กิจกรรมแลกเปลี่ยนเรียนรู้

เรื่อง การตรวจสอบระบบเทคโนโลยีสารสนเทศ
(INFORMATION TECHNOLOGY AUDITING)

วันที่ 23 กรกฎาคม 2568

แนวคิดพื้นฐาน IT AUDIT

1) General Control

เช่น การควบคุมการเข้าถึงระบบ, การเปลี่ยนแปลงระบบ, การสำรองข้อมูล ตรวจสอบว่า "ระบบมีการควบคุมทั่วไปที่ดีหรือไม่"

2) Application Control

เช่น การควบคุมความถูกต้องของข้อมูลในแอปพลิเคชัน ตรวจสอบว่า "ระบบทำงานตามวัตถุประสงค์ได้ถูกต้องหรือไม่"

ประเภทของการตรวจสอบด้าน IT

1. Security Audit (การตรวจสอบความมั่นคงปลอดภัย) เป็นการตรวจสอบด้านความมั่นคงปลอดภัย ซึ่งจะครอบคลุมทั้ง General Control และ Application Control
2. Compliance Audit (การตรวจสอบการปฏิบัติตามข้อกำหนด) ตรวจสอบว่าองค์กรปฏิบัติตามกฎหมาย ข้อบังคับ หรือมาตรฐานต่างๆ หรือไม่
3. Operational Audit (การตรวจสอบการดำเนินงาน) มุ่งเน้นที่ประสิทธิภาพและประสิทธิผลของกระบวนการทาง IT
4. Forensic Audit (การตรวจสอบเชิงสืบสวน) เป็นการตรวจสอบเมื่อมีเหตุการณ์ทุจริตหรือการโจมตีเกิดขึ้น เพื่อค้นหาหลักฐานและระบุความเสียหาย

วัตถุประสงค์หลักของ IT AUDIT

- **ความเชื่อถือได้ของข้อมูล** (Data Integrity)
ตรวจสอบว่าข้อมูลที่ได้จากระบบมีความถูกต้อง ครบถ้วน และทันเวลา
- **ความมั่นคงปลอดภัยของระบบ** (System Security)
ตรวจสอบมาตรการป้องกันภัยคุกคามทั้งจากภายในและภายนอก
- **การดำเนินงานอย่างมีประสิทธิภาพ** (Operational Effectiveness)
ตรวจสอบว่า IT สนับสนุนเป้าหมายขององค์กรอย่างมีประสิทธิภาพ
- **การปฏิบัติตามข้อกำหนด** (Compliance)
ตรวจสอบความสอดคล้องกับระเบียบภายใน กฎหมายภายนอก เช่น PDPA, ISO/IEC 27001

ขอบเขตของ IT AUDIT

- Infrastructure:

เครือข่าย ระบบเซิร์ฟเวอร์ อุปกรณ์ฮาร์ดแวร์

- Application Controls: ระบบงานเฉพาะ

เช่น ERP, ระบบเงินเดือน

- General Controls: การควบคุมทั่วไป

เช่น การจัดสิทธิ์ผู้ใช้ การสำรองข้อมูล (Backup) การควบคุมการเข้าถึง (Access Control)

มาตรฐาน/กรอบแนวทางที่ใช้

- ISACA's IT Audit Standards
- COBIT Framework (Control Objectives for Information and Related Technologies)
- ISO/IEC 27001 – มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ
- ISO/IEC 38500 การกำกับดูแลเทคโนโลยีสารสนเทศขององค์กร
- NIST Cybersecurity Framework
- IIA Standards – มาตรฐานการตรวจสอบภายในสากล (International Professional Practices Framework - IPPF)

ขั้นตอนการวางแผนการตรวจสอบ IT (IT AUDIT PLAN)

แบ่งออกเป็น 4 ขั้นตอนหลัก

1. Understand the Business เข้าใจธุรกิจและบริบทองค์กร
2. Define IT Universe กำหนดขอบเขตของระบบ IT ที่เกี่ยวข้อง
3. Perform Risk Assessment การประเมินความเสี่ยง
4. Formalize Audit Plan จัดทำแผนตรวจสอบอย่างเป็นทางการ

COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATS)

เทคนิคช่วยตรวจสอบโดยใช้คอมพิวเตอร์ ซึ่งเป็นเครื่องมือสำคัญของผู้ตรวจสอบระบบสารสนเทศ ช่วยให้สามารถ **วิเคราะห์ข้อมูลจำนวนมาก**

1. Generalized Audit Software (GAS) เช่น ACL, IDEA
2. Parallel Simulation
3. Test Data
4. Integrated Test Facility (ITF)
5. Concurrent Auditing Techniques เช่น Real-time Audit Monitor

การตรวจสอบและควบคุมระบบสารสนเทศ (IT AUDIT & CONTROL)

ประเภทของการควบคุม (Controls) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบ

1. Physical Controls (**การควบคุมทางกายภาพ**)

คือ มาตรการป้องกันภัยคุกคามที่เกี่ยวข้องกับสถานที่ อุปกรณ์ และบุคลากร เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ป้องกันความเสียหายจากภัยธรรมชาติ

2. Logical Controls (**การควบคุมทางตรรกะ / ระบบสารสนเทศ**)

คือ มาตรการที่ควบคุมการเข้าถึงระบบข้อมูล และการทำงานของโปรแกรม/ฐานข้อมูล ผ่านกลไกด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติ

ความท้าทายของการตรวจสอบ IT (CHALLENGES OF IT AUDITING)

- เข้าใจวัตถุประสงค์ของการควบคุม IT ว่าเป็นการควบคุมประเภทใด และมีจุดมุ่งหมายเพื่ออะไร
- ตระหนักถึงความสำคัญของการควบคุม ต่อองค์กร ทั้งประโยชน์ที่องค์กรได้รับจากการควบคุมนั้น (เช่น การปฏิบัติตามกฎหมาย หรือความได้เปรียบทางการแข่งขัน) และความเสียหายที่อาจเกิดขึ้นหากการควบคุมอ่อนแอหรือไม่สมบูรณ์
- ระบุว่าบุคคลหรือตำแหน่งใดมีหน้าที่รับผิดชอบ ในการปฏิบัติงานอะไรบ้าง
- สร้างสมดุลระหว่างความเสี่ยงที่เกิดขึ้นกับข้อกำหนดในการสร้างการควบคุม
- นำกรอบการควบคุมและแผนการตรวจสอบที่เหมาะสมมาใช้
- ติดตามความรู้เกี่ยวกับระเบียบวิธีและวัตถุประสงค์ทางธุรกิจให้เป็นปัจจุบันอยู่เสมอ

GENERAL CONTROLS VS. APPLICATION CONTROLS

ประเภท	ความหมาย	ตัวอย่าง	จุดเน้นในการตรวจสอบ
General Controls	การควบคุมระดับโครงสร้างพื้นฐานของระบบ IT ทั้งระบบ	• การควบคุมสิทธิ์ (Access Control) • การสำรองข้อมูล (Backup) • การรักษาความมั่นคงปลอดภัยของระบบ • การบำรุงรักษาระบบ (Change Management)	ตรวจสอบว่า สภาพแวดล้อมโดยรวมของระบบ IT มีความมั่นคงปลอดภัย และสามารถรองรับระบบงานต่าง ๆ ได้อย่างถูกต้อง
Application Controls	การควบคุมที่อยู่ในแต่ละ "โปรแกรม" หรือ "ระบบงาน"	• การตรวจสอบความถูกต้องของข้อมูลที่กรอก (Input validation) • การประมวลผลข้อมูล (Processing Control) • การควบคุมผลลัพธ์ (Output Control) • การควบคุมความครบถ้วน (Completeness)	ตรวจสอบว่า ข้อมูลที่รับเข้า ประมวลผล และส่งออกของระบบมีความถูกต้อง ครบถ้วน ตรงตามวัตถุประสงค์

สรุปมุมมองการตรวจสอบ IT จาก OPERATIONS

หัวข้อ	จุดควบคุมหลักที่ควรตรวจสอบ
Help Desk	SLA, ticket system, log การรับปัญหา
Network Admin	Firewall, access control, monitoring
Change Control	การอนุมัติ, บันทึก, rollback plan
Librarian	Source control, access limit
Data Entry	Accuracy, Validation, Audit Trail
End Users	การอบรม, การใช้งานตามบทบาท

แนวคิดหลัก 3 ประการในด้านความมั่นคงปลอดภัยทางไซเบอร์ (CYBERSECURITY)

1. Confidentiality (**การรักษาความลับ**) หมายถึงการปกป้องข้อมูลหรือระบบให้สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
2. Integrity (**ความถูกต้องและความครบถ้วน**) หมายถึงการป้องกันไม่ให้ข้อมูลหรือระบบถูกดัดแปลงแก้ไขโดยไม่ได้รับอนุญาต และการตรวจสอบให้แน่ใจว่าข้อมูลที่เก็บไว้หรือส่งต่อยังคงความถูกต้องและครบถ้วนเสมอ
3. Availability (**ความพร้อมใช้งาน**) หมายถึงการทำให้ข้อมูลหรือระบบสามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ

ระดับความมั่นคงปลอดภัย (SECURITY LEVELS)

ต้องพิจารณาตาม
- **มูลค่าของข้อมูล**
- **ผลกระทบถ้าเกิดการรั่วไหล/สูญหาย/ถูกเปลี่ยนแปลง**
- **ข้อกำหนดทางกฎหมาย/นโยบายภาครัฐ**

ตัวอย่าง

ระดับ	คำอธิบาย	มาตรการเบื้องต้น
Low (ต่ำ)	ข้อมูลทั่วไป เช่น ข่าวประชาสัมพันธ์	Password ขั้นพื้นฐาน, Anti-virus
Medium (ปานกลาง)	ข้อมูลภายใน เช่น แผนงาน, งบประมาณ	Access Control, Logging, Backup
High (สูง)	ข้อมูลส่วนบุคคล, ข้อมูลสุขภาพ	Encryption, MFA, DLP
Very High / Critical (วิกฤติ)	ข้อมูลลับรัฐ, ข้อมูลการเงินระดับสูง	Isolation, Security Audit, SOC, IR Team

Categories of Data (ประเภทของข้อมูล)

เพื่อกำหนดระดับความปลอดภัยอย่างเหมาะสม **ตัวอย่าง** การจัดกลุ่มข้อมูล

ประเภทข้อมูล	ตัวอย่าง	ระดับความปลอดภัยที่แนะนำ
Public	เว็บไซต์, ข่าวประชาสัมพันธ์	Low
Internal Use	คู่มือภายใน, อีเมลทั่วไป	Medium
Confidential	ข้อมูลพนักงาน, ข้อมูลเงินเดือน	High
Restricted / Secret	ข้อมูลสาธารณสุข, ข้อมูลราชการลับ	Very High

การควบคุมการสำรองและกู้คืนข้อมูล (SYSTEM AND DATA BACKUP AND RECOVERY CONTROLS)

1. Off-site Storage จัดเก็บสำรองนอกสถานที่
2. Cloud Backup ใช้บริการ Cloud เพื่อสำรองข้อมูล
3. Electronic Vaulting การส่งข้อมูลสำรองไปเก็บยังสถานที่ปลอดภัยแบบอัตโนมัติผ่านเครือข่ายใช้กับข้อมูลสำคัญหรือเปลี่ยนแปลงบ่อย
4. Backup Data Controls การควบคุมและตรวจสอบว่าใครสามารถเข้าถึงไฟล์สำรอง ข้อมูลมีการเข้ารหัสหรือไม่ มีการทดสอบกู้คืน (restore test) หรือไม่
5. Ethics in Data Storage จริยธรรมในการจัดเก็บข้อมูล

ประเด็นจริยธรรม

ประเด็นจริยธรรม	ตัวอย่าง
ความลับ (Confidentiality)	ไม่ควรให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลสำรอง
ความถูกต้อง (Integrity)	ห้ามเปลี่ยนแปลงข้อมูลสำรองเพื่อซ่อนความผิด
การละเมิดสิทธิส่วนบุคคล	ห้ามนำข้อมูลสำรองที่มีข้อมูลส่วนบุคคลไปใช้นอกวัตถุประสงค์
การแจ้งเตือน	ต้องแจ้งให้เจ้าของข้อมูลทราบหากข้อมูลสำรองถูกละเมิด
การปฏิบัติตามกฎหมาย	เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA), ISO/IEC 27001

ความแตกต่างของ RPO กับ RTO (Recovery Objectives)

ประเด็น	RPO (Recovery Point Objective)	RTO (Recovery Time Objective)
หมายถึง	"ข้อมูลที่ยอมให้สูญหายได้มากที่สุด"	"เวลาที่ระบบต้องกลับมาใช้งานได้เร็วที่สุด"
หน่วยวัด	ระยะเวลาของข้อมูลที่ยอมสูญได้ (นับย้อนกลับจากเวลาที่ระบบล่ม)	ระยะเวลาในการกู้ระบบให้กลับมาทำงานได้
มุ่งเน้น	ด้านข้อมูล (Data loss)	ด้านเวลา (Downtime)
ตัวอย่าง	ถ้า RPO = 4 ชม. ⟶ ข้อมูลย้อนหลัง 4 ชม. สามารถหายได้	ถ้า RTO = 2 ชม. ⟶ ระบบต้องกลับมา online ภายใน 2 ชม.

ประเภทของ OFF-SITE FACILITIES (สถานที่สำรองข้อมูล/ระบบนอกสถานที่)

- **Hot Site** คือสถานที่พร้อมใช้งานทันที มีฮาร์ดแวร์และระบบต่าง ๆ ติดตั้งครบสมบูรณ์ เหมือนมีศูนย์สำรองที่รอให้ธุรกิจย้ายไปทำงานต่อได้ทันทีแบบไม่มี downtime
- **Cold Site** คือสถานที่ว่างเปล่าที่เตรียมไว้ แต่ไม่มีอุปกรณ์ หรือระบบใด ๆ ติดตั้งไว้ล่วงหน้า ต้องใช้เวลาเตรียมระบบและอุปกรณ์ใหม่เมื่อต้องใช้งานจริง

ประเภทของ OFF-SITE FACILITIES (สถานที่สำรองข้อมูล/ระบบนอกสถานที่) (ต่อ)

- **Warm Site** เป็นสถานที่ที่มีอุปกรณ์บางส่วนและระบบสำรองบางอย่างติดตั้งไว้บ้างแล้วไม่ถึงกับพร้อมใช้งานทันที แต่เตรียมพร้อมกว่าคนใช้ Cold Site มักมีการซิงก์ข้อมูลไม่ถี่เท่า Hot Site
- **Reciprocal Agreement** เป็นข้อตกลงระหว่างสององค์กรหรือหน่วยงานที่จะให้กันและกันใช้สถานที่หรือทรัพยากรในกรณีเกิดเหตุฉุกเฉิน

รายงานการไปฝึกอบรม โครงการอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA)
หลักสูตรระดับ 2 การตรวจสอบภายในเฉพาะด้าน (Audit Specialist)
หลักสูตรการตรวจสอบระบบสารสนเทศ (Information Technology Audit Specialist)
ตามระเบียบมหาวิทยาลัยสุโขทัยธรรมาธิราช ว่าด้วยการให้ทุนฝึกอบรม ดูงาน
และประชุมทางวิชาการแก่บุคลากรของมหาวิทยาลัย

ไปเข้ารับการฝึกอบรม เรื่อง การตรวจสอบระบบสารสนเทศ (Information Technology Audit Specialist) ณ โรงแรมเซ็นทารา ไลฟ์ ศูนย์ราชการ และคอนเวนชัน เซ็นเตอร์ แจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร
ตั้งแต่วันที่ 15 กรกฎาคม 2568 ถึงวันที่ 18 กรกฎาคม 2568 รวมระยะเวลา 4 วัน

2. รายละเอียดเกี่ยวกับการไปฝึกอบรม

(1) เรื่อง การตรวจสอบระบบสารสนเทศ (Information Technology Audit Specialist)

วัตถุประสงค์ เพื่อเพิ่มพูนความรู้ในการปฏิบัติงานตรวจสอบด้านการตรวจสอบระบบสารสนเทศ (Information Technology Audit) ของผู้ตรวจสอบภายในให้มีความสามารถในประเมินความเพียงพอของการควบคุมด้าน IT และการจัดการความเสี่ยงด้าน IT

(2) ผู้เข้าร่วมการฝึกอบรม Onsite 100 คน

(3) วิธีการฝึกอบรม การบรรยายและอภิปราย โดยวิทยากรจากภาคเอกชน

(4) สาระสำคัญของการฝึกอบรม

<u>การตรวจสอบระบบสารสนเทศ (Information Technology Audit Specialist)</u>

- **แนวคิดพื้นฐาน IT Audit**

จะมุ่งเน้นไปที่การตรวจสอบการควบคุมภายในของระบบสารสนเทศที่มีอยู่แล้ว ดังนี้

1) General Control เช่น การควบคุมการเข้าถึงระบบ, การเปลี่ยนแปลงระบบ, การสำรองข้อมูล ตรวจสอบว่า "ระบบมีการควบคุมทั่วไปที่ดีหรือไม่"

2) Application Control เช่น การควบคุมความถูกต้องของข้อมูลในแอปพลิเคชัน ตรวจสอบว่า "ระบบทำงานตามวัตถุประสงค์ได้ถูกต้องหรือไม่"

- **ประเภทของการตรวจสอบด้าน IT**

1. Security Audit (การตรวจสอบความมั่นคงปลอดภัย) เป็นการตรวจสอบด้านความมั่นคงปลอดภัย ซึ่งจะครอบคลุมทั้ง General Control เช่น นโยบายความปลอดภัย, การจัดการช่องโหว่ และ Application Control เช่น การเข้ารหัสข้อมูล, Secure Coding

2. Compliance Audit (การตรวจสอบการปฏิบัติตามข้อกำหนด) ตรวจสอบว่าองค์กรปฏิบัติตามกฎหมาย, ข้อบังคับ, หรือมาตรฐานต่างๆ หรือไม่ เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA), มาตรฐาน PCI DSS สำหรับธุรกิจบัตรเครดิต ซึ่งการตรวจสอบจะพิจารณาทั้งการควบคุมทั่วไปและเฉพาะระบบงานที่เกี่ยวข้อง เช่น มีการขอความยินยอมในการใช้ข้อมูลส่วนบุคคลหรือไม่ มีการรายงานตามข้อกำหนดหรือไม่

3. Operational Audit (การตรวจสอบการดำเนินงาน) มุ่งเน้นที่ประสิทธิภาพและประสิทธิผลของกระบวนการทาง IT เพื่อให้มั่นใจว่าฝ่ายไอทีสามารถสนับสนุนเป้าหมายทางธุรกิจได้ดีเพียงใด

4. Forensic Audit (การตรวจสอบเชิงสืบสวน) เป็นการตรวจสอบเมื่อมีเหตุการณ์ทุจริตหรือการโจมตีเกิดขึ้น เพื่อค้นหาหลักฐานและระบุความเสียหาย เช่น ใครเป็นผู้ลบข้อมูลจากระบบ IP ไหน login เข้ามาระบบผิดปกติ ตรวจ log files, Email, Transaction, Image, Digital Signature

- **วัตถุประสงค์หลักของ IT Audit**

  • **ความเชื่อถือได้ของข้อมูล (Data Integrity)** ตรวจสอบว่าข้อมูลที่ได้จากระบบมีความถูกต้องครบถ้วน และทันเวลา

  • **ความมั่นคงปลอดภัยของระบบ (System Security)** ตรวจสอบมาตรการป้องกันภัยคุกคามทั้งจากภายในและภายนอก

  • **การดำเนินงานอย่างมีประสิทธิภาพ (Operational Effectiveness)** ตรวจสอบว่า IT สนับสนุนเป้าหมายขององค์กรอย่างมีประสิทธิภาพ

  • **การปฏิบัติตามข้อกำหนด (Compliance)** ตรวจสอบความสอดคล้องกับระเบียบภายในกฎหมายภายนอก เช่น PDPA, ISO/IEC 27001

- **ขอบเขตของ IT Audit**

  • **Infrastructure**: เครือข่าย ระบบเซิร์ฟเวอร์ อุปกรณ์ฮาร์ดแวร์

  • **Application Controls**: ระบบงานเฉพาะ เช่น ERP, ระบบเงินเดือน

  • **General Controls**: การควบคุมทั่วไป เช่น การจัดสิทธิ์ผู้ใช้ การสำรองข้อมูล (Backup) การควบคุมการเข้าถึง (Access Control)

- **มาตรฐาน/กรอบแนวทางที่ใช้**

  - **ISACA's IT Audit Standards**
  - **COBIT Framework** (Control Objectives for Information and Related Technologies)
  - **ISO/IEC 27001** – มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ
  - **ISO/IEC 38500** การกำกับดูแลเทคโนโลยีสารสนเทศขององค์กร
  - **NIST Cybersecurity Framework**
  - **IIA Standards** – มาตรฐานการตรวจสอบภายในสากล (International Professional Practices Framework - IPPF)

- **ขั้นตอนการวางแผนการตรวจสอบ IT (IT Audit Plan)** ซึ่งแบ่งออกเป็น 4 ขั้นตอนหลัก

1. Understand the Business (เข้าใจธุรกิจและบริบทองค์กร) เน้นการทำความเข้าใจภาพรวมขององค์กร เพื่อให้การตรวจสอบ IT สอดคล้องกับเป้าหมายและความเสี่ยงที่แท้จริง วิเคราะห์กลยุทธ์และเป้าหมายขององค์กร เข้าใจความเสี่ยงหลักขององค์กร (High Risk Profile) ศึกษาโครงสร้างการดำเนินงานของธุรกิจ เข้าใจโมเดลการให้บริการด้าน IT (IT Service Support Model)

2. Define IT Universe (กำหนดขอบเขตของระบบ IT ที่เกี่ยวข้อง) วิเคราะห์ระบบงาน IT ที่สำคัญและโครงสร้างพื้นฐานที่เกี่ยวข้อง แยกแยะองค์ประกอบพื้นฐานของธุรกิจ ระบุแอปพลิเคชันที่มีผลต่อการ

ดำเนินงาน ระบุโครงสร้างพื้นฐาน IT ที่สนับสนุนแอปพลิเคชันเหล่านั้น วิเคราะห์เทคโนโลยีที่สนับสนุนระบบ ระบุโครงการสำคัญต่างๆ คัดเลือกหัวข้อที่สมเหตุสมผลสำหรับการตรวจสอบ

3. Perform Risk Assessment (ประเมินความเสี่ยง) วิเคราะห์ความเสี่ยงทั้งจากมุมมองของ IT และธุรกิจ เพื่อจัดลำดับความสำคัญ สร้างกระบวนการประเมินความเสี่ยง ประเมินและจัดลำดับความเสี่ยงของหัวข้อที่ตรวจจากปัจจัยเสี่ยงด้าน IT ประเมินและจัดลำดับจากปัจจัยเสี่ยงด้านธุรกิจ

4. Formalize Audit Plan (จัดทำแผนตรวจสอบอย่างเป็นทางการ) สรุปและจัดทำแผนตรวจสอบให้พร้อมใช้งาน คัดเลือกหัวข้อที่จะตรวจสอบ และจัดเป็นกลุ่มงาน (Audit Engagements) กำหนดรอบการตรวจสอบ (Audit Cycle) และความถี่ (Frequency) พิจารณาเรื่องที่ผู้บริหารร้องขอหรือโอกาสในการให้คำปรึกษา ตรวจสอบและยืนยันแผนกับผู้บริหาร

- **Computer-Assisted Audit Techniques (CAATs)**

คือ **เทคนิคช่วยตรวจสอบโดยใช้คอมพิวเตอร์** ซึ่งเป็นเครื่องมือสำคัญของผู้ตรวจสอบระบบสารสนเทศ ช่วยให้สามารถ **วิเคราะห์ข้อมูลจำนวนมาก** ได้อย่างแม่นยำและมีประสิทธิภาพ

CAATs ประเภทหลัก ๆ และรายละเอียด

ประเภท	คำอธิบาย	ข้อดี	ข้อจำกัด
1. Generalized Audit Software (GAS) เช่น ACL, IDEA	โปรแกรมสำเร็จรูปสำหรับวิเคราะห์ข้อมูล (เช่น ดึงข้อมูล, ตรวจสอบรายการผิดปกติ, วิเคราะห์แนวโน้ม)	- วิเคราะห์ข้อมูลจำนวนมากจากระบบ - ใช้งานได้กับหลายระบบฐานข้อมูล	- ต้องนำข้อมูลออกจากระบบ (Offline) - ต้องเข้าใจ logic ของข้อมูล
2. Parallel Simulation	นำข้อมูลจริงจากระบบไปประมวลผลใหม่ในโปรแกรมจำลองของผู้ตรวจสอบ แล้วเปรียบเทียบผลกับระบบจริง	- ตรวจสอบความถูกต้องของกระบวนการระบบ - ไม่ต้องรบกวนระบบจริง	- ใช้เวลาสร้างโปรแกรมจำลอง - ต้องเข้าใจกระบวนการทำงานของระบบเดิมอย่างละเอียด
3. Test Data	สร้างข้อมูลจำลอง (input) แล้วป้อนเข้าสู่ระบบจริง เพื่อดูว่า logic ของระบบทำงานถูกต้องหรือไม่	- ตรวจสอบการควบคุมภายในระบบได้ตรงจุด - เหมาะกับการทดสอบ input validation	- เสี่ยงกระทบข้อมูลจริงหากใช้ใน production - ต้องมีสิทธิ์เข้าระบบเพื่อทดสอบ
4. Integrated Test Facility (ITF)	ฝังข้อมูลจำลองลงไปในระบบจริง โดยใช้ “หน่วยงานจำลอง” หรือ “บัญชีจำลอง”	- ตรวจสอบระบบแบบ Real-time - ไม่ต้องหยุดระบบเพื่อทดสอบ	- ซับซ้อนในการตั้งค่าและแยกผลลัพธ์จำลองออกจากของจริง - อาจกระทบการบันทึกบัญชีจริงหากแยกไม่ดี
5. Concurrent Auditing Techniques เช่น Real-time Audit Monitor	ติดตามและตรวจสอบข้อมูลในระบบแบบ Real-time หรือใกล้เคียง	- ตรวจจับข้อผิดพลาด/ทุจริตได้ทันที - เหมาะกับระบบที่มีการบันทึกข้อมูลตลอดเวลา	- ต้องใช้เทคโนโลยีที่เชื่อมต่อกับระบบ - ความซับซ้อนสูง ต้องร่วมมือกับฝ่าย IT

- **การตรวจสอบและควบคุมระบบสารสนเทศ (IT Audit & Control)**

ประเภทของการควบคุม (Controls) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบ มีดังนี้

1. Physical Controls (การควบคุมทางกายภาพ) คือ มาตรการป้องกันภัยคุกคามที่เกี่ยวข้องกับสถานที่ อุปกรณ์ และบุคลากร เพื่อไม่ให้ผู้ไม่เกี่ยวข้องเข้าถึงอุปกรณ์หรือข้อมูลได้ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ป้องกันความเสียหายจากภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม

2. Logical Controls (การควบคุมทางตรรกะ / ระบบสารสนเทศ) คือ มาตรการที่ควบคุมการเข้าถึงระบบข้อมูล และการทำงานของโปรแกรม/ฐานข้อมูล ผ่านกลไกด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติ

- **ความท้าทายของการตรวจสอบ IT (Challenges of IT Auditing)**
  - เข้าใจวัตถุประสงค์ของการควบคุม IT ว่าเป็นการควบคุมประเภทใด และมีจุดมุ่งหมายเพื่ออะไร
  - ตระหนักถึงความสำคัญของการควบคุม ต่อองค์กร ทั้งประโยชน์ที่องค์กรได้รับจากการควบคุมนั้น (เช่น การปฏิบัติตามกฎหมาย หรือความได้เปรียบทางการแข่งขัน) และความเสียหายที่อาจเกิดขึ้นหากการควบคุมอ่อนแอหรือไม่สมบูรณ์
  - ระบุว่าบุคคลหรือตำแหน่งใดมีหน้าที่รับผิดชอบ ในการปฏิบัติงานอะไรบ้าง
  - สร้างสมดุลระหว่างความเสี่ยงที่เกิดขึ้นกับข้อกำหนดในการสร้างการควบคุม
  - นำกรอบการควบคุมและแผนการตรวจสอบที่เหมาะสมมาใช้
  - ติดตามความรู้เกี่ยวกับระเบียบวิธีและวัตถุประสงค์ทางธุรกิจให้เป็นปัจจุบันอยู่เสมอ
- **General Controls กับ Application Controls**

คือ พื้นฐานสำคัญของการตรวจสอบระบบสารสนเทศ (IT Audit) ที่ผู้ตรวจสอบภายในควรรู้ลึกและใช้บ่อยที่สุด

General Controls vs. Application Controls

ประเภท	ความหมาย	ตัวอย่าง	จุดเน้นในการตรวจสอบ
General Controls	การควบคุมระดับโครงสร้างพื้นฐานของระบบ IT ทั้งระบบ	• การควบคุมสิทธิ์ (Access Control) • การสำรองข้อมูล (Backup) • การรักษาความมั่นคงปลอดภัยของระบบ • การบำรุงรักษาระบบ (Change Management)	ตรวจสอบว่า **สภาพแวดล้อมโดยรวมของระบบ IT มีความมั่นคงปลอดภัย** และสามารถรองรับระบบงานต่าง ๆ ได้อย่างถูกต้อง
Application Controls	การควบคุมที่อยู่ในแต่ละ “โปรแกรม” หรือ “ระบบงาน”	• การตรวจสอบความถูกต้องของข้อมูลที่กรอก (Input validation) • การประมวลผลข้อมูล (Processing Control) • การควบคุมผลลัพธ์ (Output Control) • การควบคุมความครบถ้วน (Completeness)	ตรวจสอบว่า **ข้อมูลที่รับเข้าประมวลผล และส่งออกของระบบ มีความถูกต้องครบถ้วน ตรงตามวัตถุประสงค์**

สรุปมุมมองการตรวจสอบ IT จาก Operations

หัวข้อ	จุดควบคุมหลักที่ควรตรวจสอบ
Help Desk	SLA, ticket system, log การรับปัญหา
Network Admin	Firewall, access control, monitoring
Change Control	การอนุมัติ, บันทึก, rollback plan
Librarian	Source control, access limit
Data Entry	Accuracy, Validation, Audit Trail
End Users	การอบรม, การใช้งานตามบทบาท

- **แนวคิดหลัก 3 ประการในด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)**

คือ แนวคิดสำคัญที่ใช้ในการออกแบบและประเมินระบบควบคุมด้านความมั่นคงปลอดภัยของข้อมูล (Information Security Controls) โดยมีเป้าหมายเพื่อ **รักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล** หรือที่เรียกว่า **CIA Triad** โดยจะอ้างอิงมาจาก ISC2 CC – Certified in Cybersecurity และ Cisco CCST Cybersecurity CIA ย่อมาจาก "Confidentiality, Integrity และ Availability" ซึ่งเป็นแนวคิดหลักสามประการในด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

1. Confidentiality (การรักษาความลับ) หมายถึงการปกป้องข้อมูลหรือระบบให้สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น เช่น การใช้การเข้ารหัส (Encryption) การควบคุมการเข้าถึง (Access Control) เพื่อป้องกันข้อมูลจากการถูกเปิดเผยหรือเข้าถึงโดยไม่ได้รับอนุญาต

2. Integrity (ความถูกต้องและความครบถ้วน) หมายถึงการป้องกันไม่ให้ข้อมูลหรือระบบถูกดัดแปลงแก้ไขโดยไม่ได้รับอนุญาต และการตรวจสอบให้แน่ใจว่าข้อมูลที่เก็บไว้หรือส่งต่อยังคงความถูกต้องและครบถ้วนเสมอ เช่น การใช้แฮช (Hashing) การสำรองข้อมูล (Backup) และการตรวจสอบความถูกต้องของข้อมูล (Data Validation)

3. Availability (ความพร้อมใช้งาน) หมายถึงการทำให้ข้อมูลหรือระบบสามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ เช่น การมีระบบสำรองไฟฟ้า (UPS) การป้องกัน DDoS (Distributed Denial of Service) และการมีแผนการกู้คืนระบบ (Disaster Recovery Plan)

- **ระดับความมั่นคงปลอดภัย (Security Levels)**

ไม่จำเป็นต้องเท่ากันทุกระบบ เพราะการรักษาความปลอดภัยควร "สมเหตุสมผลกับความเสี่ยง" (Risk-based Security) สรุป **"Categories of Data" (ประเภทของข้อมูล)** ที่สัมพันธ์กัน ดังนี้

Security Levels (ระดับความมั่นคงปลอดภัย)

การกำหนดระดับความปลอดภัยของระบบ IT ต้องพิจารณาตาม

- **มูลค่าของข้อมูล**
- **ผลกระทบถ้าเกิดการรั่วไหล/สูญหาย/ถูกเปลี่ยนแปลง**
- **ข้อกำหนดทางกฎหมาย/นโยบายภาครัฐ**

ตัวอย่างระดับความปลอดภัย (จากต่ำไปสูง)

ระดับ	คำอธิบาย	มาตรการเบื้องต้น
Low (ต่ำ)	ข้อมูลทั่วไป เช่น ข่าวประชาสัมพันธ์	Password ขั้นพื้นฐาน, Anti-virus
Medium (ปานกลาง)	ข้อมูลภายใน เช่น แผนงาน, งบประมาณ	Access Control, Logging, Backup
High (สูง)	ข้อมูลส่วนบุคคล, ข้อมูลสุขภาพ	Encryption, MFA, DLP
Very High / Critical (วิกฤติ)	ข้อมูลลับรัฐ, ข้อมูลการเงินระดับสูง	Isolation, Security Audit, SOC, IR Team

Categories of Data (ประเภทของข้อมูล)

เพื่อกำหนดระดับความปลอดภัยอย่างเหมาะสม ต้องจัดกลุ่มข้อมูลก่อน เช่น

ประเภทข้อมูล	ตัวอย่าง	ระดับความปลอดภัยที่แนะนำ
Public	เว็บไซต์, ข่าวประชาสัมพันธ์	Low
Internal Use	คู่มือภายใน, อีเมลทั่วไป	Medium
Confidential	ข้อมูลพนักงาน, ข้อมูลเงินเดือน	High
Restricted / Secret	ข้อมูลสาธารณสุข, ข้อมูลราชการลับ	Very High

- **การควบคุมการสำรองและกู้คืนข้อมูล (System and Data Backup and Recovery Controls)**

ซึ่งถือเป็นหัวใจสำคัญในการรักษาความมั่นคงปลอดภัยด้าน Availability ตามแนวคิด CIA Triad และยังเกี่ยวข้องกับจริยธรรม (Ethics) ด้วย เพื่อป้องกันการสูญหายของข้อมูล และให้ระบบสามารถกลับมาทำงานได้ภายหลังจากเหตุการณ์ผิดปกติ เช่น ไฟดับ, โจมตีไซเบอร์, ระบบล่ม, หรือภัยพิบัติ แนวทางการควบคุมที่สำคัญ

1. Off-site Storage จัดเก็บสำรองนอกสถานที่
   - เก็บข้อมูลสำรองไว้ **นอกสถานที่ทำงานหลัก**
   - เพื่อป้องกันการสูญหายหากสถานที่หลักเกิดไฟไหม้ น้ำท่วม ฯลฯ
   - ควรเป็นที่ปลอดภัย เช่น ศูนย์ข้อมูลสำรอง หรือหน่วยงานพันธมิตร
2. Cloud Backup
   - ใช้บริการ Cloud เช่น AWS, Azure, Google Cloud เพื่อสำรองข้อมูล
   - **ข้อดี** ยืดหยุ่น เข้าถึงได้เร็ว ขยายได้ง่าย
   - **ข้อควรระวัง** ต้องควบคุมการเข้าถึงและเข้ารหัส (encryption) ข้อมูล
3. Electronic Vaulting
   - การส่งข้อมูลสำรองไปเก็บยังสถานที่ปลอดภัยแบบอัตโนมัติผ่านเครือข่าย
   - ใช้กับข้อมูลสำคัญหรือเปลี่ยนแปลงบ่อย เช่น ฐานข้อมูลการเงิน

4. Backup Data Controls

- การควบคุมและตรวจสอบว่า
  - ใครสามารถเข้าถึงไฟล์สำรองได้?
  - ข้อมูลมีการเข้ารหัสหรือไม่?
  - มีการทดสอบกู้คืน (restore test) เป็นประจำหรือไม่?
  - มีกำหนด retention period (ระยะเวลาที่เก็บข้อมูลสำรอง) หรือไม่?

5. Ethics in Data Storage จริยธรรมในการจัดเก็บข้อมูล

ประเด็นจริยธรรม	ตัวอย่าง
ความลับ (Confidentiality)	ไม่ควรให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลสำรอง
ความถูกต้อง (Integrity)	ห้ามเปลี่ยนแปลงข้อมูลสำรองเพื่อซ่อนความผิด
การละเมิดสิทธิส่วนบุคคล	ห้ามนำข้อมูลสำรองที่มีข้อมูลส่วนบุคคลไปใช้นอกวัตถุประสงค์
การแจ้งเตือน	ต้องแจ้งให้เจ้าของข้อมูลทราบหากข้อมูลสำรองถูกละเมิด
การปฏิบัติตามกฎหมาย	เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA), ISO/IEC 27001

- **ความแตกต่างของ RPO กับ RTO (Recovery Objectives)**

ประเด็น	RPO (Recovery Point Objective)	RTO (Recovery Time Objective)
หมายถึง	"ข้อมูลที่ยอมให้สูญหายได้มากที่สุด"	"เวลาที่ระบบต้องกลับมาใช้งานได้เร็วที่สุด"
หน่วยวัด	**ระยะเวลา**ของข้อมูลที่ยอมสูญได้ (นับย้อนกลับจากเวลาที่ระบบล่ม)	**ระยะเวลา**ในการกู้ระบบให้กลับมาทำงานได้
มุ่งเน้น	ด้านข้อมูล (Data loss)	ด้านเวลา (Downtime)
ตัวอย่าง	ถ้า RPO = 4 ชม. ⟶ ข้อมูลย้อนหลัง 4 ชม. สามารถหายได้	ถ้า RTO = 2 ชม. ⟶ ระบบต้องกลับมา online ภายใน 2 ชม.

- **ประเภทของ Off-site Facilities** (สถานที่สำรองข้อมูล/ระบบนอกสถานที่)

Hot Site

- คือสถานที่พร้อมใช้งานทันที มีฮาร์ดแวร์และระบบต่าง ๆ ติดตั้งครบสมบูรณ์ เหมือนมีศูนย์สำรองที่รอให้ธุรกิจย้ายไปทำงานต่อได้ทันทีแบบไม่มี downtime (เหมาะกับองค์กรที่รับความเสี่ยง downtime ไม่ได้เลย) ตัวอย่างเช่น ศูนย์ข้อมูลสำรองที่ติดตั้งเครื่องเซิร์ฟเวอร์ ระบบเครือข่าย และข้อมูลล่าสุด

Cold Site

- สถานที่ว่างเปล่าที่เตรียมไว้ แต่ไม่มีอุปกรณ์ หรือระบบใด ๆ ติดตั้งไว้ล่วงหน้า
- ต้องใช้เวลาเตรียมระบบและอุปกรณ์ใหม่เมื่อต้องใช้งานจริง
- ข้อดีคือค่าใช้จ่ายถูกกว่า Hot Site มาก แต่ต้องยอมรับ downtime ที่นานกว่า

Warm Site

- เป็นสถานที่ที่มีอุปกรณ์บางส่วนและระบบสำรองบางอย่างติดตั้งไว้บ้างแล้ว
- ไม่ถึงกับพร้อมใช้งานทันที แต่เตรียมพร้อมกว่าคนใช้ Cold Site
- มักมีการซิงก์ข้อมูลไม่ถี่เท่า Hot Site ทำให้ต้องรอซ่อมระบบและอาจเสียเวลาบ้าง

Reciprocal Agreement

o ข้อตกลงระหว่างสององค์กรหรือหน่วยงานที่จะให้กันและกันใช้สถานที่หรือทรัพยากรในกรณีเกิดเหตุฉุกเฉิน

o แบบนี้เหมือน “เพื่อนช่วยเพื่อน” แต่ต้องมั่นใจว่าอีกฝ่ายพร้อมช่วยจริง และไม่เกิดปัญหาทับซ้อนเวลาใช้พร้อมกัน

(5) สิ่งที่ได้สังเกต รู้ เห็น หรือได้รับถ่ายทอด

การเข้ารับการฝึกอบรมโดยการบรรยายจากวิทยากรและการถาม-ตอบระหว่างวิทยากร และผู้ตรวจสอบภายในที่เข้ารับการฝึกอบรมซึ่งมาจากทั่วประเทศ หลากหลายหน่วยงาน ทำให้เกิดการแลกเปลี่ยนความรู้ในเรื่องของความรู้ และประสบการณ์ในการตรวจสอบ

(6) ข้อเสนอแนะ

1. สำหรับหลักสูตรนี้เป็นเพียงหลักสูตรเบื้องต้นซึ่งก่อให้เกิดแนวคิดการนำมาประยุกต์ใช้ในการตรวจสอบ ซึ่งผู้ตรวจสอบภายในควรได้รับการสนับสนุนให้เข้าร่วมการฝึกอบรมในแต่ละรายละเอียดของ General control และ Application control เพิ่มมากขึ้น เพื่อเพิ่มความเชื่อมันของการควบคุมด้านสารสนเทศและลดความเสี่ยงของมหาวิทยาลัย

2. การนำกรอบการตรวจสอบตามแนวทาง COBIT 2019 เป็นเรื่องที่ท้าทายของผู้ตรวจสอบภายในเนื่องจากมหาวิทยาลัยยังไม่ได้มีการนำแนวทางการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่เป็นรูปธรรม ผู้ตรวจสอบภายในควรให้ข้อเสนอแนะที่ชี้ให้เห็นถึงประโยชน์ในการนำมาตรฐานและกรอบแนวคิดในระดับสากลมาใช้ เพื่อให้เกิดเป็นแนวปฏิบัติที่ดีและทำให้มหาวิทยาลัยพัฒนาไปสู่เป้าหมายของการเป็น Digital University

3. ควรนำความรู้และประสบการณ์ที่ได้รับมาถ่ายทอดให้กับบุคลากรภายในหน่วยงานตรวจสอบภายในต่อไป

(7) ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้ตรวจสอบภายในสามารถตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Auditing) เพื่อค้นหาหลักฐานความผิดปกติที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ และเพื่อสร้างความเชื่อมั่นในการใช้ข้อมูลของแต่ละหน่วยงานภายในมหาวิทยาลัย

2. มหาวิทยาลัยสามารถนำข้อเสนอแนะและแนวทางการแก้ไขจากการตรวจสอบระบบเทคโนโลยีสารสนเทศไปปรับปรุงการควบคุมด้าน IT และการจัดการความเสี่ยงด้าน IT ของมหาวิทยาลัยให้ดียิ่งขึ้น