Institute of Internal Auditors Thailand | SET | ISACA Bangkok Chapter

IA Clinic 7/2026

Cloud Security Auditing

Coming soon

รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
Thailand Cyber Security & Privacy Officer (CSPO)
Huawei Technologies (Thailand) Co.,Ltd.

คุณกุสล ปิ่นมุข
CISA
กรรมการ ISACA Bangkok Chapter

เสวนาวันเสาร์ที่ 29 สิงหาคม 2569

เวลา 09.00-12.00 น.

ณ ห้องเสรี จินตนเสรี ชั้น 7 ตลาดหลักทรัพย์แห่งประเทศไทย

เสวนา On-site 60 ที่นั่ง หรือ Online ผ่าน Microsoft teams

เปิดลงทะเบียน

วันพฤหัสบดีที่ 20 สิงหาคม 2569
เวลา 11.00 น.

ติดต่อ IIA Thailand | member@theiiat.or.th | www.theiiat.or.th | 02-7129124 ต่อ 101-108

Institute of Internal Auditors Thailand | SET | ISACA Bangkok Chapter

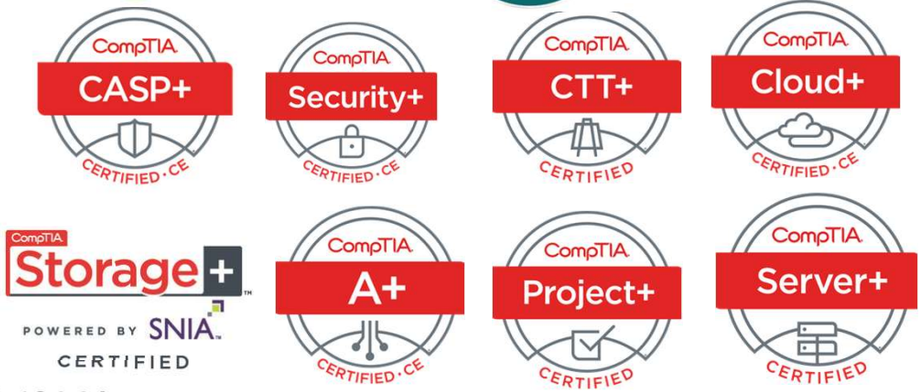
การตรวจประเมินความมั่นคงปลอดภัยของบริการ Cloud

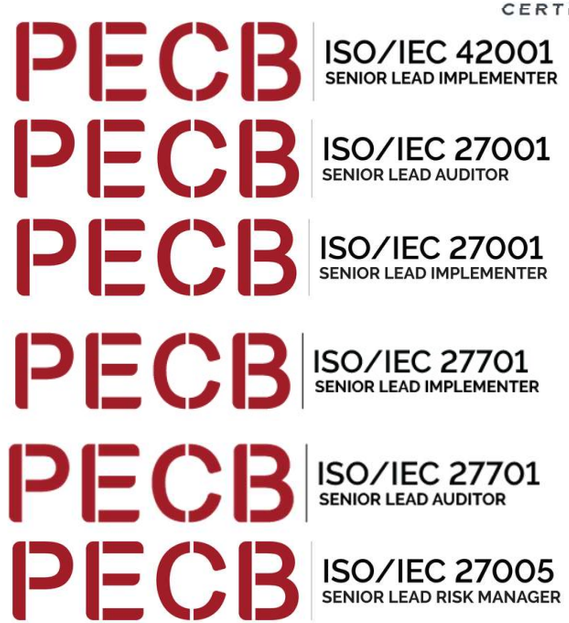
Cloud Security Auditing

รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
Thailand Cyber Security & Privacy Officer (CSPO)
Huawei Technologies (Thailand)

HUAWEI

Lifelong Learning in Practice





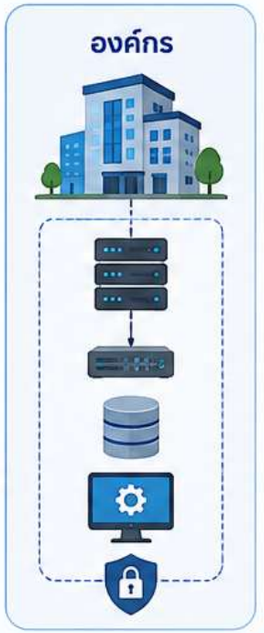
จาก Traditional IT สู่ Cloud

การเปลี่ยนแปลงรูปแบบการให้บริการเทคโนโลยีสารสนเทศ

รูปแบบตั้งเดิม (Traditional IT)

องค์กรเป็นผู้ควบคุมโดยตรงต่อ

- ศูนย์ข้อมูล (Data Center)
- เครื่องแม่ข่าย (Server)
- ระบบเครือข่าย (Network)
- ระบบจัดเก็บข้อมูล (Storage)
- ระบบปฏิบัติการ (Operating System)
- การควบคุมทางกายภาพ (Physical Security)



การเปลี่ยนจาก
"สิ่งที่องค์กรควบคุมเอง"
เป็น
"สิ่งที่องค์กรพึ่งพาผู้อื่น"

รูปแบบ Cloud

ความรับผิดชอบถูกแบ่งระหว่าง

- ผู้ให้บริการ Cloud (Cloud Service Provider: CSP)
- ผู้ใช้บริการ Cloud (Cloud Service Customer: CSC)
- ผู้พัฒนาระบบ
- ผู้ให้บริการภายนอก
- ผู้ให้บริการซอฟต์แวร์
- ผู้ประมวลผลข้อมูลช่วง (Subprocessor)

ประเด็นสำหรับ Auditor

การเปลี่ยนจาก "สิ่งที่องค์กรควบคุมเอง" เป็น "สิ่งที่องค์กรพึ่งพาผู้อื่น" ทำให้การตรวจสอบต้องเปลี่ยนจากการตรวจ Infrastructure ไปสู่การตรวจ **Governance, Responsibility, Configuration, Evidence** และ **Assurance**

Governance → Responsibility → Configuration → Evidence → Assurance

ความสำคัญของ Cloud Security Auditing

ส่วนที่ 1

รูปแบบดั้งเดิม (Traditional IT)

องค์กรเป็นผู้ควบคุมโดยตรงต่อ

- ศูนย์ข้อมูล (Data Center)
- เครื่องแม่ข่าย (Server)
- ระบบเครือข่าย (Network)
- ระบบจัดเก็บข้อมูล (Storage)
- ระบบปฏิบัติการ (Operating System)
- การควบคุมทางกายภาพ (Physical Security)

รูปแบบ Cloud

ความรับผิดชอบถูกแบ่งระหว่าง

- ผู้ให้บริการ Cloud (Cloud Service Provider: CSP)
- ผู้ใช้บริการ Cloud (Cloud Service Customer: CSC)
- ผู้พัฒนาระบบ
- ผู้ให้บริการภายนอก
- ผู้ให้บริการซอฟต์แวร์
- ผู้ประมวลผลข้อมูลช่วง (Subprocessor)

การเปลี่ยนจาก "สิ่งที่องค์กรควบคุมเอง" เป็น "สิ่งที่องค์กรพึ่งพาผู้อื่น" ทำให้การตรวจสอบต้องเปลี่ยนจากการตรวจ Infrastructure ไปสู่การตรวจ Governance, Responsibility, Configuration, Evidence และ Assurance

เหตุใด Cloud Security จึงต้องมีการตรวจประเมินเฉพาะด้าน

Cloud ก่อให้เกิดความเสี่ยงที่มีลักษณะเฉพาะ ซึ่งแตกต่างจากสภาพแวดล้อม IT แบบดั้งเดิมอย่างมีนัยสำคัญ

Misconfiguration
การกำหนดค่าระบบไม่ถูกต้อง

Improper Access Control
การจัดการสิทธิ์ไม่เหมาะสม

Third-Party Dependency
การพึ่งพาผู้ให้บริการภายนอก

Multi-Tenancy
ความเสี่ยงจากการใช้บริการร่วมกัน

API & Cloud-native Risk
การพึ่งพา API และบริการ Cloud-native

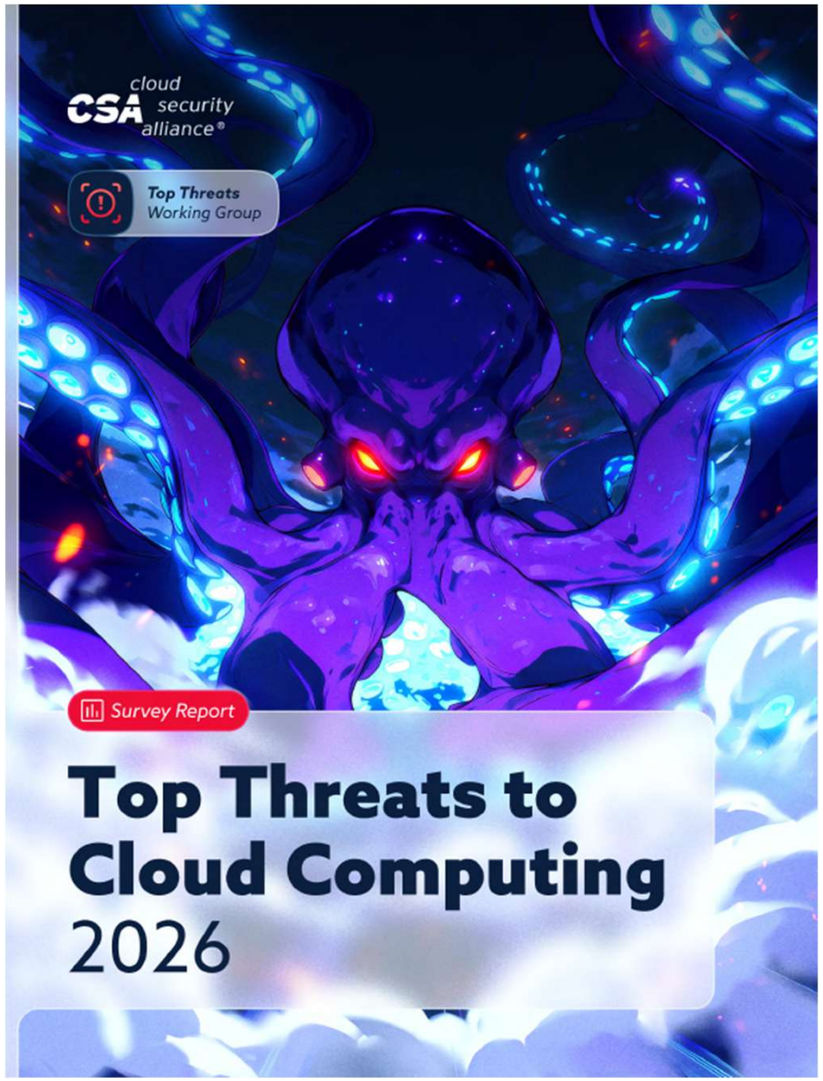
Jurisdictional & Exit Risk
ความเสี่ยงด้านเขตอำนาจศาลและการย้ายออกจากผู้ให้บริการ

Auditor ต้องประเมินทั้ง Technology + Governance + Contract + Compliance + Risk + Assurance

คำถามสำคัญ 6 ประการของผู้ตรวจประเมิน Cloud

คำถามทั้ง 6 ข้อนี้จะถูกนำกลับมาใช้ตลอดการบรรยาย และเป็นกรอบหลักในการตรวจประเมิน Cloud Security

1	**ใบรับรองของ CSP** ผู้ให้บริการมีใบรับรองแล้ว — องค์กรยังต้องตรวจอะไร?
2	**Data Location** ข้อมูลถูกจัดเก็บในประเทศไทย — ถือว่าเพียงพอหรือไม่?
3	**Data Localization** ข้อมูลหรือระบบที่มีความสำคัญสูง — ควรกำหนด Data Localization อย่างไร?
4	**ความรับผิดชอบเมื่อเกิดเหตุ** เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย — ใครเป็นผู้รับผิดชอบ?
5	**การพิสูจน์มาตรการ** มีมาตรการควบคุมแล้ว — จะพิสูจน์ได้อย่างไรว่ามาตรการทำงานจริง?
6	**Cloud Exit** หากต้องเปลี่ยนผู้ให้บริการ — องค์กรสามารถออกจาก Cloud ได้จริงหรือไม่?



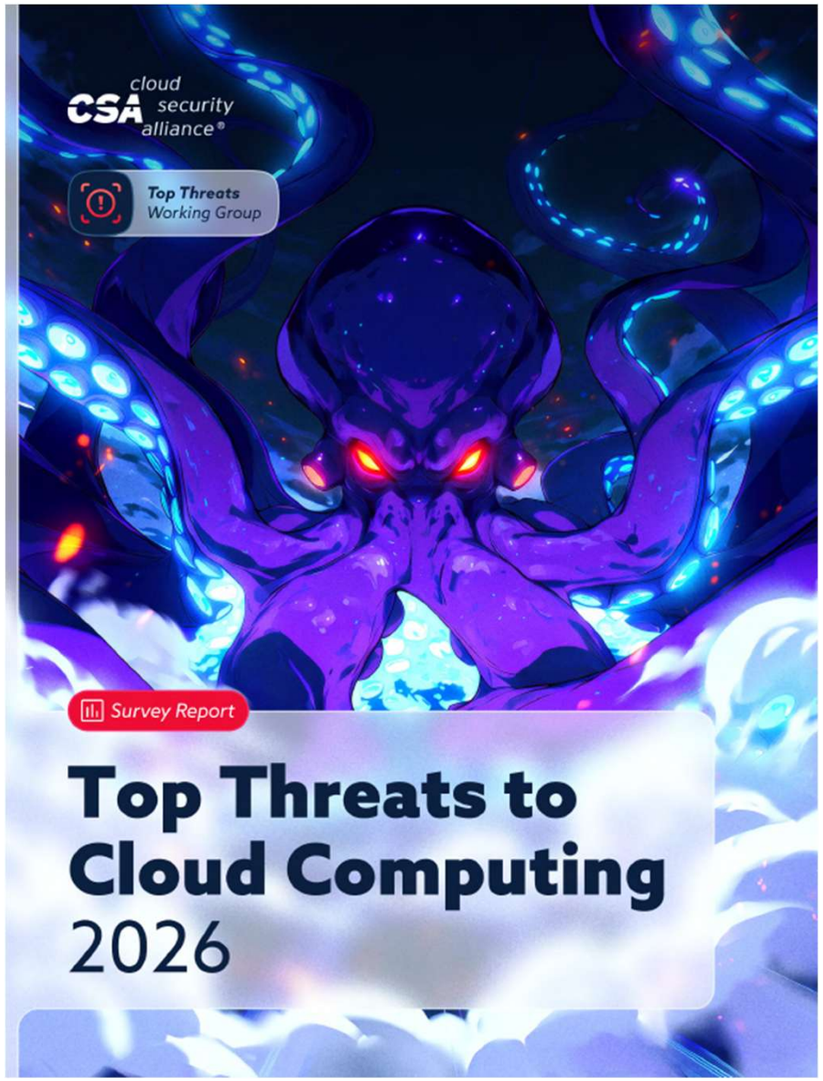
Four Priorities for 2026

1. **STRENGTHEN IDENTITY GOVERNANCE**
   Enhance controls for all identities

2. **TREAT AI SECURITY DOMAIN**
   Implement dedicated controls for AI

3. **IMPROVE CHANGE CONTROL**
   Govern third-party ecosystems effectively

4. **BUILD ORGANIZATIONAL QUALITY**
   Increase visibility, resilience, and operational awareness across cloud and AI



Rank	2026	2024
1	Inadequate Identity and Access Management *(Identity & Access Management in 2024 survey)*	Misconfiguration & Inadequate Change Control
2	AI (Artificial Intelligence)-Enhanced Attacks *(new in 2026)*	Identity & Access Management
3	Insecure Third-Party Resources	Insecure Interfaces and APIs
4	Insecure Interfaces and APIs	Inadequate Selection/Implementation of Cloud Security Strategy
5	Misconfiguration & Inadequate Change Control	Insecure Third-Party Resources
6	AI System Compromise (new in 2026)	Insecure Software Development
7	Advanced Persistent Threats	Accidental Cloud Disclosure
8	Lacking Cloud Security Strategy & Governance *(Inadequate Selection/Implementation of Cloud Security Strategy in 2024 survey)*	System Vulnerabilities
9	Insecure Software Development	Limited Cloud Visibility/Observability
10	Accidental Cloud Data Disclosure	Unauthenticated Resource Sharing
11	System Vulnerabilities	Advanced Persistent Threats

จากภัยคุกคามสู่การตรวจประเมิน

(Threat → Vulnerability → Risk → Control → Evidence)

ตัวอย่าง:

1. Threat	2. Vulnerability	3. Risk	4. Control	5. Evidence	6. Testing	7. Conclusion
การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี MFA สำหรับ Privileged Account	ผู้โจมตีสามารถเข้าถึงทรัพยากรสำคัญ	Multi-Factor Authentication	IAM Configuration + Authentication Log	ตรวจ Configuration + ทดสอบตัวอย่าง + ตรวจ Log	Control มีประสิทธิผลหรือไม่
ภัยคุกคามที่อาจโดดไปโดนกับข้อมูลหรือระบบ	จุดอ่อนหรือช่องโหว่ที่อาจถูกภัยคุกคามใช้ประโยชน์	ความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามผ่านช่องโหว่ ส่งผลกระทบต่อองค์กร	มาตรการควบคุมที่ออกแบบมาเพื่อลดหรือป้องกันความเสี่ยง	หลักฐานที่แสดงว่ามีการควบคุมและนำไปใช้งานจริง	กระบวนการตรวจสอบเพื่อประเมินว่าการควบคุมทำงานได้ตามที่กำหนดไว้หรือไม่	สรุปผลการตรวจสอบว่าการควบคุมมีประสิทธิผลเพียงใดในการลดความเสี่ยง

เริ่มต้นจากการเข้าใจภัยคุกคามและความเสี่ยง เพื่อออกแบบการตรวจที่มุ่งเน้นและสร้างคุณค่าให้กับองค์กร

Cloud Attack Surface

การใช้บริการ Cloud ทำให้พื้นที่ที่ต้องพิจารณาด้านความมั่นคงปลอดภัยไม่ได้จำกัดอยู่เฉพาะโครงสร้างพื้นฐาน แต่ครอบคลุมองค์ประกอบหลายระดับ

Identity & Access

บัญชีผู้ใช้งานและสิทธิ์การเข้าถึง รวมถึง Management Plane ช่องทางบริหารจัดการทรัพยากร Cloud

Workload & Application

VM, Container, Serverless และระบบงาน Application Services ที่ทำงานบน Cloud

Network & API

Virtual Network, Firewall, Security Group และ Application Programming Interface ที่เชื่อมต่อระบบ

Data & Configuration

ข้อมูลและฐานข้อมูล รวมถึงการกำหนดค่าทรัพยากรและ Third Party / Supply Chain

Auditor ต้องพิจารณา Attack Surface ที่สัมพันธ์กับขอบเขตการตรวจประเมิน (Audit Scope) และความเสี่ยงของบริการ

รูปแบบบริการ Cloud
(Cloud Service Models)

Infrastructure as a Service (IaaS)

องค์กรยังรับผิดชอบต่อ ระบบปฏิบัติการ Middleware Application และข้อมูล ในระดับสูง

- Data
- Application
- Middleware
- Operating System

Customer (รับผิดชอบ)

- Virtualization
- Compute
- Storage
- Network
- Physical Infrastructure

CSP (รับผิดชอบ)

ตัวอย่างบริการ

Amazon EC2, Microsoft Azure Virtual Machines, Google Compute Engine

Platform as a Service (PaaS)

CSP รับผิดชอบ Platform มากขึ้น ขณะที่ Customer เน้น Application และ Data

- Data
- Application

Customer (รับผิดชอบ)

- Runtime
- Middleware
- Operating System
- Virtualization
- Compute
- Storage
- Network
- Physical Infrastructure

CSP (รับผิดชอบ)

ตัวอย่างบริการ

Google App Engine, Azure App Service, Heroku

Software as a Service (SaaS)

CSP รับผิดชอบระบบส่วนใหญ่ แต่ Customer ยังคงต้องบริหาร Identity, Access, Data และ Configuration ที่ผู้ให้บริการเปิดให้ควบคุม

- Identity & Access
- Data
- Configuration

Customer (รับผิดชอบ)

- Application
- Middleware
- Operating System
- Virtualization
- Compute
- Storage
- Network
- Physical Infrastructure

CSP (รับผิดชอบ)

ตัวอย่างบริการ

Microsoft 365, Google Workspace, Salesforce

แบบจำลองความรับผิดชอบร่วม
(Shared Responsibility Model)

ประเด็น	CSP	Customer
ศูนย์ข้อมูลทางกายภาพ	✓	-
Hardware	✓	-
Cloud Platform	✓	-
Network Configuration	✓	-
Identity & Access	-	✓
Application	ขึ้นกับบริการ	✓
Data	-	✓
Security Monitoring	✓	✓
Incident Response	✓	✓

ข้อสำคัญ

ขอบเขตจริงต้องอ้างอิงบริการและสัญญาที่ใช้งานจริง ไม่ควรสรุปจาก Model ทั่วไปเพียงอย่างเดียว

Shared Responsibility ≠ Shared Accountability

Responsibility

ใครเป็นผู้ดำเนินการควบคุม?

Accountability

ใครต้องรับผิดชอบต่อผลลัพธ์?

ตัวอย่างที่ชัดเจน

CSP มีหน้าที่จัดให้บริการ IAM มีความสามารถด้าน MFA แต่ Customer อาจยังมีหน้าที่

- เปิดใช้ MFA
- กำหนด Policy
- ตรวจสอบ Privileged Account
- ทบทวนสิทธิ์

การที่ CSP มี Security Capability ไม่ได้หมายความว่า Customer ได้ดำเนินการ Security Control นั้นแล้ว

CSP มี ISO/IEC 27001 แล้ว ยังต้อง Audit หรือไม่?

คำตอบ: ยังต้องพิจารณาตรวจประเมิน

ตรวจ Scope ของใบรับรอง

ใบรับรองครอบคลุมบริการที่ใช้งานหรือไม่? Scope ครอบคลุม Region หรือไม่? Control ที่เกี่ยวข้องอยู่ใน Scope หรือไม่?

ตรวจ Customer Responsibility

Customer Responsibility คืออะไร? Customer Configuration ถูกต้องหรือไม่? มีข้อยกเว้นหรือไม่?

ตรวจ Evidence

Evidence เพียงพอหรือไม่? หลักฐานสนับสนุนการให้ความเชื่อมั่นได้ในระดับใด?

CSP Certification เป็นส่วนหนึ่งของ Assurance ไม่ใช่ Assurance ทั้งหมด

Certification Scope กับ Customer Scope

ต้องเปรียบเทียบ Certification Scope กับ Actual Service

และ Customer Environment

Application Scope

CSP มี ISO/IEC 27001 ครอบคลุม "Cloud Platform" แต่ Application ของ Customer อยู่ใน Scope หรือไม่?

Region Scope

Region ที่ Customer ใช้งาน อยู่ใน Scope ของใบรับรอง หรือไม่?

Managed Service Scope

Managed Service ที่ Customer ใช้เพิ่มเติมอยู่ใน Scope หรือไม่?

Assurance Hierarchy

จาก Certificate สู่ Assurance

Certificate / Attestation	หลักฐานจากผู้ให้บริการภายนอก เช่น ISO, SOC, CSA STAR
Scope Verification	ตรวจสอบขอบเขต (Scope) ครอบคลุมบริการ/ระบบ/ภูมิภาค ที่เกี่ยวข้องหรือไม่
Control Assessment	ประเมินการออกแบบของการควบคุม ตามมาตรฐาน/เกณฑ์ที่เกี่ยวข้อง
Customer Configuration	ตรวจสอบการตั้งค่าและการใช้งาน ของลูกค้า (Customer Responsibility)
Operating Evidence	รวบรวมหลักฐานจากการปฏิบัติงานจริง ในช่วงเวลาที่ตรวจสอบ
Testing	ทำการทดสอบ/สอบทาน เพื่อยืนยันการทำงาน
Effectiveness	ประเมินประสิทธิผลของการควบคุม ในการลดความเสี่ยง
Assurance	ให้ความเชื่อมั่นอย่างมีเหตุผลและ อยู่บนหลักฐานที่เพียงพอ

หลักการ “Trust but Verify”

ผู้ตรวจประเมินไม่ควร
“เชื่อเพราะมีใบรับรอง” ✗

และไม่จำเป็นต้อง
“ตรวจทุกอย่างด้วยตนเอง” ✗

แต่ควรใช้แนวทาง
Trust + Verify + Corroborate ✓

กรอบกำกับดูแล Cloud Security ของประเทศไทย

กฎหมายด้านความมั่นคงปลอดภัยไซเบอร์

กำหนดมาตรการขั้นต่ำสำหรับการดูแลความมั่นคงปลอดภัยของระบ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

กำหนดหลักเกณฑ์การประมวลผลและการคุ้มครองข้อมูลส่วนบุคคล

ข้อกำหนดของหน่วยงานกำกับดูแล

ข้อกำหนดเฉพาะของแต่ละหน่วยงานกำกับดูแลในภาคส่วนต่าง ๆ

มาตรฐานด้าน Cloud Security

มาตรฐานของ สกมช. พ.ศ. 2567 และมาตรฐานสากล ISO/IEC 27001, 27017, 27018, 27701 และ CSA STAR

หลักการ: Regulatory Requirement → Control Requirement → Audit Criteria

Cloud Responsibility Matrix

การควบคุม	CSP	Customer	ร่วมกัน
Physical Security	✓	—	—
Cloud Infrastructure	✓	—	—
Identity & Access Management	✓	✓	—
Data Classification	—	✓	—
Encryption	✓	✓	✓
Logging & Monitoring	✓	✓	✓
Incident Response	✓	✓	✓
Backup & Recovery	ขึ้นกับบริการ	✓	✓
Configuration Management	✓	✓	✓
Regulatory Compliance	—	✓	✓

ตารางนี้เป็นตัวอย่างเชิงหลักการ ต้องปรับตาม Cloud Service Model, CSP และบริการที่ใช้งานจริง

จากข้อกำหนดสู่การตรวจประเมิน
(From Audit Criteria to Audit Testing)

Audit Criteria
เกณฑ์การตรวจประเมิน
- กำหนดจากกฎหมาย มาตรฐาน นโยบาย
- ใช้เป็นเกณฑ์ในการตัดสินผลการตรวจประเมิน

Risk
ความเสี่ยงที่ต้องควบคุม
- ระบุความเสี่ยงที่อาจทำให้วัตถุประสงค์ไม่บรรลุ
- พิจารณาผลกระทบและโอกาสเกิด

Control Objective
วัตถุประสงค์ของการควบคุม
- กำหนดสิ่งที่ต้องการควบคุมเพื่อลดความเสี่ยง
- ต้องวัดผลและประเมินได้

Control Design
การออกแบบมาตรการควบคุม
- กำหนดวิธีการควบคุมให้บรรลุวัตถุประสงค์
- กำหนดผู้รับผิดชอบ กระบวนการ และเกณฑ์ต่าง ๆ

Implementation
การนำมาตรการไปปฏิบัติ
- นำมาตรการควบคุมไปใช้งานจริง
- มีการสื่อสาร ฝึกอบรม และติดตามผล

Key Message: Auditor ไม่ควรเริ่มต้นจากการค้นหา Evidence แต่ควรเริ่มจากการทำความเข้าใจ Risk และ Control Objective ก่อน

จาก Implementation สู่ Control Effectiveness

(From Implementation to Control Effectiveness)

ต่อจาก Slide ก่อนหน้า

Implementation
การนำการควบคุมไปสู่การปฏิบัติ

Operating Evidence
หลักฐานจากการปฏิบัติงานจริง
รวบรวมหลักฐานที่แสดงว่าการควบคุมถูกใช้งานจริง

Audit Testing
การทดสอบการควบคุม
ตรวจสอบและทดสอบเพื่อประเมินผลการควบคุม

Control Effectiveness
ประสิทธิผลของการควบคุม
สรุปผลว่าการควบคุมมีประสิทธิผลเพียงใด

Design Effectiveness

การควบคุมถูกออกแบบอย่างเหมาะสมหรือไม่

ตัวอย่าง:

กำหนดให้ Privileged Account ต้องใช้ MFA

Operating Effectiveness

การควบคุมถูกนำไปปฏิบัติและทำงานจริงหรือไม่

ตัวอย่าง:

ตรวจพบว่า Privileged Account ทั้งหมดมี MFA และมีหลักฐานการใช้งานจริง

ตรงนี้เป็นจุดที่สำคัญมาก เพราะการมี Control ไม่ได้แปลว่า Control มีประสิทธิผล

Policy มี
≠
Control ถูกออกแบบดี
≠
Control ถูก Implement
≠
Control ทำงานจริง
≠
Control มีประสิทธิผล

จาก Control Effectiveness สู่ Assurance

(From Control Effectiveness to Assurance)

Flow สุดท้าย:

Control Effectiveness	ประเมินว่าการควบคุมที่ออกแบบไว้สามารถลดความเสี่ยงได้ตามวัตถุประสงค์
Finding ข้อค้นพบจากการตรวจประเมิน	รวบรวมและวิเคราะห์หลักฐานเพื่อระบุจุดแข็งและจุดอ่อน
Risk Evaluation การประเมินผลกระทบและความเสี่ยง	ประเมินผลกระทบและโอกาสที่จะเกิดขึ้นจากจุดอ่อนที่พบ
Residual Risk ความเสี่ยงคงเหลือ	ประเมินความเสี่ยงที่ยังคงเหลืออยู่หลังจากมีการควบคุม
Audit Conclusion ข้อสรุปจากการตรวจประเมิน	สรุประดับประสิทธิผลของการควบคุมและผลกระทบต่อความเสี่ยงโดยรวม
Assurance การให้ความเชื่อมั่น	ให้ความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสียตามระดับความเสี่ยงที่ยอมรับได้

กรณีศึกษา: Privileged Account

Audit Criteria	กำหนดให้ Privileged Account ต้องมี MFA
Risk	การยึดครองบัญชีผู้มีสิทธิ์สูง
Control	บังคับใช้ MFA
Implementation	MFA ถูกเปิดใช้งาน
Evidence	IAM Configuration + Account List + Authentication Log
Testing	สุ่มตรวจ Privileged Account
Finding	พบ 2 จาก 50 Account ไม่มี MFA
Residual Risk	ยังมีความเสี่ยงจาก Account ที่ไม่ได้รับการป้องกัน
Conclusion	Control Partially Effective
Assurance	องค์กรสามารถให้ความเชื่อมั่นได้ในระดับหนึ่ง แต่ยังมีประเด็นที่ต้องดำเนินการแก้ไข

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

มาตรฐานของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2567 กำหนดแนวทางและมาตรการขั้นต่ำสำหรับการดูแลความมั่นคงปลอดภัยของข้อมูล บริการ และโครงสร้างพื้นฐานระบบ Cloud

วันมีผลบังคับใช้

10 กันยายน 2569

การเชื่อมโยงมาตรฐาน

ISO/IEC 27001, 27017, 27018, 27701 และ CSA STAR

การนำไปใช้

ใช้เป็น Audit Criteria และ Control Baseline ไม่ใช่เพียง Compliance Checklist

ประเด็นควบคุมที่เกี่ยวข้องกับการตรวจ Cloud

จากโครงสร้างมาตรฐาน สกมช. สามารถจัดกลุ่มประเด็นตรวจได้ดังนี้

Governance & Asset

การกำกับดูแล และการจัดการทรัพย์สิน

Access & Cryptography

การควบคุมการเข้าถึง และการเข้ารหัสและการจัดการกุญแจ

Operations & Network

ความมั่นคงปลอดภัยการปฏิบัติการและความมั่นคงปลอดภัยเครือข่าย

Development & Third Party

การพัฒนาระบบอย่างปลอดภัย และผู้ให้บริการภายนอก

Incident Management

การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

Regulatory Requirement สู่ Audit Criteria

ตัวอย่าง

ข้อกำหนด	ต้องมีการควบคุมการเข้าถึง
Audit Criteria	องค์กรมีการควบคุมการเข้าถึงตามหลัก Least Privilege หรือไม่?
Control Objective	จำกัดการเข้าถึงเฉพาะผู้มีสิทธิ์
Evidence	IAM Configuration / Access Review
Testing	ตรวจ Population + Sampling + Configuration

Compliance กับ Security Assurance

Compliance

"ปฏิบัติตามข้อกำหนดหรือไม่?"

Security Assurance

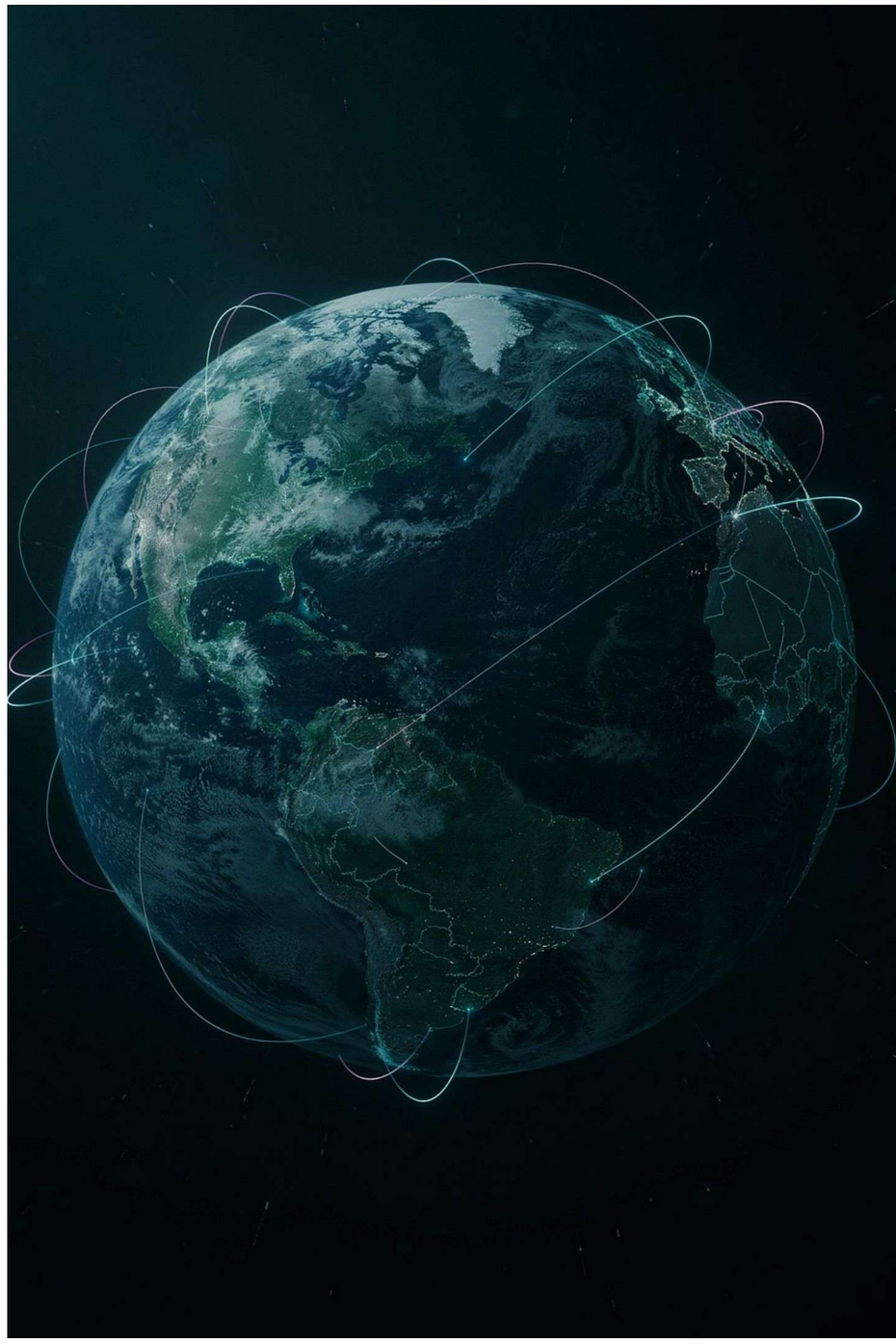
"เรามีหลักฐานเพียงพอที่จะเชื่อได้หรือไม่ว่าความเสี่ยงได้รับการควบคุมอย่างเหมาะสม?"

ดังนั้น

Compliance เป็นส่วนหนึ่งของ Assurance แต่ไม่ใช่ทั้งหมดของ Assurance

Data Sovereignty & Data Localization

อธิปไตยข้อมูลไม่ได้พิจารณาเพียงว่าข้อมูลถูกเก็บไว้ที่ใด
แต่รวมถึงกฎหมาย การเข้าถึง อำนาจควบคุม และเขตอำนาจศาล
ที่ครอบคลุมข้อมูลนั้น



อธิปไตยข้อมูล (Data Sovereignty)

กฎหมายที่ใช้บังคับ

ข้อมูลอยู่ภายใต้กฎหมายใด? ผู้ให้บริการหรือ Subprocessor อยู่ภายใต้เขตอำนาจใด?

การเข้าถึงและอำนาจควบคุม

ใครสามารถเข้าถึงข้อมูล? ใครมีอำนาจควบคุม? Encryption Key ถูกควบคุมโดยใคร?

การประมวลผลและที่ตั้ง

ข้อมูลถูกประมวลผลที่ใด? ไม่ใช่เพียงแค่ถูกจัดเก็บที่ใด

Data Residency เป็นเพียงองค์ประกอบหนึ่งของ Data Sovereignty
— "ข้อมูลอยู่ประเทศไทย" ไม่ได้หมายความว่าครอบคลุมทุกมิติของ Data Sovereignty

"ข้อมูลอยู่ประเทศไทย" เพียงพอหรือไม่?

ไม่ควรสรุปจาก Location เพียงอย่างเดียว Auditor ควรตรวจสอบครบทุกมิติ

Primary Storage

ข้อมูลหลักอยู่ที่ใด?

Backup & DR

Backup และ Disaster Recovery อยู่ที่ใด?

Data Processing

ข้อมูลถูกประมวลผลที่ใด?

Metadata & Logging

Metadata และ Log อยู่ที่ใด?

Encryption Key

กุญแจเข้ารหัสถูกควบคุมโดยใคร?

Administrative Access

ผู้ดูแลระบบอยู่ที่ใด?

Subprocessor

ผู้ประมวลผลช่วงอยู่ที่ใด?

Cross-Border Transfer

มีการโอนข้อมูลข้ามพรมแดนหรือไม่?

Jurisdiction & Deletion

อยู่ภายใต้กฎหมายใด? พิสูจน์การลบข้อมูลได้หรือไม่?

Data Sovereignty Assessment

(Data Sovereignty Assessment)

ให้ประเมินอย่างเป็นระบบ เพื่อให้มั่นใจว่าข้อมูลถูกจัดเก็บและประมวลผลตามข้อกำหนดด้านอำนาจอธิปไตยของข้อมูล

Data	Classification	Criticality	Processing	Storage	Backup / DR	Key Management	Administrative Access	Subprocessor	Jurisdiction
ระบุข้อมูลที่อยู่ในขอบเขตการประเมิน • ประเภทข้อมูล (Personal, Confidential, Restricted ฯลฯ) • แหล่งที่มาของข้อมูล • เจ้าของข้อมูล	จัดระดับความลับของข้อมูล • Public • Internal • Confidential • Restricted	ประเมินความสำคัญและผลกระทบหากข้อมูลรั่วไหลหรือสูญหาย • Impact ต่อองค์กร • Impact ต่อบุคคล • Legal / Regulatory Impact • Reputation Impact	พิจารณาการประมวลผลของข้อมูล • สถานที่ประมวลผล • ผู้ประมวลผล • วัตถุประสงค์การประมวลผล • การส่งข้อมูลข้ามแดน (Cross-border Transfer)	พิจารณาสถานที่จัดเก็บข้อมูลหลัก • ประเทศที่จัดเก็บ • ประเภทบริการ (IaaS / PaaS / SaaS) • Region / Zone • Data Residency	พิจารณาการสำรองข้อมูลและแผนกู้คืนระบบ • สถานที่สำรองข้อมูล • ความถี่ในการสำรองข้อมูล • แผน DR และสถานที่กู้คืน • การทดสอบแผน DR	พิจารณาการจัดการกุญแจเข้ารหัส • ใครเป็นผู้ถือครองกุญแจ • สถานที่จัดการกุญแจ • วิธีการหมุนเวียนกุญแจ • การแยกบทบาท (Separation of Duty)	พิจารณาการเข้าถึงโดยผู้ดูแลระบบ • ผู้ดูแลของ CSP • สิทธิ์การเข้าถึง • การเข้าถึงจากประเทศใดบ้าง • การบันทึกและติดตามการเข้าถึง	พิจารณาผู้ประมวลผลช่วง (Subprocessor) • รายชื่อ Subprocessor • สถานที่ตั้ง • ข้อตกลงและภาระผูกพัน • ความสามารถในการควบคุมและตรวจสอบ	พิจารณากฎหมายและอำนาจศาลที่เกี่ยวข้อง • กฎหมายคุ้มครองข้อมูลส่วนบุคคล • กฎหมายของประเทศที่มีอำนาจบังคับใช้ • ความเสี่ยงจากกฎหมายต่างประเทศ (เช่น Cloud Act)

Exit — พิจารณาความสามารถในการออกจากบริการ (Exit Strategy)

- ความสามารถในการส่งออกข้อมูล
- รูปแบบข้อมูล (Export Format)
- ระยะเวลาการส่งคืนข้อมูล
- การลบข้อมูลอย่างถาวร
- ค่าใช้จ่ายในการออกจากบริการ
- ผลกระทบต่อธุรกิจเมื่อย้ายออก

ผลลัพธ์ของการประเมิน

- ☑ ทราบตำแหน่งและการไหลของข้อมูล
- ☑ มั่นใจว่าสอดคล้องกับกฎหมายและข้อกำหนด
- ☑ ลดความเสี่ยงด้านกฎหมายและชื่อเสียง
- ☑ สนับสนุนการตัดสินใจเลือกใช้ Cloud Service อย่างเหมาะสม
- ☑ เตรียมความพร้อมสำหรับการตรวจสอบ (Audit)

Risk-Based Data Localization

ไม่ควรใช้หลัก "ข้อมูลทุกประเภทต้องอยู่ในประเทศ" แต่ควรพิจารณาตามปัจจัยความเสี่ยง

Data & System Criticality

ระดับความสำคัญของข้อมูล (Data Criticality) และความสำคัญของระบบ (System Criticality) เป็นปัจจัยหลักในการพิจารณา

National Security & Regulatory

ผลกระทบต่อความมั่นคง (National Security Impact) และข้อกำหนดทางกฎหมาย (Regulatory Requirements) ที่บังคับใช้

Jurisdictional & Exposure Risk

ความเสี่ยงด้านเขตอำนาจศาล (Jurisdictional Risk) และผลกระทบจากการเปิดเผยข้อมูล

Cross-Border Processing Necessity

ความจำเป็นในการประมวลผลข้ามประเทศ ซึ่งอาจมีเหตุผลทางธุรกิจที่ชัดเจน

ระบบและข้อมูลที่มีผลกระทบสูง

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณาครบทุกมิติ

Location
ข้อมูลอยู่ที่ใด?

Jurisdiction
อยู่ภายใต้กฎหมายใด?

Access
ใครสามารถเข้าถึง?

Processing
ใครประมวลผล?

Key Management
ใครควบคุมกุญแจ?

Resilience & Exit
หาก Region หยุดทำงานจะเกิดอะไรขึ้น?
หากต้องย้ายออกจะทำอย่างไร?

แนวปฏิบัติระหว่างประเทศ (International Practices)

EU/ENISA Benchmark

ใช้แนวปฏิบัติของสหภาพยุโรปและหน่วยงาน ENISA เป็น Benchmark เพื่อพิจารณาเรื่อง

- Cloud Security
- Cloud Assurance
- Data Protection
- Resilience
- Supply Chain
- Sovereignty
- Dependency Risk

ข้อควรระวัง

แนวปฏิบัติของ EU/ENISA ไม่ควรถูกนำเสนอเสมือนเป็นกฎหมายที่ใช้บังคับกับทุกองค์กรในประเทศไทย

แต่ควรใช้เป็น **International Benchmark / Reference Practice** เพื่อเปรียบเทียบและยกระดับมาตรฐานการตรวจประเมิน

การนำแนวปฏิบัติสากลมาใช้ต้องปรับให้สอดคล้องกับบริบทและข้อกำหนดของประเทศไทย

คำถามสำหรับ Auditor ด้าน Data Sovereignty

เมื่อมีการใช้ Cloud ให้ถามคำถามเหล่านี้อย่างเป็นระบบ

- **ข้อมูลอยู่ที่ไหน? ถูกประมวลผลที่ไหน?**
  ตรวจสอบทั้ง Primary Storage, Backup และ Disaster Recovery
- **Encryption Key และ Administrator อยู่ที่ไหน?**
  ตรวจสอบว่าใครควบคุมกุญแจเข้ารหัส และผู้ดูแลระบบตั้งอยู่ที่ใด
- **Subprocessor อยู่ที่ไหน? อยู่ภายใต้กฎหมายใด?**
  ตรวจสอบผู้ประมวลผลช่วงและเขตอำนาจศาลที่ครอบคลุม
- **หากต้องลบข้อมูล เราพิสูจน์การลบได้หรือไม่?**
  ตรวจสอบกระบวนการและหลักฐานการลบข้อมูลอย่างถาวร

สรุปสาระสำคัญ: Cloud Security Auditing

Shared Responsibility

ความรับผิดชอบถูกแบ่งระหว่าง CSP และ Customer — Auditor ต้องระบุให้ชัดว่าใครรับผิดชอบอะไร

Control Effectiveness

การมี Policy ≠ Control ทำงานจริง — ต้องตรวจทั้ง Design และ Operating Effectiveness

Data Sovereignty

"ข้อมูลอยู่ในประเทศ" ไม่เพียงพอ — ต้องประเมินครบทุกมิติตั้งแต่ Storage ถึง Jurisdiction

Assurance ≠ Compliance

Compliance เป็นส่วนหนึ่งของ Assurance — Auditor ต้องให้ความเชื่อมั่นที่มีหลักฐานรองรับ

เริ่มจาก Audit Criteria → Risk → Control Objective → Evidence → Testing → Conclusion → Assurance

บทบาทของมาตรฐานต่อ Cloud Audit

แนวคิดที่ไม่ถูกต้อง

มาตรฐานไม่ควรถูกใช้ในลักษณะ

"ตรวจมาตรฐานทีละฉบับ"

เพราะจะทำให้การตรวจประเมินขาดทิศทางและไม่สามารถเชื่อมโยงกับความเสี่ยงที่แท้จริงขององค์กรได้

แนวคิดที่ถูกต้อง: ใช้เป็น Audit Criteria

มาตรฐานควรถูกนำมาใช้เป็น **Audit Criteria** เพื่อกำหนดองค์ประกอบสำคัญของการตรวจประเมิน ได้แก่

- สิ่งที่ต้องควบคุม
- วัตถุประสงค์ของการควบคุม
- ขอบเขตการตรวจประเมิน
- หลักฐานที่ต้องรวบรวม
- วิธีการทดสอบ

SLIDE 36

ISO/IEC 27001 — ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ISO/IEC 27001 ใช้เป็น **กรอบหลัก** ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ครอบคลุมมิติสำคัญหลายด้าน

Governance & Risk
Governance, Risk Management, Security Objectives

Control Management
Control Management, Internal Audit, Management Review

Continual Improvement
กระบวนการปรับปรุงอย่างต่อเนื่องตามวงจร PDCA

ใน Cloud Audit: ใช้ตรวจว่า Cloud Security ถูกบูรณาการเข้ากับ ISMS ขององค์กรหรือไม่
— ไม่ใช่แค่ว่า CSP มีใบรับรองหรือเปล่า

ISO/IEC 27017 — แนวปฏิบัติด้านความมั่นคงปลอดภัยสำหรับบริการ Cloud

ประเด็นเฉพาะของ Cloud

ISO/IEC 27017 เน้นประเด็นที่มีลักษณะเฉพาะของสภาพแวดล้อม Cloud ซึ่งไม่ครอบคลุมใน ISO/IEC 27001 ทั่วไป ได้แก่

- Shared Responsibility
- Cloud Service Provision
- Cloud Service Customer
- Virtual Environment
- Cloud Operations
- Customer / Provider Responsibilities

บทบาทของ Auditor

ใช้ ISO/IEC 27017 เป็น **เกณฑ์เพิ่มเติม** จาก ISO/IEC 27001 เพื่อพิจารณาความเสี่ยงเฉพาะของ Cloud ที่ต้องการการควบคุมในระดับที่ละเอียดกว่ามาตรฐานทั่วไป โดยเฉพาะในประเด็น Shared Responsibility ที่ต้องกำหนดให้ชัดเจนว่าใครรับผิดชอบส่วนใด

SLIDE 38

ISO/IEC 27018 — การคุ้มครองข้อมูลส่วนบุคคลใน Public Cloud

PII Protection

เน้นการคุ้มครอง Personally Identifiable Information (PII) และการประมวลผลข้อมูลส่วนบุคคลอย่างโปร่งใส

การควบคุมการประมวลผล

ครอบคลุมการควบคุมการประมวลผล การลบข้อมูล และการเปิดเผยข้อมูลต่อบุคคลที่สาม

เหมาะกับ Public Cloud + Personal Data

เหมาะสำหรับการ Audit ที่เกี่ยวข้องกับ Public Cloud ที่มีการประมวลผลข้อมูลส่วนบุคคล

CSA Cloud Controls Matrix (CSA CCM)

ภาพรวม CCM

CCM เป็น **กรอบการควบคุมเฉพาะสำหรับ Cloud** ที่ช่วยจัดโครงสร้างการประเมิน Security Controls ของ Cloud Environment ปัจจุบัน CSA เผยแพร่ **CCM v4.1** ซึ่งมี **207 Controls ใน 17 Security Domains**

ตัวอย่าง Security Domains

- Audit & Assurance
- Application & Interface Security
- Business Continuity
- Configuration Management
- Cryptography
- Data Security & Privacy
- Governance
- Identity & Access

CAIQ — Consensus Assessments Initiative Questionnaire

CAIQ เป็นชุดคำถามแบบ **Yes/No** ที่ใช้ประเมินมาตรการควบคุมด้าน Cloud โดยอยู่ในรูปแบบที่สามารถใช้สอบถาม CSP อย่างเป็นระบบ ตาม CSA ระบุว่า CAIQ ช่วยประเมิน Security Controls ของ Cloud Provider ได้อย่างมีโครงสร้าง

CSP Assessment

ประเมินความสามารถด้านความมั่นคงปลอดภัยของผู้ให้บริการ Cloud

Third-Party Risk Assessment

ใช้ประเมินความเสี่ยงจากบุคคลที่สามในห่วงโซ่อุปทาน

Security Due Diligence

ใช้ในกระบวนการตรวจสอบความพร้อมด้านความมั่นคงปลอดภัย

Audit Preparation & Evidence

ใช้เตรียมการตรวจประเมินและรวบรวม Control Evidence

CSA STAR — Security, Trust, Assurance and Risk

CSA STAR คืออะไร?

CSA STAR เป็นโครงการด้าน **Cloud Security Assurance** ที่ให้ระดับการรับรองแตกต่างกันตามความเข้มข้นของการประเมิน

ระดับสำคัญ

STAR Level 1 — Self-Assessment

องค์กรประเมินตนเองและเผยแพร่ผลการประเมินต่อสาธารณะ

STAR Level 2 — Certification / Third-Party Attestation

ผ่านการรับรองหรือการตรวจสอบโดยบุคคลที่สาม

⚠ ประเด็นสำคัญสำหรับ Auditor: STAR เป็นหลักฐานด้าน Provider Assurance แต่ต้องพิจารณาความเกี่ยวข้องกับบริการและ Customer Environment ที่ตรวจจริง — ไม่สามารถใช้ปิดประเด็น Audit ได้ทั้งหมด

การใช้ Framework ร่วมกัน

ตัวอย่างแนวทาง

Regulation	กฎหมาย ข้อบังคับ และแนวทางจากหน่วยงานกำกับดูแล
ISO/IEC 27001	ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ISO/IEC 27017 / 27018	แนวทางสำหรับการรักษาความมั่นคงปลอดภัยของบริการคลาวด์ และข้อมูลส่วนบุคคล
CSA CCM	แนวทางการควบคุมความมั่นคงปลอดภัยบนคลาวด์
Customer Control	การควบคุมที่ลูกค้าต้องดำเนินการตามความรับผิดชอบ
Audit Evidence	หลักฐานที่เกี่ยวข้องและเพียงพอต่อการตรวจประเมิน
Testing	การทดสอบและประเมินประสิทธิผลของการควบคุม

ไม่จำเป็นต้องตรวจทุก Framework แยกจากกัน

สิ่งสำคัญคือการสร้าง Control Mapping และหลีกเลี่ยงการตรวจซ้ำ

เป้าหมายคือ ตรวจเท่าที่จำเป็น ครอบคลุมในสิ่งที่สำคัญ และให้ Assurance ได้อย่างมีประสิทธิภาพ

กระบวนการตรวจประเมิน Cloud (Cloud Security Audit Methodology)

Cloud Security Audit Lifecycle

แนวทางการตรวจประเมินความมั่นคงปลอดภัยสำหรับบริการ Cloud อย่างเป็นระบบ เพื่อให้ได้หลักฐานที่เพียงพอและสรุปผลได้อย่างน่าเชื่อถือ

1. Planning

- กำหนดวัตถุประสงค์ ขอบเขตเบื้องต้น และแนวทางการตรวจประเมิน
- ทำความเข้าใจธุรกิจ บริการ Cloud ที่ใช้ และผู้มีส่วนเกี่ยวข้อง
- จัดทำแผนการตรวจ และกำหนดทรัพยากรที่จำเป็น

2. Scoping

- กำหนดขอบเขตการตรวจประเมินให้ชัดเจน
- ระบุบริการ ระบบ ข้อมูล สภาพแวดล้อม ระยะเวลา และข้อยกเว้น
- ระบุผู้ให้บริการ Cloud (CSP) และ Third Party ที่เกี่ยวข้อง

3. Risk Assessment

- ระบุและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัย Cloud
- พิจารณาความเสี่ยงตาม Shared Responsibility
- จัดลำดับความเสี่ยง เพื่อกำหนดประเด็นสำคัญที่ต้องตรวจสอบ

4. Define Criteria

- กำหนดเกณฑ์การตรวจประเมินจากกฎหมาย มาตรฐาน นโยบาย สัญญา และแนวปฏิบัติที่เกี่ยวข้อง
- จัดทำ Audit Program และ Checklist

5. Identify Controls

- ระบุมาตรการควบคุมที่เกี่ยวข้องเพื่อลดความเสี่ยง ให้สอดคล้องกับเกณฑ์การตรวจประเมิน
- จัดทำ Control Matrix / Responsibility Matrix
- ระบุวัตถุประสงค์ของการควบคุม (Control Objectives)

6. Obtain Evidence

- รวบรวมหลักฐานจากผู้ให้บริการ Cloud (CSP) และจากองค์กร
- เอกสาร นโยบาย การตั้งค่า Log รายงาน ผลการทดสอบ และหลักฐานอื่นๆ
- ประเมินความเพียงพอ และความน่าเชื่อถือของหลักฐาน

7. Test Controls

- ทดสอบการออกแบบ (Design Effectiveness)
- ทดสอบการปฏิบัติจริง (Operating Effectiveness)
- ใช้เทคนิคการตรวจสอบ เช่น Inspection, Observation, Sampling, Re-performance, CAATs
- บันทึกผลการทดสอบและข้อสังเกต

8. Evaluate Findings

- ประเมินผลการทดสอบ วิเคราะห์สาเหตุและผลกระทบ
- จัดระดับความรุนแรง และระบุความเสี่ยงคงเหลือ (Residual Risk)
- จัดลำดับประเด็นที่ต้องดำเนินการ

9. Report

- จัดทำรายงานผลการตรวจประเมิน
- นำเสนอข้อค้นพบ ข้อเสนอแนะ และแผนการปรับปรุง
- สื่อสารกับผู้บริหารและผู้มีส่วนเกี่ยวข้อง

10. Follow-up

- ติดตามการดำเนินการปรับปรุงแก้ไขตามข้อเสนอแนะ
- ประเมินผลความเพียงพอของการแก้ไข
- ปิดประเด็นการตรวจสอบ และรวบรวมบทเรียนเพื่อพัฒนาการตรวจในครั้งถัดไป

หลักการสำคัญ (Key Principles)

- เป็นอิสระ (Independence)
- มีความสามารถและความเชี่ยวชาญ (Competence)
- ใช้หลักฐานและข้อมูลเป็นฐาน (Evidence-based)
- เน้นความเสี่ยง (Risk-based)
- รักษาความลับและจริยธรรมวิชาชีพ (Confidentiality)

เป้าหมายสุดท้าย (Ultimate Goal)

ให้ความเชื่อมั่นอย่างสมเหตุสมผลว่า การควบคุมด้านความมั่นคงปลอดภัยของบริการ Cloud ได้รับการออกแบบ นำไปปฏิบัติ และทำงานอย่างมีประสิทธิผลเพียงพอที่จะลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

การกำหนดขอบเขต (Audit Scoping)

องค์ประกอบที่ต้องระบุอย่างชัดเจน

- CSP และ Cloud Service
- Account / Tenant
- Region
- Application
- Data
- Environment
- Business Process
- Third Party / Subprocessor

ข้อควรระวัง

"Cloud ทั้งองค์กร" ไม่ใช่ Audit Scope ที่เพียงพอ

ต้องกำหนด Boundary ให้ตรวจสอบได้อย่างชัดเจน มีขอบเขตที่วัดได้ และสามารถระบุได้ว่าอะไรอยู่ใน Scope และอะไรอยู่นอก Scope

การตรวจประเมินตามความเสี่ยง (Risk-Based Auditing)

ไม่จำเป็นต้องให้ทุกระบบมี Audit Intensity เท่ากัน ควรจัดลำดับความสำคัญตามปัจจัยความเสี่ยง

Business Criticality

ระบบที่สำคัญต่อการดำเนินธุรกิจหลัก
ควรได้รับการตรวจอย่างเข้มข้นกว่า

Data Criticality & Regulatory Impact

ข้อมูลที่มีความอ่อนไหวสูงและระบบที่อยู่ภายใต้
กฎระเบียบต้องได้รับความสนใจเป็นพิเศษ

Threat Exposure & Architecture Complexity

ระบบที่เปิดรับภัยคุกคามสูงหรือ
มีสถาปัตยกรรมซับซ้อนต้องการการตรวจที่ลึกกว่า

Third-Party Dependency

การพึ่งพาบุคคลที่สามเพิ่มความเสี่ยง
และต้องพิจารณาในการกำหนด Audit Priority

การกำหนดเกณฑ์การตรวจประเมิน (Audit Criteria)

เกณฑ์การตรวจประเมินสามารถมาจากหลายแหล่ง ซึ่ง Auditor ต้องเลือกและผสมผสานให้เหมาะสมกับบริบทขององค์กร

กฎหมาย & กฎระเบียบ
กฎหมาย กฎระเบียบ และสัญญาที่เกี่ยวข้อง

นโยบายองค์กร
นโยบายภายในและ Security Baseline ขององค์กร

ISO/IEC Standards
ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018

CSA CCM & Cloud Standards
CSA CCM และ Cloud Security Standard ที่เกี่ยวข้อง

หลักฐานการตรวจประเมิน (Audit Evidence)

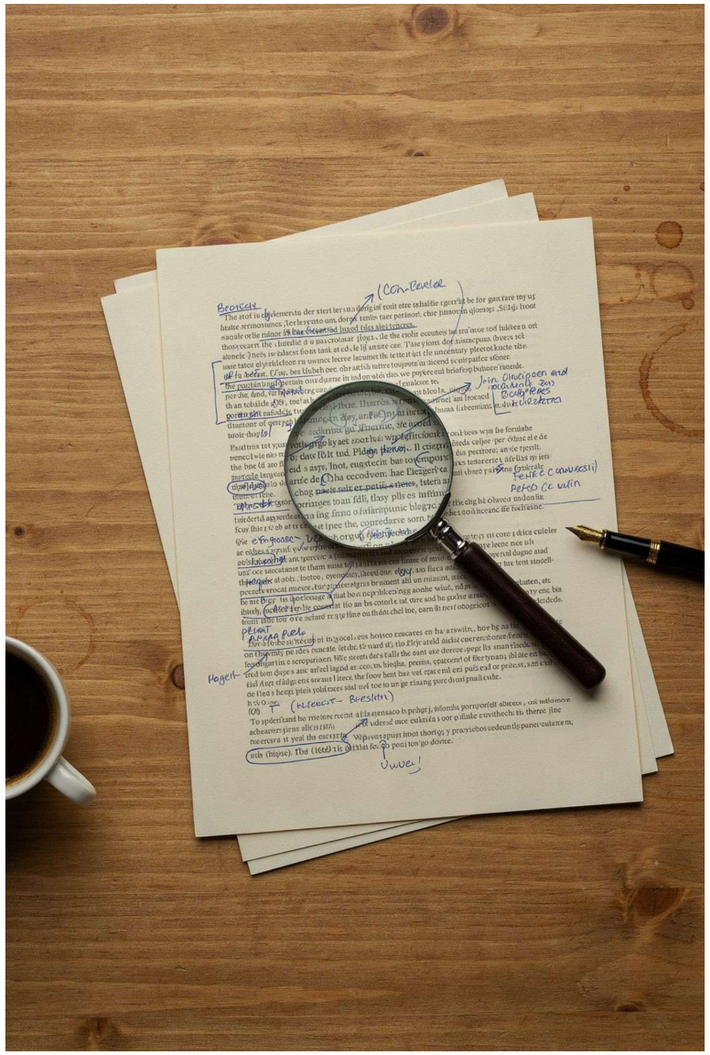
CSP Evidence

- ISO Certificate
- SOC Report
- STAR / CAIQ
- Assurance Report
- Security Whitepaper

Customer Evidence

- Policy / Procedure / Architecture Diagram
- IAM Configuration / Access Review
- Security Configuration / Network Configuration
- Log / Monitoring Report / Incident Record
- Backup Report / DR Test / Certificate
- Contract / Configuration Export

Auditor ต้องประเมินหลักฐานทั้งสองฝั่ง — CSP Evidence และ Customer Evidence
— เพราะการมีใบรับรองของ CSP ไม่ได้หมายความว่า Customer Environment ปลอดภัย



Evidence ไม่เท่ากับ Effectiveness

มี Policy ≠ ปฏิบัติจริง

การมีนโยบายเป็นลายลักษณ์อักษรไม่ได้พิสูจน์ว่ามีการนำไปปฏิบัติจริง

มี Configuration ≠ Control ทำงานจริง

การตั้งค่าที่ถูกต้องไม่ได้หมายความว่า Control ทำงานได้อย่างต่อเนื่องและมีประสิทธิผล

มี Certificate ≠ Customer Environment Secure

ใบรับรองของ CSP ครอบคลุมเฉพาะ Scope ของ CSP ไม่ใช่ Customer Configuration

มี Log ≠ มีการ Monitoring อย่างมีประสิทธิผล

การบันทึก Log ไม่ได้หมายความว่ามีการวิเคราะห์และตอบสนองต่อเหตุการณ์จริง

ดังนั้น Auditor ต้องทำ: **Evidence + Testing + Corroboration**

Cloud Audit Question Bank

ชุดคำถามหลักสำหรับผู้ตรวจประเมิน Cloud ที่ครอบคลุม Domain สำคัญ

Domain	คำถามสำคัญ
Governance	ใครเป็นเจ้าของและผู้รับผิดชอบ Cloud Service?
Scope	บริการใดอยู่ในขอบเขตการตรวจประเมิน?
IAM	ใครสามารถเข้าถึงทรัพยากรที่สำคัญ?
Configuration	Configuration Baseline ถูกกำหนดและทบทวนหรือไม่?
Data	ข้อมูลถูกจัดเก็บและประมวลผลที่ใด?
Encryption	ใครเป็นผู้ควบคุม Encryption Key?
Logging	มีการบันทึกและติดตามกิจกรรมที่สำคัญหรือไม่?
Incident	หากเกิดเหตุการณ์ ใครต้องดำเนินการและแจ้งใคร?
Resilience	หาก Cloud Service หยุดให้บริการ ระบบจะดำเนินการอย่างไร?
Exit	สามารถย้ายข้อมูลและบริการออกจาก CSP ได้จริงหรือไม่?

Key Message: คำถามที่ดีจะนำไปสู่ Evidence ที่ดี และ Evidence ที่ดีจะนำไปสู่ Assurance ที่น่าเชื่อถือ

Design Effectiveness และ Operating Effectiveness

Design Effectiveness

การควบคุมถูก**ออกแบบ**อย่างเหมาะสมต่อความเสี่ยงหรือไม่? — ตรวจว่า Control ถูกกำหนดไว้อย่างถูกต้อง

Operating Effectiveness

การควบคุมถูก**นำไปปฏิบัติและทำงานอย่างต่อเนื่อง**จริงหรือไม่? — ตรวจว่า Control ทำงานได้จริงในทางปฏิบัติ

ตัวอย่าง: MFA

1

Design

MFA ถูกกำหนดไว้ใน Policy

2

Operating

MFA ถูกเปิดใช้จริงในระบบ

3

Evidence

Log แสดงการใช้ MFA จริง

4

Testing

สุ่มทดสอบ Account เพื่อยืนยัน

ตัวอย่าง Audit Test: MFA สำหรับ Privileged Account

Audit Objective

ประเมินว่า Privileged Account ได้รับการป้องกันด้วย MFA

Evidence ที่ต้องรวบรวม

- IAM Policy
- Account Population
- MFA Configuration
- Authentication Log

ขั้นตอนการทดสอบ

1. ตรวจ Population ของ Account ทั้งหมด
2. ระบุ Privileged Account
3. ตรวจ MFA Status ของแต่ละ Account
4. สุ่มตัวอย่าง Account
5. ตรวจ Authentication Log
6. ตรวจ Exception ที่ได้รับการยกเว้น

Conclusion

Control มีประสิทธิผล / ไม่มีประสิทธิผล / มีข้อจำกัด

ตัวอย่าง Audit Test: Cloud Configuration & Access Control

Cloud Configuration

- Public Access
- Security Group
- Firewall
- Encryption
- Logging
- Storage
- IAM

Access Control

- User Account
- Privileged Account
- Service Account
- MFA
- Least Privilege
- Access Review
- Joiner-Mover-Leaver
- Dormant Account

Configuration Baseline ต้องสัมพันธ์กับ Risk และ Security Policy ขององค์กร

ตัวอย่าง Audit Test: Data Security & Logging/Monitoring

Data Security

- Data Classification
- Encryption at Rest
- Encryption in Transit
- Key Management
- Backup
- Retention
- Data Deletion
- Data Transfer
- Data Localization

Logging & Monitoring

- Log Coverage
- Log Collection
- Log Retention
- Log Integrity
- Monitoring
- Alerting
- SIEM Integration
- Incident Correlation

Incident Response — Cloud Incident Response Audit

แผนและโครงสร้าง
Incident Response Plan, Roles & Responsibilities, Contact Point, Escalation

การดำเนินการ
Notification, Evidence Preservation, Communication

การทดสอบและปรับปรุง
Tabletop Exercise, Lessons Learned

คำถามสำคัญ: เมื่อเกิดเหตุ ใครต้องทำอะไร ภายในเวลาเท่าใด และมีหลักฐานว่ากระบวนการทำงานได้จริงหรือไม่?

Business Continuity & Cloud Resilience

สิ่งที่ต้องตรวจ

- Backup
- Disaster Recovery
- RTO (Recovery Time Objective)
- RPO (Recovery Point Objective)
- Availability
- Region Failure
- CSP Outage
- Recovery Testing

หลักการสำคัญ

แผนที่ไม่เคยทดสอบ ไม่ควรถูกถือว่าเป็นหลักฐานเพียงพอของความสามารถในการกู้คืน

Auditor ต้องตรวจว่ามีการทดสอบ DR จริง มีผลการทดสอบ และมีการแก้ไขข้อบกพร่องที่พบ

Cloud Exit Readiness

"ถ้าต้องออกจาก CSP พรุ่งนี้ เราทำได้หรือไม่?"

ตรวจ

Data Portability	สามารถย้ายข้อมูลออกจาก CSP ไปยังผู้ให้บริการอื่นหรือระบบขององค์กรได้หรือไม่
Data Export	สามารถส่งออกข้อมูลได้ครบถ้วน ง่าย และเป็นระบบหรือไม่
Data Format	ข้อมูลอยู่ในรูปแบบมาตรฐาน ไม่ผูกกับ proprietary format หรือไม่
Application Dependency	Application พึ่งพา service เฉพาะของ CSP มากน้อยเพียงใด
API Dependency	ใช้ API หรือ service เฉพาะของ CSP ที่ย้ายออกได้ยากหรือไม่
Contractual Exit	สัญญามีเงื่อนไขการยกเลิก การคืนข้อมูล และการช่วยเหลือในการออกหรือไม่
Exit Cost	มีค่าใช้จ่ายในการออกจากระบบ หรือค่าปรับหรือไม่ และเท่าใด
Exit Time	ต้องใช้เวลาในการออกจากระบบ นานเท่าใดจึงจะเสร็จสมบูรณ์
Data Deletion	สามารถลบข้อมูลทั้งหมดออกจากระบบของ CSP ได้อย่างสมบูรณ์ และมีหลักฐานยืนยันหรือไม่

เป้าหมายคือ "ออกจากระบบได้จริง รวดเร็ว ปลอดภัย และคุ้มค่า"
เพื่อลดความเสี่ยงจากการพึ่งพาผู้ให้บริการ (Vendor Lock-in)

Vendor Lock-in

ความเสี่ยงจากการพึ่งพาผู้ให้บริการ

Technical Lock-in	ใช้บริการเฉพาะของ CSP ที่ไม่สามารถทดแทนด้วยผู้ให้บริการอื่นได้ง่าย
Data Lock-in	ย้ายข้อมูลออกได้ยาก เพราะรูปแบบข้อมูลเฉพาะหรือข้อจำกัดของเครื่องมือ
Application Lock-in	Application พึ่งพา Platform, Service หรือ Features เฉพาะ
Contractual Lock-in	สัญญาและเงื่อนไขการออกที่เข้มงวด มีข้อจำกัดหรือภาระผูกพันระยะยาว
Financial Lock-in	ต้นทุนในการย้ายสูง ทั้งค่าธรรมเนียม การย้ายข้อมูล และการปรับปรุงระบบ

แนวทางลดความเสี่ยง เลือกใช้มาตรฐานเปิด (Open Standards) ออกแบบสถาปัตยกรรมที่ยืดหยุ่น มีแผน Exit Strategy และทบทวนสัญญาอย่างรอบคอบ

Exit Plan กับ Exit Capability

ความเข้าใจผิดที่พบบ่อย

มี Exit Plan ≠ สามารถ Exit ได้จริง

การมีแผนบนกระดาษไม่ได้พิสูจน์ว่าองค์กรสามารถดำเนินการ Exit ได้จริงในทางปฏิบัติ

Auditor ควรตรวจ

- มีแผนหรือไม่?
- มีผู้รับผิดชอบหรือไม่?
- มีงบประมาณหรือไม่?
- มี Technology ทางเลือกหรือไม่?
- เคยทดสอบหรือไม่?
- สามารถ Export Data ได้จริงหรือไม่?

คุณภาพของหลักฐานการตรวจประเมิน (Audit Evidence Sufficiency & Reliability)

การมีหลักฐานไม่ได้หมายความว่าหลักฐานนั้นเพียงพอสำหรับการสรุปผลการตรวจประเมิน Auditor ควรพิจารณา 4 มิติ

ความเพียงพอ (Sufficiency)
มีหลักฐานมากพอที่จะสนับสนุนข้อสรุปหรือไม่?

ความเหมาะสม (Appropriateness)
หลักฐานเกี่ยวข้องกับ Audit Objective หรือไม่?

ความน่าเชื่อถือ (Reliability)
หลักฐานมาจากแหล่งที่น่าเชื่อถือหรือไม่?

ความทันสมัย (Timeliness)
หลักฐานสะท้อนสภาพแวดล้อมในช่วงเวลาที่ตรวจหรือไม่?

ตัวอย่าง: Screenshot หนึ่งภาพอาจแสดงว่า MFA เปิดใช้งาน แต่ยังไม่เพียงพอที่จะยืนยันว่า Privileged Account ทั้งหมดเปิด MFA และมีการใช้งานจริงอย่างต่อเนื่อง จึงอาจต้องใช้ Configuration + Account Population + Log + Sampling

ตัวอย่าง Cloud Audit Procedure: Privileged Access

Audit Objective

ประเมินประสิทธิผลของการควบคุม Privileged Access

Audit Criteria

- Least Privilege
- Multi-Factor Authentication (MFA)
- Access Review
- Privileged Account Management

Audit Evidence

- IAM Configuration
- Privileged Account List
- Access Review Record
- Authentication Log
- Exception Record

Audit Procedure (8 ขั้นตอน)

1. ขอรายชื่อ Privileged Account ทั้งหมด
2. ตรวจสอบสิทธิ์และบทบาทของแต่ละ Account
3. ตรวจสอบ MFA Configuration
4. ตรวจสอบ Account ที่ได้รับ Exception
5. สุ่มตัวอย่าง Account
6. ตรวจสอบ Authentication Log
7. เปรียบเทียบกับ Policy และ Control Requirement
8. สรุปผล Control Effectiveness

Cloud Audit Trail | จาก Audit Criteria สู่ Assurance

Requirement	ข้อกำหนด กฎหมาย มาตรฐาน นโยบายหรือสัญญา ที่องค์กรต้องปฏิบัติตาม
Risk	ความเสี่ยงที่อาจเกิดขึ้นหากไม่ปฏิบัติตามข้อกำหนด หรือควบคุมไม่เพียงพอ
Control Objective	วัตถุประสงค์ของการควบคุม เพื่อจัดการหรือลดความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้
Control	มาตรการควบคุมที่ออกแบบและนำมาใช้ เพื่อให้บรรลุวัตถุประสงค์
Evidence	หลักฐานที่แสดงว่ามาตรการควบคุมถูกนำไปใช้งานจริง และมีการปฏิบัติอย่างต่อเนื่อง
Audit Procedure	วิธีการตรวจสอบเพื่อให้ได้มาซึ่งหลักฐานที่เหมาะสม และเพียงพอ
Testing	การทดสอบ/ตรวจสอบการควบคุม เพื่อประเมินการออกแบบและการปฏิบัติจริง
Finding	ผลการตรวจสอบ ข้อค้นพบ และหลักฐานประกอบ
Residual Risk	ความเสี่ยงที่ยังคงเหลืออยู่ หลังจากมาตรการควบคุมทำงานแล้ว
Audit Conclusion	ข้อสรุปโดยรวมเกี่ยวกับประสิทธิผลของการควบคุม และผลกระทบต่อความเสี่ยง
Assurance	ความเชื่อมั่นอย่างมีเหตุผล ว่าการควบคุมสามารถลดความเสี่ยง ได้อย่างเหมาะสมและอยู่ในระดับที่ยอมรับได้

Key Message

Cloud Security Audit ไม่ใช่การตรวจว่ามีเอกสารหรือ Control หรือไม่

แต่เป็นกระบวนการประเมินว่าการควบคุมสามารถ **ลดความเสี่ยงได้จริงหรือไม่**

และมี**หลักฐานเพียงพอ**ที่จะสนับสนุน ข้อสรุปดังกล่าวหรือไม่

หลักฐานที่เพียงพอ + การทดสอบที่เหมาะสม + การประเมินความเสี่ยงอย่างรอบด้าน = **ความเชื่อมั่นที่น่าเชื่อถือ (Reliable Assurance)**

กรณีศึกษา: ระบบสำคัญบน Public Cloud

สมมติองค์กรมี

- ระบบสำคัญต่อการให้บริการ
- ข้อมูลที่มีความอ่อนไหวสูง
- Public-facing Application
- ผู้ดูแลระบบหลายราย
- Third-Party Integration
- Backup / DR ต่าง Region

องค์กรแจ้งว่า

"CSP มี ISO/IEC 27001 และระบบอยู่บน Cloud ที่มี Data Center ในประเทศไทย"

คำถาม

เพียงพอสำหรับการให้ Assurance หรือไม่?

Auditor จะตรวจอะไร?

1

Governance
ใครรับผิดชอบ Cloud Service?

2

Scope
บริการใดอยู่ใน Audit Scope?

3

Data
ข้อมูลอยู่ที่ใด?

4

IAM
ใครเข้าถึงทรัพยากร?

5

Configuration
Configuration ปลอดภัยหรือไม่?

6

Monitoring
ตรวจจับเหตุการณ์ได้หรือไม่?

7

Resilience
หาก Cloud ล่มทำอย่างไร?

8

Exit
หากต้องเปลี่ยน CSP ทำได้หรือไม่?

Case Finding และ
Finding → Risk → Recommendation

Finding 1: Privileged Account ไม่มี MFA

Risk: Unauthorized Access — บัญชีที่มีสิทธิ์สูงไม่ได้รับการป้องกันด้วย MFA ทำให้เสี่ยงต่อการถูกโจมตี

Recommendation: บังคับใช้ MFA, Privileged Access Management, Periodic Access Review, Monitoring

Finding 2: Backup ถูกจัดเก็บในต่างประเทศ

ต้องตรวจเพิ่มเติม: Contract, Regulation, Data Classification, DR Requirement, Jurisdiction, Encryption — เพื่อประเมินว่าเป็นความเสี่ยงที่ยอมรับได้หรือไม่

Finding 3: CSP มี ISO/IEC 27001 แต่ไม่ครอบคลุม Customer

Customer Configuration ไม่ได้อยู่ในขอบเขตของ Certificate ดังนั้น Certificate จึง**ไม่สามารถใช้ปิดประเด็น Audit ได้ทั้งหมด**

CCAK และ Cloud Auditing Profession

Certificate of Cloud Auditing Knowledge (CCAK)

องค์ความรู้ของ CCAK ครอบคลุม

CCAK เป็น credential ที่พัฒนาโดย **Cloud Security Alliance (CSA) และ ISACA** เพื่อเติมช่องว่างด้านความรู้เชิงเทคนิคสำหรับผู้ปฏิบัติงานด้าน IT Audit, Security และ Risk ในบริบทของ Cloud

- Cloud Governance & Compliance Program
- CCM และ CAIQ
- Cloud Threat Analysis
- Cloud Compliance Assessment & Auditing
- CCM Auditing
- Continuous Assurance and Compliance
- STAR Program

สมรรถนะของ Cloud Auditor

Cloud Auditor ควรมีความรู้แบบบูรณาการใน 4 ด้านหลัก

Audit

- Risk Assessment
- Audit Planning
- Evidence & Testing
- Reporting

Cloud

- IaaS / PaaS / SaaS
- Cloud Architecture
- Shared Responsibility
- Cloud-native Technology

Security

- IAM / Encryption
- Network / Application
- Monitoring

Governance

- Compliance / Third Party
- Data Sovereignty
- Contract / Assurance

Key Takeaways & Auditor's Mindset

1 **ใบรับรองของ CSP ≠ Customer Secure**
ต้องตรวจ Scope + Responsibility + Customer Controls

2 **Data Residency ≠ Data Sovereignty**
ต้องพิจารณา Location + Jurisdiction + Access + Processing

3 **Shared Responsibility ต้องมาพร้อม Accountability**
ต้องกำหนดให้ชัดว่า ใครทำอะไร ใครรับผิดชอบ และใครต้องพิสูจน์

4 **Control ต้องมี Evidence และ Testing**
Policy ≠ Implementation ≠ Effectiveness

5 **Cloud Security ต้องรวม Resilience และ Exit**
Secure Cloud ต้องสามารถ Detect → Respond → Recover → Exit

Auditor's Mindset: อย่าเริ่มจาก "มี Control หรือไม่?" ให้เริ่มจาก **"Risk คืออะไร?"** แล้วถามต่อว่า Control เพียงพอหรือไม่ Evidence อยู่ที่ไหน จะทดสอบอย่างไร Control ทำงานจริงหรือไม่ และ Residual Risk ที่เหลืออยู่ยอมรับได้หรือไม่

Questions & Discussion

Cloud Security Auditing

ขอขอบพระคุณทุกท่านที่สละเวลาเข้าร่วมกิจกรรม