat

Monitoring & Audit

Real-time Monitoring + Quarterly Compliance + Annual External Audit

Crypto-agility

เปลี่ยน Algorithm ได้เร็ว + Track Deprecation + Roadmap สู่ Post-Quantum

เทคโนโลยีการเข้ารหัสที่ผู้ปฏิบัติงานต้องรู้จัก

5 ประเภทการเข้ารหัสหลัก + เครื่องมือสำคัญในตลาด

Symmetric

AES-256-GCM (แนะนำ)
AES-128-GCM (Min)
ChaCha20-Poly1305

✗ DES, 3DES, RC4, ECB

Asymmetric / Sign

RSA-2024+ (Min)
RSA-3072 (แนะนำ)
ECDSA P-256/P-384
EdDSA (Ed25519)

Hash

SHA-256/384/512
SHA-3
bcrypt/scrypt/Argon2id

✗ MD5, SHA-1

KDF / MAC

HMAC-SHA-256+
HKDF
PBKDF2 ≥ 600k iters

Post-Quantum

ML-KEM (Kyber)
ML-DSA (Dilithium)
SLH-DSA (SPHINCS+)
(FIPS 203/204/205)

🛠 เทคโนโลยีและเครื่องมือสำคัญ

Cloud KMS
AWS KMS / Azure KV / GCP KMS

Cloud HSM
CloudHSM / Dedicated HSM / FIPS 140-2 L3

External / HYOK
Thales / Entrust / Fortanix DSM

Secret Mgmt
HashiCorp Vault / CyberArk

Confidential Computing
AWS Nitro Enclaves / Intel SGX / AMD SEV-SNP

Service Mesh / mTLS
Istio / Linkerd / Consul Connect

App-level Encrypt
AWS Encryption SDK / Tink / libsodium

CSPM Monitoring
Wiz / Prisma / Defender / Orca

5.2.4 การเข้ารหัส (Cryptography)

5.2.4.2 การจัดการกุญแจ

Key Management

ข้อกำหนดสำหรับ

CSC -

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.4.2 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ระบุกุญแจ**สำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และ**ดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ**

ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดย CSC CSC ต้อง**ขอข้อมูล**ดังต่อไปนี้**เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจ**สำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์
- ประเภทของกุญแจ
- ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัส เช่น การสร้าง เปลี่ยนแปลง หรือปรับปรุง จัดเก็บ หมดอายุการใช้งาน เรียกคืน เก็บรักษา และทำลาย
- ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดย CSC

ค) CSC ต้อง**ไม่อนุญาตให้ CSP จัดเก็บและจัดการกุญแจ**สำหรับการเข้ารหัส**เมื่อ CSC ใช้กุญแจเข้ารหัสของตนเอง**

ก

ระบุกุญแจ + จัดทำขั้นตอน

ต้องทำ 2 สิ่ง: (1) จัดทำ Cryptographic Key Inventory ของแต่ละบริการคลาวด์ — ระบุ ประเภท จำนวน ที่อยู่ และใช้กับข้อมูลใด (2) มี Procedure การจัดการกุญแจที่เป็นเอกสารและบังคับใช้ได้จริง

ข

ขอข้อมูลจาก CSP เป็นลายลักษณ์อักษร

ครอบคลุม: ประเภทกุญแจ (AES-256-GCM, RSA-3072, ECC P-256) / วงจรชีวิตทั้ง 7 ขั้นตอน / ข้อกำหนดเฉพาะของระบบ KMS / ขั้นตอนแนะนำสำหรับ CSC เช่น ความถี่ Rotation, Backup, Audit Log

ค

กฎเหล็ก: CSP ห้ามถือกุญแจของ CSC

เมื่อ CSC เลือกใช้ Customer-managed Key (CMK/BYOK) เพื่อควบคุมกุญแจของตน ต้องไม่ปล่อยให้ CSP เห็นกุญแจ Plaintext — ในทางปฏิบัติคือใช้ External Key Store / HYOK / Hardware HSM ของ CSC เอง

Shared Responsibility ของการจัดการกุญแจ

ใครรับผิดชอบอะไรใน IaaS / PaaS / SaaS — ไล่ทีละกิจกรรมในวงจรชีวิต

กิจกรรม	IaaS	PaaS	SaaS
Key Inventory & Policy Definition	CSC	CSC	CSC
Key Generation (CSP default)	CSP	CSP	CSP
Key Generation (Customer-managed)	CSC	CSC	CSC (ถ้ารองรับ)
Key Storage (HSM / KMS)	CSP	CSP	CSP
Rotation Policy Setting	CSC	CSC	CSP
Rotation Execution	Shared	Shared	CSP
Revocation / Destruction	CSC	CSC	CSC สั่ง / CSP ทำ
Audit Log Generation	CSP	CSP	CSP
BYOK Import	CSC	CSC	มักไม่รองรับ
HYOK / External KMS	CSC	CSC	ไม่รองรับ
Compliance Reporting	CSP	CSP	CSP

CSC = ผู้ใช้บริการคลาวด์ CSP = ผู้ให้บริการคลาวด์ Shared = ทั้งสองฝ่ายร่วมกัน

6 หลักการสำคัญของการจัดการกุญแจ

Foundation Principles — ฝังในทุก KMS Design และ Policy

01 Confidentiality of Key Material

กุญแจต้องไม่ปรากฏ Plaintext ใน Memory / Log / Disk / Network — ต้องอยู่ใน Cryptographic Boundary เสมอ

02 Separation of Duties

ผู้สร้าง / ผู้ใช้ / ผู้ตรวจสอบ ต้องเป็นคนละบุคคล — ป้องกัน Single Point of Compromise

03 Least Privilege

ให้สิทธิ์ใช้ (Encrypt/Decrypt) เท่านั้น — ไม่ใช่ Export หรือ Delete

04 Crypto-agility

เปลี่ยน Algorithm / Key Length ได้โดยไม่กระทบ Application Logic — เตรียมพร้อมสำหรับ PQC

05 Defense in Depth

Hierarchical Key Architecture: DEK → KEK → Root Key — จำกัด Blast Radius เมื่อเกิดเหตุ

06 Auditability

Audit Log แบบ Tamper-evident เก็บอย่างน้อย 1 ปี — รองรับ Compliance และ Forensic

วงจรชีวิตของกุญแจ 7 ขั้นตอน

Key Lifecycle ตาม NIST SP 800-57 และ ISO/IEC 11770

1 Generate
CSPRNG ใน HSM
FIPS 140-2/3

→

2 Distribute
Key Wrapping
RSA-OAEP / AES-KW

→

3 Store
HSM / KMS /
Secure Enclave

→

4 Use
ผ่าน KMS API
App ไม่เห็น Plaintext

→

5 Rotate
Automated ตาม
Cryptoperiod

→

6 Archive
Decrypt-only สำหรับ
ข้อมูลเก่า

→

7 Destroy
Crypto-shredding
+ Certificate

ข้อผิดพลาดที่พบบ่อยในแต่ละขั้นตอน

⚠ **Generate:** ใช้ rand() / math.random() ที่ Entropy ต่ำ — ต้องใช้ /dev/urandom หรือ HSM

⚠ **Store:** Commit Key ลง Git Repository — ใช้ Secret Manager + Pre-commit Hook

⚠ **Distribute:** ส่งกุญแจผ่าน Email / Slack / Plaintext — ต้อง Key Wrapping เท่านั้น

⚠ **Rotate:** ไม่หมุนเพราะกลัวกระทบระบบ — เก็บ Old Key เป็น Decrypt-only แล้ว Rotate ได้

ประเภทของกุญแจที่ใช้ในระบบจริง

Symmetric / Asymmetric / Hierarchical Keys — เลือก Algorithm และ Length ที่เหมาะสม

ประเภทกุญแจ	วัตถุประสงค์การใช้งาน	Algorithm แนะนำ
Symmetric Key	Encrypt/Decrypt ด้วยกุญแจเดียว เร็ว เหมาะข้อมูลปริมาณมาก	*AES-128/256 (GCM, CBC) / ChaCha20-Poly1305*
Asymmetric Key	Public Encrypt / Private Decrypt — Key Exchange, Signature	*RSA-2048/3072/4096 / ECC P-256/P-384 / Ed25519*
Data Encryption Key (DEK)	กุญแจเข้ารหัสข้อมูลจริง หมุนได้บ่อย (Per-object)	*AES-256 / Rotate เร็ว*
Key Encryption Key (KEK)	ใช้ Encrypt DEK — ชั้นกลางของ Envelope Encryption	*AES-256 / Rotate ปีละครั้ง*
Master / Root Key	เข้ารหัส KEK เก็บใน HSM + Dual Control	*AES-256 / RSA-4096 / FIPS 140-3 Level 3+*
Signing Key	ลงนามดิจิทัล — ระบุตัวตน + ความสมบูรณ์ของข้อมูล	*RSA-2048+ / ECC P-256+ / Ed25519*
HMAC / MAC Key	ตรวจสอบ Message Integrity และ Authenticity	*HMAC-SHA256 / HMAC-SHA384*
TLS / Code Signing	เข้ารหัสการสื่อสาร / ลงนาม Software, Container	*RSA-2048+, ECC P-256 / RSA-3072+, ECC P-384*

เลือก Key Management Model ให้เหมาะกับความเสี่ยง

4 รูปแบบสถาปัตยกรรมการจัดการกุญแจเข้ารหัส

Envelope Encryption (Cloud-native KMS)

Application สร้าง DEK / KMS Wrap ด้วย KEK / เก็บ Ciphertext + Wrapped DEK

+ Performance สูง
+ Cost ต่ำ
+ Native integration
- CSP เห็น KEK

ง่ายสุด — เหมาะ Workload ทั่วไป

BYOK (Bring Your Own Key)

CSC สร้าง Key Material ใน On-prem HSM / Wrap ด้วย Public Key ของ CSP / Import เข้า Cloud KMS

+ CSC ควบคุม Origin
+ ตอบ PDPA / PCI-DSS
- CSP เห็นใน Boundary ตน
- Operations ซับซ้อน

เหมาะ: Regulated Data — Audit ได้

HYOK / External KMS (Hold Your Own Key)

External KM ใน DC ของ CSC / Cloud Service เรียกผ่าน XKS / EKM / CSP ไม่เคยเห็น Plaintext Key

+ Sovereign Control เต็มที่
+ ตอบกฎหมายข้ามชาติได้
- Latency สูง
- Cost สูงสุด

เหมาะ: Top-secret / Sovereign Data

Hierarchical Multi-tenant (Root → TMK → DEK)

Root Key ใน HSM (1 ดอก/Region) / Tenant Master Key ต่อลูกค้า / DEK ต่อ Resource

+ Crypto-shred ลูกค้าได้ทันที
+ Blast Radius จำกัด
+ เหมาะ SaaS Multi-tenant
- Design ซับซ้อน

เหมาะ: SaaS Provider

เครื่องมือและมาตรฐานในระบบนิเวศ Key Management

Reference — KMS / HSM / Secret Manager / Standards

Cloud-native KMS

AWS KMS, Azure Key Vault
GCP KMS, OCI Vault
IBM Key Protect, Alibaba KMS

HSM (Cloud / On-prem)

AWS CloudHSM, Azure Dedicated HSM
Thales Luna, Entrust nShield
Utimaco, Marvell, YubiHSM 2

External Key / HYOK

Thales CipherTrust
Fortanix DSM, Entrust KeyControl
Equinix SmartKey

Secret Management

HashiCorp Vault
AWS Secrets Manager
CyberArk Conjur, Doppler

Certificate / PKI

AWS Certificate Manager
Azure KV Certificates, GCP CAS
HashiCorp Vault PKI, Let's Encrypt

มาตรฐานหลักที่ต้องอ้างอิงในการออกแบบและตรวจสอบ

FIPS 140-2/3	NIST SP 800-57	ISO/IEC 11770	PKCS #11	X.509 v3
Crypto Module Level 1-4	Key Management Pt.1-3	Key Management Framework	API สำหรับ HSM/Token	Certificate Format (PKI)

5 หลุมพรางที่พบบ่อยและวิธีแก้

Common Mistakes vs Best Practices

1 Hardcode Key ใน Source Code

X ปัญหา

AWS Access Key, API Token, Database Password ถูก commit ลง Git Public Repository

✓ แนวทาง

ใช้ Secret Manager + Pre-commit Hook (git-secrets, talisman) + Rotate ทันทีเมื่อตรวจพบ

2 ไม่เปลี่ยนกุญแจเพราะกลัวระบบล่ม

X ปัญหา

Key อายุเกิน 3-5 ปี ไม่เคย rotate เพราะ กลัวกระทบ Production

✓ แนวทาง

ใช้ Automated Rotation + เก็บ Old Key เป็น Decrypt-only / Test Rotation ใน Staging ก่อน

3 Single Custodian โดยไม่มี Dual Control

X ปัญหา

Admin คนเดียวเข้าถึง Master Key ได้ — ไม่มี M-of-N Quorum

✓ แนวทาง

ตั้ง Quorum 2-of-3 หรือ 3-of-5 ใน HSM + ใช้ Activation Cards แยกบุคคล

4 Audit Log ไม่ Tamper-evident

X ปัญหา

เก็บ Log ใน Disk ที่ Admin แก้ไขได้ — ไม่มี Integrity Verification

✓ แนวทาง

ส่ง Log ไปยัง SIEM แบบ Write-once / Append-only พร้อม Cryptographic Hash Chain

5 ไม่มีแผน Crypto-agility สำหรับ PQC

X ปัญหา

Application Hardcode RSA / ECC โดย Algorithm Name อยู่ใน Business Logic

✓ แนวทาง

แยก Algorithm จาก Business Logic / ใช้ Algorithm Identifier ใน Metadata

5.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

5.2.5.1 ตำแหน่งของศูนย์ข้อมูล

Data Center Location

ข้อกำหนดสำหรับ

CSC | CSP

ทำไม “ตำแหน่งของศูนย์ข้อมูล” จึงเป็นหัวใจของอธิปไตยข้อมูลไทย

Data Localization • Sovereignty • Business Continuity — กรอบคิดสำหรับ CSC, CSP และผู้ตรวจประเมิน

ข้อกำหนด 5.2.5.1 ในมาตรฐานคลาวด์ ฯ

กำหนดให้ศูนย์ข้อมูลหลัก (Primary DC) ของบริการคลาวด์ต้องตั้งอยู่ในประเทศไทย และศูนย์ข้อมูลสำรอง (DR) ต้องอยู่ในไทยหรือในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้ที่สุด เช่น สิงคโปร์ ฮ่องกง

ประกาศ สกมช. เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลในไทย พ.ศ. 2567

เฉพาะกรณีที่ผลการประเมินและจัดระดับผลกระทบในด้านความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ อยู่ในระดับสูง จึงจำเป็นต้องปฏิบัติตามข้อกำหนด 5.2.5.1 ตามมาตรฐานคลาวด์ ฯ อย่างเคร่งครัด

อธิปไตยข้อมูล

Data Sovereignty
อยู่ใต้กฎหมายไทย

กำกับดูแลได้

Regulatory Oversight
สกมช. ตรวจสอบได้

ลด Latency

Real-time Service
บริการประชาชน

ความต่อเนื่อง

Business Continuity
RTO/RPO ตามเกณฑ์

80%

ของหน่วยงานภาครัฐทั่วโลกจะมีข้อกำหนด Data Localization ภายในปี 2027 (Gartner, 2024)

ภัยคุกคามที่บรรเทาได้

Data Sovereignty Loss • PDPA Cross-border Non-compliance • High Latency • DR Failure • Geopolitical Risk • Audit Limitation

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.5.1 ในบริบทบริการคลาวด์

ตัวบทมาตรฐาน	ความหมายในทางปฏิบัติ (Practical Meaning)
CSC: ก) ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)	เลือกบริการคลาวด์ที่ Region หลักอยู่ในไทย เช่น “Bangkok Region”, “Thailand Central” และยืนยันด้วยเอกสาร Region Attestation จาก CSP เก็บเป็นหลักฐาน Audit
CSP: ก) ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)	ต้องมี DC ดำเนินงานจริงในอาณาเขตไทย ไม่ว่าจะเป็นกรรมสิทธิ์ เช่า หรือ Co-location — และผ่านมาตรฐาน Tier III ขึ้นไป (TIA-942 / Uptime Institute)
CSP: ข) ต้องจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย (Data Localization) หรือ อยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของ CSC ให้มากที่สุด รวมถึงสิงคโปร์และเขตปกครองพิเศษฮ่องกง	เพื่อ DR และ Business Continuity — หาก CSP จัด DR ในไทยไม่ได้ ต้องเลือก Region ใน SEA ที่ Latency ใกล้สุด เช่น Singapore, Hong Kong, Jakarta, KL

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

ความรับผิดชอบ	IaaS	PaaS	SaaS
จัดตั้งและดำเนินงานศูนย์ข้อมูลในไทย	CSP	CSP	CSP
รับรอง Tier ของศูนย์ข้อมูล (TIA-942 / Uptime)	CSP	CSP	CSP
เปิดเผยที่ตั้งทางภูมิศาสตร์ของ Region	CSP	CSP	CSP
จัดให้มี DR Site ใน SEA	CSP	CSP	CSP
เลือก Region ที่ตั้งของ Workload	CSC	CSC	CSP*
กำหนด Data Residency Policy ภายในองค์กร	CSC	CSC	CSC
ตั้งค่า Region Pinning / Data Boundary	CSC	CSC†	CSP‡
จัดเก็บหลักฐานที่ตั้งจาก CSP	CSC	CSC	CSC
ตรวจสอบ Sub-processors และตำแหน่ง	CSC	CSC	CSC
กำกับ DR/BCP ตาม RTO/RPO	CSC+CSP	CSC+CSP	CSP*

** CSC ต้องตรวจสอบและตกลง † บางบริการเท่านั้น ‡ ระบุใน Service Agreement*

Architecture Patterns สำหรับหน่วยงาน CII ไทย

เลือก Pattern A–D ตามระดับความสำคัญของข้อมูลและความสามารถขององค์กร

Pattern A

Single Region in Thailand

Primary:
Thailand Region (multi-AZ)

DR:
AZ ต่างจังหวัดในไทย

เหมาะกับ:
ข้อมูล Top Secret / High Sensitivity

Pattern B

Dual Region Thailand–SEA

Primary:
Thailand Region

DR:
Singapore / Hong Kong

เหมาะกับ:
Workload ที่ต้องการ Geographical Diversity

Pattern C

Hybrid On-premise + Cloud

Primary:
On-premise ในไทย

DR:
Thailand Cloud Region

เหมาะกับ:
องค์กรที่ลงทุน DC ในไทยอยู่แล้ว

Pattern D

Multi-cloud in Thailand

Primary:
CSP A (Thailand)

DR:
CSP B (Thailand)

เหมาะกับ:
ลด Vendor Lock-in / กำกับ Sovereignty

เกณฑ์เลือก Pattern:
ระดับความ Sensitive ของข้อมูล • ความพร้อมของ CSP ใน Thailand Region • RTO/RPO ที่ต้องการ • งบประมาณและ Vendor Risk

Verification Stack — พิสูจน์ว่าข้อมูลอยู่ใน Region ไทยจริง

Layered Evidence: เอกสาร + สัญญา + เทคนิค + Operation — ไม่มี Single Source of Truth

Layer 1 — Certification
ISO 27001/27017/27018/27701 • SOC 2 Type II • TIA-942 Tier

Layer 2 — Contract
Master Service Agreement • DPA • Service Description • SLA

Layer 3 — Technical
Latency Test • IP Geolocation (MaxMind / ipinfo / RIPE) • Traceroute

Layer 4 — Operation
Logs, Console Settings, CSPM Output, Real-time Drift Detection

Auditor Evidence Pack

- ☐ Region Attestation Letter จาก CSP
- ☐ ใบรับรอง ISO ระบุ Scope = Thailand DC
- ☐ DPA ระบุ Primary + DR Region
- ☐ Org Policies / Service Control Policies
- ☐ Sub-processor List ปัจจุบัน
- ☐ Latency Test Report (จาก ISP ไทย)
- ☐ Cloud Asset Inventory พร้อม Tag
- ☐ Exception Register

5.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

5.2.5.2 การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย

Secure Disposal or Reuse of Equipment

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.5.2 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้องร้องขอการ**ยืนยันว่า CSP มีนโยบายและขั้นตอนในการกำจัด**หรือ นำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย

3 + 1 ภาระหน้าที่ของ CSC

1. **ขอ (Request)**
   ขอ Trust Center, Compliance Report, SOC 2 Type II, ISO 27001/27017/27018 Audit Statement ที่ระบุการ Disposal/Reuse
2. **ตรวจ (Review)**
   อ่าน Service Description / SLA / DPA ว่าสอดคล้องกับนโยบายของตน — และทำ Gap Analysis
3. **จัดเก็บ (Retain)**
   เก็บเอกสารเป็น Audit Evidence ขององค์กร พร้อมระบุวันหมดอายุของใบรับรอง
4. **Sanitize ฝั่งตน**
   ลบ Object/DB/Snapshot, Disable + Delete Customer-managed Key (CMK), Sanitize End-user Device

⚖ Key Takeaway

Accountability ทาง PDPA ยังคงอยู่กับ Data Controller (มักเป็น CSC) — "จ้างคนทำ" ไม่ได้แปลว่า "พ้นความรับผิด" ผู้ตรวจประเมินจะมองหา Confirmation Letter + Evidence ที่ระบุว่า CSC "ขอ–ตรวจ–เก็บ" จริง ไม่ใช่แค่ทำสัญญา

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.5.2 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้องตรวจสอบให้แน่ใจว่ามีการเตรียมการสำหรับการ**กำจัดหรือนำทรัพยากร** (เช่น อุปกรณ์ ที่เก็บข้อมูล ไฟล์ หน่วยความจำ) **กลับมาใช้ใหม่อย่างปลอดภัยและทันท่วงที**

ข) เพื่อวัตถุประสงค์ในการกำจัดหรือนำกลับมาใช้ใหม่อย่างมั่นคงปลอดภัย และไม่สามารถกู้คืนข้อมูลกลับมาได้ อุปกรณ์ที่มี**สื่อจัดเก็บข้อมูลที่อาจมีข้อมูลส่วนบุคคลต้องได้รับการปฏิบัติเสมือนว่ามีข้อมูลส่วนบุคคลจริง**

Equipment
Server, Storage Array, Network Gear

Data Storage
HDD, SSD, NVMe, Tape, Optical

Files (Logical)
Objects, DB, Snapshot, Replica, Backup

Memory
RAM, vRAM, Cache, vTPM

หลักการ "Treat as PII"

- **ISO/IEC 27018:2019 ระบุว่า อุปกรณ์ที่ "อาจ" มี PII ต้องได้รับการปฏิบัติเสมือนมี PII จริง**
- ระบบ Multi-tenant ไม่สามารถระบุได้ทันทีว่าสื่อชิ้นไหนเคยถูกใช้โดย CSC ที่จัดเก็บ PII
- CSP จึงต้องใช้มาตรฐานสูงสุด (NIST 800-88 Purge หรือ Destroy) กับสื่อทุกชิ้นโดยไม่แบ่งระดับ
- ครอบคลุม HDD (Degauss/Crypto-erase/Shred), SSD/NVMe (Crypto-erase + Shred), Tape (Degauss/Shred), RAM (Power-off + Zeroing)

ตัวอย่างการกำหนด SLA เพื่อดำเนินการอย่าง "ทันท่วงที"

Reclaim Storage Block	≤ 24 ชั่วโมง
Crypto-erase (Key Deletion)	7–30 วัน pending
Physical Shred ของสื่อ	≤ 72 ชั่วโมง
Issue Certificate of Destruction	≤ 5 วันทำการ

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
Physical media destruction (HDD/SSD shred, degauss)	CSP	CSP	CSP
Hypervisor-level memory zeroing & vDisk wipe	CSP	CSP	CSP
Guest OS / VM data wipe ก่อนปลดประจำการ	CSC	Shared	CSP
ลบ Snapshot / Backup / Replica ที่ CSC สร้าง	CSC	CSC	Shared
Cryptographic Erasure (Customer-managed Key)	CSC	CSC	Shared
Disposal ของ Object / Blob / File ใน Storage	CSC	CSC	Shared
Sanitization ของ End-user Device (Laptop SaaS)	CSC	CSC	CSC
Sub-CSP / Co-location Disposal Oversight	CSP	CSP	CSP
Data Retention & Deletion Policy (Application)	CSC	CSC	Shared
จัดเก็บ Confirmation Letter / Audit Report จาก CSP	CSC	CSC	CSC

Legend

- CSP — ผู้ให้บริการรับผิดชอบหลัก
- CSC — ผู้ใช้บริการรับผิดชอบหลัก
- Shared — รับผิดชอบร่วม

💡 Accountability ทาง PDPA ยังอยู่กับ Data Controller (มักเป็น CSC) ทุกกรณี

เลือกวิธี Sanitize ให้เหมาะกับสื่อ

ตัวอย่าง Matrix: ประเภทสื่อ × วิธีการที่แนะนำ — ตามระดับ Confidentiality

ประเภทสื่อ	Clear (Low)	Purge (Moderate)	Destroy (High/Top Secret)
Magnetic HDD	Overwrite ≥ 1 pass	Crypto-erase / Degauss	Shred (DIN 66399 H-5+)
SSD / NVMe / Flash	Built-in Sanitize Cmd	Crypto-erase (ATA/NVMe Secure Erase)	Crypto-erase + Shred
Magnetic Tape (LTO)	Overwrite full tape	Degauss	Degauss + Shred
Optical (CD/DVD/Blu-ray)	N/A	Shred	Shred (DIN 66399 O-3+)
Volatile Memory (RAM)	Power-off	Power-off + Zeroing	Cold-boot Mitigation + Scrub
Cloud Object/Block Storage	Delete via Console	Crypto-erase (Customer-managed Key)	Crypto-erase + Verify Reclaim Log
Self-Encrypting Drive (SED)	Instant Secure Erase (ISE)	ISE + Verify	ISE + Physical Shred

ความท้าทายเชิงเทคนิคที่ผู้ปฏิบัติงานต้องรู้

7 ข้อผิดพลาด ที่ทำให้ "คิดว่าลบแล้ว" แต่ข้อมูลยังกู้คืนได้

SSD Wear-leveling

Overwriting แบบเดิมไม่รับประกันการทำลายข้อมูลใน Hidden Cell — ต้องใช้ Crypto-erase หรือ Physical Destruction

Snapshot Residue

Snapshot และ Replica อาจค้างอยู่หลัง Volume หลักถูกลบ — ต้องตรวจ Dependency Graph

Cross-region Spread

Cross-region Replication ทำให้ข้อมูลกระจาย — ต้องระบุทุก Region และลบให้ครบ

Immutable Backup

Object Lock / WORM Backup ลบไม่ได้ก่อน Retention หมด — ต้องบันทึก Exception

CMK Disable ≠ Delete

Key ที่ "Disable" บางบริการต้องรอ 7–30 วันถึงจะ Key Material ถูกทำลาย

Multi-tenant Residual

Block Storage อาจมี Residual จาก Tenant ก่อนหน้า — CSP ต้องมี Zero-on-allocation

Cache Layer Lag

CDN, In-memory Cache อาจค้างข้อมูลแม้ Source ถูกลบ — ต้อง Purge cache อย่างชัดเจน

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.1 การจัดการการเปลี่ยนแปลง

Change Management

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.6.1 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) กระบวนการจัดการการเปลี่ยนแปลงของ CSC **ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นจาก CSP**

ตีความ — 4 สิ่งที่ CSC ต้องทำ

1. **มี Change Management Process ของตนเอง**
   เป็นเอกสารและบังคับใช้จริงในองค์กร

2. **รับและประมวลผล Notification จาก CSP**
   Subscription / Webhook

3. **ทำ Impact Analysis ทุกครั้ง**
   ประเมินผลต่อ Application, Data, Compliance, Operation

4. **ตัดสินใจและตอบสนอง**
   Test • Communication • Mitigation • Acceptance • Migration

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.6.1 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลแก่ CSC เกี่ยวกับการเปลี่ยนแปลงในบริการคลาวด์ที่อาจส่งผลเสียต่อบริการคลาวด์** ข้อมูลต่อไปนี้จะช่วยให้ CSC ระบุถึงผลกระทบของการเปลี่ยนแปลงที่อาจมีผลต่อความมั่นคงปลอดภัยสารสนเทศ
- ประเภทของการเปลี่ยนแปลง
- วันที่และเวลาที่วางแผนไว้ของการเปลี่ยนแปลง
- คำอธิบายทางเทคนิคเกี่ยวกับการเปลี่ยนแปลงของบริการคลาวด์และระบบที่เกี่ยวข้อง (Underlying Systems)
- การแจ้งเตือนการเริ่มต้นและการเปลี่ยนแปลงที่เสร็จสมบูรณ์

ข) เมื่อ CSP ให้บริการคลาวด์ที่ขึ้นอยู่กับ**ผู้ให้บริการรายย่อยของ CSP** CSP อาจจำเป็นต้อง**แจ้งการเปลี่ยนแปลง**ที่เกิดขึ้นให้ CSC ทราบ

ตีความ — 5 ประเภทของ Change ที่ CSP ต้องสื่อสาร

STANDARD	NORMAL	EMERGENCY	DEPRECATION	PRICING/TERM
Quarterly Maintenance ที่อยู่ใน Calendar	Major Version Upgrade ที่ต้องผ่าน CAB	Security Patch ที่ต้อง Deploy ทันที	เลิกใช้ Feature / API / Region	เปลี่ยนแปลงที่กระทบ Compliance หรือ Risk

องค์ประกอบของกระบวนการจัดการการเปลี่ยนแปลง

องค์ประกอบที่สามารถปรับให้เหมาะสมกับความเสี่ยงและขนาดองค์กร

CR — Change Request (CR)
บันทึก Scope, Reason, Impact, Rollback, Test Plan

CT — Change Categorization
Standard / Normal / Emergency ตาม Workflow

IA — Impact & Risk Assessment
ประเมินผลต่อ CIA, Compliance, CX, Cost

AU — Authorization / CAB
หลีกเลี่ยง Single Person Approval

TV — Test & Validation
Pre-prod, Security Test, Performance, UAT

IP — Implementation Plan
Sequence, Owner, Rollback Trigger

CP — Communication Plan
ก่อน / ระหว่าง / หลัง Change

PIR — Post-Implementation Review
ทบทวนผล เก็บ Lesson Learned

CC — Change Calendar
Freeze Period, Maintenance Window, Blackout

RE — Records & Evidence
หลักฐานทุกขั้นตอนเพื่อ Audit & Compliance

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
Physical Datacenter / Hardware	CSP	CSP	CSP
Hypervisor / Host OS	CSP	CSP	CSP
Network ใต้ Tenant (Backbone)	CSP	CSP	CSP
Managed Service Platform (DB, Queue)	—	CSP	CSP
Application Logic / Business Function	CSC	CSC	CSP
Guest OS / Middleware ใน VM	CSC	CSP	CSP
Configuration ของ Tenant (IAM, ACL, SG)	CSC	CSC	CSC
Data Schema / Encryption Key (CMK)	CSC	CSC	CSC
รับ Change Notification จาก Sub-CSP	CSP	CSP	CSP
ส่ง Change Notification ให้ CSC	CSP	CSP	CSP
Impact Analysis ต่อระบบของ CSC	CSC	CSC	CSC

CSC = ผู้ใช้บริการคลาวด์ CSP = ผู้ให้บริการคลาวด์ Shared = ร่วมรับผิดชอบ

วงจรชีวิตของ Change — 7 ระยะตามแนว ITIL

ปรับใช้สำหรับคลาวด์ ผ่าน Test/Stage/Prod separation และการสื่อสารหลายฝ่าย

KPI สำคัญในแต่ละระยะ

Change Success Rate ≥ 95% • Change-related Incident ≤ 5% • Unauthorized Change → 0 • Emergency Change ไม่เกิน 10% • Configuration Drift Rate

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.2 การบริหารจัดการความจุ

Capacity Management

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ฝั่ง CSC (ผู้ใช้บริการคลาวด์)

ตีความข้อกำหนด 5.2.6.2 ในบริบทของผู้ใช้บริการคลาวด์

(ก) ความสอดคล้องของ Capacity กับความต้องการ

ตัวบทมาตรฐาน

ก) CSC ต้อง**ตรวจสอบ**ให้แน่ใจ**ว่าขีดความสามารถของทรัพยากร**ที่ตกลงกันไว้ในบริการคลาวด์นั้น**ตรงตามข้อกำหนดของ CSC**

ตีความ — 2 สิ่งที่ CSC ต้องทำ

1. **กำหนดความต้องการของระบบงานให้ชัด**
   Resource ที่ต้องใช้, Peak Load, Response Time ที่ยอมรับได้
2. **ตรวจสอบ Tier/SLA ของ CSP**
   ให้ตอบสนองความต้องการ โดยเฉพาะ Hard Limits และ Quota

(ข) Monitoring + Forecasting อย่างต่อเนื่อง

ตัวบทมาตรฐาน

ข) CSC ต้อง**ตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการ**ด้านขีดความสามารถของทรัพยากรของบริการคลาวด์เพื่อให้มั่นใจในประสิทธิภาพของบริการคลาวด์เมื่อเวลาผ่านไป

ตีความ — Forecast 3 ระยะ

Short	**ระยะสั้น**	Day / Week — ตอบสนอง Peak ประจำ
Mid	**ระยะกลาง**	Month / Quarter — Budget Cycle
Long	**ระยะยาว**	Year+ — Trend, Forecast

ถอดรหัสตัวบทมาตรฐาน — ฝั่ง CSP (ผู้ให้บริการคลาวด์)

ตีความข้อกำหนด 5.2.6.2 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้องตรวจสอบขีดความสามารถของทรัพยากรทั้งหมดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการขาดแคลนทรัพยากร

ตีความสิ่งที่ต้องทำ

01 Monitor Total Capacity

Aggregate ของทุก Tenant รวมกัน — Compute Pool, Storage Pool, Network และ Control Plane Capacity — 24×7

02 Monitor per-Tenant

ป้องกัน Noisy Neighbor — Isolate CPU, Memory, IOPS, Bandwidth เพื่อไม่ให้ Tenant รายเดียวกระทบรายอื่น

03 Capacity Procurement

เตรียม Buffer Capacity และจัดหา/ติดตั้งฮาร์ดแวร์ตาม Lead Time ของ Server / Storage / Network Equipment

04 Disclose to CSC

เผยแพร่ Service Quotas / Limits ทั้ง Soft & Hard Limit ผ่าน Documentation / Trust Center / Compliance Portal

⚠ ข้อสังเกตสำคัญ การขาดแคลนความจุ ถูกนิยามใน ISO/IEC 27017 ว่าเป็น 'สาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ' ไม่ใช่แค่ปัญหา Operations

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

CSC รับผิดชอบหลัก | CSP รับผิดชอบหลัก | ร่วมรับผิดชอบ (Shared)

กิจกรรม / Layer	IaaS	PaaS	SaaS
กำหนดความต้องการความจุของระบบงาน	CSC	CSC	CSC
เลือก Service Tier / Instance Size / Plan	CSC	CSC	CSC
Monitor การใช้งานที่ระดับ Workload	CSC	CSC	Shared
ตั้งค่า Auto-scale / Scale-out / Scale-in	CSC	Shared	CSP
จัดการ Storage Capacity (Volume / DB)	CSC	Shared	CSP
Forecasting & Capacity Planning	CSC	CSC	CSC
ขอเพิ่ม Service Quota / Soft Limit	Shared	Shared	Shared
Monitor Total Platform Capacity	CSP	CSP	CSP
Underlying Infra (Compute/Storage Pool)	CSP	CSP	CSP
เผยแพร่ Service Quotas ให้ CSC	CSP	CSP	CSP
Capacity Planning ของ DR / Cross-Region	CSC	Shared	Shared

องค์ประกอบของกระบวนการ Capacity Management

กระบวนการตาม ITIL 4 ประกอบด้วย 6 ส่วนที่ทำงานเชื่อมโยงกัน

01 Demand Management

รับและวิเคราะห์ความต้องการ Capacity จากธุรกิจ ทั้งปัจจุบันและที่คาดการณ์

Business Capacity Forecasting

02 Capacity Planning

แปลความต้องการเป็นแผนการจัดเตรียมทรัพยากร — Type, ปริมาณ, Timeline, งบประมาณ

Quarterly / Annual Plan

03 Capacity Monitoring

ติดตามการใช้งานจริง เทียบกับ Plan และ Threshold ที่กำหนด

Service & Component Monitoring

04 Performance Analysis

วิเคราะห์ Bottleneck ระบุปัญหา Performance จาก Capacity Constraint นำไปสู่ Tuning

USE Method · SLO/SLI

05 Capacity Adjustment

ปรับขนาด / Quota / Tier ตามผล Monitor — Manual, Auto-scaling, Reserved

HPA · VPA · Auto-scale

06 Reporting & Review

รายงานสถานะให้ Stakeholders + ทบทวนแผนเป็นระยะ

Monthly Review · QBR

ประเภทของ Capacity ในระบบคลาวด์ — มากกว่าแค่ CPU/Memory

ติดตามครอบคลุมทุกมิติของ Capacity ไม่ใช่เพียงสิ่งที่คุ้นเคยจาก On-premise

01

Compute

CPU, vCPU, Memory, Container Limit, GPU/TPU

02

Storage

Volume Size, Object GB/TB, IOPS, Throughput, Snapshot

03

Network

Bandwidth, Connections, PPS, NAT Gateway, LB Limit

04

API / Control Plane

API Calls/sec, Throttling Rate, Resources/Region

05

Identity

IAM Users, Roles, Federated Sessions, OAuth Tokens

06

Service-specific

Lambda Concurrent, RDS Connections, S3 Bucket, State Tx

07

Backup & Recovery

Backup Storage, Snapshot Count, Backup Window, Restore

08

Logging & Telemetry

Log Ingestion, Log Storage, Metric Cardinality, Trace

09

Security

WAF Rules, NSG/SG Rules, Certificates, KMS Ops/sec

10

Cost / Budget

Monthly Budget, Dept/Project Budget, Reserved Commitment

เครื่องมือและเทคโนโลยีสำคัญ (Vendor-Neutral)

แบ่งตามหมวด — ผู้ปฏิบัติงานเลือกตาม Architecture และ Maturity ขององค์กร

Cloud-native Monitoring

เครื่องมือพื้นฐานพร้อมแพลตฟอร์ม — Metric, Alert, Dashboard

ตัวอย่าง

- AWS CloudWatch
- Azure Monitor
- GCP Operations
- Alibaba CloudMonitor

Quota Management

ตรวจสอบและขอเพิ่ม Quota ของบริการต่าง ๆ

ตัวอย่าง

- AWS Service Quotas
- Azure Subscription Limits
- GCP Quotas

Multi-cloud Observability

รวม Metric / Log / Trace จากหลาย Cloud ในที่เดียว

ตัวอย่าง

- Datadog
- New Relic
- Dynatrace
- Splunk
- Grafana Cloud

FinOps & Cost

เชื่อม Capacity เข้ากับ Cost

ตัวอย่าง

- AWS Cost Explorer
- Azure Cost Mgmt
- CloudHealth
- Apptio
- Vantage

Auto-scaling

ขยาย/ลดทรัพยากรอัตโนมัติตาม Demand

ตัวอย่าง

- AWS Auto Scaling Group
- Kubernetes HPA/VPA
- Cluster Autoscaler
- KEDA (Kubernetes Event-driven Autoscaling)
- Karpenter

Capacity Planning

ทำ Forecasting และ Right-sizing สำหรับ Workload

ตัวอย่าง

- VMware vRealize
- Densify
- Spot.io
- Cast.ai

Infrastructure as Code

บันทึก Capacity Config ในรูป Code — Auditable

ตัวอย่าง

- Terraform
- CloudFormation
- Azure Bicep
- Pulumi
- Crossplane

Load / Capacity Testing

Validate Capacity Plan ก่อน Go-live

ตัวอย่าง

- k6
- Locust
- JMeter
- Gatling
- Tsung

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.3 การสำรองข้อมูล

Information Backup

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.6.3 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) ในกรณีที่ CSP มีความสามารถในการสำรองข้อมูลซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ CSC ต้องขอข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลจาก CSP นอกจากนี้ CSC ต้องทำการ**ตรวจสอบเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดในการสำรองข้อมูล**หรือไม่

ข) CSC มีหน้าที่รับผิดชอบในการ**ดำเนินการสำรองข้อมูลเมื่อ CSP ไม่ได้ให้บริการนี้**

กรณีที่ 1 — CSP มีบริการ Backup

1 ขอ Specifications

เป็นลายลักษณ์อักษร — Service Description, Trust Portal, SLA

2 เปรียบเทียบ Backup Spec กับ Backup Requirement

RTO/RPO, Retention, ความถี่, Encryption, Storage Location

3 บันทึก Gap Analysis

ระบุ Gap ที่เหลือพร้อมแผนเสริม เช่น Backup ซ้ำใน Region/Account อื่น

กรณีที่ 2 — CSP ไม่ให้บริการ Backup

1 CSC ต้องสำรองเอง

Self-Backup โดยใช้เครื่องมือของตน

2 เลือกเทคโนโลยีให้เหมาะ

Backup as a Service · Snapshot/Export ของ CSP · Backup Software ใน Workload

3 จัดทำหลักฐานครบ

นโยบาย · ขั้นตอน · Schedule · Log · Restore Test · Integrity Verification

⚠ Auditor มักพบ Finding เมื่อ CSC "เชื่อ" CSP โดยไม่ขอเอกสาร — Replication / HA / Snapshot ของ CSP ไม่ใช่ Backup เสมอไป

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.6.3 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลจำเพาะของความสามารถในการสำรองข้อมูล**แก่ CSC ข้อมูลจำเพาะควรมีข้อมูลต่อไปนี้ตามความเหมาะสม
- ขอบเขตและกำหนดการของการสำรองข้อมูล
- วิธีการสำรองข้อมูลและรูปแบบข้อมูล รวมถึงวิธีการเข้ารหัส หากมีความเกี่ยวข้อง
- ระยะเวลาเก็บรักษาข้อมูลสำรอง
- ขั้นตอนการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง
- ขั้นตอนและระยะเวลาที่เกี่ยวข้องกับการกู้คืนข้อมูลจากการสำรองข้อมูล
- ขั้นตอนในการทดสอบความสามารถในการสำรองข้อมูล
- สถานที่จัดเก็บข้อมูลสำรอง

ข) CSP ต้อง**ให้บริการการเข้าถึงข้อมูลสำรองที่ปลอดภัยและแยกออกจากกัน** หากบริการดังกล่าวมีการนำเสนอให้ CSC

Scope & Schedule
Resource ที่ครอบคลุม, ความถี่ Daily/Hourly, Backup Window

Method & Format
Full/Incremental/Snapshot · Raw/Native DB/Object · Compression

Encryption
AES-256-GCM · TLS 1.2+ · Default/CMK/BYOK Key Management

Retention
Default Retention · Configurable Range · Compliance Mode

Integrity Verification
Checksum/Hash · Frequency · Failure Notification Channel

Restore Procedure & SLA
Self-service หรือ CSP · Estimated Time · Granularity File/Volume

Test Procedure
ความถี่ที่ CSP ทดสอบ · วิธีที่ CSC ทดสอบได้ · รายงานที่เข้าถึงได้

Storage Location
Region · Country · Cross-Region · Data Sovereignty

🔒 นอกจากนี้ CSP ต้องออกแบบให้ Backup ของลูกค้าแต่ละราย "แยกออกจากกัน" (Logical Separation) — Tenant Isolation + KMS Key แยก + RBAC + MFA + Audit Log

ตาราง Shared Responsibility — การสำรองข้อมูลแยกตาม Service Model

ใครรับผิดชอบอะไรในแต่ละชั้น IaaS / PaaS / SaaS — อ้างอิง ISO/IEC 17789 และ 27017

CSC ผู้ใช้บริการ — รับผิดชอบหลัก | CSP ผู้ให้บริการ — รับผิดชอบหลัก | Shared ร่วมรับผิดชอบ — ต้องตกลง | — ไม่เกี่ยวข้องโดยตรง

กิจกรรม / Layer	IaaS	PaaS	SaaS
Backup Policy & RTO/RPO ของข้อมูลตน	CSC	CSC	CSC
จัดเก็บข้อมูลใน Workload (OS, DB, File)	CSC	Shared	CSP
Backup ของ Hypervisor / Hardware / Infra	CSP	CSP	CSP
Backup ของ Managed Service (DBaaS, Storage)	CSC	Shared	CSP
Backup ของ Application Data ใน SaaS	—	—	Shared
Backup ของ Configuration / IaC	CSC	CSC	CSC
Backup ของ Identity และ Access Policy	CSC	CSC	Shared
Encryption Key Management สำหรับ Backup	Shared	Shared	Shared
Cross-Region / Cross-Account Backup	CSC	Shared	CSP
Immutable / Air-gapped Backup	CSC	Shared	Shared
Integrity Verification ของ Backup	Shared	Shared	CSP
Restore Test (กู้คืนทดสอบ)	CSC	Shared	Shared
Backup Retention & Deletion (PDPA)	CSC	Shared	Shared
Audit Log การเข้าถึง Backup	Shared	Shared	CSP
Backup Specifications Disclosure	CSP	CSP	CSP

หมายเหตุ: รายละเอียดต้องอ้างอิงสัญญาและ Service Description ของ CSP แต่ละราย — ต้องเป็นลายลักษณ์อักษร

ประเภทและรูปแบบเทคโนโลยี Backup ในระบบคลาวด์

Technical Perspective — เลือกประเภทให้สอดคล้อง RTO/RPO และความสำคัญของระบบ

Full

สำรองข้อมูลทั้งหมดในแต่ละรอบ — ใช้พื้นที่มากแต่ Restore ง่ายสุด

Weekly Full Backup ของ DB

Incremental

สำรองเฉพาะข้อมูลที่เปลี่ยนตั้งแต่ Backup ครั้งล่าสุด

Daily Incremental หลัง Weekly Full

Differential

สำรองข้อมูลที่เปลี่ยนตั้งแต่ Full Backup ครั้งล่าสุด

Daily Differential สำหรับ App Server

Snapshot

จุดอ้างอิงในเวลา โดยไม่ Copy ข้อมูลเต็ม (Copy-on-Write)

EBS Snapshot, Azure Disk Snapshot

Replication / CDP

ส่งข้อมูลไปปลายทางอย่างต่อเนื่อง — RPO ใกล้ 0

DBaaS Cross-Region Replication

App-consistent

Quiesce Application ก่อน Backup เพื่อให้ State สมบูรณ์

VSS-aware, DB-quiesced Snapshot

Crash-consistent

Backup ระดับ Block/Volume โดยไม่ Quiesce App

Volume Snapshot ทั่วไป

Immutable / WORM

Backup ที่ห้ามแก้ไข/ลบ ภายในช่วง Retention

Object Lock, Vault Lock

Air-gapped

Backup ที่ตัดขาดทางตรรกะ/กายภาพจาก Production

Offline Tape, Separate Account/Region

BaaS / SaaS Backup

บริการ Backup จาก Third-party บนคลาวด์

Veeam BaaS, Druva, OwnBackup

มาตรฐานและกรอบที่เกี่ยวข้อง — กฎ 3-2-1-1-0 และ Encryption Standards

หลักคิดสำคัญที่ผู้ปฏิบัติงานต้องเข้าใจและสามารถใช้สื่อสารต่อ Stakeholder

หลัก 3-2-1-1-0

3 Copies
ข้อมูลต้นฉบับ + Backup สอง Copy

2 Media Types
เก็บอย่างน้อย 2 รูปแบบเช่น Disk + Object Storage

1 Offsite
อย่างน้อย 1 Copy อยู่นอก พื้นที่ Production / Region

1 Immutable
อย่างน้อย 1 Copy เป็น Immutable / Air-gapped

0 Errors
ผ่าน Integrity และ Restore Test โดยไม่มีข้อผิดพลาด

Standards Reference

Encryption Algorithm
AES-256 GCM/CBC (At-rest), TLS 1.2+ (In-transit)

Hashing & Integrity
SHA-256/512 สำหรับ Checksum, HMAC สำหรับ Authentication

Key Management
KMIP, NIST SP 800-57, FIPS 140-2/3 Level 2-4 สำหรับ HSM

Backup Format
OVF, VMDK, RAW, QCOW2 · DB Dump · Object Format Parquet/Avro

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.4 การบันทึกเหตุการณ์

Event Logging

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.6.4 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**จัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์**และ**ตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนด**เหล่านั้นหรือไม่

Key Words

DEFINE

นิยามเหตุการณ์ที่ต้องบันทึก

REQUIREMENTS

กำหนดข้อมูลในแต่ละ log

VERIFY

พิสูจน์ว่าบริการทำได้จริง

ถอดรหัสในทางปฏิบัติ — CSC ต้องทำ 4 ขั้นตอน

1. **ระบุเหตุการณ์ที่ต้องบันทึก**
   เช่น Login, IAM change, Privileged action, Data access, Configuration change
2. **กำหนดรายละเอียดของข้อมูล**
   timestamp · user id · source IP · action type · resource id · result/status
3. **กำหนดระยะเวลาเก็บ**
   พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ≥ 90 วัน
4. **ตรวจสอบให้ได้ว่าทำได้จริง**
   ใช้ Service Description · SOC2/ISO 27017 Report · Contract Schedule · ทดสอบจริง

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.6.4 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ผู้ใช้บริการสามารถบันทึกเหตุการณ์**

ข) ในกรณีที่เป็นไปได้ **บันทึกเหตุการณ์ควรบันทึกว่าข้อมูลส่วนบุคคลได้รับการเปลี่ยนแปลงหรือไม่** (เพิ่ม แก้ไข หรือลบ) จากเหตุการณ์นั้น และ**โดยใคร** (Audit Log) ในกรณีที่มีผู้ให้บริการหลายรายเข้ามาเกี่ยวข้องในการให้บริการจากหลากหลายประเภทบริการของสถาปัตยกรรมอ้างอิงประมวลผลคลาวด์ อาจมีบทบาทที่แตกต่างหรือแบ่งปันกันในการปฏิบัติตามข้อนี้

1

PROVIDE

จัดให้มีเครื่องมือ

Management Activity Log · Data Access Log · Export ออกไปยัง storage ของลูกค้า

2

DISCLOSE

เปิดเผยขอบเขต

ระบุว่าฟีเจอร์ใดบันทึกเหตุการณ์ใด ระดับใด · schema · retention

3

AUDIT PII

Operator Audit Log

เมื่อ CSP สัมผัส PII ต้องบันทึก เพิ่ม/แก้ไข/ลบ พร้อมระบุตัวบุคคล

4

DELIVER

เปิดเผยให้ลูกค้า

เมื่อมีคำขออย่างชอบธรรม ต้องส่งมอบ audit log แก่ CSC ได้

Shared Responsibility — ใครรับผิดชอบ Log ในแต่ละชั้น

ขอบเขตเปลี่ยนตาม Service Model · IaaS · PaaS · SaaS

ชั้นของระบบ (Layer)	IaaS	PaaS	SaaS
Physical / Hypervisor logs	CSP	CSP	CSP
Network fabric / VPC fabric	CSP	CSP	CSP
Control Plane / IAM log	CSP จัดให้ · CSC เปิดและเก็บ	CSP จัดให้ · CSC เปิดและเก็บ	CSP จัดให้ · CSC review
VPC Flow / Network log	CSC	Shared	CSP
Guest OS / Container log	CSC	CSP managed	CSP
Application log	CSC	CSC	CSP
Application audit (PII)	CSC	CSC	CSP จัดให้ · CSC review
Data Access log	CSC	Shared	CSP
Centralized SIEM	CSC	CSC	CSC (อาจใช้ของ CSP)
Log Retention & Immutability	Shared	Shared	CSP (option ให้ CSC)

CSP รับผิดชอบ CSC รับผิดชอบ Shared

6 องค์ประกอบของกระบวนการบันทึกเหตุการณ์ที่ดี

Policy · Catalog · Architecture · Operations · Protection · Continuous Improvement

01

P

Policy & Standards

นโยบายระดับองค์กร (Logging Policy) ระบุขอบเขต บทบาท และระยะเก็บ

02

C

Catalog of Events

บัญชีเหตุการณ์ที่ต้องบันทึก แยกตามประเภทระบบและประเภทข้อมูล

03

A

Architecture & Pipeline

สถาปัตยกรรม Log แบบรวมศูนย์ พร้อม schema และ pipeline กลาง

04

O

Operations

Log review, alert handling, การ rotate และ archive อย่างเป็นวงจร

05

P

Protection

ป้องกัน log จากการถูกแก้ไข ลบ หรือเข้าถึงโดยมิชอบ — Immutable

06

I

Continuous Improvement

KPI · Coverage · MTTD · Tune Use Case · ทบทวนปีละครั้ง

ประเภทของ Log และเครื่องมือ

รู้จักประเภทของ Log · เลือก Tool ให้เหมาะกับขนาดและงบ

8 ประเภท Log ที่ต้องรู้จัก

- **Cloud Management/Activity** · API call · IAM change · resource create/update
- **Identity / Sign-in** · Authn success/failure · MFA · conditional access
- **Network Flow** · VPC Flow · NSG Flow · ปริมาณและทิศทางทราฟฟิก
- **OS / Container / Pod** · Syslog · Windows Event · Kubernetes audit · stdout
- **Application** · Business event · error · warning · debug
- **Application Audit** · Approve/Reject · view record · export data
- **Data Plane / Object Access** · Object access · DB query log · BigQuery audit
- **Security Service** · WAF · IDS/IPS · EDR/XDR · CASB · DLP

เครื่องมือสำคัญในตลาด

- **Cloud-native logging** · CloudWatch · Azure Monitor · GCP Logging
- **Cloud-native audit** · CloudTrail · Activity Log · Cloud Audit Logs
- **SIEM** · Splunk · Sentinel · Chronicle · Elastic · QRadar · Wazuh
- **SOAR** · Automation playbook สำหรับ Incident Response
- **Log Shippers** · Fluent Bit · Fluentd · Logstash · Filebeat · Vector
- **Immutable Storage** · S3 Object Lock · Azure Immutable Blob · GCS Object Lock
- **Observability Pipeline** · Cribl · Vector · Tenzir — route/mask/dedup ก่อนเข้า SIEM
- **Cloud-native SIEM** · Microsoft Sentinel · Chronicle SIEM · Datadog Cloud SIEM

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.5 การปกป้องข้อมูลในบันทึกเหตุการณ์

Protection of Log information

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.6.5 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์ เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึง**ต้องมีมาตรการ** เช่น การควบคุมการเข้าถึง **เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์**ที่ตั้งไว้เท่านั้น

ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ใน**บันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด** (Log Retention) และเอกสารระบุไว้

(ก) ปกป้องตามวัตถุประสงค์

Log อาจมี PII → ต้องมี Access Control ให้ใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น

1. **จำแนกประเภท Log**
   ระบุว่า Log ใดมี PII / ข้อมูลลับ / Log ทั่วไป
2. **กำหนด Role + Least Privilege**
   SOC Analyst, DPO, Auditor — ไม่ใช่ทุกคน
3. **ระบุวัตถุประสงค์ของ Log**
   Security / Troubleshooting / Compliance
4. **ห้ามใช้นอกวัตถุประสงค์**
   เช่น ใช้ Log ติดตามพนักงาน — ต้องมีกฎหมายรองรับ

(ข) ลบเมื่อครบกำหนด (อัตโนมัติ)

ต้องมีขั้นตอนลบ Log เมื่อครบ Retention — ดีที่สุดคือเป็นอัตโนมัติ + มีเอกสารกำกับ

1. **Log Retention Schedule**
   ระบุประเภท Log + ระยะเวลา + เหตุผลตามกฎหมาย
2. **Lifecycle Policy อัตโนมัติ**
   ลบเมื่อหมดเวลา — ไม่พึ่งคนกดลบ
3. **ตรวจสอบยืนยันว่าลบจริง**
   Storage Metric + Deletion Report จากระบบ
4. **Audit Trail ของการลบ**
   Meta-log ของ DeleteObject + Approval Record

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

Layer / กิจกรรม	IaaS	PaaS / SaaS
Physical Infra & Hypervisor Log	**CSP**	**CSP**
Cloud Control-plane Audit Log	**CSP ผลิต / CSC กำหนดสิทธิ์**	**CSP ผลิต / CSC กำหนดสิทธิ์**
OS-level Log บน VM	**CSC**	**CSP (SaaS) / ร่วม (PaaS)**
Application Log	**CSC**	**CSC (PaaS) / CSP (SaaS)**
Database Audit Log	**CSC**	**CSP เปิดให้ดู, CSC ตั้ง Retention**
Network Flow Log	**CSC เปิดเอง + กำหนดสิทธิ์**	**CSP จัดให้ผ่าน Service Logs**
กำหนด Retention Period	**CSC (ใต้ค่าสูงสุดของ CSP)**	**CSC (ใต้ค่าสูงสุดของ CSP)**
ลบ Log อัตโนมัติ	**CSC ตั้ง Lifecycle**	**CSP จัดให้, CSC กำหนดพารามิเตอร์**
Tamper-proof (Object Lock/WORM)	**CSC เปิด Object Lock**	**CSP จัดให้, CSC ตรวจสอบ**

CSP รับผิดชอบ **CSC รับผิดชอบ** **ร่วมรับผิดชอบ (Shared)**

หลักการพื้นฐานการปกป้องข้อมูลในบันทึกเหตุการณ์

5 หลักการ + 6 องค์ประกอบของกระบวนการที่ดี

5 หลักการสำคัญ

1 Purpose Limitation

ใช้ Log ตามวัตถุประสงค์ที่ระบุไว้เท่านั้น (PDPA)

2 Least Privilege Access

เข้าถึง Log น้อยที่สุดเท่าที่จำเป็น

3 Integrity Protection

ห้ามแก้ Log โดยไม่ทิ้งร่องรอย

4 Storage Limitation

ลบเมื่อหมดความจำเป็น (PDPA)

5 Account ability

Meta-log ของการเข้าถึงและการลบ Log เอง

องค์ประกอบของกระบวนการที่ดี (6 อย่าง)

- 1) Log Inventory & Classification
- 2) Log Retention Schedule
- 3) Access Control Matrix
- 4) Integrity & Tamper-evidence
- 5) Disposal Procedure
- 6) Review & Continual Improvement

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.6 บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน

Administrator and Operator Logs

ข้อกำหนดสำหรับ

CSC -

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.6.6 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) หากมีการให้สิทธิพิเศษให้แก่ **CSC การใช้สิทธิพิเศษนั้นต้องมีการบันทึกเหตุการณ์และ**ประสิทธิภาพของ**การดำเนินการ**เหล่านั้น
CSC ต้องพิจารณาว่าความสามารถในการบันทึกเหตุการณ์ที่ CSP จัดหาให้นั้นเหมาะสมหรือไม่ หรือ **CSC ต้องใช้ความสามารถในการบันทึกเหตุการณ์เพิ่มเติมหรือไม่**

ตีความข้อกำหนด

01

กรณี CSP "สิทธิ์ Admin" กับ CSC

เมื่อ CSP ส่งมอบสิทธิ์พิเศษ เช่น admin tenant, root บน VM — CSC ต้อง log การใช้สิทธิ์นั้น พร้อม performance ของแต่ละ operation (สำเร็จ/ล้มเหลว เวลา)

02

CSC ต้องประเมิน Native Logging

CSC ต้องตรวจสอบว่า logging built-in ของ CSP (เช่น CloudTrail, Activity Log, Audit Log) เพียงพอกับความเสี่ยงและข้อกำหนดทางกฎหมายขององค์กรหรือไม่

03

ถ้าไม่พอ — เสริม Logging เอง

ลงทุนเพิ่ม เช่น OS-level audit (auditd / Sysmon), EDR, third-party SIEM agent หรือเปิด feature ของ CSP ที่เก็บค่าบริการเพิ่ม เพื่อปิด gap ของการเก็บหลักฐาน

คำสำคัญ — Privileged Operation · Performance · Determine · Additional Logging Capabilities

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
Hypervisor / Hardware Admin Activity	CSP	CSP	CSP
Cloud Management Plane (API / Console)	Shared	Shared	Shared
Guest OS / VM-level Admin (root, sudo, RDP)	CSC	N/A (CSP managed)	N/A
Database Admin (DDL / DML Privileged)	CSC	Shared	CSP เปิดเผยรายงาน
Application-level Admin (Tenant, RBAC)	CSC	CSC	Shared
Log Retention & Archival	CSC	Shared	Shared
Log Integrity Protection	CSC + CSP (ตามชั้น)	Shared	CSP
Log Analysis & Alerting	CSC	CSC	CSC ใช้ log จาก CSP

CSC รับผิดชอบ | CSP รับผิดชอบ | Shared / แบ่งร่วม

*N/A = ไม่เกี่ยวข้องในชั้นนี้ของ Service Model

เครื่องมือเชิงเทคนิค — 10 ประเภทเทคโนโลยีที่ต้องรู้จัก

ทำงานร่วมกันเป็นชั้นๆ ตั้งแต่ Cloud Plane · OS · DB · Identity · Storage · Analytics

CA — CLOUD AUDIT LOG (Management Plane)

API call · resource change จาก console/CLI/SDK

AWS CloudTrail · Azure Activity Log · GCP Cloud Audit Logs · OCI Audit · Huawei CTS

ID — IAM / IDENTITY PROVIDER LOG

Login · MFA challenge · role assumption

Azure AD/Entra Sign-in · IAM Access Analyzer · Okta System Log

OS — OS-LEVEL AUDIT

sudo · exec · file access ที่ guest OS

Linux auditd · Windows Event Log (Security) · Sysmon · OSSEC

DB — DATABASE ACTIVITY MONITORING (DAM)

DDL/DML ของ privileged user

PostgreSQL pgaudit · MySQL audit plugin · Imperva · IBM Guardium

PAM — PRIVILEGED ACCESS MGT (PAM)

Centralize credential และ session

CyberArk · BeyondTrust · Delinea HashiCorp Vault · AWS Session Mgr

SR — SESSION RECORDING

บันทึก admin action แบบ vdo/text

JumpServer · Teleport · Apache Guacamole · Cloud-native session manager

SIEM — SIEM / LOG AGGREGATION

รวบรวมและวิเคราะห์ log

Splunk · Elastic SIEM · MS Sentinel IBM QRadar · Sumo Logic · Wazuh (OSS)

AI — UEBA (Behavior Analytics)

ตรวจจับพฤติกรรมผิดปกติของ admin

Exabeam · Securonix
MS Defender for Cloud Apps

SO — SOAR / AUTOMATION

แจ้งเตือน / การตอบสนองอัตโนมัติ

Cortex XSOAR · Splunk SOAR Tines · n8n

OS+ — OBJECT STORAGE / LOG LAKE

เก็บ log ระยะยาวต้นทุนต่ำ

S3 + Glacier · Azure Blob Archive GCS Coldline · Object Lock (WORM)

💡 **เลือก stack ให้เหมาะกับงบและขนาด — เริ่มจาก Cloud Audit + IAM Log → ขยายเป็น SIEM + UEBA + PAM ตามลำดับความเสี่ยง**

10 Detection Use Cases ที่ควรเฝ้าระวัง — สำหรับ Privileged Action

ตัวอย่างการกำหนด SLA ตามผลกระทบ — RED = ตอบสนองทันที · AMBER = ใน 30 นาที · TEAL = Daily Review

01
Root / Global Admin Login
เมื่อใดก็ตาม → Alert ทันที + Verify ตัวบุคคล

RED
SLA: ภายในไม่กี่นาที

02
Disable Logging Feature
ปิด CloudTrail / Activity Log / Audit Log → Critical Alert

RED
SLA: ภายในไม่กี่นาที

03
Delete Log / Audit Data
ลบ log file / S3 bucket / Storage account → Critical Alert

RED
SLA: ภายในไม่กี่นาที

04
IAM Policy Privilege Escalation
เพิ่มสิทธิ์ Admin/Owner ให้ identity ใหม่

RED
SLA: ภายในไม่กี่นาที

05
New Long-Lived Credential
สร้าง access key / static credential / API key ใหม่

AMBER
SLA: ภายใน 30 นาที

06
MFA Disabled / Changed
ปิด MFA หรือเปลี่ยน MFA method ของ admin

AMBER
SLA: ภายใน 30 นาที

07
Unusual Geo-location Login
Admin login จาก geo ที่ไม่ปกติ (ต่างประเทศ ที่ไม่เคย)

AMBER
SLA: ภายใน 30 นาที

08
Off-hours Admin Activity
Admin login นอกเวลาทำการ — เทียบกับ baseline

AMBER
SLA: ภายใน 30 นาที

09
Impossible Travel / Brute Force
Login 2 ครั้งจากระยะทางที่เป็นไปไม่ได้

AMBER
SLA: ภายใน 30 นาที

10
KMS Key Disable / Unscheduled Rotate
ปิด encryption หรือ rotate KMS โดยไม่ได้กำหนดเวลา

TEAL
SLA: Daily review

อ้างอิง: MITRE ATT&CK Cloud Matrix · CIS Controls v8 · NIST SP 800-92 — เขียน detection rule ในรูปแบบ Sigma / KQL / SPL

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.7 การซิงโครไนซ์นาฬิกา

Clock Synchronization

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.6.7 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกา**ที่ใช้ในระบบของ CSP

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลแก่ CSC เกี่ยวกับนาฬิกา**ที่ระบบของ CSP ใช้ และข้อมูลเกี่ยวกับ**วิธีที่ CSC สามารถซิงโครไนซ์นาฬิกา**ภายในกับนาฬิกาในบริการคลาวด์

CSC — ผู้ใช้บริการคลาวด์

"ขอข้อมูล รับมา และนำไปใช้ให้ตรงกัน"

- ร้องขอ Time Source ของ CSP เป็นทางการ (Service Description / Trust Center)
- ออกแบบสถาปัตยกรรม NTP/PTP ภายในให้ชี้ไปแหล่งเวลาของ CSP
- ตั้งค่า OS / Container / Application พร้อม NTS หรือ Symmetric Key
- Monitor Time Drift และ Alert เมื่อเกินเกณฑ์ (>1 วินาที)
- จัดเก็บหลักฐาน Configuration และ Drift Report เพื่อ Audit

CSP — ผู้ให้บริการคลาวด์

"เปิดเผยให้โปร่งใส และส่งมอบแหล่งเวลาที่เชื่อถือได้"

- เปิดเผย Time Architecture (Stratum, แหล่งอ้างอิง GPS/Atomic/NIST)
- จัดเตรียม NTP/PTP Endpoint ใน VPC/VNet พร้อมเอกสาร
- จัดทำ Shared Responsibility Matrix ระบุขอบเขตชัดเจน
- เปิดเผย Drift Metric ผ่าน Trust Center / Status Page
- แจ้งล่วงหน้าเรื่อง Leap Second (Smear vs Step)

Shared Responsibility Matrix ตามรูปแบบบริการคลาวด์

การแบ่งความรับผิดชอบในการซิงโครไนซ์นาฬิกาแยกตาม IaaS / PaaS / SaaS

CSC รับผิดชอบ | CSP รับผิดชอบ | Shared (ร่วมกัน)

กิจกรรม	IaaS	PaaS	SaaS
ดูแลแหล่งเวลาอ้างอิง (GPS/Atomic/Stratum 1)	CSP	CSP	CSP
ดูแลความแม่นยำของ Host / Hypervisor	CSP	CSP	CSP
ตั้งค่าและซิงค์นาฬิกาของ Guest OS / VM	CSC	Shared	CSP
ตั้งค่านาฬิกาของ Container / Pod	CSC	Shared	CSP
ตั้งค่านาฬิกาของ Application Log / Audit Log	CSC	CSC	CSP
เปิดเผย NTP Endpoint และเอกสารคู่มือ	CSP	CSP	CSP
ตรวจสอบ Time Drift และแจ้งเตือน	CSC	Shared	CSP
บันทึก Audit Evidence ของการซิงค์	CSC	Shared	Shared
ทบทวนสัญญา/SLA เรื่องเวลา	CSC	CSC	CSC

ข้อสังเกต: SaaS ภาระตกที่ CSP เกือบทั้งหมด แต่ CSC ยังต้อง "รับ Log ที่มี Timestamp ตรงกับมาตรฐานเวลาขององค์กร"

เทคโนโลยีและโปรโตคอลในมุมเทคนิค (Vendor-Neutral)

เลือกเครื่องมือให้เหมาะกับ Workload — จาก NTP พื้นฐานสู่ PTP สำหรับ Sub-microsecond

NTP v4

RFC 5905

Network Time Protocol
Protocol พื้นฐาน ความแม่นยำ 1–100 ms ใน LAN/WAN — เหมาะกับระบบทั่วไป

NTS

RFC 8915

เพิ่ม Authentication และ Integrity ด้วย TLS — แนะนำให้ใช้แทน NTP เปล่า

PTP

IEEE 1588-2019

Precision Time Protocol
ความแม่นยำ Sub-microsecond — สำหรับ 5G, Trading, Industrial

GPS/GNSS

Stratum 0/1

แหล่งอ้างอิงระดับ Authoritative ใน Data Center; เสี่ยง Spoofing/Jamming

Atomic Clock

Cesium/Rubidium

เวลาที่ไม่ขึ้นกับสัญญาณภายนอก ใช้ในผู้ให้บริการคลาวด์รายใหญ่

RFC 3161

Trusted Timestamp

Time-Stamp Protocol สำหรับ e-Signature และงานพิสูจน์ทางกฎหมาย

chrony

Linux Daemon

ทันสมัยที่สุด จัดการ VM Drift และ Hypervisor Pause ได้ดี รองรับ NTS

W32Time

Windows

NTP Client ของ Windows; Domain-joined sync กับ DC; ต้อง reliable time source

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.8 การจัดการช่องโหว่ทางเทคนิค

Management of Technical Vulnerabilities

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.6.8 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน ข้อ 5.2.6.8

ก) CSC ต้อง**ขอข้อมูลจาก CSP เกี่ยวกับการจัดการช่องโหว่ทางเทคนิค** ที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ CSC

ต้อง**ระบุช่องโหว่ทางเทคนิคที่ CSC จะเป็นผู้รับผิดชอบ**ในการจัดการ และ**กำหนดกระบวนการในการจัดการ**ให้ชัดเจน

ถอดความเป็นภาษาที่อ่านง่าย: CSC ต้องทำ 3 อย่างหลัก

01 ขอข้อมูลจาก CSP

ขอรายละเอียดเรื่อง Patch Cadence, การแจ้งล่วงหน้า, การจัด Severity และการสื่อสารกับลูกค้า

02 ระบุขอบเขตความรับผิดชอบของตน

ระบุชัดว่า ช่องโหว่ส่วนใด ที่ CSC ต้องเป็นผู้รับผิดชอบ ขึ้นอยู่กับรูปแบบ IaaS / PaaS / SaaS

03 กำหนดกระบวนการจัดการของตน

ครอบคลุม Discover – Assess – Prioritize – Remediate – Verify – Report อย่างชัดเจน

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.6.8 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน ข้อ 5.2.6.8

ก) CSP ต้อง**ให้ข้อมูล CSC เกี่ยวกับการจัดการช่องโหว่ทางเทคนิค**ที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ

CSP ต้องเปิดเผยข้อมูล 6 หมวดต่อ CSC (โดยไม่เปิดเผยรายละเอียดที่อาจถูกใช้โจมตี)

01 นโยบายและขั้นตอน

นโยบายและขั้นตอนการจัดการช่องโหว่ของ CSP

02 ความถี่ในการสแกน

วิธีการและความถี่ที่ CSP สแกนช่องโหว่ในชั้นที่ตนรับผิดชอบ

03 Security Advisory

ช่องทางแจ้งช่องโหว่ใหม่ + Maintenance Window สำหรับ Patch

04 Severity & SLA

การจัดลำดับความรุนแรงและ SLA ในการแก้ไข

05 Shared Responsibility

เมทริกซ์ที่ระบุว่าใครต้อง Patch ส่วนใดในแต่ละ Service

06 Vulnerability Disclosure

ช่องทาง CVD ให้ CSC รายงานช่องโหว่ที่พบกลับมาที่ CSP

Shared Responsibility Matrix — ใครรับผิดชอบช่องโหว่ชั้นใด

การแบ่งความรับผิดชอบตามรูปแบบบริการ IaaS / PaaS / SaaS

ชั้นของระบบ	IaaS	PaaS	SaaS
Data (ข้อมูล)	CSC	CSC	CSC
Application	CSC	CSC	CSP
Runtime / Middleware	CSC	CSP	CSP
OS / Container Image	CSC	CSP	CSP
Hypervisor / Container Runtime	CSP	CSP	CSP
Hardware / Network / Facility	CSP	CSP	CSP
Configuration ของ CSC	CSC	CSC	CSC
IAM Policy / Credentials	CSC	CSC	CSC

คำอธิบาย

- CSC = Cloud Service Customer
- CSP = Cloud Service Provider

Key Insight

Configuration และ IAM ของ CSC ยังคงอยู่ใต้ความรับผิดชอบของ CSC แม้ใช้ SaaS เต็มรูปแบบ

ตัวอย่าง: Bucket ที่เปิด Public, MFA ที่ไม่ได้บังคับ, Role ที่ Over-privileged

Misconfiguration คือช่องโหว่ของคลาวด์ที่พบบ่อยที่สุด ไม่ใช่ CVE — ต้องมี CSPM

กระบวนการ Vulnerability Management — 6 ขั้นตอน

Continuous Process: Discover – Assess – Prioritize – Remediate – Verify – Report

1 Discover

ค้นหา

Asset Discovery, Continuous Scanning, Threat Intel Feeds, SBOM

2 Assess

ประเมิน

เก็บ CVSS, Exploitability (KEV/EPSS), Business Context, Reachability

3 Prioritize

จัดลำดับ

Risk-based Approach ไม่ใช่ CVSS เพียงอย่างเดียว

4 Remediate

แก้ไข

Patch / Config Fix / Compensating Control / Risk Acceptance

5 Verify

ยืนยัน

Rescan, Penetration Testing, Validation

6 Report

รายงาน

Dashboard, Executive Report, Compliance Evidence

เชื่อมโยงกับข้อกำหนดอื่นของ สกมช.

Change Management

Patch = การเปลี่ยนแปลงที่ต้องผ่าน Change Process

Inventory of Assets

ต้องรู้ว่ามี Asset อะไรก่อนหา Vulnerability

KPI สำหรับวัดผล และ Maturity Level ขององค์กร

Metrics ที่ Auditor จะถาม และเส้นทางการพัฒนา 5 ระดับ

KPI หลักที่ควรติดตาม

MTTD	**Mean Time to Detect** ตั้งแต่ CVE เผยแพร่ → ระบบค้นพบ
MTTP	**Mean Time to Patch** ตั้งแต่ค้นพบ → ติดตั้ง Patch สำเร็จ
MTTR	**Mean Time to Remediate** รวม Patch + Config + Compensating
Coverage	**% Asset Coverage** Asset ที่อยู่ใน Scope ของ Scanner
SLA Breach	**% Critical/High Open > SLA** ช่องโหว่ที่เกิน SLA ขององค์กร
KEV Match	**Exploitable on Internet** ช่องโหว่ที่อยู่ใน KEV ของ CISA
Reopen	**Reopen Rate** ช่องโหว่ที่ปิดแล้วถูกเปิดใหม่

Maturity Level 5 ระดับ

L5	**Optimizing** MTTP < 14 วัน, Coverage 99%, Reopen < 5%
L4	**Managed** VM Automation, CNAPP+SCA+IaC, MTTP < 30 วัน
L3	**Defined** มี SLA และ Scanner ต่อเนื่อง, MTTP 30-60 วัน
L2	**Reactive** มีนโยบายแต่ Implement ไม่สม่ำเสมอ MTTP > 90 วัน
L1	**Ad-hoc** ไม่มีนโยบาย, Free Scanner เป็นครั้งคราว, ไม่มี KPI

เทคโนโลยีและเครื่องมือสำคัญ

Toolchain สำหรับการจัดการช่องโหว่ทั้ง Build-time และ Runtime

VA

Vulnerability Scanner

Network/Host-based VA สำหรับ VM และ Network Device

CSPM

Cloud Posture Mgmt

ตรวจ Misconfiguration ของ Cloud Services

CWPP

Workload Protection

Runtime Protection ของ VM และ Container

CNAPP

Cloud Native AppPP

รวม CSPM + CWPP + CIEM ในแพลตฟอร์มเดียว

SCA

Software Composition

Scan Open Source Dependency ใน CI/CD

SAST/DAST

App Security Testing

Static + Dynamic Application Security Testing

Container

Image Scanner

Scan Container Image ก่อน Push และ Runtime

IaC

Infra-as-Code Scanner

Checkov, tfsec สำหรับ Terraform/CloudFormation

SBOM

Software Bill of Materials

CycloneDX, SPDX format สำหรับ Component Inventory

Patch

Patch Orchestration

Patch Manager + Configuration Management

TIP

Threat Intelligence

CISA KEV, FIRST EPSS, ThaiCERT, Vendor Bulletins

VDP

Vuln Disclosure

Coordinated Vulnerability Disclosure ตาม ISO 29147

5.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

5.2.6.9 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน

Separation of Development, Testing and Operational Environments

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.6.9 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐานสำหรับ CSC

ก) ใน**กรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคล**สำหรับวัตถุประสงค์**ในการทดสอบ**ได้ **ต้องมีการประเมินความเสี่ยง** มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อ**ลดความเสี่ยง**ที่ระบุไว้ให้น้อยที่สุด

ความหมายเชิงปฏิบัติของ CSC

หลีกเลี่ยงการใช้ PII โดยปริยาย — ใช้ Synthetic Data หรือข้อมูลที่ถูก Anonymize / Pseudonymize เป็นทางเลือกแรก หากเลี่ยงไม่ได้ ต้องทำ Risk Assessment อย่างเป็นทางการและบันทึกหลักฐานทั้งหมด

5 สิ่งที่ CSC ต้องทำเมื่อต้องใช้ PII ใน Test

01	**Risk Assessment** ประเมินความเสี่ยงเป็นทางการ ครอบคลุมโอกาส–ผลกระทบ
02	**Technical Controls** Data Masking, Tokenization, Encryption, Access Control, Logging
03	**Organizational Controls** Data Use Agreement, Training, Retention สั้น
04	**Evidence** เก็บหลักฐานการประเมินและมาตรการเพื่อ Auditor
05	**Logical Separation** แยก Subscription/Project/Account/Network/IAM/Storage/KMS

⚠ ข้อห้ามสำคัญ — ห้าม Copy Production Database ทั้งก้อนไปยัง Dev โดยไม่ Mask

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

CSP มีบทบาทคู่ — แยกสภาพแวดล้อมของตน และจัดเครื่องมือให้ CSC แยกได้ง่าย

ตัวบทมาตรฐานสำหรับ CSP

ก) ใน**กรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคล**สำหรับวัตถุประสงค์**ในการทดสอบ**ได้ **ต้องมีการประเมินความเสี่ยง** มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อ**ลดความเสี่ยง**ที่ระบุไว้ให้น้อยที่สุด

Internal Boundary

แยก Dev/Test/Prod ของตนเองอย่างชัดเจน เช่น Region/Cell/Cluster

Tooling for CSC

เตรียม Account / Subscription / Project / Tenant ให้ CSC แยกได้สะดวก

Consent for PII

ห้ามใช้ PII ของลูกค้าใน Dev/Test ของ CSP เว้นแต่ผ่าน Risk Assessment + Consent

Disclosure

เปิดเผยมาตรการแยก/คุ้มครอง PII ใน Service Description / SR Matrix

Promotion Pipeline

Dev → Test → Prod ภายในของ CSP มี Change Management & Security Test

Audited Evidence

SOC 2 Type II, ISO 27001/27017/27018/27701, CSA STAR

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม	IaaS	PaaS	SaaS
Account / Project / Subscription Hierarchy	CSC	CSC	SHARED
Network / VPC / Subnet Separation	CSC	SHARED	CSP
IAM / RBAC / Role Design	CSC	CSC	SHARED
Hypervisor / Physical Host Isolation	CSP	CSP	CSP
Application & Code Separation	CSC	CSC	CSC
Test Data Management (Masking, Synthetic)	CSC	CSC	SHARED
Risk Assessment เมื่อใช้ PII ในการทดสอบ	CSC	CSC	SHARED
Logging / Audit Trail ข้ามสภาพแวดล้อม	SHARED	SHARED	CSP
Compliance Certification (SOC2, ISO 27018)	CSP	CSP	CSP

CSC รับผิดชอบ CSP รับผิดชอบ แบ่งร่วม (Shared)

5.2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

5.2.7.1 นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล

Information Transfer Policies and Procedures

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.7.1 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล **ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล** รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ

ข) CSC ต้อง**ขอให้ CSP ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส)** เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง

ตัวบทมาตรฐาน

ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล **ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล** รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ

ข) หากเป็นไปได้ ต้องขอให้ CSC ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง

ฝั่งผู้ใช้บริการคลาวด์ (CSC)

ก. ทะเบียนสื่อทางกายภาพ

ทุกครั้งที่ใช้ External HDD / USB / Backup Tape ถ่ายโอนข้อมูล PII ต้องบันทึก:

ประเภทสื่อ, ผู้ส่ง/ผู้รับที่ได้รับอนุญาต, วัน-เวลา, จำนวน

ข. ร้องขอมาตรการเพิ่มเติมจาก CSP

ต้องร้องขอให้ CSP จัดให้มีการเข้ารหัส (Encryption) เพื่อให้ข้อมูลถูกเข้าถึงได้เฉพาะที่ปลายทาง

— ไม่ใช่ระหว่างทาง

ฝั่งผู้ให้บริการคลาวด์ (CSP)

ก. ระบบบันทึกสื่อทางกายภาพในศูนย์ข้อมูล

ทุกครั้งที่ใช้ External HDD / USB / Backup Tape ถ่ายโอนข้อมูล PII ต้องบันทึก:

ประเภทสื่อ, ผู้ส่ง/ผู้รับที่ได้รับอนุญาต, วัน-เวลา, จำนวน

ข. ร้องขอให้ CSC ใช้มาตรการเพิ่มเติม

หากเป็นไปได้ ต้องร้องขอให้ CSC ใช้ Client-side Encryption เพื่อให้ข้อมูลเข้าถึงได้ที่ปลายทางเท่านั้น

Shared Responsibility Matrix — ใครรับผิดชอบอะไร

การแบ่งความรับผิดชอบเปลี่ยนตามรูปแบบบริการ IaaS / PaaS / SaaS

Legend: CSC รับผิดชอบ | CSP รับผิดชอบ | Shared (ร่วมกัน)

กิจกรรม / Layer	IaaS	PaaS	SaaS
กำหนดนโยบายถ่ายโอนข้อมูล	CSC	CSC	CSC
ทะเบียนสื่อทางกายภาพของ CSC (USB/HDD)	CSC	CSC	CSC
ทะเบียนสื่อทางกายภาพในศูนย์ข้อมูล	CSP	CSP	CSP
จัดการ Encryption Key (Customer-managed)	CSC	Shared	Shared
จัดการ Encryption Key (Provider-managed)	CSP	CSP	CSP
เข้ารหัส In-Transit (TLS) ระดับเครือข่าย	Shared	Shared	CSP
Client-side Encryption ก่อนอัปโหลด	CSC	CSC	CSC
Server-side Encryption ที่ปลายทาง	Shared	CSP	CSP
Hardware Wipe / สื่อพิจารณาทำลาย	CSP	CSP	CSP
Authorization ผู้ส่ง/ผู้รับสื่อทางกายภาพ	CSC	CSC	CSC
Audit Log ของการถ่ายโอน	Shared	Shared	Shared
DLP สำหรับ Outbound (Email/USB/Upload)	CSC	Shared	Shared

ความเสี่ยงและภัยคุกคามที่ต้องคำนึงถึง

เหตุการณ์ที่เกิดขึ้นจริง — บทเรียนจากทั่วโลก

MITM Attack

ผู้โจมตีดักจับการสื่อสาร ผ่าน Wi-Fi สาธารณะ
หรือ Hijack DNS/BGP

สูญหายของสื่อทางกายภาพ

USB/HDD บรรจุ PII สูญหายระหว่างขนส่ง

Insider Threat

พนักงานคัดลอกข้อมูลใส่ USB และนำออกโดยไม่มี Log
IP/Customer Data รั่ว

Weak Encryption

TLS 1.0/1.1, Deprecated Cipher > ถูก Decrypt ได้
— Fail PCI-DSS และ ISO 27018

Cross-border Transfer

ส่ง PII ไป Region ต่างประเทศ โดยไม่มี Safeguard
— ผิด PDPA มาตรา 28

User Error

ส่งอีเมลผิดคน / Upload ผิด Bucket ที่เป็น Public
— S3 Bucket Public Leak

องค์ประกอบของกระบวนการที่ดี (Process Perspective)

7 องค์ประกอบที่ทำให้ Information Transfer Control ทำงานได้จริง

Documented Policy

เอกสารนโยบายและ SOP
อนุมัติโดยผู้บริหาร

Authorization Workflow

ผู้ส่ง/ผู้รับ ที่อนุญาต
และขั้นตอนอนุมัติ

Register / Logging

บันทึกการถ่ายโอน
ทั้งกายภาพและอิเล็กฯ

Encryption Standard

Algorithm, Key Length,
Cipher Suite ระบุชัด

Periodic Review

ทบทวนปีละครั้ง
หรือเมื่อเปลี่ยนสำคัญ

Awareness & Training

ฝึกอบรมพนักงาน
เรื่องการถ่ายโอนปลอดภัย

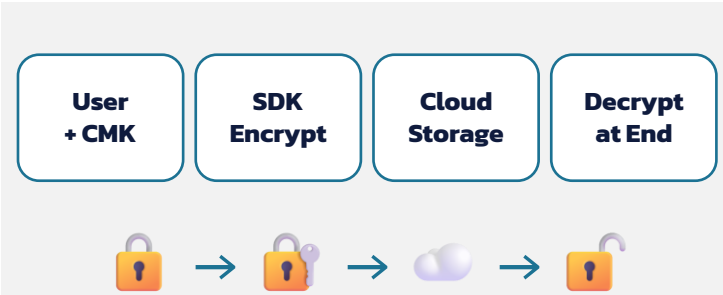
Incident Response

กระบวนการแจ้ง/สอบสวน
เมื่อเกิดเหตุละเมิด

ตัวอย่าง Architecture Patterns 3 รูปแบบ

เลือกรูปแบบที่เหมาะกับบริบทขององค์กรและประเภทข้อมูล

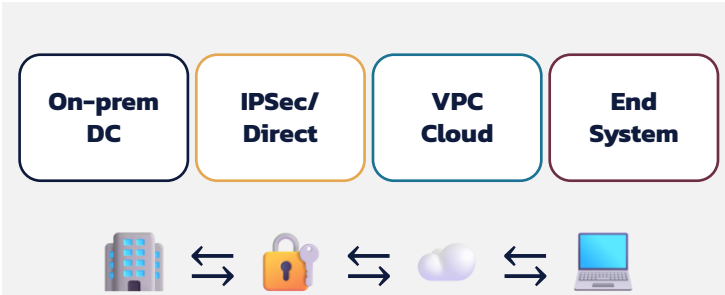
Pattern 1
End-to-End Encrypted Upload (Client-side)



User → Client SDK เข้ารหัสด้วย CMK → HTTPS/TLS 1.3 → Object Storage (เข้ารหัสซ้ำ) → ปลายทางถอดรหัสด้วย CMK เท่านั้น

เหมาะกับ: PII สูง / Medical Records / Trade Secret

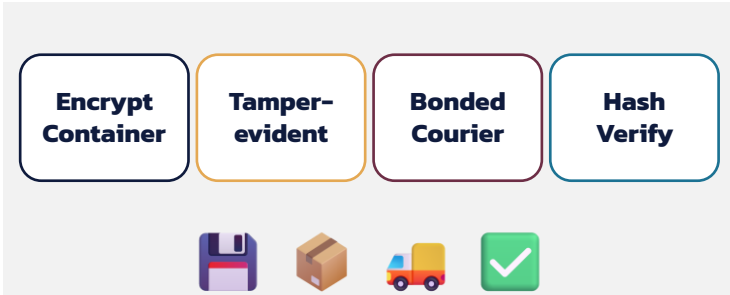
Pattern 2
Site-to-Site VPN + In-Transit Encryption



On-premise DC → IPSec VPN/Direct Connect ที่เข้ารหัส MACsec → VPC ใน Cloud → ระบบปลายทาง (Server-side Encryption)

เหมาะกับ: Hybrid Cloud / การถ่าย Workload ปริมาณมาก

Pattern 3
Physical Media Transfer with Encrypted Container



สร้าง LUKS/BitLocker Container บน External HDD → คัดลอกข้อมูล → Tamper-evident Bag → Bonded Courier → ตรวจ Hash → ทำลาย Container

เหมาะกับ: Initial Migration / Region ที่ไม่มี Direct Connect

5.2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

5.2.7.2 การแบ่งแยกในเครือข่าย

Segregation in Networks

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.7.2 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**จัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่า** (Tenant) ในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน และ**ตรวจสอบว่า CSP มีคุณสมบัติตรง**ตามข้อกำหนดเหล่านั้นหรือไม่

ตัวบทมาตรฐาน

ก) CSP ต้องบังคับใช้การแยกการเข้าถึงเครือข่ายในกรณีต่อไปนี้
- การ**แบ่งแยกระหว่างผู้เช่าในสภาพแวดล้อมที่มีผู้เช่าหลายราย**
- **การแยกระหว่างสภาพแวดล้อม**การดูแลระบบ**ภายในของ CSP** และสภาพแวดล้อมการประมวลผลบน**คลาวด์ของ CSC**

ข) CSP ต้อง**ช่วย CSC ตรวจสอบการแบ่งแยก**ที่ดำเนินการโดย CSP

CSC — ผู้ใช้บริการคลาวด์

1. **Define Segregation Requirements**
   นิยามความต้องการแยกเครือข่ายของตน เพื่อบรรลุ Tenant Isolation
2. **Verify CSP Capability**
   ตรวจสอบหลักฐานจาก CSP — SOC 2 Type II, ISO 27017, CSA STAR, Pentest
3. **Implement ภายในขอบเขต**
   ออกแบบ VPC/Subnet/Security Group ภายใน Account พร้อม Microsegmentation
4. **ทดสอบและทบทวน**
   Vulnerability Assessment, Pentest, Configuration Review สม่ำเสมอ

CSP — ผู้ให้บริการคลาวด์

1. **Enforce Tenant Segregation**
   บังคับใช้การแยกระหว่างผู้เช่าตั้งแต่ Physical ถึง Control Plane
2. **แยก Management จาก Workload**
   Internal Admin ต้องไม่ใช้เส้นทางเดียวกับ Customer Workload
3. **เปิดเผยกลไกและหลักฐาน**
   Service Description, Shared Responsibility Matrix, Assurance Reports
4. **ให้เครื่องมือ Verify แก่ CSC**
   Flow Log, Audit API, Tenant Health Check, IR Notification

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

CSC รับผิดชอบ | CSP รับผิดชอบ | Shared (ร่วมกัน)

กิจกรรม / Layer	IaaS	PaaS	SaaS
Physical Network / Underlay Fabric	CSP	CSP	CSP
Hypervisor / Virtual Switch (vSwitch)	CSP	CSP	CSP
แยก Management Plane จาก Customer Workload	CSP	CSP	CSP
กำหนด VPC / VNet / Project ของ Tenant	CSC	Shared	CSP
ออกแบบ Subnet, Routing และ Network ACL	CSC	Shared	CSP
Security Group / NSG / Firewall Rules	CSC	Shared	CSP
แยก Production / Non-Prod / Management	CSC	CSC	Shared
Microsegmentation East-West (Workload)	CSC	Shared	CSP
ตรวจสอบ Egress / Ingress Traffic	CSC	Shared	Shared
จัดเก็บและส่งออก Flow Log / NSG Log	Shared	Shared	Shared

เทคโนโลยีที่ใช้ในการแบ่งแยกเครือข่าย

ชุดเครื่องมือสำหรับสร้างชั้น Defense-in-Depth — เลือกใช้ให้เหมาะกับ Workload

VPC / VNet

พื้นที่เครือข่ายของลูกค้าแต่ละราย — หน่วยเริ่มต้นของ Tenant Isolation

Subnet / Route Table

แบ่ง VPC เป็นโซน Public / Private / Database / Management

Security Group / NSG

Stateful Firewall ระดับ Workload — คุม North-South & East-West

Network ACL (NACL)

Stateless Filter ระดับ Subnet — ชั้น Defense-in-Depth เสริม

Next-Gen Firewall

ตรวจสอบ Traffic ที่ Choke Point เช่น Hub VPC, Transit Gateway

Service Mesh (mTLS)

Microsegmentation ระดับ Service-to-Service สำหรับ Microservices

Private Endpoint

เข้าถึง Managed Service โดยไม่ผ่าน Public Internet

CSPM Tool

ตรวจจับ Misconfiguration และ Configuration Drift ของ Network Rules

Zero Trust (ZTNA)

ทดแทน VPN แบบ Flat — Authorize Per-session, Per-resource

ตัวอย่าง Network Flow Matrix ระหว่าง Trust Zone

ใช้บันทึกว่าโซนใดติดต่อกันได้บ้าง • ✓ = อนุญาต • ✗ = ไม่อนุญาต • ! = ผ่าน Inspection

From \ To	Public DMZ	App Tier	DB Tier	Management	Audit/Log
Public DMZ	–	✓	✗	✗	!
App Tier	✗	–	✓	✗	!
DB Tier	✗	✗	–	✗	!
Management	!	!	!	–	!
Audit/Log	✗	✗	✗	✗	–

💡 *ผูก Trust Zone กับ Tagging Strategy ของ Cloud — เพื่อให้ Policy บังคับใช้ได้แบบอัตโนมัติ และทบทวนได้*

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

5.2.8.1 การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Requirements Analysis and Specification

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.8.1 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้องกำหนด**ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์** จากนั้น**ประเมินว่าบริการของ CSP สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่**

ข) สำหรับการประเมินนี้ CSC ต้อง**ขอข้อมูลเกี่ยวกับความสามารถ**ในการรักษาความมั่นคงปลอดภัยสารสนเทศ**จาก CSP**

ตัวบทมาตรฐาน

ก) CSP ต้อง**ให้ข้อมูลแก่ CSC เกี่ยวกับความสามารถ**ในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ตนใช้ ข้อมูลนี้ต้องเป็นข้อมูลโดย**ไม่เปิดเผยข้อมูลที่อาจเป็นประโยชน์ต่อบุคคลที่มีเจตนาร้าย**

CSC — ผู้ใช้บริการคลาวด์

- **Business Impact Analysis (BIA)**
  จำแนกระดับความสำคัญและ Sensitivity ก่อนย้าย Cloud
- **CIA + Privacy + Compliance**
  ระบุ Confidentiality, Integrity, Availability, Non-repudiation, PDPA
- **SSLOs ที่วัดได้**
  Encryption strength, Logging retention, IR time, RPO/RTO
- **Vendor Assessment (CAIQ/SIG)**
  ส่งคำถามและตรวจเอกสาร ISO/SOC2/STAR
- **Gap Analysis + Compensating**
  บันทึก Risk Acceptance ที่ลงนามโดย Risk Owner
- **Re-evaluation อย่างน้อยปีละ 1 ครั้ง**
  หรือเมื่อมี Material Change ของ CSP

CSP — ผู้ให้บริการคลาวด์

- **Service Description ละเอียด**
  Functional + Security per Service / Region / Tier
- **Shared Responsibility Matrix**
  ลงรายละเอียดระดับ Sub-control ทั้ง IaaS / PaaS / SaaS
- **Security Whitepaper**
  Defense-in-Depth โดยไม่เปิดเผย Vendor/Version
- **Compliance Reports**
  ISO 27001/27017/27018, SOC 2 Type II, CSA STAR, สกมช.
- **Customer Trust Portal**
  Self-service + NDA + Audit Log ของการเข้าถึง
- **Change Notification**
  แจ้งล่วงหน้า ≥ 30 วันสำหรับ Sub-processor / Region

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
ระบุข้อกำหนดด้านความมั่นคงปลอดภัยของธุรกิจ	CSC	CSC	CSC
ระบุข้อกำหนดด้านกฎหมาย / ข้อบังคับ	CSC	CSC	CSC
เอกสารความสามารถด้าน Security ของบริการ	CSP	CSP	CSP
เปิดเผย Compliance Reports (SOC 2, ISO 27001 ...)	CSP	CSP	CSP
Vendor Risk Assessment ก่อนตัดสินใจใช้	CSC	CSC	CSC
ข้อกำหนดเทคนิคของ Workload (Encryption, Isolation)	Shared	Shared	Shared
ออกแบบ Architecture ที่ตอบสนองข้อกำหนด	CSC	Shared	Shared
Service Description / Responsibility Matrix	CSP	CSP	CSP
ปฏิบัติตามที่ระดับ Infrastructure (Physical/Host/Hyper.)	CSP	CSP	CSP
ปฏิบัติตามที่ระดับ Application / Data / Config	CSC	Shared	Shared
Ongoing Monitoring (กำกับติดตามต่อเนื่อง)	Shared	Shared	Shared
Evidence for Audit	Shared	Shared	Shared
Re-assessment เมื่อมี Change	CSC	CSC	CSC

CSC = CSC รับผิดชอบหลัก CSP = CSP รับผิดชอบหลัก Shared = แบ่งร่วม

8 ขั้นตอน Implement Control สำหรับ CSP — เปิดเผยพอดี ปลอดภัย ครบถ้วน

Inform without Enable — ให้ข้อมูลพอที่ลูกค้าจะประเมิน แต่ไม่กลายเป็น Threat Intel ให้ผู้โจมตี

1	**Security Capability Inventory**	รวบรวมความสามารถด้าน Security ทุก Service / Tier / Region
2	**Service Description ครบถ้วน**	Functional + Security + SLA + Limitations + Supported Compliance
3	**Shared Responsibility Matrix**	ลงรายละเอียดระดับ Sub-control สำหรับ IaaS / PaaS / SaaS
4	**Third-party Attestation**	ISO 27001/27017/27018, SOC 2 Type II, CSA STAR L2, สกมช., FedRAMP
5	**Master CAIQ / SIG Response**	Knowledge Repository + Trained Pre-sales Security Engineer
6	**Security Whitepaper**	Defense-in-Depth + Isolation + IAM + Logging โดยไม่เปิด Vendor/Version
7	**Customer Trust Portal**	Self-service + Access Control + Audit Log + NDA Workflow
8	**Change Notification**	ระยะเวลาแจ้งล่วงหน้า ≥ 30 วัน สำหรับ Sub-processor / Region / Encryption

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

5.2.8.2 นโยบายการพัฒนาที่ปลอดภัย

Secure Development Policy

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.8.2 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ขอข้อมูลจาก CSP** เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติใน**การพัฒนาที่ปลอดภัยของ CSP**

ตัวบทมาตรฐาน

ก) CSP **ต้องให้ข้อมูล**เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติใน**การพัฒนาความปลอดภัยของตน** ในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล

CSC — Cloud Service Customer

ภารกิจหลัก

ขอข้อมูลและประเมินกระบวนการพัฒนาของ CSP

หลักฐานที่ต้องตรวจ

Approved Policy, Attestation Report (ISO 27001/27017, SOC 2 Type II, CSA STAR L2)

CSP — Cloud Service Provider

ภารกิจหลัก

จัดทำและเปิดเผยกระบวนการพัฒนาที่ปลอดภัย

หลักฐานที่ต้องตรวจ

Approved Policy, SBOM, Code Signing, SAST/DAST/SCA ลงนามโดย CISO/CTO ทบทวน ≥ ปีละครั้ง

กระบวนการอ้างอิง

NIST SSDF v1.1, OWASP SAMM v2, BSIMM, ISO/IEC 27034, Microsoft SDL

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม / Layer	IaaS	PaaS	SaaS
นโยบาย Secure Development ของแพลตฟอร์ม	CSP	CSP	CSP
นโยบาย Secure Dev ของ Workload ที่ CSC พัฒนาเอง	CSC	CSC	Shared
Hardening Image / OS	CSC	Shared	CSP
Code Review, SAST/DAST ของ Application	CSC	CSC	CSP
SBOM (Software Bill of Materials)	Shared	Shared	CSP
จัดการ Secret / Key ใน Source Code	CSC	CSC	CSP
แยก Environment (Dev / Test / Prod)	CSC	Shared	CSP
ห้ามใช้ PII จริงใน Non-production	CSC	CSC	CSP
Vendor Assessment (CSC ประเมินกระบวนการของ CSP)	CSC	CSC	CSC
Penetration Test / DAST ก่อน Release	CSC	Shared	CSP

CSC รับผิดชอบ | CSP รับผิดชอบ | Shared (ร่วมกัน)

Anatomy of a Mature Secure SDLC

6 Phases + 5 Cross-cutting Layers ที่ครอบคลุมตลอดวงจรชีวิตการพัฒนาซอฟต์แวร์

Plan	Design	Build	Test	Release	Maintain
01	02	03	04	05	06
Security Req, Threat Modeling, PIA, Abuse Case	Secure Architecture, Defense-in-Depth, Crypto Review	Secure Coding Std, Peer Review, Secret Mgmt	SAST / DAST / IAST / SCA, Pentest, Red Team	Go/No-Go, Code Signing, SBOM, Approval	VDP, Continuous Scan, Patch Mgmt, Decommission

Cross-cutting Layers — ชั้นกำกับที่ครอบคลุมทุก Phase

1	2	3	4	5
Governance	**Tooling**	**Education**	**Supply Chain**	**Metrics**
Policy, Standards, KPI	SCM, CI/CD, SAST/DAST/SCA	Dev Training, Security Champion	3rd-party Review, SBOM, SLSA	MTTR, Defect Density, Test Coverage

5.2.9 การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

5.2.9.1 นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก

Information Security Policy for Supplier Relationships

ข้อกำหนดสำหรับ

CSC	-

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.9.1 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ระบุว่า CSP เป็นผู้ให้บริการภายนอก**ประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูล CSC ของ CSP

ข้อกำหนด 5.2.9.1

01 เพิ่ม CSP เป็น Supplier

ทบทวน/จัดทำ Supplier Categorization Matrix — Cloud Service Provider เป็นหมวดย่อย

02 กำหนดกระบวนการเฉพาะ CSP

Cloud Vendor Risk Assessment, Onboarding Workflow, Exit Plan ที่ต่างจาก Supplier ทั่วไป

03 เกณฑ์ประเมิน Assessment

ISO 27001/27017/27018, SOC 2 Type II, สกมช., PDPA Compliance, CSA STAR Registry

04 บทบาท + Approval Workflow

ระบุ Owner ในการประเมิน อนุมัติ ติดตาม ทบทวนตลอดวงจรชีวิตของ CSP

สิ่งที่ CSP ควรทำสนับสนุน CSC

Trust Center	Compliance Pack	DPA Template	Sub-processor List	Service Description
ISO Cert, SOC 2, Pen Test	ตอบ VAQ ของ CSC ได้เร็ว	ตาม PDPA / GDPR	เปิดเผย Supply Chain	IaaS/PaaS/SaaS, Region, SRM

Auditor มองหา: นโยบาย Supplier ที่ระบุ CSP ชัดเจน + เชื่อมโยงข้อกำหนดอื่นในมาตรฐานคลาวด์ + Vendor Risk Assessment Records จริง

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

Layer / กิจกรรม	IaaS	PaaS	SaaS
Data / ข้อมูลและการจำแนกประเภท	CSC	CSC	CSC
Application Configuration	CSC	CSC	Shared
Identity & Access (IAM)	CSC	Shared	Shared
Operating System / Runtime	CSC	CSP	CSP
Network Controls (VPC, FW, Seg.)	Shared	Shared	CSP
Hypervisor / Virtualization	CSP	CSP	CSP
Physical / Data Center	CSP	CSP	CSP
Compliance Evidence + Right to Audit	Shared	Shared	Shared

CSC รับผิดชอบหลัก | CSP รับผิดชอบหลัก | Shared / แบ่งร่วม

7 องค์ประกอบของกระบวนการบริหาร CSP ที่ดี

จาก Policy → Categorization → Risk Assessment → Onboarding → Monitoring → Review → Exit

1 Supplier Policy

เอกสารนโยบาย, ระบุ Scope, Principle, Categorization, Authority, Review Cycle

2 Categorization

แบ่ง Tier 1/2/3 หรือ High/Medium/Low ตามระดับความเสี่ยง

3 Risk Assessment

Questionnaire + Evidence + Risk Scoring + Approval Workflow

4 Onboarding

Contract + DPA + Access Provisioning + Cloud Service Inventory

5 Continuous Monitoring

CSPM, Security Rating, Compliance Renewal

6 Periodic Review

ทบทวนตามรอบ + Trigger Review เมื่อมีเหตุการณ์

7 Exit / Termination

Return/Delete Data + Cert. of Destruction + Knowledge Transfer

วงจรชีวิตของการบริหาร CSP — 6 ขั้นตอนที่ต้องสะท้อนในนโยบาย

1. Pre-engagement	2. Engagement	3. Onboarding	4. Operation	5. Review / Renewal	6. Exit
RFP, Due Diligence, เลือก CSP	เจรจาสัญญา, DPA, SLA, Right to Audit, Exit Clause	Provisioning, Config Baseline, Awareness ของ Cloud Service Owner	Day-to-day, Incident Coordination, Change Mgmt	ทบทวนตามรอบ + Renew Contract + Compliance Evidence	Data Portability + Account Closure + Cert. of Destruction

Pro Tip: เริ่มจาก Categorization ที่ดี — ถ้าจัดประเภท Supplier ผิด ระดับการประเมินก็จะผิดทั้งหมด

ความท้าทายเชิงเทคนิคที่ผู้ปฏิบัติงานต้องเตรียมรับมือ

Cloud เปลี่ยนเร็ว • Sub-processor ลึก • Audit Right จำกัด • Sovereignty • Shadow IT • Multi-cloud

Capability Drift

Cloud Service เปลี่ยน Feature เร็ว — Risk Profile เปลี่ยน ต้องมี Continuous Assessment

→ Solution: ตั้ง Trigger Review: Material Change, Service Update, Region Add

Sub-processor Transparency

CSP ใหญ่อาจมี Sub-processor หลักร้อยราย — ประเมิน Supply Chain ลึกเป็นภาระ

→ Solution: ขอ Approved Sub-processor List + 30-day Change Notification

Right to Audit จำกัด

Public Cloud มัก audit on-site ไม่ได้ — ต้องพึ่ง Independent Audit Reports

→ Solution: ใช้ SOC 2 Type II + ISO 27001 + CSA STAR แทนการ on-site audit

Data Residency & Sovereignty

Region/Zone ของ CSP มีผลทางกฎหมาย — กฎ Cross-border ของ PDPA

→ Solution: ระบุ Region ใน Contract + Data Localization Clause

Shadow IT / Shadow Cloud

Business Unit สมัครใช้ SaaS เอง ไม่ผ่านฝ่าย IT

→ Solution: ใช้ CASB + SaaS Discovery + Procurement Gate

Integration / Multi-cloud

เมื่อรวม CSP หลายราย ความซับซ้อนเพิ่มแบบทวีคูณ

→ Solution: Standardize on Common Control Framework (CCM v4)

5.2.9 การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

5.2.9.2 การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก

Addressing Security within Supplier Agreements

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — ผู้ใช้บริการคลาวด์ (CSC) vs ผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.9.2 ในบริบทของบริการคลาวด์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ยืนยันบทบาทและความรับผิดชอบ**ด้านความมั่นคงปลอดภัยสารสนเทศที่**เกี่ยวข้องกับบริการคลาวด์** ดังที่อธิบายไว้ในข้อตกลงการให้บริการ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้

- การป้องกันมัลแวร์
- การสำรองข้อมูล
- มาตรการควบคุมการเข้ารหัส
- การจัดการช่องโหว่
- การจัดการเหตุการณ์
- การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค
- การทดสอบความปลอดภัย
- การตรวจสอบ
- การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ
- การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ
- การยืนยันตัวตน และการควบคุมการเข้าถึง
- การจัดการข้อมูลประจำตัวและการเข้าถึง

ตัวบทมาตรฐาน

ก) CSP ต้อง**ระบุมาตร**การรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่ง CSP จะนำมาใช้**เป็นส่วนหนึ่งของข้อตกลง**เพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่าง CSP และ CSC สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้

- การป้องกันมัลแวร์
- การสำรองข้อมูล
- มาตรการควบคุมการเข้ารหัส
- การจัดการช่องโหว่
- การจัดการเหตุการณ์
- การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค
- การทดสอบความปลอดภัย
- การตรวจสอบ
- การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ
- การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ
- การยืนยันตัวตน และการควบคุมการเข้าถึง
- การจัดการข้อมูลประจำตัวและการเข้าถึง

CSC ผู้ใช้บริการคลาวด์

สิ่งที่ต้องยืนยัน

- CSC ต้องยืนยันบทบาท–ความรับผิดชอบ
- ด้านความมั่นคงปลอดภัยที่ระบุในข้อตกลง
- ครอบคลุมอย่างน้อย 12 กระบวนการ
- และต้องสอดคล้องกับความเสี่ยง กฎหมาย และมาตรฐานขององค์กร

นัยของคำว่า "ยืนยัน"

- มิใช่แค่ลงนามสัญญา — ต้อง "ตรวจสอบ" ครอบคลุมความเสี่ยง
- ตรวจให้สอดคล้องกับ พ.ร.บ. ไซเบอร์ฯ, มาตรฐานคลาวด์
- เก็บหลักฐานการตรวจ

CSP ผู้ให้บริการคลาวด์

สิ่งที่ต้องระบุ

- CSP ต้องระบุมาตรการที่ CSP จะดำเนินการ
- ภายในข้อตกลงให้ครบ 12 กระบวนการ
- เพื่อขจัดความเข้าใจผิด — และเปิดเผยว่า
- มาตรการเหล่านี้แตกต่างกันตาม IaaS / PaaS / SaaS

เครื่องมือสนับสนุน

- Service Description + Shared Responsibility Matrix
- Trust Portal เผยแพร่ Compliance Reports
- เผยแพร่ Subprocessor List + Notification Mechanism

หัวใจของข้อกำหนดมิใช่ "การมีข้อตกลง" แต่คือ "การมั่นใจว่าข้อตกลงระบุมาตรการครบและทั้งสองฝ่ายเข้าใจตรงกัน"

12 กระบวนการที่ควรครอบคลุมในข้อตกลง

Indicative List — ในทางปฏิบัติผู้ตรวจคาดหวังว่าครอบคลุมครบทั้ง 12 หัวข้อ

01
Malware Protection
Hypervisor / OS / App — ใครรับผิดชอบ

02
Backup
Frequency, Retention, Restore SLA, Test

03
Cryptographic Controls
Algorithm, BYOK/HYOK, Key Rotation

04
Vulnerability Management
Patch Cadence, Scanning, Severity SLA

05
Incident Management
Notification Timeline, Severity, Cooperation

06
Technical Compliance
Reports ที่จะส่ง, Frequency, Monitoring

07
Security Testing
Pentest Scope, Permission, Reporting

08
Auditing
Right-to-Audit, Doc. Access, Frequency

09
Evidence / Logging
Collection, Retention, Legal Hold Access

10
Termination Protection
Data Return Format, Destruction Certificate

11
Auth & Access Control
MFA, SSO, Privileged Access

12
Identity & Access Management
Federation, JML, Periodic Review

Shared Responsibility Matrix — IaaS / PaaS / SaaS (ตอนที่ 1)

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

CSC CSP Shared

กิจกรรม / Layer	IaaS	PaaS	SaaS
Malware Protection — Guest OS	CSC	Shared	CSP
Malware Protection — Hypervisor / Platform	CSP	CSP	CSP
Backup — Application Data & Config	CSC	Shared	Shared
Backup — Infrastructure & Continuity	CSP	CSP	CSP
Crypto — Data at Rest (BYOK / HYOK)	Shared	Shared	Shared
Crypto — Data in Transit (TLS)	Shared	Shared	CSP
Vulnerability Mgmt — Guest OS / Middleware	CSC	Shared	CSP
Vulnerability Mgmt — Hypervisor / Infra	CSP	CSP	CSP
Incident Mgmt — Notify CSC	Shared	Shared	Shared
Technical Compliance Checking	Shared	Shared	Shared

Shared Responsibility Matrix — IaaS / PaaS / SaaS (ตอนที่ 2)

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

CSC CSP Shared

กิจกรรม / Layer	IaaS	PaaS	SaaS
Incident Mgmt — Responsibility for Event	Shared	Shared	Shared
Security Testing (Pentest / Vuln Scan)	Shared	Shared	Shared
Auditing — เปิดให้ CSC ตรวจ (SOC 2)	Shared	Shared	Shared
Log Collection — Customer Workload Logs	CSC	Shared	Shared
Log Collection — Infrastructure Logs	CSP	CSP	CSP
Protection upon Termination	Shared	Shared	Shared
Auth & Access Control — End-user / Workload	CSC	Shared	Shared
IAM — Provider Console	Shared	Shared	Shared
Subcontractor Disclosure (4th Party)	CSP	CSP	CSP
ระบุมาตรการในข้อตกลง (Specify in Agreement)	Shared	Shared	Shared

5.2.9 การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

5.2.9.3 ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร

Information and Communication Technology Supply Chain

ข้อกำหนดสำหรับ	
-	CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.9.3 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน

ก) หาก CSP ใช้บริการคลาวด์ของผู้ให้บริการรายย่อย: CSP ต้อง**ตรวจสอบ**ให้แน่ใจ**ว่าระดับความมั่นคงปลอดภัย**สารสนเทศของ**ผู้ให้บริการรายย่อย**นั้นได้รับการดูแล**ไม่น้อยกว่า CSC**

ข) เมื่อ CSP ให้บริการคลาวด์ตามห่วงโซ่อุปทาน: CSP ต้อง**กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก** และ**ขอให้ผู้ให้บริการภายนอก**แต่ละราย ดำเนินกิจกรรมการ**บริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์**

ก) Inheritance — Sub-CSP ต้องไม่ต่ำกว่า

เมื่อ **CSP ใช้บริการของ peer CSP (Sub-CSP)** ต้องตรวจสอบให้ได้ว่า Sub-CSP รักษาระดับความปลอดภัยให้ลูกค้าได้

ไม่น้อยกว่า ระดับที่ CSP ให้บริการแก่ CSC

ในทางปฏิบัติหมายถึง:

- เลือก Sub-CSP ที่ได้รับการรับรองอย่างน้อย เทียบเท่ากับตัวเอง (ISO 27001/27017)
- เปรียบเทียบ SLA · การเข้ารหัส · IAM · Incident Mgmt ของ Sub-CSP กับมาตรฐานของ CSP
- บันทึก Pre-contract Assessment เป็นหลักฐาน
- ทบทวนตามรอบ (Annual Review) เมื่อ Sub-CSP มีการเปลี่ยนแปลงสำคัญหรือเกิดเหตุ

ข) Cascading — กำหนดวัตถุประสงค์แก่ Supplier

เมื่อ CSP ให้บริการคลาวด์โดยอาศัยห่วงโซ่อุปทาน CSP ต้อง **กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัย** (Security Objectives) ให้แก่ Supplier แต่ละราย พร้อม **ขอให้ Supplier ทำ Risk Management** เพื่อบรรลุวัตถุประสงค์เหล่านั้น

ตัวอย่างวัตถุประสงค์เชิงปริมาณ:

- Availability ≥ 99.95% · Patch Critical ≤ 7 วัน
- Encryption at rest AES-256 · in transit TLS 1.2+
- Notify confirmed breach ภายใน 24 ชั่วโมง
- Sub-processor list update รายไตรมาส
- Independent audit report annually

Shared Responsibility ตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

กิจกรรม	IaaS	PaaS	SaaS
จัดทำและประกาศ Sub-processor List	CSP	CSP	CSP
ประเมินความเสี่ยง Sub-CSP / Supplier	CSP	CSP	CSP
กำหนดวัตถุประสงค์ความปลอดภัยให้ Supplier	CSP	CSP	CSP
ทำสัญญา / DPA กับ Sub-CSP	CSP	CSP	CSP
แจ้ง CSC เมื่อมีการเปลี่ยน Sub-CSP	CSP	CSP	CSP
ประเมินความเสี่ยงของ CSP ที่ตนเลือกใช้	CSC	CSC	CSC
ตรวจรายงานความปลอดภัยอิสระ	Shared	Shared	Shared
กำหนดข้อสัญญา Supply Chain (CSP–CSC)	Shared	Shared	Shared
กำหนด Sub-CSP ที่อนุญาตสำหรับ Workload ตน	CSC	CSC	Shared
Incident Response เมื่อ Sub-CSP ถูกโจมตี	Shared	Shared	Shared

CSC CSP Shared

สิ่งที่ CSP ต้องดำเนินการ — 9 ภารกิจหลัก

พิสูจน์ได้ว่า CSP กำกับห่วงโซ่ของตนตลอดวงจรชีวิต ไม่ใช่เพียงมีนโยบาย

01 SCRM Policy & Plan
นโยบายและแผนที่ผู้บริหารอนุมัติ

02 Supplier Inventory + Tiering
ทะเบียน Sub-CSP/Supplier ตาม Tier

03 Pre-contract Due Diligence
ตรวจประเมินก่อนทำสัญญา + ทบทวนตามรอบ

04 Security Objectives ใน SLA
วัตถุประสงค์เป็นลายลักษณ์อักษรในสัญญา

05 ขอให้ Supplier ทำ Risk Management
ส่งหลักฐานตามรอบ (Risk Treatment, SOA)

06 Sub-processor List + Trust Portal
เปิดเผย + กลไกแจ้งเตือนการเปลี่ยนแปลง

07 Continuous Monitoring
Security Rating, Threat Intel, Pen-test

08 Incident Coordination
ครอบคลุม Supplier Breach + แจ้ง CSC โปร่งใส

09 Termination & Exit Plan
ข้อกำหนด Data Return/Destruction

5.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

5.2.10.1 ความรับผิดชอบและขั้นตอน

Responsibilities and Procedures

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.10.1 ในบริบทของผู้ใช้บริการคลาวด์

ตัวบทมาตรฐาน (CSC)

ก) CSC ต้อง**ตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุการณ์**ด้านความมั่นคงปลอดภัยสารสนเทศ และต้องตรวจสอบให้แน่ใจว่า**เป็นไปตามข้อกำหนดของ CSC**

ข) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การ**ทบทวนโดย CSC หรือทบทวนร่วมกันระหว่าง CSP และ CSC** ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตน **เพื่อพิจารณาว่าได้มีการละเมิด**ข้อมูลที่เกี่ยวข้องกับ**ข้อมูลส่วนบุคคล**เกิดขึ้นหรือไม่

ถอดความเป็นภาษาที่อ่านง่าย

01 ห้ามรับเอกสารของ CSP มาแบบไม่อ่าน

ต้องอ่าน วิเคราะห์ และเปรียบเทียบว่าการแบ่งบทบาทของ CSP ครอบคลุมความต้องการของตนครบถ้วนหรือไม่

02 ปิดช่องว่างด้วย Compensating Control

หากพบจุดที่ CSP ไม่ครอบคลุม ต้องเจรจาเพิ่มเติม หรือกำหนดมาตรการเสริมภายในเพื่อปิดช่องว่าง

03 ทุกเหตุการณ์ต้องนำไปสู่การทบทวน

ไม่ว่าจะเป็นเหตุในระบบของ CSC หรือที่ CSP แจ้ง — CSC ต้องทบทวนเพื่อพิจารณา Personal Data Breach

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.10.1 ในบริบทของผู้ให้บริการคลาวด์

ตัวบทมาตรฐาน (CSP)

ก) CSP ต้อง**กำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์**ด้านความมั่นคงปลอดภัยสารสนเทศระหว่าง CSC และ CSP โดย**เป็นส่วนหนึ่งของข้อกำหนดบริการ**

ข) CSP ต้อง**จัดเตรียมเอกสารให้ CSC** ครอบคลุม
- **ขอบเขตของเหตุการณ์**ด้านความมั่นคงปลอดภัยสารสนเทศ**ที่ CSP จะรายงานต่อ CSC**
- **ระดับการเปิดเผย**การตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและการตอบสนองที่เกี่ยวข้อง
- **กรอบเวลาเป้าหมายที่จะมีการแจ้งเหตุ**การณ์ด้านความมั่นคงปลอดภัยสารสนเทศเกิดขึ้น
- **ขั้นตอนการแจ้งเหตุ**การณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- **ข้อมูลติดต่อสำหรับการจัดการปัญหา**ที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- **การเยียวยา**ใด ๆ ที่สามารถนำไปใช้ได้หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศบางอย่างขึ้น

ค) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การ**ทบทวนโดย CSC หรือทบทวนร่วมกันระหว่าง CSP และ CSC** ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตน **เพื่อพิจารณาว่าได้มีการละเมิด**ข้อมูลที่เกี่ยวข้องกับ**ข้อมูลส่วนบุคคล**เกิดขึ้นหรือไม่

ขอบเขตการรายงาน

ประเภทของเหตุการณ์ที่ CSP จะรายงานให้ CSC ทราบ

ระดับการเปิดเผย

ข้อมูลรายละเอียดที่จะเปิดเผยในแต่ละระดับของเหตุการณ์

กรอบเวลาแจ้งเตือน

SLA ระยะเวลาแจ้งเตือน เช่น 4 ชม. / 24 ชม. / 72 ชม.

ขั้นตอนการแจ้ง

Channel, Format, Escalation Path ที่ใช้แจ้งเหตุ

ข้อมูลติดต่อ

Primary / Secondary contact และ Out-of-band channel

การเยียวยา

Credit, Refund, Forensics support, SLA Penalty

Shared Responsibility Matrix · การแบ่งความรับผิดชอบตามรูปแบบบริการ

การแบ่งความรับผิดชอบระหว่าง CSP และ CSC แตกต่างตามรูปแบบบริการ IaaS / PaaS / SaaS

CSC รับผิดชอบ | CSP รับผิดชอบ | Shared (ร่วมกัน)

กิจกรรม	IaaS	PaaS	SaaS
จัดทำนโยบายการจัดการเหตุการณ์ภายใน	CSC	CSC	CSC
กำหนดขอบเขตเหตุการณ์ที่ CSP จะรายงาน	CSP	CSP	CSP
ตรวจจับเหตุระดับ Infrastructure / Hypervisor	CSP	CSP	CSP
ตรวจจับเหตุระดับ OS / Middleware	CSC	Shared	CSP
ตรวจจับเหตุระดับ Application / Data	CSC	CSC	Shared
การแจ้งเตือนระหว่าง CSP กับ CSC	Shared	Shared	Shared
Containment & Mitigation	Shared	Shared	CSP
Forensics ระดับ Infra	CSP	CSP	CSP
Forensics ระดับ Application / Data	CSC	CSC	Shared
พิจารณา Personal Data Breach	Shared	Shared	Shared
แจ้ง สคส. ภายใน 72 ชั่วโมง	CSC	CSC	CSC
ทบทวนหลังเหตุการณ์ (Post-Incident)	Shared	Shared	Shared

วงจรการจัดการเหตุการณ์ 4 ระยะ — Incident Response Lifecycle

อ้างอิง NIST SP 800-61 และ ISO/IEC 27035 — ใช้ได้ทั้งฝั่ง CSC และ CSP

PHASE 01
PREPARATION

การเตรียมการ

- กำหนดนโยบาย ขั้นตอน และทีมงาน
- จัดหาเครื่องมือ เทคโนโลยี
- ฝึกอบรม และซ้อมแผน (Drills / Tabletop)
- จัดทำ Playbook และ Runbook

PHASE 02
DETECTION & ANALYSIS

ตรวจจับและวิเคราะห์

- Monitoring และ Alerting ต่อเนื่อง
- คัดกรองข้อมูลเบื้องต้น (Triage)
- จัดประเภทและจัดลำดับความรุนแรง
- เก็บหลักฐานต้นทาง (Initial evidence)

PHASE 03
CONTAIN • ERADICATE • RECOVER

กักกัน-กำจัด-ฟื้นฟู

- ตัดวงจรการโจมตี (Containment)
- ลบ Malicious component ออกจากระบบ
- ฟื้นฟูระบบจาก Backup ที่สะอาด
- ยืนยันสถานะปกติก่อนเปิดบริการ

PHASE 04
POST-INCIDENT ACTIVITY

หลังเหตุการณ์

- ทบทวน Root Cause Analysis
- ปรับปรุงกระบวนการและเครื่องมือ
- รายงานต่อผู้บริหารและหน่วยกำกับ
- เก็บหลักฐานตามนโยบาย retention

บทบาทและความรับผิดชอบในการจัดการเหตุการณ์บนคลาวด์

ทั้ง CSC และ CSP ควรกำหนดบทบาทเหล่านี้ไว้ในเอกสารและทำให้คนเข้าใจตรงกัน

Incident Commander

ผู้มีอำนาจตัดสินใจในช่วงเกิดเหตุ เปลี่ยนได้ตามระยะ

SOC Team

เฝ้าระวังและคัดกรองเหตุการณ์เบื้องต้น 24×7

Cloud Ops Team

ปฏิบัติการบน Console / API ของ CSP ได้คล่อง

DFIR / Forensics

เก็บและวิเคราะห์หลักฐานทางดิจิทัล

Communication Lead

สื่อสารภายใน-ภายนอก รวมถึงสื่อมวลชน

DPO / Privacy Officer

ตัดสินใจเรื่องแจ้ง Personal Data Breach

Legal Counsel

ที่ปรึกษากฎหมาย การเปิดเผยและความรับผิด

Executive Sponsor

ผู้บริหารระดับสูง รับ Briefing และอนุมัติ

CSP Liaison

ผู้ประสานงานกับ CSP สำหรับฝั่ง CSC

ความท้าทายเชิงเทคนิคที่ทีมต้องรู้ก่อนลงมือ

ไม่ใช่ทุกเทคนิคใน On-premise จะใช้ได้กับคลาวด์ — เตรียมรับมือล่วงหน้า

Log Retention จำกัด

Log บางประเภทของ CSP ถูกเก็บเพียง 90 วันโดย Default — ต้อง Export ไป Long-term storage

Multi-region / Multi-account

Log กระจายหลายที่ — ต้อง Centralized Logging Pattern เพื่อ Correlate

Ephemeral Workloads

Container / Serverless อายุสั้น เก็บหลักฐานยาก ต้องตั้ง Auto-snapshot

Encrypted Traffic

TLS Inspection ทำได้จำกัดในคลาวด์ — ต้องพึ่ง Application-layer logs

Shared Service Limits

การ Containment อาจกระทบบริการอื่นที่ใช้ shared resource ร่วมกัน

API Rate Limit

การดึง Log ผ่าน API จำนวนมาก อาจถูก throttle จาก CSP

Cross-cloud Correlation

ใน Multi-cloud การเชื่อมโยงเหตุข้ามคลาวด์ต้องใช้ Schema กลาง

Chain of Custody

Hash, Timestamp, Witness — ต้องเก็บแบบ Immutable เพื่อใช้ทางกฎหมายได้

5.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

5.2.10.2 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

Reporting Information Security Events

ข้อกำหนดสำหรับ

CSC | CSP

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ใช้บริการคลาวด์ (CSC)

ตีความข้อกำหนด 5.2.10.2 ในบริบทของผู้ใช้บริการคลาวด์

CSC ต้องร้องขอข้อมูลจาก CSP เกี่ยวกับกลไกการรายงานทั้ง 3 ทิศทาง พร้อมเก็บหลักฐานเชิงประจักษ์

ตัวบทมาตรฐาน

ก) CSC ต้อง**ขอข้อมูลจาก CSP เกี่ยวกับกลไก**สำหรับ
- **CSC รายงานเหตุการณ์**ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบ**ต่อ CSP**
- **CSP เพื่อรับรายงาน**เกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ**ที่ตรวจพบโดย CSP**
- **CSC เพื่อติดตามสถานะของเหตุการณ์**ความมั่นคงปลอดภัยสารสนเทศที่รายงาน

01 บันทึกช่องทาง Inbound

ค้นหาช่องทางที่ CSP เปิดให้ CSC แจ้งเหตุ

- Web Portal, Email, Phone, Chat, In-app Form
- ระยะเวลาตอบสนองตาม SLA
- ข้อมูลขั้นต่ำที่ต้องส่ง (Subject, Severity, Service, Tenant, Contact)
- ตัวอย่าง: AWS Support, Azure Service Health, GCP Support

02 บันทึกกลไก Outbound

ค้นหาว่า CSP แจ้งเหตุกลับมาผ่านช่องทางใด

- Security Contact / Admin Portal
- Service Health Page / Customer Bulletin
- Targeted vs. Public Notification
- เวลา Notification ที่ผูกพันใน SLA

03 บันทึกระบบ Status Tracking

ระบุวิธีติดตามสถานะเหตุที่แจ้งไปแล้ว

- Ticket ID อัตโนมัติ
- Self-service Portal / Email Update
- RSS / Webhook / API Integration
- Post-Incident Report (PIR) สำหรับ Sev สูง

ถอดรหัสตัวบทมาตรฐาน — สำหรับผู้ให้บริการคลาวด์ (CSP)

ตีความข้อกำหนด 5.2.10.2 ในบริบทของผู้ให้บริการคลาวด์

CSP ต้องจัดให้มีกลไก Inbound, Outbound และ Status Tracking พร้อม SLA และหลักฐาน

ตัวบทมาตรฐาน

ก) CSP ต้องมีกลไกสำหรับ

- **CSC รายงานเหตุ**การณ์ความมั่นคงปลอดภัยสารสนเทศ**ต่อ CSP**
- **CSP เพื่อรายงาน**เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ**ต่อ CSC**
- **CSC เพื่อติดตามสถานะของเหตุการณ์**ความมั่นคงปลอดภัยสารสนเทศที่รายงาน

CSC

Cloud Service Customer

ผู้รายงาน:
- พนักงาน CSC
- Internal SOC
- Threat Intel
- Customer Support ภายใน

① Inbound Channel (CSC → CSP) →

Web Portal · Email · Phone · In-app · Trust Center · 24x7 · Auto Ticket ID · Ack SLA

② Outbound Channel (CSP → CSC) ←

Targeted Notification · Public Status Page · Admin Portal Alert · Customer Bulletin · Pre-registered Contact

③ Status Tracking ↔

Self-service Portal · Ticket Status (Open/Investigating/Mitigated/Closed) · RSS/Webhook/API · Post-Incident Report

CSP

Cloud Service Provider

ผู้รับ/ผู้ส่ง:
- CSP IR Team
- Customer Support 24x7
- CSP DPO
- Trust & Safety

CSP ต้องเปิดเผยทั้ง 3 ทิศทางใน Service Description / Customer Agreement / Documentation Portal และอัปเดตเมื่อเปลี่ยนแปลง

ตาราง Shared Responsibility — IaaS / PaaS / SaaS

เจ้าของความรับผิดชอบหลัก: เขียว = CSC, ส้ม = CSP, เหลือง = แบ่งร่วม

CSC CSP Shared

กิจกรรม / Layer	IaaS	PaaS	SaaS
ตรวจจับเหตุการณ์ใน Application ของ CSC	CSC	CSC	Shared
ตรวจจับใน Platform / Runtime	CSC	CSP	CSP
ตรวจจับใน Hypervisor / Infra	CSP	CSP	CSP
ช่องทาง Inbound (CSC → CSP)	CSP	CSP	CSP
Internal Reporting Form ของ CSC	CSC	CSC	CSC
Targeted Notification (CSP → CSC ที่ได้รับผลกระทบ)	CSP	CSP	CSP
Public Status / Service Disruption	CSP	CSP	CSP
Status Tracking ของ Ticket	CSP	CSP	CSP
จัดประเภท Severity เบื้องต้น	Shared	Shared	Shared
ส่งต่อ Regulator (สกมช., สคส.)	CSC	CSC	CSC

วงจรชีวิตและองค์ประกอบการรายงานเหตุการณ์

Reporting คือ Phase 2 ของ ISO/IEC 27035 — เป็นประตูสู่กระบวนการ Incident Management ทั้งหมด

Plan & Prepare	Detection & Reporting	Assessment & Decision	Responses	Lessons Learned
เตรียมกลไก ช่องทาง บุคลากร	ตรวจพบและรายงาน — 5.2.10.2	ประเมินและตัดสินใจ	ตอบสนองและบรรเทา	บทเรียนและปรับปรุง

▼ 5.2.10.2 อยู่ใน Phase 2 — Detection & Reporting

① Trigger ที่ชัด

เหตุใดต้องรายงาน — ใคร เห็นอะไร เมื่อใด

② Channel หลายช่อง

Email · Hotline · Web Form · ChatOps

③ Form ข้อมูลขั้นต่ำ

Subject · Severity · Service · Time · Contact

④ Auto Ticket Generation

ออก ID อัตโนมัติ — ไม่สูญหายระหว่างทาง

⑤ Acknowledgement SLA

ตอบรับภายใน 15 นาที (Sev 1)

⑥ Triage & Severity

ประเมินผลกระทบและจัดลำดับ

⑦ Status Tracking

ผู้แจ้งดูสถานะได้ตลอดเวลา

⑧ Closure & PIR

ปิดเคสและสรุปบทเรียน

⑨ Lessons Learned Loop

Input สู่ Risk และ Improvement

Thank You

Website: https://cloudsecurity.ncsa.or.th/
Email: cloudsecurity.info@ncsa.or.th

INFOTEC