มหาวิทยาลัยราชภัฏกำแพงเพชร
เลขที่ ๖๐๕๘
วันที่ ๑๗/๐๙/๒๕๖๙
เวลา ๑๖:๓๐ น.

เลขที่สถาบันวิจัยฯ ๐๓๕๐/๒๒
กันยายน ๒๕๖๙

บันทึกข้อความ

ส่วนราชการ หน่วยตรวจสอบภายใน
ที่ ตสน.๐๐๖๓/๒๕๖๙ วันที่ ๑๗ กันยายน ๒๕๖๙
เรื่อง สรุปองค์ความรู้ที่ได้รับจากการเข้าอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายใน (CGIA) หลักสูตรระดับ ๒ ด้านการตรวจสอบระบบสารสนเทศ (Information Technology Audit Specialist)

เรียน อธิการมหาวิทยาลัยราชภัฏกำแพงเพชร

ตามระเบียบกระทรวงการคลัง ว่าด้วยค่าใช้จ่ายในการฝึกอบรม การจัดงาน และการประชุมระหว่างประเทศ (ฉบับที่ ๓) พ.ศ.๒๕๕๕ ส่วนที่ ๒ ค่าใช้จ่ายของผู้เข้ารับการฝึกอบรม ข้อ ๒๘ ให้ผู้เข้ารับการฝึกอบรมหรือผู้สังเกตการณ์ที่เข้ารับการฝึกอบรมที่ส่วนราชการ หรือหน่วยงานอื่นจัดการฝึกอบรม จัดทำรายงานผลการเข้ารับการฝึกอบรมเสนอหัวหน้าส่วนราชการ ต้นสังกัดภายใน ๖๐ วันนับแต่วันเดินทางกลับถึงสถานที่ปฏิบัติราชการ

บัดนี้ข้าพเจ้า นางสาววราภรณ์ คล้ามสถิต และนางสาวศุภลักษณ์ สมโภชน์ ได้เดินทางกลับถึงสถานที่ปฏิบัติราชการแล้ว จึงขอรายงานผลการเข้ารับการฝึกอบรม โดยสรุปองค์ความรู้ที่ได้รับจากการเข้าอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายใน (CGIA) หลักสูตรระดับ ๒ ด้านการตรวจสอบระบบสารสนเทศ (Information Technology Audit Specialist) ดังเอกสารแนบ

จึงเรียนมาเพื่อโปรดทราบ

(นางสาววราภรณ์ คล้ามสถิต)
นักตรวจสอบภายใน
Signature Code : F๒NQiKaXoYccVaoMbuSn

เรียนอธิการบดีมหาวิทยาลัยราชภัฏกำแพงเพชร เพื่อโปรดทราบ

(รองศาสตราจารย์พรเพ็ญ โชชัย)
หัวหน้าหน่วยตรวจสอบภายใน
๑๗ กันยายน ๒๕๖๙
Signature Code : F๖NSiKfG๙WaVpjuhbmfl

เรียน รองอธิการบดีฝ่ายบริหาร
เพื่อโปรดทราบ ขอรายงานผลการเข้ารับการฝึกอบรมฯ

(นางชมภัค จารุฑีฆัมพร)
ปฏิบัติหน้าที่ในตำแหน่งหัวหน้างานธุรการและสารบรรณ
อิเล็กทรอนิกส์
๑๘ กันยายน ๒๕๖๙
Signature Code : Fy๘uiljbENWmetzFfHqY

การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Audit Specialist)

วิชา การตรวจสอบ IT
วิทยากร : อาจารย์นันทชัย ศิริพันธ์

---

1. วัตถุประสงค์และความสำคัญของ IT Audit ในยุค 2026

การตรวจสอบไอทีไม่ได้จำกัดอยู่เพียงแค่การตรวจสอบความถูกต้องของระบบงาน แต่เป็นเครื่องมือสำคัญในการบริหารจัดการความเสี่ยงสมัยใหม่ โดยมีวัตถุประสงค์หลักดังนี้

- **ความเข้าใจในยุคดิจิทัล :** เข้าใจแนวคิด IT Audit ที่สอดคล้องกับเทคโนโลยีปัจจุบัน
- **การบริหารจัดการความเสี่ยงใหม่ :** รับรู้และเท่าทันต่อภัยคุกคามไซเบอร์ที่ซับซ้อนและรุนแรงขึ้น
- **การใช้เครื่องมือสมัยใหม่ :** เรียนรู้เทคนิคการตรวจสอบอัตโนมัติและการใช้ AI ช่วยตรวจสอบ
- **การปฏิบัติตามกฎระเบียบ :** เข้าใจข้อบังคับใหม่ๆ เช่น PDPA และมาตรฐานความปลอดภัยสากล
- **ประสิทธิภาพในการดำเนินงาน :** สามารถวางแผนและดำเนินการตรวจสอบได้อย่างเห็นผล

ปัจจัยเร่งการเปลี่ยนแปลงในปี 2026

อ้างอิงจากรายงาน ISACA State of Digital Trust 2024 และ Deloitte Tech Trends 2025 ปัจจัยสำคัญที่ส่งผลต่อการตรวจสอบไอที ได้แก่ การเร่งตัวของ Digital Transformation, การใช้ Cloud-First Strategy ในองค์กรส่วนใหญ่ และการนำ AI เข้ามามีบทบาทในกระบวนการธุรกิจ

2. วิวัฒนาการแนวคิดพื้นฐานของการตรวจสอบไอที

การเปลี่ยนแปลงใน IT Landscape บังคับให้ขอบเขตและวิธีการตรวจสอบต้องพัฒนาจากรูปแบบเดิมไปสู่รูปแบบใหม่ ดังตารางเปรียบเทียบต่อไปนี้

หัวข้อเปรียบเทียบ	รูปแบบดั้งเดิม (Traditional IT)	รูปแบบสมัยใหม่ (Modern IT)
โครงสร้างระบบ	On-premise Infrastructure	Cloud-Native
การรักษาความปลอดภัย	Perimeter Security (เน้นขอบเขต)	Zero Trust (ไม่ไว้วางใจส่วนใดเลย)
กระบวนการควบคุม	Manual Process	Automated Controls
ฐานการตรวจสอบ	Compliance-based (เน้นกฎระเบียบ)	Risk-based (เน้นความเสี่ยง)

กรอบการทำงาน IT Audit สมัยใหม่ (Modern Framework)

1. **Risk Assessment:** การประเมินความเสี่ยงแบบ Dynamic ที่ปรับเปลี่ยนตามสถานการณ์
2. **Control Testing:** การทดสอบการควบคุมแบบ Continuous เพื่อการเฝ้าระวังตลอดเวลา
3. **Technology Integration:** การใช้ AI/ML เป็นผู้ช่วยหลักในการวิเคราะห์และตรวจสอบ
4. **Stakeholder Engagement:** การสื่อสารเชิงรุกกับผู้มีส่วนได้ส่วนเสียทุกระดับ

3. ประเภทและขอบเขตของการตรวจสอบไอที

การตรวจสอบไอทีสมัยใหม่แบ่งออกเป็น 4 ด้านหลัก เพื่อให้ครอบคลุมทุกมิติขององค์กร

- **Security Audit (การตรวจสอบความมั่นคงปลอดภัย):** ครอบคลุมทั้งการควบคุมทั่วไป (General Control) เช่น นโยบายความปลอดภัย และการควบคุมระดับระบบงาน (Application Control) เช่น การเข้ารหัสข้อมูล (Encryption) และการเขียนโปรแกรมอย่างปลอดภัย (Secure Coding)

- **Compliance Audit (การตรวจสอบการปฏิบัติตามข้อกำหนด):** เน้นการปฏิบัติตามกฎหมายและมาตรฐาน เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และมาตรฐาน PCI DSS สำหรับธุรกิจบัตรเครดิต
- **Operational Audit (การตรวจสอบการดำเนินงาน):** มุ่งเน้นประสิทธิภาพและประสิทธิผลของกระบวนการ IT เพื่อสนับสนุนเป้าหมายทางธุรกิจ
- **Forensic Audit (การตรวจสอบเชิงสืบสวน):** การสืบค้นหลักฐานเมื่อเกิดเหตุการณ์ทุจริตหรือการโจมตีทางไซเบอร์ เพื่อระบุความเสียหายและผู้กระทำผิด

4. ประเภทเครื่องมือที่ใช้ในการตรวจสอบ

ประเภทเครื่องมือ	ตัวอย่างซอฟต์แวร์
Basic Desktop	Microsoft Excel, Microsoft Access
Specialized Auditing	ACL, IDEA, Arbutus, SAS
Visualization	Tableau, Qlik, Power BI
Integrated Query	PeopleSoft, SAP, Oracle, JDE
Advanced/Server-based	R, Python, Rapidminer, SQL (SELECT statement)

หมายเหตุ: จากรายงาน Gartner Magic Quadrant เครื่องมือในกลุ่ม Microsoft, Tableau และ Qlik จัดว่าเป็นผู้นำในด้าน Analytics และ Business Intelligence Platforms

5. แนวคิดพื้นฐานและการบริหารจัดการการตรวจสอบ IT

- **ประเภทของการตรวจสอบ IT:** ครอบคลุมด้านความมั่นคงปลอดภัย (Security), การปฏิบัติตามข้อกำหนด (Compliance) เช่น PDPA, การตรวจสอบการดำเนินงาน (Operational) และการตรวจสอบเชิงสืบสวน (Forensic)
- **มาตรฐานที่ใช้:** อ้างอิงมาตรฐานสากลอย่าง **Global Internal Audit Standards (IIA)**, แนวทางการตรวจสอบเทคโนโลยี **GTAG** และกรอบการกำกับดูแล **COBIT 2019**
- **กระบวนการตรวจสอบ:** เริ่มจากการทำความเข้าใจธุรกิจ (Understand the Business) การกำหนดขอบเขต (Define IT Universe) การประเมินความเสี่ยง (Risk Assessment) และการจัดทำแผนการตรวจสอบ (Audit Plan)

6. การประเมินความเสี่ยงและการวางแผน (Risk Assessment)

- **เกณฑ์การประเมิน:** พิจารณาจาก **โอกาสที่จะเกิด (Likelihood)** และ **ผลกระทบ (Impact)** โดยมีการจัดลำดับความสำคัญ (Risk Ranking) เพื่อกำหนดรอบความถี่ในการเข้าตรวจ
- **วัตถุประสงค์:** เพื่อทำความเข้าใจความเสี่ยงและจัดสรรทรัพยากรการตรวจให้สอดคล้องกับระดับความเสี่ยงของแต่ละระบบ

7. เทคโนโลยีและการวิเคราะห์ข้อมูล (Data Analytics)

- **เครื่องมือ:** มีตั้งแต่เครื่องมือพื้นฐานอย่าง Excel, Access ไปจนถึงเครื่องมือวิเคราะห์ข้อมูลขั้นสูง (Specialized Auditing Software) และระบบบริหารธุรกิจอัจฉริยะ (Business Intelligence) เช่น **Power BI, Tableau, Qlik**
- **ทักษะทางเทคนิค:** ผู้ตรวจสอบควรมีความรู้ด้านภาษา **SQL** เพื่อจัดการฐานข้อมูล, การอ่าน **ER-Diagram** เพื่อเข้าใจความสัมพันธ์ของข้อมูล รวมถึงการใช้โปรแกรมอย่าง **Python** หรือ **RapidMiner** สำหรับการทำ Data Science และ AI

8. ความมั่นคงปลอดภัยสารสนเทศ (IT Security)

- **หลักการ CIA Triad:** การรักษาความปลอดภัยข้อมูลประกอบด้วย 3 เสาหลักคือ **ความลับ (Confidentiality)**, **ความถูกต้องครบถ้วน (Integrity)** และ **สภาพพร้อมใช้งาน (Availability)**
- **การควบคุม:** ครอบคลุมทั้งความปลอดภัยทางกายภาพ (Physical Security), การควบคุมระบบเครือข่าย (Firewall, Topology), การสำรองข้อมูล (Backup) และการกู้คืนระบบ โดยพิจารณาค่า **RPO (ระยะเวลาข้อมูลสูญหายที่ยอมรับได้)** และ **RTO (ระยะเวลาหยุดชะงักที่ยอมรับได้)**

9. กฎหมายและการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

- **บทบาทหน้าที่:** เน้นการปฏิบัติตาม **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562** และมาตรฐานสากลอย่าง **GDPR**
- **ประเด็นสำคัญ:** การกำหนดบทบาทผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor), การจัดการความยินยอม (Consent), สิทธิของเจ้าของข้อมูล และแนวทางการส่งข้อมูลไปต่างประเทศ

10. การพัฒนาและปฏิบัติการระบบ (System Development & Operations)

- **การควบคุมการเปลี่ยนแปลง:** การแก้ไขระบบต้องได้รับการอนุมัติ มีการทดสอบใน Sandbox และต้องมีการทำเอกสาร (Documentation) ที่ชัดเจน
- **เทคนิคการพัฒนา:** การใช้เทคนิคการพัฒนาโปรแกรมแบบรวดเร็ว (RAD) และการตรวจสอบโครงสร้างพื้นฐานของระบบ (Web/System Infrastructure)

สรุปได้ว่า หลักสูตรนี้มุ่งเน้นให้ผู้ตรวจสอบภายในมีความสามารถในการ**บูรณาการความรู้ด้านเทคโนโลยีสมัยใหม่เข้ากับกระบวนการตรวจสอบ** เพื่อประเมินความเสี่ยงและเพิ่มประสิทธิภาพในการดำเนินงานขององค์กรภาครัฐให้สอดคล้องกับมาตรฐานสากลและข้อกฎหมาย

◆ <u>COBIT คืออะไร?</u>

COBIT (Control Objectives for Information and Related Technologies) คือ กรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance & Management Framework) ซึ่งพัฒนาโดย ISACA (Information Systems Audit and Control Association) ซึ่งเป็นองค์กรระดับสากลด้านการกำกับดูแลระบบสารสนเทศ การตรวจสอบ และความมั่นคงปลอดภัยสารสนเทศ

มีจุดประสงค์หลักเพื่อช่วยให้องค์กรสามารถ:

- สร้างคุณค่า (Value Creation) จากการลงทุนใน IT
- บริหารจัดการและควบคุม IT อย่างมีประสิทธิภาพ
- เชื่อมโยง IT กับเป้าหมายขององค์กร (Enterprise Goals)
- สร้างสมดุลระหว่างความเสี่ยง เทคโนโลยี และคุณค่า
- ลดความเสี่ยงและควบคุม IT ได้อย่างเหมาะสม
- ปฏิบัติสอดคล้องกับกฎหมาย กฎระเบียบ และมาตรฐานต่าง ๆ (เช่น GDPR, PDPA, ITGC)

แนวคิดหลักของ COBIT

COBIT มีหลักคิดสำคัญ 5 ประการ (5 Principles) ได้แก่

1. Meeting Stakeholder Needs เน้นการสร้างคุณค่าให้กับผู้มีส่วนได้ส่วนเสีย (Stakeholders) โดยพิจารณาความต้องการ ความคาดหวัง และความเสี่ยง

2. Covering the Enterprise End-to-End ขอบเขตครอบคลุมทั้งองค์กร ไม่เฉพาะแค่ IT รวมไปถึงการรวมการกำกับดูแล (Governance) และการบริหารจัดการ (Management)

3. Applying a Single Integrated Framework ผสานมาตรฐานสากลอื่น ๆ เช่น ITIL, ISO/IEC 27001, TOGAF และ PMBOK มาไว้ในกรอบเดียว

4. Enabling a Holistic Approach ใช้ตัวขับเคลื่อนที่เรียกว่า “Enablers” จำนวน 7 ประการ เพื่อให้การดำเนินการสอดคล้องและมีประสิทธิภาพ (ทั้งนโยบาย กระบวนการ ข้อมูล คน และเทคโนโลยี)

5. Separating Governance from Management แยกบทบาทการกำกับดูแล (Governance) ออกจากการบริหารจัดการ (Management) อย่างชัดเจน

◆ **ความแตกต่างระหว่าง General Control** (การควบคุมทั่วไป) และ **Application Control** (การควบคุมระบบงาน) มีรายละเอียดดังนี้:

1. General Control (การควบคุมทั่วไป)

- **นิยาม:** เป็นการควบคุมที่นำมาใช้กับ**สภาพแวดล้อมทางด้าน IT โดยรวม** หรือโครงสร้างพื้นฐานด้านไอที (IT Infrastructure) ซึ่งครอบคลุมทั้งส่วนผสมของระบบ เครือข่าย ข้อมูล บุคลากร และกระบวนการต่าง ๆ
- **ขอบเขต:** มีลักษณะครอบคลุมกว้าง ๆ เพื่อให้มั่นใจว่าสภาพแวดล้อมโดยรวมของระบบสารสนเทศมีความปลอดภัยและทำงานได้อย่างถูกต้อง
- **ตัวอย่าง:** นโยบายความปลอดภัย (Security Policy) และการจัดการช่องโหว่ (Vulnerability Management)

2. Application Control (การควบคุมระบบงาน)

- **นิยาม:** เป็นการควบคุมที่เกี่ยวข้องกับ**การทำงานเฉพาะด้านของระบบแอปพลิเคชัน** ที่สนับสนุนกระบวนการทางธุรกิจที่เฉพาะเจาะจง
- **ขอบเขต:** เน้นไปที่กระบวนการทางธุรกิจแต่ละส่วน (Individual Business Processes) เพื่อให้มั่นใจว่าการประมวลผลข้อมูลในระบบงานนั้น ๆ มีความถูกต้อง ครบถ้วน และเชื่อถือได้
- **ตัวอย่าง :**
    - การตรวจสอบความถูกต้องของข้อมูล (Data Edits)
    - การกระทบยอดผลรวมการประมวลผล (Balancing of Processing Totals)
    - การบันทึกรายการ (Transaction Logging) และการรายงานข้อผิดพลาด
    - การเข้ารหัสข้อมูล (Encryption) และการเขียนโปรแกรมอย่างปลอดภัย (Secure Coding)

สรุปความแตกต่างสำคัญ: General Control จะเน้นที่การดูแล **"ภาพรวมและโครงสร้างพื้นฐาน"** ของระบบไอทีในองค์กร ในขณะที่ **Application Control** จะเน้นที่การควบคุม **"ฟังก์ชันการทำงานเฉพาะจุด"** ภายในซอฟต์แวร์หรือระบบงานเพื่อดูแลความถูกต้องของข้อมูลในแต่ละกระบวนการธุรกิจ

◆ ในการกู้คืนระบบหลักสูตร CGIA มีการกำหนดตัวชี้วัดสำคัญสองประการคือ **RPO** และ **RTO** ซึ่งมีความหมายดังนี้

1. Recovery Point Objective (RPO)

- **ความหมาย:** เป็นการกำหนดเป้าหมายโดยอ้างอิงจาก **"ปริมาณข้อมูลที่ยอมรับได้ว่าจะสูญหาย" (Acceptable data loss)**
- **จุดเน้น:** ระบุถึงจุดย้อนหลังในอดีตที่เร็วที่สุดที่องค์กรยอมรับได้ในการกู้คืนข้อมูลกลับมาใช้งาน ตัวอย่างเช่น หากกำหนด RPO ไว้ที่ 4 ชั่วโมง ข้อมูลที่กู้คืนกลับมาจะต้องมีอายุไม่เกิน 4 ชั่วโมงก่อนเกิดเหตุขัดข้อง หากสูญหายมากกว่านั้นจะถือว่าไม่เป็นไปตามเป้าหมาย

2. Recovery Time Objective (RTO)

- **ความหมาย:** เป็นการกำหนดเป้าหมายโดยอ้างอิงจาก **"ระยะเวลาหยุดชะงักของระบบที่ยอมรับได้" (Acceptable downtime)**
- **จุดเน้น:** ระบุถึงระยะเวลาที่เร็วที่สุดที่การดำเนินงานทางธุรกิจจะต้อง **"กลับมาเริ่มต้นใหม่ได้" (Resume)** หลังจากเกิดเหตุการณ์หยุดชะงัก ตัวอย่างเช่น หากกำหนด RTO ไว้ที่ 2 ชั่วโมง ระบบและกระบวนการทางธุรกิจจะต้องกลับมาใช้งานได้ภายใน 2 ชั่วโมงหลังจากที่ระบบล่ม

สรุปความสัมพันธ์:

- RPO จะมองไปที่ **"ข้อมูลในอดีต"** ว่าหายไปได้มากน้อยแค่ไหนก่อนเกิดเหตุ
- RTO จะมองไปที่ **"อนาคต"** ว่าจะใช้เวลานานแค่ไหนหลังจากเกิดเหตุเพื่อให้ระบบกลับมาใช้งานได้ปกติ

การเลือกกลยุทธ์ในการกู้คืน (Recovery Strategies) จะต้องพิจารณาจากความสำคัญของกระบวนการทางธุรกิจ ต้นทุน และระยะเวลาที่ต้องใช้เพื่อให้สอดคล้องกับค่า RPO และ RTO ที่กำหนดไว้

◆ หลักการ **CIA Triad** ถือเป็นเสาหลักสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) ซึ่งประกอบด้วยองค์ประกอบ 3 ประการ ดังนี้

1. ความลับ (Confidentiality) หมายถึง การธำรงไว้ซึ่งข้อมูลให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

- **จุดประสงค์:** เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- **การนำไปใช้:** มีการกำหนดระดับความลับของข้อมูล (Security Levels) เช่น **Top Secret, Secret, Confidential** และ **Unclassified** เพื่อให้ความสำคัญกับการควบคุมที่เหมาะสมกับความเสี่ยง, นอกจากนี้ยังเกี่ยวข้องกับการพิสูจน์ตัวตน (Authentication) เพื่อระบุว่าใครมีสิทธิ์เข้าถึงข้อมูลใด

2. ความถูกต้องครบถ้วน (Integrity) หมายถึง การทำให้มั่นใจว่าข้อมูลมีความถูกต้อง แม่นยำ และไม่ถูกแก้ไขเปลี่ยนแปลงโดยพลการ,

- **จุดประสงค์:** ป้องกันการสูญหาย การแก้ไข หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
- **การนำไปใช้:** ในระบบฐานข้อมูลจะมีการใช้ **Integrity Controls** เช่น การกำหนด Primary Key ที่ไม่ซ้ำกันและไม่เป็นค่าว่าง เพื่อรักษาความสัมพันธ์ของข้อมูลให้ถูกต้องครบถ้วนเสมอ, นอกจากนี้ยังรวมถึงการใช้ฟังก์ชัน Hash เพื่อตรวจสอบว่าข้อมูลไม่ถูกแก้ไขระหว่างทาง

3. สภาพพร้อมใช้งาน (Availability) หมายถึง การที่ระบบหรือข้อมูลมีความพร้อมที่จะให้ผู้มีสิทธิ์เรียกใช้งานได้ในเวลาที่ต้องการ

- **จุดประสงค์:** เพื่อให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่องและลดความเสี่ยงจากการหยุดชะงักของระบบ
- **การนำไปใช้:** เกี่ยวข้องโดยตรงกับการวางแผนอุบัติภัยและการกู้คืนระบบ (Business Continuity & Disaster Recovery) โดยมีการกำหนดค่า **RPO** (จุดที่ข้อมูลสูญหายได้) และ **RTO** (ระยะเวลาที่ระบบต้องกลับมาใช้งานได้) รวมถึงการสำรองข้อมูล (Backup) อย่างสม่ำเสมอเพื่อให้ข้อมูลพร้อมกลับมาใช้งานได้ทันที

สรุปความสำคัญ: ผู้ตรวจสอบสารสนเทศจะใช้หลักการ CIA นี้เป็นเกณฑ์ในการประเมินว่า มาตรการควบคุม (Controls) ที่องค์กรติดตั้งไว้นั้น **"เพียงพอ"** ที่จะรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลสำคัญและระบบงานหรือไม่

◆ **กฎหมาย PDPA (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)** มีบทบาทสำคัญอย่างยิ่งต่อการตรวจสอบ ไอทีภาครัฐ โดยทำหน้าที่เป็นกรอบเกณฑ์ทางกฎหมายที่ผู้ตรวจสอบภายในต้องนำมาใช้ประเมินการดำเนินงานของหน่วยงาน สรุปได้ดังนี้:

1. เป็นหัวใจหลักของการตรวจสอบการปฏิบัติตามข้อกำหนด (Compliance Audit)

การตรวจสอบไอทีในปัจจุบันต้องรวมเอา PDPA เข้าเป็นส่วนหนึ่งของ **Compliance Audit** เพื่อประเมินว่าหน่วยงานภาครัฐมีการปฏิบัติตามกฎหมายและมาตรฐานต่างๆ อย่างถูกต้องหรือไม่ โดยครอบคลุมทั้ง:

- **การควบคุมทั่วไป (General Control):** เช่น นโยบายการรักษาความปลอดภัยข้อมูลของหน่วยงาน
- **การควบคุมระบบงาน (Application Control):** เช่น ระบบการเข้ารหัสข้อมูล (Encryption) ในแอปพลิเคชันที่เก็บข้อมูลประชาชน

2. บทบาทหน้าที่โดยตรงของผู้ตรวจสอบในด้านความเป็นส่วนตัว

หลักสูตร บทบาทหลักของผู้ตรวจสอบในด้านนี้คือการทำให้มั่นใจว่ากฎหมายและระเบียบที่เกี่ยวข้องกับความเป็นส่วนตัวได้ถูกสื่อสารไปยังผู้ที่มีส่วนรับผิดชอบอย่างทั่วถึง นอกจากนี้ยังต้องทำงานร่วมกับที่ปรึกษาทางกฎหมายเพื่อระบุขั้นตอนที่จำเป็นในการปฏิบัติตามข้อกำหนดทั้งหมดของกฎหมาย

3. แนวทางในการตรวจสอบสิทธิและหน้าที่ (Audit Guidelines)

PDPA กำหนดแนวทางให้ผู้ตรวจสอบภาครัฐต้องตรวจสอบประเด็นสำคัญ ดังนี้

- **โครงสร้างการบริหารจัดการ:** ตรวจสอบว่ามีการจัดตั้งโครงสร้างเพื่อดูแลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดหรือไม่
- **บทบาทหน้าที่:** ตรวจสอบว่ามีการกำหนดหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษรที่ชัดเจนหรือไม่
- **กระบวนการและแบบฟอร์ม:** ตรวจสอบความถูกต้องของแบบฟอร์มขอความยินยอม (Consent Form) และกระบวนการขอใช้สิทธิต่างๆ ของเจ้าของข้อมูล
- **การรักษาความมั่นคงปลอดภัย:** ตรวจสอบมาตรการทางเทคนิคเพื่อป้องกันข้อมูลรั่วไหล

4. การตรวจสอบหน้าที่ของผู้ควบคุมข้อมูล (Data Controller)

ผู้ตรวจสอบต้องตรวจสอบว่าหน่วยงานในฐานะผู้ควบคุมข้อมูลทำหน้าที่ได้ครบถ้วนตาม **มาตรา 37** หรือไม่ ซึ่งรวมถึง :

- การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- การมีระบบตรวจสอบเพื่อลบหรือทำลายข้อมูลเมื่อหมดความจำเป็น
- **การแจ้งเหตุละเมิด:** ต้องมีกลไกที่สามารถแจ้งเหตุข้อมูลรั่วไหลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ได้ **ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุ

5. เครื่องมือในการกำกับดูแลและสร้างความเชื่อมั่น สำหรับภาครัฐ PDPA ทำหน้าที่เป็นเครื่องมือสำคัญในการกำกับดูแลการดำเนินงาน ช่วยให้สามารถตรวจสอบการทำงานของหน่วยงานรัฐเองและภาคธุรกิจที่เกี่ยวข้องให้มีความถูกต้องเหมาะสม ซึ่งจะช่วยส่งเสริมภาพลักษณ์ที่ดีของประเทศและสร้างความเชื่อมั่นให้กับประชาชนในการรับบริการจากรัฐว่าข้อมูลของเขาจะถูกจัดการอย่างโปร่งใสและตรวจสอบได้

◆ **เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย** หรือ **CAATs (Computer Assist Audit Techniques)** หลักสูตร CGIA ช่วยเพิ่มประสิทธิภาพการตรวจสอบผ่านโอกาสสำคัญ (Opportunities) และเทคนิคเฉพาะด้านต่างๆ ดังนี้

1. เพิ่มผลิตผลและประหยัดต้นทุน (Productivity and Cost Savings)

- **ประมวลผลข้อมูลจำนวนมาก:** ช่วยให้ผู้ตรวจสอบสามารถ**ประมวลผลข้อมูลปริมาณมหาศาลได้คราวละมากๆ** ตามความต้องการ ซึ่งมีประสิทธิภาพสูงกว่าการตรวจสอบด้วยมือ
- **ประหยัดเวลาในการเขียนโปรแกรม:** การใช้ซอฟต์แวร์ตรวจสอบสำเร็จรูป (**Generalized Audit Software - GAS**) ช่วยให้ผู้ตรวจสอบ**ใช้งานได้ทันทีและประหยัดเวลา** โดยไม่ต้องมีความรู้ลึกซึ้งด้านภาษาโปรแกรมมิ่ง (Programming Language)
- **ความสามารถในการนำกลับมาใช้ซ้ำ:** โปรแกรมการตรวจสอบที่สร้างขึ้นสามารถ**นำกลับมาใช้งานซ้ำได้ในคราวต่อๆ ไป** ช่วยลดค่าใช้จ่ายและเวลาในการเตรียมการระยะยาว

2. เพิ่มประสิทธิภาพในการเข้าถึงและวิเคราะห์ข้อมูล (Efficiency in Data Access)

- **การเข้าถึงข้อมูลที่หลากหลาย (Compatibility):** เครื่องมืออย่าง GAS สามารถเชื่อมต่อและเข้าถึงข้อมูลได้หลายประเภท ทำให้ผู้ตรวจสอบทำงานกับระบบงานที่แตกต่างกันได้สะดวกขึ้น
- **ความสามารถในการวิเคราะห์ขั้นสูง:** ช่วยในการคำนวณค่าทางสถิติ, การจัดกลุ่มเพื่อหาแบบแผน (Classification), การตรวจสอบข้อมูลซ้ำ (Duplicate testing) และการตรวจสอบช่องว่างของข้อมูล (Gap testing) ซึ่งช่วยให้พบความผิดปกติที่การตรวจสอบทั่วไปอาจมองข้าม

3. การบริหารความเสี่ยงและการตรวจสอบที่ครอบคลุม (Audit Risk Management)

- **ตรวจสอบได้ครบ 100%:** แทนที่จะสุ่มตรวจเพียงบางส่วน ผู้ตรวจสอบสามารถใช้เครื่องมือ **Data Mining** เพื่อ**ค้นหาจากทุกระเบียนข้อมูล (Every record)** เพื่อระบุรายการที่อาจมีการทุจริตได้อย่างแม่นยำ
- **การจำลองสถานการณ์จริง:** เทคนิค **Parallel Simulation** ช่วยให้ผู้ตรวจสอบสร้างโปรแกรมเลียนแบบการทำงานของระบบจริง เพื่อเปรียบเทียบผลลัพธ์ได้อย่าง**เป็นอิสระจากกระบวนการผลิตปกติ (Production Run)**

4. การตรวจสอบและระบุปัญหาอย่างต่อเนื่องและรวดเร็ว

- **การตรวจสอบอย่างต่อเนื่อง (Continuous Monitoring):** เทคนิคอย่าง **SCARF** (System Control Audit Review File) ช่วยในการติดตามรายการที่เกิดขึ้นและสุ่มตรวจรายการที่ผิดเงื่อนไขได้ตลอดเวลา
- **ระบุปัญหาได้ทันที:** เทคนิคอย่าง **Snapshot** ช่วยให้พบปัญหาและแก้ไขได้อย่างรวดเร็ว โดยการแทรกคำสั่งตรวจสอบไว้ในจุดต่างๆ ของโปรแกรมเพื่อดูการไหลของข้อมูล
- **ทดสอบภายใต้สภาวะจริง:** การใช้ **Integrated Test Facility (ITF)** ทำให้ผู้ตรวจสอบสามารถทดสอบระบบภายใต้สภาวะการทำงานจริงร่วมกับรายการปกติ ทำให้ทราบผลการตรวจสอบและประเมินระบบได้ทันที

สรุปได้ว่า CAATs เป็นเครื่องมือสำคัญที่ตอบโจทย์ความกดดันในปัจจุบันที่หน่วยงานตรวจสอบต้อง **"ทำงานให้ได้มากขึ้นด้วยทรัพยากรที่น้อยลง" (Do more with less)** โดยการนำเทคโนโลยีมาช่วยยกระดับคุณภาพและความทั่วถึงในการตรวจสอบ

◆ **การเลือกใช้เครื่องมือสำหรับทำ Data Analytics ของผู้ตรวจสอบ หลักสูตร CGIA** สามารถแบ่งออกเป็นกลุ่มตามลักษณะการใช้งานและความซับซ้อนของข้อมูลได้ดังนี้

1. เครื่องมือพื้นฐาน (Basic Desktop) เป็นเครื่องมือที่ผู้ตรวจสอบส่วนใหญ่คุ้นเคยและใช้งานได้ในระดับเริ่มต้น

- **Microsoft Excel:** ใช้สำหรับการวิเคราะห์ข้อมูลเบื้องต้น

- **Microsoft Access:** ใช้สำหรับการจัดการฐานข้อมูลในระดับสำนักงาน

2. ซอฟต์แวร์สำหรับการตรวจสอบโดยเฉพาะ (Specialized Auditing Software) เป็นเครื่องมือที่มีฟังก์ชันออกแบบมาเพื่องานตรวจสอบ (GAS) ช่วยให้ประมวลผลข้อมูลได้คราวละมาก ๆ และมีชุดคำสั่งพื้นฐาน เช่น การคำนวณค่าเสื่อมราคาหรือการจัดชั้นลูกหนี้

- **ACL**
- **IDEA**
- **Arbutus**
- **SAS**

3. เครื่องมือวิเคราะห์ข้อมูลและสร้างภาพข้อมูล (Specialized DA Visualization) เน้นการดึงข้อมูลมาวิเคราะห์และนำเสนอในรูปแบบภาพ (Dashboard) เพื่อให้เห็นแนวโน้มหรือความผิดปกติได้ชัดเจน

- **Tableau**
- **Power BI**
- **Qlik**

4. เครื่องมือวิเคราะห์ข้อมูลขั้นสูง (Advance Data Analytic Tools) เหมาะสำหรับงานวิเคราะห์ที่มีความซับซ้อนสูง เช่น การทำ Data Science หรือ AI:

Python: ภาษาที่ได้รับความนิยมสูง มี Library รองรับการทำ Data Science, Machine Learning และ AI ได้เป็นอย่างดี

R: เน้นการวิเคราะห์ทางสถิติและประมวลผลข้อมูลขนาดใหญ่ (Big Data)

RapidMiner: โปรแกรมที่ช่วยในการออกแบบ Workflow เพื่อวิเคราะห์ข้อมูล

5. เครื่องมือสืบค้นข้อมูลในระบบงาน (Integrated Query & Report Writers)

Query Tools: ใช้ดึงข้อมูลจากระบบหลักขององค์กรโดยตรง เช่น **SAP, Oracle, PeopleSoft**

Report Writers: ใช้ในการสร้างรายงานจากฐานข้อมูล เช่น **Cognos, Business Objects**

นอกจากนี้ ผู้ตรวจสอบควรมีความรู้ใน **ภาษา SQL** ซึ่งเป็นภาษามาตรฐานในการจัดการและเรียกดูข้อมูลจากระบบฐานข้อมูลเชิงสัมพันธ์ เพื่อให้สามารถเข้าถึงข้อมูลจากแหล่งที่แตกต่างกันได้อย่างอิสระ

◆ **เทคนิค Parallel Simulation** (การประมวลผลคู่ขนาน) เป็นหนึ่งในเทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (**CAATs**) ที่มีความสำคัญในการตรวจสอบความถูกต้องของระบบงาน โดยมีรายละเอียดเพิ่มเติม ดังนี้

- **แนวคิดหลัก:** เป็นการที่ผู้ตรวจสอบ**สร้างโปรแกรมขึ้นมาเพื่อเลียนแบบการทำงาน (Simulate) ของระบบงานจริง (Production Run)** เพื่อทดสอบว่าระบบที่องค์กรใช้งานอยู่นั้นประมวลผลได้ถูกต้องตามเงื่อนไขที่ควรจะเป็นหรือไม่
- **การใช้ข้อมูลจริง:** เทคนิคนี้จะใช้**ข้อมูลที่ผ่านขั้นตอนการปฏิบัติงานจริงมาแล้ว** มาเข้าสู่โปรแกรมจำลองที่ผู้ตรวจสอบสร้างขึ้น เพื่อเปรียบเทียบผลลัพธ์
- **ความเป็นอิสระในการตรวจสอบ:** การตรวจสอบด้วยวิธีนี้สามารถทำได้**โดยอิสระจากกระบวนการผลิตปกติ (Production Run)** และผู้ตรวจสอบสามารถเลือกระดับความละเอียดในการตรวจได้ว่าจะตรวจสอบเพียงบางขั้นตอนหรือครอบคลุมทุกขั้นตอนของระบบงาน
- **ความยืดหยุ่นด้านเวลา:** ผู้ตรวจสอบสามารถพัฒนาระบบตรวจสอบจำลองนี้ขึ้นมาภายหลังจากที่หน่วยงานได้นำระบบงานจริงลงใช้งานแล้วก็ได้

- **เงื่อนไขสำคัญสำหรับผู้ตรวจสอบ**
    - ผู้ตรวจสอบจำเป็นต้อง**มีความเข้าใจในตัวระบบงาน (Application)** นั้น ๆ ดีเพียงพอที่จะเขียนโปรแกรมเลียนแบบเงื่อนไขการประมวลผลได้อย่างถูกต้อง
    - เมื่อได้ข้อมูลจากการประมวลผลของทั้งโปรแกรมจำลองและโปรแกรมจริงแล้ว จะนำผลลัพธ์ทั้งสองมา**เปรียบเทียบความแตกต่างโดยใช้คอมพิวเตอร์**เพื่อระบุจุดผิดปกติ

สรุปได้ว่าเทคนิคนี้ช่วยให้ผู้ตรวจสอบสามารถยืนยันความถูกต้องของตรรกะการประมวลผลในระบบงานจริงได้อย่างมั่นใจ โดยใช้ข้อมูลจริงมาทดสอบในสภาพแวดล้อมที่ควบคุมโดยผู้ตรวจสอบเอง

◆ **เทคนิค Test Data (ข้อมูลทดสอบ)** เป็นวิธีการตรวจสอบความถูกต้องของการทำงานในระบบคอมพิวเตอร์ โดยผู้ตรวจสอบจะจัดเตรียมชุดข้อมูลและคำนวณผลลัพธ์ที่ถูกต้องไว้ล่วงหน้า จากนั้นจึงนำไปประมวลผลด้วยโปรแกรมระบบงานจริงเพื่อเปรียบเทียบผลลัพธ์

สถานการณ์ที่ควรเลือกใช้เทคนิค Test Data มีตัวอย่างดังนี้

1. การตรวจสอบตรรกะการประมวลผลที่ซับซ้อน: เมื่อต้องการยืนยันว่าโปรแกรมคำนวณค่าต่างๆ ได้ถูกต้องตามเงื่อนไขทางธุรกิจหรือไม่ เช่น การคำนวณเงินเดือนที่มีเงื่อนไขภาษีและสวัสดิการที่หลากหลาย หรือการจัดชั้นลูกหนี้ตามอายุหนี้ ซึ่งการใช้ Test Data จะช่วยให้สังเกตเห็นข้อบกพร่องในตรรกะของโปรแกรมได้ง่ายกว่าการไปไล่ตรวจจากข้อมูลจริงจำนวนมาก

2. การทดสอบภายหลังการแก้ไขปรับปรุงระบบ (Regression Testing): ในกรณีที่ระบบงานมีการแก้ไขโค้ดโปรแกรมหรือเพิ่มฟังก์ชันใหม่ ผู้ตรวจสอบสามารถนำชุดข้อมูลทดสอบชุดเดิมที่เคยใช้มาประมวลผลซ้ำ เพื่อมั่นใจว่าการแก้ไขนั้นไม่กระทบกับส่วนงานเดิมที่เคยทำงานได้ถูกต้องอยู่แล้ว

3. การตรวจสอบมาตรการควบคุมการนำเข้าข้อมูล (Input Controls): ใช้เพื่อทดสอบว่าระบบมี "Edit checks" ที่มีประสิทธิภาพหรือไม่ เช่น

Limit checks: ลองป้อนจำนวนเงินที่ติดลบหรือสูงเกินกว่าเพดานที่กำหนดเพื่อดูว่าระบบตัดรายการหรือไม่

Check digits: ลองป้อนเลขที่บัญชีที่ผิดหลักตรวจสอบเพื่อดูว่าระบบตรวจพบความผิดปกติหรือไม่

Range tests: ทดสอบการป้อนข้อมูลที่อยู่นอกช่วงวันที่หรือค่าที่ยอมรับได้

4. การยืนยันความถูกต้องของระบบงานใหม่ (System Implementation): ในขั้นตอนการตรวจรับระบบก่อนใช้งานจริง (UAT) ผู้ตรวจสอบสามารถใช้ Test Data เพื่อยืนยันว่าระบบใหม่ทำงานได้ตรงตามความต้องการ (User Requirements) และเงื่อนไขที่ออกแบบไว้

5. การตรวจสอบความถูกต้องครบถ้วนของฐานข้อมูล (Database Integrity): ใช้ทดสอบว่าระบบมีการควบคุม Primary Key ไม่ให้ซ้ำกันหรือเป็นค่าว่าง (Null) ตามหลักการ Integrity Controls หรือไม่

ข้อควรระวังสำคัญ: ผู้ตรวจสอบต้องมั่นใจว่าโปรแกรมที่นำมาทดสอบนั้นเป็น **"ตัวเดียวกับที่ใช้ในการปฏิบัติงานจริง"** และต้องระมัดระวังไม่ให้ข้อมูลทดสอบเข้าไปปนเปื้อนหรือทำให้ข้อมูลจริงในระบบเสียหาย

◆ **เทคนิค Integrated Test Facility (ITF)** และ **Test Data** เป็นเทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (CAATs) ที่มีความคล้ายคลึงกันตรงที่ใช้ชุดข้อมูลทดสอบเพื่อตรวจสอบความถูกต้องของระบบงาน แต่มีข้อแตกต่างที่สำคัญในด้านสภาวะแวดล้อมและวิธีการจัดการ ดังนี้

1. สภาวะแวดล้อมในการทดสอบ

Test Data (ข้อมูลทดสอบ): เป็นการนำชุดข้อมูลที่เตรียมไว้ล่วงหน้ามาประมวลผลด้วยโปรแกรมระบบงานจริง เพื่อดูว่าผลลัพธ์ที่ได้ตรงกับที่คาดการณ์ไว้หรือไม่ โดยทั่วไปมักจะทำแยกส่วนจากกระบวนการปฏิบัติงานจริง

ITF (การทดสอบในระบบงานจริง): เป็นการตรวจสอบที่ทำไป **"พร้อม ๆ กับการปฏิบัติงานจริง" (Production Run)** ข้อมูลทดสอบจะไหลเข้าสู่ระบบไปพร้อมกับรายการปกติของหน่วยงาน

2. การแยกข้อมูลและหน่วยรับตรวจ

Test Data: ผู้ตรวจสอบใช้ข้อมูลที่จำลองขึ้นมาเพื่อทดสอบตรรกะของโปรแกรม

ITF: ใช้สิ่งที่เรียกว่า **"Dummy Entity"** (หน่วยจำลองหรือรหัสสมมติ) เข้าช่วย ข้อมูลของ ITF จะถูกบันทึกเข้าระบบจริงแต่จะถูกแยกออกจากรายงานการควบคุม (Control Report) ในงานประจำ เพื่อไม่ให้ไปปะปนกับรายการปกติขององค์กร

3. ระยะเวลาและความสม่ำเสมอ

Test Data: มักทำเป็นครั้งคราว เช่น เมื่อมีการแก้ไขโปรแกรมหรือต้องการยืนยันความถูกต้องเฉพาะจุด

ITF: สามารถ**ตรวจสอบได้อย่างสม่ำเสมอ**และต่อเนื่องโดยไม่มีกำหนดการล่วงหน้า เหมาะสำหรับระบบงานที่มีการแก้ไขเพิ่มเติมบ่อยๆ

4. การกำจัดข้อมูลหลังการตรวจสอบ

Test Data: เนื่องจากมักทำในสภาพแวดล้อมทดสอบ จึงไม่มีประเด็นเรื่องข้อมูลตกค้างในบัญชีจริง

ITF: มีความยุ่งยากกว่า เพราะรายการทดสอบที่ส่งเข้าไปพร้อมระบบงานจริง**ต้องถูกนำออกจากบัญชี** โดยการลงรายการปรับปรุงด้วยมือหรือใช้โปรแกรมช่วย หากขจัดข้อมูล (ITF Data) ออกไม่หมด จะเสี่ยงต่อความผิดพลาดของข้อมูลในระบบบัญชีจริง

5. ต้นทุนและประสิทธิภาพ

Test Data: ผู้ตรวจสอบต้องเสียเวลามากในการจัดเตรียมข้อมูลและคำนวณผลลัพธ์ที่คาดหวัง

ITF: มี**ต้นทุนในการประมวลผลต่ำ**เพราะข้อมูลถูกประมวลผลไปพร้อมกับรายการปกติ แต่จะมีต้นทุนสูงหากต้องแก้ไขโปรแกรมเพื่อขจัดผลรายการทดสอบออกไป

สรุปสั้นๆ: Test Data คือการเอาข้อมูลปลอมไปใส่โปรแกรมจริงเพื่อดูผลลัพธ์ (มักทำแยกส่วน) ในขณะที่ **ITF** คือการสร้าง "ลูกค้าปลอม" ไว้ในระบบจริง แล้วส่งรายการเข้าไปประมวลผลร่วมกับลูกค้าคนอื่นๆ เพื่อทดสอบระบบภายใต้สภาวะการทำงานจริง

◆ **แนวทางการตรวจสอบหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีรายละเอียดที่ผู้ตรวจสอบต้องประเมินและพิจารณาดังนี้

1. โครงสร้างและการบริหารจัดการ (Management Structure)

ผู้ตรวจสอบควรดำเนินการตรวจสอบการจัดทำ**โครงสร้างการบริหารจัดการ**ให้เป็นไปตามกฎหมาย ซึ่งรวมถึง

- **การกำหนดบทบาทและหน้าที่:** ต้องมีการระบุหน้าที่ความรับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร
- **การแต่งตั้งตัวแทน:** ในกรณีที่มีความจำเป็นต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทนนั้นต้องอยู่ในราชอาณาจักรและได้รับการมอบอำนาจเป็นหนังสือ
- **การจัดทำนโยบาย:** ตรวจสอบว่ามีการจัดทำนโยบายที่จำเป็น เช่น **นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)** และนโยบายการรักษาความมั่นคงปลอดภัย

2. มาตรการรักษาความมั่นคงปลอดภัย (Security Measures)

ผู้ควบคุมข้อมูลมีหน้าที่จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** โดยผู้ตรวจสอบต้องพิจารณาองค์ประกอบ 3 ด้าน (CIA Triad) ดังนี้

- **ความลับ (Confidentiality):** ป้องกันการเข้าถึงข้อมูลโดยมิชอบ
- **ความถูกต้องครบถ้วน (Integrity):** ป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ

- **สภาพพร้อมใช้งาน (Availability):** เพื่อให้สามารถเรียกใช้งานข้อมูลได้เมื่อต้องการ
- **การป้องกันเมื่อต้องให้ข้อมูลแก่ผู้อื่น:** หากมีการส่งข้อมูลให้บุคคลอื่นหรือผู้ประมวลผลข้อมูล ต้องมีมาตรการป้องกันการใช้ข้อมูลโดยมิชอบ

3. กระบวนการและแบบฟอร์ม (Processes and Forms) ผู้ตรวจสอบต้องประเมินความถูกต้องของกระบวนการต่าง ๆ ได้แก่

- **การขอความยินยอม (Consent):** ตรวจสอบแบบฟอร์มขอความยินยอม (Consent Form) และกระบวนการจัดการความยินยอม (Consent Management Procedure) ให้เป็นไปตามเงื่อนไขทางกฎหมาย เช่น การใช้ภาษาที่อ่านง่ายและเข้าถึงได้ง่าย
- **การแจ้งรายละเอียด (Notification):** ตรวจสอบว่ามีการแจ้งวัตถุประสงค์ ระยะเวลาการเก็บรักษา และรายละเอียดการติดต่อให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูล
- **สิทธิของเจ้าของข้อมูล:** ตรวจสอบแบบฟอร์มและกระบวนการขอใช้สิทธิต่าง ๆ (Data Subject Request Form/Procedure) เช่น สิทธิการเข้าถึงข้อมูล หรือสิทธิการขอให้ลบข้อมูล

4. การจัดการวงจรชีวิตข้อมูล (Data Lifecycle Management)

- **การตรวจสอบการลบหรือทำลาย:** ตรวจสอบว่าหน่วยงานมีระบบการตรวจสอบเพื่อดำเนินการ**ลบหรือทำลายข้อมูล** เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อข้อมูลนั้นเกินความจำเป็น
- **การจัดการข้อมูลเอกสารและสารสนเทศ:** ตรวจสอบการบริหารจัดการข้อมูลทั้งในรูปแบบสิ่งพิมพ์และระบบเทคโนโลยีสารสนเทศ

5. การจัดการเมื่อเกิดเหตุละเมิด (Data Breach Management)

ผู้ตรวจสอบต้องยืนยันว่าหน่วยงานมีกลไกในการ**แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล**ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.):

- ต้องแจ้งโดยไม่ชักช้า**ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุเท่าที่จะทำได้
- ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล ต้องแจ้งเหตุให้เจ้าของข้อมูลทราบพร้อม**แนวทางการเยียวยา**ด้วย

6. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross Border Transfer)

ตรวจสอบว่ามีการกำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ สำหรับการส่งหรือโอนข้อมูลไปยังต่างประเทศ ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

🔍 ความแตกต่างระหว่าง Risk Governance กับ Risk Management

หัวข้อ	Risk Governance (การกำกับดูแลความเสี่ยง)	Risk Management (การบริหารความเสี่ยง)
นิยาม	กระบวนการกำหนดทิศทาง นโยบาย โครงสร้าง และการกำกับติดตามการบริหารความเสี่ยง	กระบวนการระบุ ประเมิน ตอบสนอง และติดตามความเสี่ยง
เป้าหมาย	เพื่อให้มั่นใจว่าองค์กรมีระบบการจัดการความเสี่ยงที่เหมาะสม และสอดคล้องกับเป้าหมายและนโยบาย	เพื่อลดผลกระทบและความน่าจะเป็นของความเสี่ยงต่อการดำเนินงาน
ผู้รับผิดชอบหลัก	คณะกรรมการ ผู้บริหารระดับสูง เช่น นายก อบจ. หรือ ปลัด อบจ.	เจ้าหน้าที่ หน่วยงานภายใน ผู้ตรวจสอบภายใน

หัวข้อ	Risk Governance (การกำกับดูแลความเสี่ยง)	Risk Management (การบริหารความเสี่ยง)
กรอบแนวทาง	กำหนดนโยบาย Framework เช่น COSO ERM / ISO 31000	ใช้เครื่องมือ เทคนิค เช่น Risk Register, Heatmap, Internal Control
การมีส่วนร่วมของ Stakeholder	สูงมาก เนื่องจากเกี่ยวข้องกับการตัดสินใจเชิงนโยบาย	ปานกลาง ถึงสูง ขึ้นอยู่กับระดับของความเสี่ยง
ผลลัพธ์ที่คาดหวัง	การมีระบบบริหารความเสี่ยงที่โปร่งใส รับผิดชอบได้ (accountable)	การลดเหตุการณ์ไม่พึงประสงค์ และเพิ่มโอกาสในการบรรลุเป้าหมาย

สรุปองค์ความรู้เรื่อง **"ความเสี่ยงและการควบคุมด้าน IT"** โดยครอบคลุมตั้งแต่การเชื่อมโยงกลยุทธ์ไอทีกับธุรกิจ ไปจนถึงเทคนิคการตรวจสอบสมัยใหม่และกฎหมายที่เกี่ยวข้อง ดังนี้

1. การเชื่อมโยง IT กับธุรกิจ (IT-Business Alignment)

แนวคิดหลัก: IT ต้องสนับสนุนองค์กรใน 3 ระดับ ได้แก่ **ระดับกลยุทธ์ (Strategic Objectives)**, **ระดับกระบวนการทางธุรกิจ (Business Processes)** และ **ระดับปฏิบัติการ (Operational Efficiency)**

ความเสี่ยงหากไม่สอดคล้องกัน: จะทำให้การลงทุนไม่คุ้มค่า ระบบไม่ตอบโจทย์ผู้ใช้ และเกิด **Shadow IT** (การที่พนักงานนำซอฟต์แวร์/Cloud มาใช้เองโดยไม่ผ่านการอนุมัติ) ซึ่งเพิ่มความเสี่ยงด้านความปลอดภัย

การกำกับดูแล: ควรใช้กรอบการทำงานอย่าง **COBIT**, **IT Balanced Scorecard** และมีการตั้งคณะกรรมการ **IT Steering Committee** เพื่อกำกับดูแล

2. โอกาสและความเสี่ยงจากเทคโนโลยี

โอกาส: ช่วยในด้าน **Automation** (ลดความผิดพลาดจากมนุษย์), **Data Analytics** (ช่วยในการตัดสินใจและคาดการณ์) และ **Digital Transformation** (สร้างมูลค่าเพิ่มให้องค์กร)

ความเสี่ยง: ประกอบด้วยภัยคุกคามทางไซเบอร์ (Phishing, Ransomware), ระบบล่ม (System Failure), ปัญหาความถูกต้องของข้อมูล (Data Integrity) และการเข้าถึงโดยไม่ได้รับอนุญาต

การบริหารจัดการ: ต้องสร้างความสมดุลระหว่าง **นวัตกรรม (Innovation)** กับ **การควบคุม (Control)** และระหว่าง **ความเร็ว (Speed)** กับ **ความปลอดภัย (Security)**

3. การบริหารความเสี่ยงด้าน IT (IT Risk Management)

ขั้นตอน: เริ่มจากการค้นหา (Discover), ประเมิน (Assess), รับมือ (Respond) และติดตามผล (Monitor)

เครื่องมือ: ใช้ **Risk Matrix** (Likelihood x Impact) เพื่อจัดลำดับความสำคัญ และใช้ **Risk Register** เพื่อบันทึกความเสี่ยงทั้งหมด รวมถึงกำหนด **KRI (Key Risk Indicator)** เป็นสัญญาณเตือนภัยล่วงหน้า

ประเภทความเสี่ยง: แบ่งเป็น Inherent Risk (ความเสี่ยงก่อนมีมาตรการควบคุม) และ Residual Risk (ความเสี่ยงที่เหลืออยู่หลังควบคุมแล้ว)

4. การควบคุมด้าน IT (IT Controls)

ประเภทหลัก:

- **IT General Controls (ITGC):** การควบคุมระดับโครงสร้างพื้นฐาน เช่น การเข้าถึง (Access Control), การบริหารการเปลี่ยนแปลง (Change Management) และการปฏิบัติงาน (IT Operations)
- **Application Controls:** การควบคุมเฉพาะระบบงาน ครอบคลุมขั้นตอนการนำข้อมูลเข้า (Input), ประมวลผล (Processing) และแสดงผล (Output)

วัตถุประสงค์การควบคุม: แบ่งเป็น **Preventive** (ป้องกัน), **Detective** (ตรวจจับ) และ **Corrective** (แก้ไข)

5. การแบ่งแยกหน้าที่ (Segregation of Duties: SoD)

หลักการ: ไม่มีใครสามารถควบคุมกระบวนการสำคัญได้เพียงคนเดียว เพื่อป้องกันการทุจริตและข้อผิดพลาด

ตัวอย่าง: ผู้พัฒนา (Developer) ต้องไม่ใช่คนเดียวกับผู้ทดสอบ (Tester) หรือผู้ปฏิบัติงาน (Operator)

มาตรการชดเชย: หากแบ่งแยกหน้าที่ไม่ได้สมบูรณ์ ต้องมีการตรวจสอบ Log หรือการกำกับดูแลจากฝ่ายบริหาร (Management Oversight) เข้ามาช่วย

6. การตรวจสอบแบบ IT-Driven Audit

ความเปลี่ยนแปลง: เปลี่ยนจากการตรวจสอบแบบเดิม (สุ่มตรวจเอกสาร) มาเป็นการใช้ข้อมูล 100% ผ่านเครื่องมืออย่าง **Data Analytics**, **CAATs** และการตรวจสอบอย่างต่อเนื่อง (**Continuous Auditing**)

ทักษะที่จำเป็น: ผู้ตรวจสอบต้องมีความรู้ด้านไอที, การวิเคราะห์ข้อมูล, ความตระหนักด้าน Cybersecurity และการเรียนรู้อย่างต่อเนื่อง

7. กฎหมาย IT และการทุจริต (Fraud)

กฎหมายหลัก 4 ฉบับ: PDPA (คุ้มครองข้อมูลส่วนบุคคล), **พ.ร.บ. ไซเบอร์**, **พ.ร.บ. คอมพิวเตอร์** และ **พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์**

ประเด็นสำคัญของ PDPA: การกำหนดนโยบายความเป็นส่วนตัว, การขอความยินยอม และการแจ้งเหตุละเมิดข้อมูลภายใน **72 ชั่วโมง**

ทฤษฎีทุจริต (Fraud Triangle): ประกอบด้วย **แรงกดดัน (Pressure)**, **โอกาส (Opportunity)** และ **การหาข้ออ้าง (Rationalization)** โดย IT มักจะเป็นตัวขยาย "โอกาส" หากขาดการควบคุมที่ดี

◆ **Shadow IT** คือ การที่พนักงานนำซอฟต์แวร์ แอปพลิเคชัน หรือบริการ Cloud ภายนอกมาใช้ในการทำงานโดย**ไม่ได้รับการอนุมัติจากฝ่าย IT** ขององค์กร เช่น การใช้ Google Drive ส่วนตัวส่งข้อมูลลูกค้าแทนระบบที่องค์กรกำหนด

จากการวิเคราะห์ตามแหล่งที่มา ความเสี่ยงของ Shadow IT มีประเด็นสำคัญดังนี้:

- **ความเสี่ยงด้านความปลอดภัย (Security Risk):** เนื่องจากการใช้เครื่องมือภายนอกไม่ได้ผ่านการตรวจสอบหรืออนุมัติจากฝ่าย IT จึงอาจไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอตามมาตรฐานองค์กร
- **การละเมิดนโยบายและกฎหมาย (Non-compliance):** การนำข้อมูลออกไปไว้นอกระบบที่ควบคุมได้ อาจทำให้องค์กร**ละเมิดนโยบายความปลอดภัย**ภายใน และ**ผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA)** หากมีการรั่วไหลของข้อมูลลูกค้า

- **คุณภาพและประสิทธิภาพของข้อมูล (Data Integrity & Efficiency):** เมื่อพนักงานหลีกเลี่ยงไปใช้ระบบอื่น จะส่งผลกระทบโดยตรงต่อ**คุณภาพของข้อมูล**ที่องค์กรจัดเก็บ และทำให้ประสิทธิภาพการทำงานในภาพรวมลดลงเนื่องจากข้อมูลกระจัดกระจาย
- **สัญญาณเตือนความไม่สอดคล้อง (IT-Business Misalignment):** การแพร่หลายของ Shadow IT ในองค์กรถือเป็น**สัญญาณเตือน (Warning Signal)** ว่าระบบไอทีปัจจุบันที่องค์กรจัดหาให้นั้น**ไม่ตอบโจทย์การใช้งานจริง**ของพนักงาน

สรุปได้ว่า Shadow IT ไม่ได้เป็นเพียงปัญหาทางเทคนิค แต่เป็นความเสี่ยงเชิงกลยุทธ์ที่สะท้อนถึงช่องว่างระหว่างความต้องการของธุรกิจกับระบบไอทีที่องค์กรมีอยู่

◆ **ความเสี่ยงด้าน IT ที่สำคัญได้ 4 ประเภทหลัก** ซึ่งเป็นประเด็นที่ผู้ตรวจสอบต้องให้ความสำคัญและจัดการอย่างจริงจัง ดังนี้

1. **Cyber Attack (การโจมตีทางไซเบอร์):** เป็นภัยคุกคามจากภายนอกที่มุ่งเป้าทำลายระบบหรือขโมยข้อมูล เช่น **Phishing, Ransomware และ DDoS** ซึ่งส่งผลกระทบต่อความมั่นคงปลอดภัยและความน่าเชื่อถือขององค์กร
2. **System Failure (ระบบล่มหรือทำงานผิดพลาด):** ความเสี่ยงที่ระบบและโครงสร้างพื้นฐานหยุดชะงักหรือไม่สามารถทำงานได้ตามปกติ ทำให้การดำเนินธุรกิจต้องหยุดชะงักและขาดความต่อเนื่อง
3. **Data Integrity Issue (ปัญหาความถูกต้องครบถ้วนของข้อมูล):** ความเสี่ยงที่ข้อมูลจะสูญหาย ถูกแก้ไข หรือมีความผิดพลาดในกระบวนการประมวลผล ทำให้ข้อมูลที่ได้ขาดความแม่นยำและไม่สามารถนำไปใช้ตัดสินใจได้อย่างถูกต้อง
4. **Unauthorized Access (การเข้าถึงโดยไม่ได้รับอนุญาต):** การที่บุคคลที่ไม่มีสิทธิ์หรือไม่มีอำนาจหน้าที่สามารถเข้าถึงระบบหรือข้อมูลสำคัญขององค์กรได้ ซึ่งอาจนำไปสู่การทุจริตหรือข้อมูลรั่วไหล

หมายเหตุเพิ่มเติม: ในหัวข้อถัดไปของเอกสาร (หัวข้อ 4.1) มีการขยายความเสี่ยงด้าน IT ออกเป็น **5 ประเภท** ตามผลกระทบต่อเป้าหมายองค์กร ได้แก่ **Strategic Risk** (ความเสี่ยงเชิงกลยุทธ์), **Operational Risk** (ความเสี่ยงด้านปฏิบัติการ), **Compliance Risk** (ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย เช่น PDPA), **Cybersecurity Risk** (ความเสี่ยงไซเบอร์) และ **Data Risk** (ความเสี่ยงด้านข้อมูล)

◆ **หลักการ Principle of Least Privilege (PoLP)** หรือการกำหนดสิทธิขั้นต่ำที่จำเป็น เป็นแนวคิดพื้นฐานสำคัญในการบริหารจัดการสิทธิของผู้ใช้งาน ซึ่งมีรายละเอียดดังนี้:

1. **นิยามและความหมาย:** คือการ**กำหนดสิทธิการเข้าถึงข้อมูลและระบบให้เหมาะสม** โดยมอบสิทธิให้แก่ผู้ใช้งาน**เท่าที่จำเป็น**ต่อการปฏิบัติงานตามหน้าที่เท่านั้น เพื่อไม่ให้ผู้ใช้งานมีอำนาจในระบบเกินความจำเป็น
2. **บทบาทในโครงสร้างการควบคุม:** หลักการนี้ถือเป็นส่วนหนึ่งของ **การควบคุมการเข้าถึง (Access Control)** ซึ่งจัดเป็นหนึ่งในเสาหลักของ **การควบคุมทั่วไปด้านไอที (IT General Controls - ITGC)** ที่เป็นรากฐานความปลอดภัยของทั้งองค์กร
3. **ประเภทของการควบคุม:** ถูกจัดอยู่ในกลุ่ม **การควบคุมเชิงป้องกัน (Preventive Control)** ซึ่งเป็นการออกแบบมาเพื่อปิดกั้นหรือป้องกันไม่ให้เกิดข้อผิดพลาด หรือการเข้าถึงข้อมูลโดยมิชอบตั้งแต่เริ่มต้น
4. **ความสำคัญต่อความปลอดภัยขององค์กร:**
    - **ลดโอกาสการเข้าถึงโดยมิชอบ (Unauthorized Access):** ช่วยป้องกันไม่ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้าถึงระบบหรือข้อมูลสำคัญได้

- **ลดโอกาสในการทุจริต (Fraud):** การจำกัดสิทธิช่วยลด "โอกาส" (Opportunity) ซึ่งเป็นหนึ่งในองค์ประกอบของ **Fraud Triangle** โดยป้องกันไม่ให้พนักงานคนใดคนหนึ่งมีสิทธิเหนือกระบวนการสำคัญมากเกินไปจนสามารถกระทำการทุจริตได้โดยไม่มีใครตรวจสอบ
- **สนับสนุนการแบ่งแยกหน้าที่ (Segregation of Duties - SoD):** หลักการ PoLP ช่วยให้การแบ่งแยกหน้าที่เป็นไปอย่างมีประสิทธิภาพ เช่น การแยกสิทธิระหว่างผู้พัฒนา (Developer), ผู้ทดสอบ (Tester) และผู้ปฏิบัติงาน (Operator) ออกจากกันอย่างชัดเจน

5. **จุดที่ผู้ตรวจสอบต้องให้ความสำคัญ:** ผู้ตรวจสอบควรระวังกลุ่มผู้ใช้งานที่มีสิทธิสูง เช่น **Admin Account** หรือ **Privileged User** เพราะหากบุคคลเหล่านี้มีสิทธิกว้างขวางโดยไม่มีการตรวจสอบซ้ำ (Secondary Review) หรือไม่ปฏิบัติตามหลักสิทธิขั้นต่ำ จะถือเป็นจุดที่มีความเสี่ยงสูงสุดต่อองค์กร

สรุปได้ว่า หลักการนี้คือการทำให้มั่นใจว่า **"ไม่มีใครควบคุมหรือเข้าถึงได้ทุกอย่าง"** เพื่อสร้างระบบการตรวจสอบและถ่วงดุลที่มีประสิทธิภาพภายในองค์กร

◆ **แนวทางการป้องกัน Shadow IT** ในหน่วยงานภาครัฐตามที่ระบุในแหล่งข้อมูล มุ่งเน้นไปที่การแก้ปัญหาที่ต้นเหตุและการสร้างระบบกำกับดูแลที่เข้มแข็ง ดังนี้:

1. การสร้างความสอดคล้องระหว่าง IT และภารกิจขององค์กร (IT-Business Alignment)

หัวใจสำคัญของการป้องกัน Shadow IT คือการทำให้ระบบที่หน่วยงานจัดหาให้สามารถ**ตอบโจทย์การใช้งานจริง**ของบุคลากรได้

การออกแบบระบบตามความต้องการ: ต้องพัฒนาหรือจัดหาไอทีที่สนับสนุนกระบวนการทางธุรกิจ (Business Processes) และเพิ่มประสิทธิภาพในการปฏิบัติงาน (Operational Efficiency) อย่างแท้จริง

การพิจารณาร่วมกัน: โครงการไอทีควรได้รับการพิจารณาร่วมกันระหว่างฝ่ายไอทีและฝ่ายที่ต้องใช้งานจริง เพื่อให้มั่นใจว่าระบบจะถูกนำไปใช้งานและไม่ถูกหลีกเลี่ยง

2. การกำกับดูแลและการบริหารจัดการ (IT Governance & Structures)

การมีโครงสร้างการกำกับดูแลที่ชัดเจนจะช่วยลดช่องว่างที่ทำให้เกิดการลักลอบใช้เครื่องมือภายนอก

คณะกรรมการกำกับดูแล (IT Steering Committee): จัดตั้งคณะกรรมการเพื่อดูแลนโยบายไอทีในภาพรวมและตรวจสอบว่าการลงทุนไอทีคุ้มค่าและตอบโจทย์องค์กรหรือไม่

การใช้กรอบมาตรฐานสากล: นำกรอบการทำงานอย่าง **COBIT** มาใช้เป็นแนวทางในการกำกับดูแลและบริหารจัดการไอทีอย่างเป็นระบบ

แผนกลยุทธ์ไอที: ต้องมีแผนกลยุทธ์ไอทีที่เป็นลายลักษณ์อักษรและผ่านการอนุมัติจากผู้บริหารระดับสูง เพื่อให้ทิศทางปฏิบัติเป็นไปในทางเดียวกัน

3. การกำหนดนโยบายและมาตรการควบคุม (Policies & Access Controls)

นโยบายความมั่นคงปลอดภัย: จัดทำนโยบายการรักษาความปลอดภัยด้านสารสนเทศที่ชัดเจน ครอบคลุมถึงแนวปฏิบัติในการใช้ซอฟต์แวร์และบริการ Cloud ภายนอก

การควบคุมการเข้าถึง (Access Control): ใช้หลักการ **Principle of Least Privilege** เพื่อกำหนดสิทธิการเข้าถึงข้อมูลและระบบให้เหมาะสมกับหน้าที่ความรับผิดชอบ

การระบุตัวตนที่เข้มงวด: นำการยืนยันตัวตนหลายปัจจัย (**MFA**) มาใช้เพื่อเพิ่มความปลอดภัยในการเข้าถึงระบบงานของรัฐ

4. บทบาทของผู้ตรวจสอบ (Auditor's Perspective)

ผู้ตรวจสอบภายในมีบทบาทสำคัญในการเป็น "สัญญาณเตือนภัย" เมื่อพบว่ามีการใช้ Shadow IT ในหน่วยงาน

การเฝ้าระวังสัญญาณเตือน: หากพบพนักงานใช้เครื่องมือนอกระบบจำนวนมาก (Shadow IT แพร่หลาย) ให้สันนิษฐานว่าระบบไอทีปัจจุบันอาจไม่ตอบโจทย์การทำงาน

การตรวจสอบ Risk Register: ตรวจสอบรายการความเสี่ยงว่ามีการระบุความเสี่ยงที่เกิดจากการใช้เทคโนโลยีภายนอกที่ไม่อนุมัติไว้หรือไม่ และมีแผนรับมืออย่างไร

การใช้ Data Analytics: ใช้การวิเคราะห์ข้อมูลเพื่อตรวจจับความผิดปกติในการรับ-ส่งข้อมูลไปยังบริการภายนอกที่ไม่ได้กำหนดไว้

5. การปฏิบัติตามกฎหมาย (Compliance)

หน่วยงานต้องตระหนักว่า Shadow IT เพิ่มความเสี่ยงต่อการผิดกฎหมายสำคัญ โดยเฉพาะ **PDPA**

การป้องกันข้อมูลรั่วไหล: การใช้เครื่องมือที่ไม่อนุมัติอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล ซึ่งหากเกิดเหตุต้องแจ้งต่อหน่วยงานกำกับดูแลภายใน **72 ชั่วโมง**

การควบคุมความปลอดภัย: ต้องมั่นใจว่ามาตรการควบคุม (Security Control) ครอบคลุมถึงทุกช่องทางที่มีการประมวลผลข้อมูลส่วนบุคคลของประชาชน

สรุปได้ว่า แนวทางป้องกันที่ดีที่สุดคือการทำให้ไอทีของภาครัฐ**ทำงานได้ง่ายและปลอดภัยพอ**ที่พนักงานไม่จำเป็นต้องแสวงหาเครื่องมือภายนอกมาใช้เอง

◆ **ความแตกต่างระหว่าง Inherent Risk** และ **Residual Risk** ตามที่ระบุในเอกสารประกอบการเรียนมีรายละเอียดดังนี้

- **Inherent Risk (ความเสี่ยงที่มีอยู่แต่เดิม):** หมายถึง **ระดับความเสี่ยงที่ประเมินได้ก่อนที่จะมีการนำมาตรการควบคุมใดๆ เข้ามาใช้**, เป็นความเสี่ยงโดยธรรมชาติของกิจกรรมหรือระบบนั้นๆ หากไม่มีการป้องกันเลย
- **Residual Risk (ความเสี่ยงที่เหลืออยู่):** หมายถึง **ระดับความเสี่ยงที่ยังคงเหลืออยู่หลังจากที่องค์กรได้นำมาตรการควบคุม (Controls) มาใช้จัดการแล้ว**,

ประเด็นสำคัญที่ผู้ตรวจสอบต้องพิจารณา: เป้าหมายของการบริหารความเสี่ยงคือ การใช้มาตรการควบคุมต่างๆ เพื่อลดระดับความเสี่ยงจาก Inherent Risk ลงมาให้เป็น Residual Risk โดยที่องค์กรจะต้องดูแลให้ **Residual Risk อยู่ในระดับที่ยอมรับได้ (Acceptable level)**

ทั้งนี้ ในการประเมินความเสี่ยงทั้งสองรูปแบบ จะใช้สูตรพื้นฐานเดียวกันคือการพิจารณาจาก **โอกาสที่จะเกิด (Likelihood)** คูณกับ **ผลกระทบ (Impact)** แล้วนำผลลัพธ์ที่ได้ไปจัดลำดับความสำคัญบน **Risk Matrix** เพื่อเลือกแนวทางการตอบสนองต่อความเสี่ยงที่เหมาะสมต่อไป

◆ **ความแตกต่างระหว่าง ITGC (IT General Controls)** และ **Application Controls** สรุปได้ดังนี้

1. IT General Controls (ITGC) - การควบคุมทั่วไปด้านไอที

นิยาม: เป็นการควบคุมในระดับ**โครงสร้างพื้นฐาน (Infrastructure)** ของเทคโนโลยีสารสนเทศ

ขอบเขต: มีลักษณะครอบคลุมกว้างขวาง**ทั้งองค์กร** เพื่อสร้างรากฐานความมั่นคงปลอดภัยให้กับทุกระบบงาน

องค์ประกอบหลัก:

- **การควบคุมการเข้าถึง (Access Control):** การกำหนดสิทธิตามหลักการสิทธิขั้นต่ำที่จำเป็น (Principle of Least Privilege)
- **การบริหารจัดการการเปลี่ยนแปลง (Change Management):** การควบคุมการแก้ไขระบบผ่านกระบวนการอนุมัติที่ชัดเจน

- **การปฏิบัติงานด้านไอที (IT Operations):** การดูแลระบบให้มีความเสถียรและพร้อมใช้งานตลอด 24 ชั่วโมง

2. Application Controls - การควบคุมระบบงาน

นิยาม: เป็นการควบคุมที่ออกแบบมา**เฉพาะเจาะจงภายในแอปพลิเคชัน**หรือซอฟต์แวร์นั้นๆ

ขอบเขต: เน้นไปที่การสนับสนุน**กระบวนการทางธุรกิจเฉพาะอย่าง** เพื่อให้มั่นใจในคุณภาพของข้อมูล

วงจรการควบคุม: ครอบคลุมการทำงานของข้อมูลใน 3 ขั้นตอนหลัก คือ

- **การนำข้อมูลเข้า (Input):** ตรวจสอบความถูกต้องตั้งแต่จุดเริ่มต้น
- **การประมวลผล (Processing):** มั่นใจว่าระบบคำนวณและจัดการข้อมูลได้ถูกต้อง
- **การแสดงผล (Output):** ข้อมูลที่ออกมามีความครบถ้วนและแม่นยำ

ตารางสรุปความแตกต่าง

ประเด็นเปรียบเทียบ	IT General Controls (ITGC)	Application Controls
ระดับการควบคุม	ระดับโครงสร้างพื้นฐาน (Infrastructure)	ระดับซอฟต์แวร์/ระบบงาน (Application)
ขอบเขตพื้นที่	ครอบคลุมทั้งองค์กร	เฉพาะเจาะจงรายกระบวนการธุรกิจ
เป้าหมายหลัก	สร้างรากฐานความปลอดภัยโดยรวม	ดูแลความถูกต้องครบถ้วนของข้อมูล
ตัวอย่าง	การตั้งรหัสผ่าน, การอนุมัติแก้โค้ดระบบ	การตรวจสอบยอดรวม, การดักจับข้อมูลผิด

โดยสรุป **ITGC** เปรียบเสมือนการสร้างบ้านให้แข็งแรงและปลอดภัยในภาพรวม ส่วน **Application Controls** เปรียบเสมือนการตรวจสอบความถูกต้องของกิจกรรมหรืองานแต่ละชิ้นที่เกิดขึ้นภายในบ้านหลังนั้น

◆ **กลยุทธ์การตอบสนองต่อความเสี่ยง (Risk Response)** ในการบริหารจัดการไอที ประกอบการเรียนมี 4 รูปแบบหลักที่องค์กรสามารถเลือกใช้ได้ตามความเหมาะสม ดังนี้

1. **Avoid (หลีกเลี่ยง):** เป็นการตัดสินใจ**ยกเลิกหรือปรับเปลี่ยนกิจกรรม**ที่เป็นต้นเหตุซึ่งก่อให้เกิดความเสี่ยงนั้นๆ เพื่อไม่ให้ความเสี่ยงเกิดขึ้นเลย
2. **Reduce (ลดความเสี่ยง):** เป็นการ**ใช้มาตรการควบคุม (Controls)** เข้ามาจัดการเพื่อลดโอกาสที่จะเกิด (Likelihood) หรือลดระดับความรุนแรงของผลกระทบ (Impact) ที่จะเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้
3. **Transfer (โอนย้าย):** เป็นการ**โอนความเสี่ยงไปยังบุคคลที่สาม** เพื่อช่วยรับภาระหากเกิดความเสียหายขึ้น ตัวอย่างที่ชัดเจนคือ **การทำประกันภัยไซเบอร์ (Cyber Insurance)**
4. **Accept (ยอมรับ):** เป็นการที่องค์กร**ยินยอมรับความเสี่ยง**นั้นไว้ มักใช้ในกรณีที่ความเสี่ยงมีระดับต่ำมาก หรือเมื่อพิจารณาแล้วพบว่า**ค่าใช้จ่ายในการจัดการความเสี่ยงนั้นสูงกว่ามูลค่าของผลกระทบ**ที่จะได้รับ

การเลือกใช้กลยุทธ์เหล่านี้ ฝ่ายบริหารจะพิจารณาจากผลการประเมินใน **Risk Matrix** เพื่อตัดสินใจเลือกมาตรการที่ให้ประสิทธิภาพสูงสุดต่อองค์กร

◆ **กลยุทธ์การตอบสนองต่อความเสี่ยง (Risk Response)** ประกอบการเรียน มี 4 รูปแบบหลักที่องค์กรสามารถเลือกใช้เพื่อให้เหมาะสมกับระดับความเสี่ยงและบริบทขององค์กร ดังนี้

1. **Avoid (หลีกเลี่ยง):** เป็นการตัดสินใจ**ยกเลิกหรือปรับเปลี่ยนกิจกรรม**ที่เป็นต้นเหตุสำคัญซึ่งก่อให้เกิดความเสี่ยงนั้น เพื่อป้องกันไม่ให้ความเสี่ยงเกิดขึ้นตั้งแต่แรก
2. **Reduce (ลดความเสี่ยง):** เป็นการ**นำมาตรการควบคุม (Controls) เข้ามาใช้** เพื่อลดโอกาสที่จะเกิด (Likelihood) หรือลดความรุนแรงของผลกระทบ (Impact) ที่อาจเกิดขึ้นให้อยู่ในระดับที่องค์กรยอมรับได้
3. **Transfer (โอนย้าย):** เป็นการ**โอนความเสี่ยงไปยังบุคคลที่สาม**ให้ช่วยรับภาระแทนในกรณีที่เกิดความเสียหายขึ้น ตัวอย่างเช่น **การทำประกันภัยไซเบอร์ (Cyber Insurance)**
4. **Accept (ยอมรับ):** เป็นการที่องค์กร**ยินยอมรับความเสี่ยง**นั้นไว้ มักใช้กับความเสี่ยงที่มีระดับต่ำหรือพิจารณาแล้วว่า**ค่าใช้จ่ายในการจัดการความเสี่ยงนั้นสูงกว่ามูลค่าความเสียหาย**ที่จะได้รับหากเกิดเหตุการณ์จริง

การเลือกใช้กลยุทธ์เหล่านี้จะช่วยให้องค์กรสามารถจัดการความเสี่ยงด้านไอทีได้อย่างเป็นระบบและมีประสิทธิภาพภายใต้ทรัพยากรที่มีอยู่จำกัด

◆ **ตัวอย่างของการควบคุมแบบ Preventive** (เชิงป้องกัน) และ **Detective** (เชิงตรวจจับ) มีรายละเอียดและตัวอย่างที่สำคัญดังนี้

1. การควบคุมเชิงป้องกัน (Preventive Control) เป็นการออกแบบมาเพื่อ **"ป้องกัน"** ไม่ให้เกิดข้อผิดพลาดหรือเหตุการณ์ที่ไม่พึงประสงค์ขึ้นตั้งแต่เริ่มต้น

- **นโยบายความปลอดภัยสารสนเทศ:** กำหนดแนวทางที่ชัดเจนในการใช้งานและปกป้องข้อมูล
- **การแบ่งแยกหน้าที่ (Segregation of Duties - SoD):** ป้องกันไม่ให้บุคคลใดบุคคลหนึ่งมีอำนาจควบคุมกระบวนการสำคัญทั้งหมดเพียงคนเดียว เพื่อลดความเสี่ยงการทุจริต
- **การควบคุมการเข้าถึง (Logical Access Controls):** เช่น การใช้รหัสผ่านที่ซับซ้อน, การยืนยันตัวตนหลายปัจจัย (MFA) และการกำหนดสิทธิเข้าถึงตามหลักสิทธิขั้นต่ำที่จำเป็น (Least Privilege)
- **การอนุมัติรายการ (Approval):** ต้องมีการอนุมัติก่อนดำเนินกิจกรรมสำคัญ เช่น การขอแก้ไขระบบงาน

2. การควบคุมเชิงตรวจจับ (Detective Control) เป็นการออกแบบมาเพื่อ **"ตรวจพบ"** ข้อผิดพลาดหรือเหตุการณ์ที่ผิดปกติหลังจากที่เกิดขึ้นแล้ว

- **ร่องรอยการตรวจสอบ (Audit Trails):** การบันทึกรายละเอียดกิจกรรมต่างๆ ในระบบเพื่อให้สามารถย้อนกลับมาตรวจสอบได้
- **การตรวจสอบ Log (Log Monitoring):** การเฝ้าสังเกตและวิเคราะห์บันทึกการใช้งานระบบ เพื่อค้นหารูปแบบการทำงานที่ผิดปกติ เช่น การพยายามล็อกอินผิดพลาดซ้ำๆ หรือการล็อกอินนอกเวลาทำการ
- **รายงานรายการผิดปกติ (Exception Report):** รายงานที่ระบุถึงธุรกรรมหรือพฤติกรรมที่เบี่ยงเบนไปจากค่ามาตรฐาน เพื่อให้ผู้บริหารหรือผู้ตรวจสอบติดตามได้ทันที
- **การวิเคราะห์ข้อมูล (Data Analytics):** การใช้เทคนิคทางสถิติหรือซอฟต์แวร์เพื่อค้นหารูปแบบการทุจริตที่ซ่อนอยู่ เช่น การตรวจพบการจ่ายเงินซ้ำ (Duplicate Payment) หรือการตรวจสอบตามกฎของ Benford
- **การตรวจนับพัสดุหรือทรัพย์สิน:** เพื่อเปรียบเทียบจำนวนที่มีอยู่จริงกับข้อมูลในระบบ

ข้อสรุปเพิ่มเติม: นอกจากการควบคุมสองแบบข้างต้นแล้ว เอกสารยังกล่าวถึง **Corrective Control** (การควบคุมเชิงแก้ไข) ซึ่งเน้นที่การกู้คืนและแก้ไขความเสียหาย เช่น **การสำรองข้อมูล (Backup and Recovery)** และการแก้ไขข้อผิดพลาดของโปรแกรม (Bug Fixing) เพื่อไม่ให้เกิดปัญหาเดิมซ้ำอีก

◆ **แนวทางการตรวจสอบ Application Controls ในขั้นตอนการนำข้อมูลเข้า (Input)**

"ความเสี่ยงและการควบคุมด้าน IT" เน้นไปที่การสร้างความมั่นใจว่าข้อมูลที่เข้าสู่ระบบมีความถูกต้องครบถ้วน และได้รับอนุญาต โดยมีแนวทางที่สำคัญดังนี้

1. การประเมินประสิทธิผลของการออกแบบ (Design Effectiveness) ผู้ตรวจสอบต้องประเมินว่ามาตรการควบคุมในขั้นตอน Input ถูกออกแบบมาอย่างเหมาะสมเพื่อรับมือกับความเสี่ยงหรือไม่:

- **ความชัดเจนของนโยบาย:** ตรวจสอบว่ามีกระบวนการและขั้นตอนการนำเข้าข้อมูลที่ชัดเจน ครอบคลุม และมีการสื่อสารให้ผู้ปฏิบัติงานทราบหรือไม่
- **ความเหมาะสมของเทคโนโลยี:** พิจารณาว่าเครื่องมือที่ใช้ในการบันทึกข้อมูลมีฟังก์ชันป้องกันข้อผิดพลาดที่ตอบโจทย์ความถูกต้องของข้อมูล (Data Integrity) หรือไม่
- **การแบ่งแยกหน้าที่ (SoD):** ตรวจสอบว่ามีการแยกหน้าที่ระหว่าง **"ผู้บันทึกข้อมูล" (Requester)** และ **"ผู้อนุมัติรายการ" (Approver)** เพื่อป้องกันการนำข้อมูลที่ผิดพลาดหรือการทุจริตเข้าสู่ระบบ

2. การประเมินประสิทธิผลของการดำเนินงาน (Operating Effectiveness) เป็นการตรวจสอบว่าในทางปฏิบัติจริง มาตรการควบคุมขั้นตอน Input ทำงานได้อย่างถูกต้องสม่ำเสมอ:

- **การทดสอบการควบคุม (Test of Control):** สุ่มตรวจสอบตัวอย่างรายการที่ถูกบันทึกเข้าระบบ เพื่อดูว่ารายการเหล่านั้นผ่านการตรวจสอบความถูกต้องและได้รับการอนุมัติจากผู้มีอำนาจตามที่กำหนดไว้หรือไม่
- **การทดสอบแบบ Walkthrough:** ผู้ตรวจสอบควรใช้วิธีการติดตามกระบวนการตั้งแต่จุดเริ่มต้นที่ข้อมูลถูกนำเข้า (Input) ไหลไปสู่การประมวลผล เพื่อยืนยันว่าการทำงานจริงสอดคล้องกับคู่มือหรือขั้นตอนที่บันทึกไว้

3. การใช้เทคนิคการวิเคราะห์ข้อมูล (Data Analytics) ผู้ตรวจสอบสามารถใช้เครื่องมือวิเคราะห์ข้อมูล (Data Analytics) เพื่อตรวจสอบความผิดปกติในขั้นตอน Input ได้ครอบคลุม 100% ของรายการทั้งหมด

- **Duplicate Detection:** ตรวจสอบการบันทึกรายการซ้ำซ้อน เช่น การจ่ายเงินซ้ำ (Duplicate Payment)
- **Gap & Sequence Analysis:** ตรวจสอบความต่อเนื่องของเลขที่เอกสารนำเข้า เพื่อหาว่ามีรายการใดสูญหายหรือถูกข้ามไปหรือไม่
- **Exception Report:** ตรวจสอบรายงานรายการที่ผิดปกติ ซึ่งระบุธุรกรรมที่มีพฤติกรรมเบี่ยงเบนไปจากค่ามาตรฐานที่กำหนดไว้ในขั้นตอนการนำเข้า

4. การตรวจสอบร่องรอยและบันทึกกิจกรรม (Log Monitoring)

- **Authentication Log:** ตรวจสอบบันทึกการเข้าใช้งานเพื่อดูว่าใครเป็นผู้นำข้อมูลเข้าสู่ระบบ มีการเข้าใช้งานนอกเวลาทำการที่ผิดปกติ หรือใช้รหัสผ่านของผู้อื่นหรือไม่
- **Change Log:** ติดตามการแก้ไขข้อมูลสำคัญ เช่น การแก้ไขข้อมูลเงินเดือน หรือข้อมูลลูกค้า ว่าใครเป็นคนทำ และได้รับอนุญาตหรือไม่

การตรวจสอบที่ได้ผลลัพธ์ดีที่สุดคือการรวบรวมหลักฐานทั้งในรูปแบบเอกสาร (Documentary Evidence) และหลักฐานจากการปฏิบัติงานจริง (Operational Evidence) เพื่อยืนยันว่าระบบควบคุมขั้นตอน Input มีความแข็งแกร่งเพียงพอ

◆ **การควบคุมระบบงาน (Application Controls)** ถูกออกแบบมาเพื่อดูแลความถูกต้องของข้อมูลตลอดทั้ง**วงจรข้อมูล** โดยแบ่งออกเป็น 3 ขั้นตอนหลักตามลักษณะการทำงาน ดังนี้:

1. การควบคุมการนำข้อมูลเข้า (Input Control)

- **จุดเน้น:** มุ่งเน้นไปที่ขั้นตอนแรกสุดคือ **"การรับข้อมูลเข้าสู่ระบบ"**
- **วัตถุประสงค์:** เพื่อให้มั่นใจว่าข้อมูลที่ถูกป้อนเข้าสู่ระบบมีความถูกต้อง ครบถ้วน และเป็นรายการที่ได้รับอนุญาตจริง
- **บทบาท:** ทำหน้าที่เป็นด่านแรกในการคัดกรองข้อมูลก่อนจะถูกนำไปประมวลผลต่อ.

2. การควบคุมการประมวลผล (Processing Control)

- **จุดเน้น:** มุ่งเน้นไปที่ขั้นตอนการทำงานภายในของซอฟต์แวร์หรือระบบงาน
- **วัตถุประสงค์:** เพื่อให้มั่นใจว่าระบบมีการ**คำนวณและจัดการข้อมูล**ได้อย่างถูกต้องแม่นยำตามตรรกะ (Logic) หรือเงื่อนไขที่โปรแกรมกำหนดไว้
- **บทบาท:** ดูแลความถูกต้องในระหว่างที่ข้อมูลกำลังถูกเปลี่ยนแปลงหรือจัดกระทำโดยระบบ

3. การควบคุมการแสดงผล (Output Control)

- **จุดเน้น:** มุ่งเน้นไปที่ขั้นตอนสุดท้ายคือ **"ผลลัพธ์หรือรายงาน"** ที่ได้จากระบบ
- **วัตถุประสงค์:** เพื่อให้มั่นใจว่าข้อมูลหรือรายงานที่แสดงผลออกมานั้นมีความ**ถูกต้องและครบถ้วน** ก่อนจะนำไปใช้งานต่อ
- **บทบาท:** ตรวจสอบความแม่นยำของผลผลิตสุดท้ายที่ระบบสร้างขึ้น

สรุปความแตกต่าง: การควบคุมทั้ง 3 ประเภทนี้ทำงานร่วมกันเป็นลำดับขั้น

- **Input** คุมที่ "ต้นทาง" (ข้อมูลดิบ)
- **Processing** คุมที่ "ตัวเครื่องจักร" (กระบวนการคำนวณ)
- **Output** คุมที่ "ปลายทาง" (ผลลัพธ์/รายงาน)

ทั้งหมดนี้มีเป้าหมายร่วมกันคือการรักษาความถูกต้องครบถ้วนของข้อมูล (**Data Integrity**) ตั้งแต่ต้นจนจบกระบวนการ

◆ **การตรวจสอบ Log Monitoring** เพื่อค้นหาการทุจริต เป็นกระบวนการตรวจสอบเชิงตรวจจับ (**Detective Control**) ที่สำคัญอย่างยิ่งในการระบุพฤติกรรมผิดปกติที่อาจนำไปสู่การทุจริตในระบบไอที โดยข้อมูลจากแหล่งข้อมูลได้ให้รายละเอียดแนวทางการตรวจสอบอย่างมีประสิทธิภาพไว้ดังนี้

1. ประเภทของ Log ที่ต้องให้ความสำคัญเป็นพิเศษ

เพื่อให้การตรวจสอบครอบคลุมโอกาสในการทุจริต ผู้ตรวจสอบควรเน้นไปที่ Log 3 กลุ่มหลัก

- **Authentication Log:** ตรวจสอบการล็อกอินเพื่อหาความผิดปกติ เช่น การพยายามล็อกอินผิดพลาดซ้ำๆ หลายครั้ง (ซึ่งอาจเป็นการพยายามเดาสุ่มรหัสผ่าน), การล็อกอินจาก **IP Address ที่ไม่รู้จัก**, หรือการเข้าใช้งาน**นอกเวลาทำการ** (เช่น ช่วงกลางคืนหรือวันหยุด) ซึ่งเป็นหนึ่งในสัญญาณเตือนภัย (Warning Signal) ของการทุจริต
- **Change Log:** ใช้สำหรับติดตามการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญในระบบ โดยต้องระบุได้ว่า **"ใคร เปลี่ยนอะไร เมื่อไหร่ และเปลี่ยนจากค่าเดิมเป็นค่าอะไร"** โดยเฉพาะข้อมูลทางการเงิน ข้อมูลเงินเดือน หรือข้อมูลส่วนบุคคล ซึ่งอาจถูกลักลอบแก้ไขเพื่อผลประโยชน์ส่วนตัว
- **Privileged Access Log:** เป็นจุดที่มีความเสี่ยงสูงสุด จึงต้องเฝ้าระวังการใช้งานของกลุ่ม **Admin หรือ Privileged User** อย่างเข้มงวด เนื่องจากกลุ่มนี้มีสิทธิในการเข้าถึงและจัดการระบบในระดับสูง

หากขาดการตรวจสอบซ้ำ (Secondary Review) อาจทำให้สามารถกระทำการทุจริตและลบหลักฐานทิ้งได้ง่าย

2. เทคนิคการตรวจสอบเพื่อตรวจจับการทุจริต

- **การใช้เป็นมาตรการชดเชย (Compensating Control):** ในกรณีที่องค์กรไม่สามารถแบ่งแยกหน้าที่ (**SoD**) ได้อย่างสมบูรณ์ การหมั่นตรวจสอบ Log (Review Log) จะทำหน้าที่เป็นมาตรการชดเชยเพื่อป้องกันไม่ให้บุคคลเพียงคนเดียวใช้อำนาจเหนือกระบวนการสำคัญไปในทางที่ผิด
- **การวิเคราะห์พฤติกรรมผิดปกติ (Anomaly Detection):** ตรวจสอบธุรกรรมที่มีพฤติกรรมเบี่ยงเบนไปจากมาตรฐาน เช่น การทำรายการด้วยจำนวนเงินเล็กน้อยแต่บ่อยครั้ง (Salami Attack) หรือการทำรายการที่มียอดเงินสูงผิดปกติ
- **Audit Trails:** ต้องมั่นใจว่าระบบมีการบันทึกกิจกรรมทุกอย่างโดยอัตโนมัติ ครบถ้วน และที่สำคัญที่สุดคือ **"ต้องไม่สามารถแก้ไขได้"** เพื่อให้ใช้เป็นหลักฐานในการตรวจสอบย้อนหลังได้เสมอ

3. การบูรณาการร่วมกับ Data Analytics

ในยุคปัจจุบันที่ข้อมูลมีมหาศาล ผู้ตรวจสอบควรใช้เทคนิค **Data Analytics** เข้ามาช่วยในการตรวจสอบ Log:

- **Exception Report:** การตั้งค่าระบบให้สรุปรายงานรายการที่ผิดปกติออกมาโดยเฉพาะ เพื่อให้ผู้ตรวจสอบสามารถมุ่งเป้าไปที่จุดเสี่ยงได้ทันที แทนการไล่ตรวจ Log ทั้งหมด
- **การตรวจสอบแบบ 100%:** การใช้เครื่องมืออย่าง ACL, IDEA หรือ Python ช่วยให้สามารถวิเคราะห์ Log ได้ครบทุกระเบียนข้อมูล (100%) เพื่อหาความสัมพันธ์หรือรูปแบบการทุจริตที่ซับซ้อนซึ่งการสุ่มตรวจแบบเดิมอาจมองข้าม

4. ข้อกำหนดและการเก็บรักษา (Log Retention)

ตามกฎหมายและมาตรฐานสากล องค์กรมีหน้าที่ต้องเก็บรักษา Log ไว้เพื่อการตรวจสอบ

- **พ.ร.บ. คอมพิวเตอร์ฯ:** กำหนดให้ต้องเก็บรักษา Log ไว้ไม่น้อยกว่า **90 วัน**
- **มาตรฐานอื่นๆ:** เช่น ระเบียบธนาคารอาจกำหนดให้เก็บ 5-7 ปี หรือตามมาตรฐาน ISO 27001 แนะนำที่ 1 ปี เพื่อให้เพียงพอต่อการตรวจสอบย้อนหลังหากพบเหตุทุจริตในภายหลัง

◆ **แนวทางการตรวจสอบหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)**

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มุ่งเน้นไปที่การตรวจสอบว่าหน่วยงานปฏิบัติตามกฎหมายและมาตรการรักษาความปลอดภัยที่กำหนดไว้ในฐานะผู้ประมวลผล โดยมีประเด็นสำคัญดังนี้

1. การกำกับดูแลและโครงสร้างหน้าที่ (Governance & Compliance)

- **การกำหนดบทบาทหน้าที่:** ตรวจสอบว่ามีการระบุหน้าที่และความรับผิดชอบระหว่างผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผลข้อมูล (Processor) อย่างชัดเจนเป็นลายลักษณ์อักษรตามข้อกำหนดของกฎหมาย
- **นโยบายความเป็นส่วนตัว (Privacy Policy):** ตรวจสอบว่ามีนโยบายหรือกระบวนการปฏิบัติงานที่สอดคล้องกับวัตถุประสงค์ที่ผู้ควบคุมข้อมูลกำหนด โดยต้องไม่มีการประมวลผลนอกเหนือจากที่ได้รับมอบหมาย

2. มาตรการรักษาความมั่นคงปลอดภัย (Security Controls)

ผู้ประมวลผลมีหน้าที่หลักในการดูแลความปลอดภัยของข้อมูล ซึ่งผู้ตรวจสอบควรประเมินดังนี้

- **การควบคุมการเข้าถึง (Access Control):** ตรวจสอบการกำหนดสิทธิเข้าถึงข้อมูลตามหลักสิทธิขั้นต่ำที่จำเป็น (**Principle of Least Privilege**) และการยืนยันตัวตนหลายปัจจัย (**MFA**)

- **การปกป้องข้อมูล (Data Protection):** ประเมินการใช้เทคโนโลยีเพื่อป้องกันข้อมูล เช่น **การเข้ารหัสข้อมูล (Encryption)** เพื่อลดความเสี่ยงจากการรั่วไหล
- **การทดสอบระบบ:** ตรวจสอบว่ามีการทดสอบและประเมินความมั่นคงปลอดภัยของระบบงานที่ใช้ประมวลผลข้อมูลอย่างสม่ำเสมอ

3. การบันทึกและติดตามร่องรอย (Log Monitoring & Audit Trails)

- **ร่องรอยการตรวจสอบ (Audit Trails):** ต้องมีระบบการบันทึกกิจกรรม (**Log**) ที่เกิดขึ้นกับข้อมูลส่วนบุคคลอย่างครบถ้วนและไม่สามารถแก้ไขได้ เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่า "ใคร ทำอะไร กับข้อมูลใด เมื่อไหร่"
- **การตรวจสอบการเข้าถึง (Authentication Log):** ตรวจติดตามการล็อกอินที่ผิดปกติ เช่น การพยายามเข้าถึงนอกเวลาทำการ หรือจาก IP Address ที่ไม่รู้จัก เพื่อป้องกันการทุจริตหรือการเข้าถึงโดยมิชอบ
- **การเก็บรักษา Log (Log Retention):** ตรวจสอบว่ามีการเก็บรักษา Log ไว้ตามระยะเวลาที่กฎหมายกำหนด (เช่น ขั้นต่ำ 90 วันตาม พ.ร.บ. คอมพิวเตอร์ฯ)

4. การจัดการวงจรชีวิตข้อมูลและการแจ้งเหตุ (Data Management)

- **การจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization):** ตรวจสอบว่ามีการจัดเก็บและประมวลผลข้อมูลเฉพาะที่จำเป็นตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น
- **กระบวนการแจ้งเหตุละเมิด:** ตรวจสอบความพร้อมของกระบวนการแจ้งเหตุเมื่อพบการละเมิดข้อมูลส่วนบุคคล เพื่อให้ผู้ควบคุมข้อมูลสามารถดำเนินการรายงานต่อหน่วยงานกำกับดูแลได้**ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุ

5. การตรวจสอบความสอดคล้องในทางปฏิบัติ (Effectiveness Testing)

- **Design Effectiveness:** ตรวจสอบว่ามาตรการที่วางไว้ถูกออกแบบมาให้รับมือกับความเสี่ยงด้านข้อมูล (Data Risk) ได้จริง
- **Operating Effectiveness:** ใช้วิธีการสุ่มตรวจสอบรายการ (**Test of Control**) หรือการเดินดูหน้างานจริง (**Walkthrough**) เพื่อยืนยันว่ามาตรการเหล่านั้นถูกนำไปปฏิบัติอย่างสม่ำเสมอ

สรุปได้ว่า ผู้ตรวจสอบต้องยืนยันให้ได้ว่าผู้ประมวลผลข้อมูลมี**เกราะป้องกัน (IT Controls)** ที่แข็งแกร่งพอ และมี**ร่องรอยการทำงาน (Audit Trails)** ที่โปร่งใส เพื่อลดความเสี่ยงทั้งด้านปฏิบัติการและด้านกฎหมาย

การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Audit Specialist)
วิชา การกำกับดูแลด้าน IT และ วิชา การตรวจสอบ Information Security

วิทยากร : อาจารย์พัทยา ปานสุวรรณ

◆ **COBIT คืออะไร?**

COBIT (Control Objectives for Information and Related Technologies) คือ กรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance & Management Framework) ซึ่งพัฒนาโดย ISACA (Information Systems Audit and Control Association) ซึ่งเป็นองค์กรระดับสากลด้านการกำกับดูแลระบบสารสนเทศ การตรวจสอบ และความมั่นคงปลอดภัยสารสนเทศ

มีจุดประสงค์หลักเพื่อช่วยให้องค์กรสามารถ:

- สร้างคุณค่า (Value Creation) จากการลงทุนใน IT
- บริหารจัดการและควบคุม IT อย่างมีประสิทธิภาพ
- เชื่อมโยง IT กับเป้าหมายขององค์กร (Enterprise Goals)
- สร้างสมดุลระหว่างความเสี่ยง เทคโนโลยี และคุณค่า
- ลดความเสี่ยงและควบคุม IT ได้อย่างเหมาะสม
- ปฏิบัติสอดคล้องกับกฎหมาย กฎระเบียบ และมาตรฐานต่าง ๆ (เช่น GDPR, PDPA, ITGC)

แนวคิดหลักของ COBIT

COBIT มีหลักคิดสำคัญ 5 ประการ (5 Principles) ได้แก่:

1. Meeting Stakeholder Needs เน้นการสร้างคุณค่าให้กับผู้มีส่วนได้ส่วนเสีย (Stakeholders) โดยพิจารณาความต้องการ ความคาดหวัง และความเสี่ยง
2. Covering the Enterprise End-to-End ขอบเขตครอบคลุมทั้งองค์กร ไม่เฉพาะแค่ IT รวมไปถึงการรวมการกำกับดูแล (Governance) และการบริหารจัดการ (Management)
3. Applying a Single Integrated Framework ผสานมาตรฐานสากลอื่น ๆ เช่น ITIL, ISO/IEC 27001, TOGAF และ PMBOK มาไว้ในกรอบเดียว
4. Enabling a Holistic Approach ใช้ตัวขับเคลื่อนที่เรียกว่า “Enablers” จำนวน 7 ประการ เพื่อให้การดำเนินการสอดคล้องและมีประสิทธิภาพ (ทั้งนโยบาย กระบวนการ ข้อมูล คน และเทคโนโลยี)
5. Separating Governance from Management แยกบทบาทการกำกับดูแล (Governance) ออกจากการบริหารจัดการ (Management) อย่างชัดเจน

◆ **ความแตกต่างระหว่าง General Control** (การควบคุมทั่วไป) และ **Application Control** (การควบคุมระบบงาน) มีรายละเอียดดังนี้

1. General Control (การควบคุมทั่วไป)

- **นิยาม:** เป็นการควบคุมที่นำมาใช้กับ**สภาพแวดล้อมทางด้าน IT โดยรวม** หรือโครงสร้างพื้นฐานด้านไอที (IT Infrastructure) ซึ่งครอบคลุมทั้งส่วนผสมของระบบ เครือข่าย ข้อมูล บุคลากร และกระบวนการต่าง ๆ
- **ขอบเขต:** มีลักษณะครอบคลุมกว้าง ๆ เพื่อให้มั่นใจว่าสภาพแวดล้อมโดยรวมของระบบสารสนเทศมีความปลอดภัยและทำงานได้อย่างถูกต้อง

- **ตัวอย่าง:** นโยบายความปลอดภัย (Security Policy) และการจัดการช่องโหว่ (Vulnerability Management)

2. Application Control (การควบคุมระบบงาน)

- **นิยาม:** เป็นการควบคุมที่เกี่ยวข้องกับ**การทำงานเฉพาะด้านของระบบแอปพลิเคชัน** ที่สนับสนุนกระบวนการทางธุรกิจที่เฉพาะเจาะจง
- **ขอบเขต:** เน้นไปที่กระบวนการทางธุรกิจแต่ละส่วน (Individual Business Processes) เพื่อให้มั่นใจว่าการประมวลผลข้อมูลในระบบงานนั้น ๆ มีความถูกต้อง ครบถ้วน และเชื่อถือได้
- **ตัวอย่าง :**
    - การตรวจสอบความถูกต้องของข้อมูล (Data Edits)
    - การกระทบยอดผลรวมการประมวลผล (Balancing of Processing Totals)
    - การบันทึกรายการ (Transaction Logging) และการรายงานข้อผิดพลาด
    - การเข้ารหัสข้อมูล (Encryption) และการเขียนโปรแกรมอย่างปลอดภัย (Secure Coding)

สรุปความแตกต่างสำคัญ: General Control จะเน้นที่การดูแล **"ภาพรวมและโครงสร้างพื้นฐาน"** ของระบบไอทีในองค์กร ในขณะที่ **Application Control** จะเน้นที่การควบคุม **"ฟังก์ชันการทำงานเฉพาะจุด"** ภายในซอฟต์แวร์หรือระบบงานเพื่อดูแลความถูกต้องของข้อมูลในแต่ละกระบวนการธุรกิจ

◆ ในการกู้คืนระบบหลักสูตร CGIA มีการกำหนดตัวชี้วัดสำคัญสองประการคือ **RPO** และ **RTO** ซึ่งมีความหมายดังนี้

1. Recovery Point Objective (RPO)

- **ความหมาย:** เป็นการกำหนดเป้าหมายโดยอ้างอิงจาก **"ปริมาณข้อมูลที่ยอมรับได้ว่าจะสูญหาย" (Acceptable data loss)**
- **จุดเน้น:** ระบุถึงจุดย้อนหลังในอดีตที่เร็วที่สุดที่องค์กรยอมรับได้ในการกู้คืนข้อมูลกลับมาใช้งาน ตัวอย่างเช่น หากกำหนด RPO ไว้ที่ 4 ชั่วโมง ข้อมูลที่กู้คืนกลับมาจะต้องมีอายุไม่เกิน 4 ชั่วโมงก่อนเกิดเหตุขัดข้อง หากสูญหายมากกว่านั้นจะถือว่าไม่เป็นไปตามเป้าหมาย

2. Recovery Time Objective (RTO)

- **ความหมาย:** เป็นการกำหนดเป้าหมายโดยอ้างอิงจาก **"ระยะเวลาหยุดชะงักของระบบที่ยอมรับได้" (Acceptable downtime)**
- **จุดเน้น:** ระบุถึงระยะเวลาที่เร็วที่สุดที่การดำเนินงานทางธุรกิจจะต้อง **"กลับมาเริ่มต้นใหม่ได้" (Resume)** หลังจากเกิดเหตุการณ์หยุดชะงัก ตัวอย่างเช่น หากกำหนด RTO ไว้ที่ 2 ชั่วโมง ระบบและกระบวนการทางธุรกิจจะต้องกลับมาใช้งานได้ภายใน 2 ชั่วโมงหลังจากที่ระบบล่ม

สรุปความสัมพันธ์

- **RPO** จะมองไปที่ **"ข้อมูลในอดีต"** ว่าหายไปได้มากน้อยแค่ไหนก่อนเกิดเหตุ
- **RTO** จะมองไปที่ **"อนาคต"** ว่าจะใช้เวลานานแค่ไหนหลังจากเกิดเหตุเพื่อให้ระบบกลับมาใช้งานได้ปกติ

การเลือกกลยุทธ์ในการกู้คืน (Recovery Strategies) จะต้องพิจารณาจากความสำคัญของกระบวนการทางธุรกิจ ต้นทุน และระยะเวลาที่ต้องใช้เพื่อให้สอดคล้องกับค่า RPO และ RTO ที่กำหนดไว้

◆ หลักการ **CIA Triad** ถือเป็นเสาหลักสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) ซึ่งประกอบด้วยองค์ประกอบ 3 ประการ ดังนี้

1. ความลับ (Confidentiality) หมายถึง การธำรงไว้ซึ่งข้อมูลให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

- **จุดประสงค์:** เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- **การนำไปใช้:** มีการกำหนดระดับความลับของข้อมูล (Security Levels) เช่น **Top Secret, Secret, Confidential** และ **Unclassified** เพื่อให้ความสำคัญกับการควบคุมที่เหมาะสมกับความเสี่ยง, นอกจากนี้ยังเกี่ยวข้องกับการพิสูจน์ตัวตน (Authentication) เพื่อระบุว่าใครมีสิทธิ์เข้าถึงข้อมูลใด

2. ความถูกต้องครบถ้วน (Integrity) หมายถึง การทำให้มั่นใจว่าข้อมูลมีความถูกต้อง แม่นยำ และไม่ถูกแก้ไขเปลี่ยนแปลงโดยพลการ

- **จุดประสงค์:** ป้องกันการสูญหาย การแก้ไข หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
- **การนำไปใช้:** ในระบบฐานข้อมูลจะมีการใช้ **Integrity Controls** เช่น การกำหนด Primary Key ที่ไม่ซ้ำกันและไม่เป็นค่าว่าง เพื่อรักษาความสัมพันธ์ของข้อมูลให้ถูกต้องครบถ้วนเสมอ, นอกจากนี้ยังรวมถึงการใช้ฟังก์ชัน Hash เพื่อตรวจสอบว่าข้อมูลไม่ถูกแก้ไขระหว่างทาง

3. สภาพพร้อมใช้งาน (Availability) หมายถึง การที่ระบบหรือข้อมูลมีความพร้อมที่จะให้ผู้มีสิทธิ์เรียกใช้งานได้ในเวลาที่ต้องการ

- **จุดประสงค์:** เพื่อให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่องและลดความเสี่ยงจากการหยุดชะงักของระบบ
- **การนำไปใช้:** เกี่ยวข้องโดยตรงกับการวางแผนอุบัติภัยและการกู้คืนระบบ (Business Continuity & Disaster Recovery) โดยมีการกำหนดค่า **RPO** (จุดที่ข้อมูลสูญหายได้) และ **RTO** (ระยะเวลาที่ระบบต้องกลับมาใช้งานได้) รวมถึงการสำรองข้อมูล (Backup) อย่างสม่ำเสมอเพื่อให้ข้อมูลพร้อมกลับมาใช้งานได้ทันที

สรุปความสำคัญ: ผู้ตรวจสอบสารสนเทศจะใช้หลักการ CIA นี้เป็นเกณฑ์ในการประเมินว่า มาตรการควบคุม (Controls) ที่องค์กรติดตั้งไว้นั้น **"เพียงพอ"** ที่จะรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลสำคัญและระบบงานหรือไม่

◆ **กฎหมาย PDPA (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)** มีบทบาทสำคัญอย่างยิ่งต่อการตรวจสอบ ไอทีภาครัฐ โดยทำหน้าที่เป็นกรอบเกณฑ์ทางกฎหมายที่ผู้ตรวจสอบภายในต้องนำมาใช้ประเมินการดำเนินงานของหน่วยงาน สรุปได้ดังนี้

1. เป็นหัวใจหลักของการตรวจสอบการปฏิบัติตามข้อกำหนด (Compliance Audit)

การตรวจสอบไอทีในปัจจุบันต้องรวมเอา PDPA เข้าเป็นส่วนหนึ่งของ **Compliance Audit** เพื่อประเมินว่าหน่วยงานภาครัฐมีการปฏิบัติตามกฎหมายและมาตรฐานต่างๆ อย่างถูกต้องหรือไม่ โดยครอบคลุมทั้ง

- **การควบคุมทั่วไป (General Control):** เช่น นโยบายการรักษาความปลอดภัยข้อมูลของหน่วยงาน
- **การควบคุมระบบงาน (Application Control):** เช่น ระบบการเข้ารหัสข้อมูล (Encryption) ในแอปพลิเคชันที่เก็บข้อมูลประชาชน

2. บทบาทหน้าที่โดยตรงของผู้ตรวจสอบในด้านความเป็นส่วนตัว

หลักสูตร บทบาทหลักของผู้ตรวจสอบในด้านนี้คือการทำให้มั่นใจว่ากฎหมายและระเบียบที่เกี่ยวข้องกับความเป็นส่วนตัวได้ถูกสื่อสารไปยังผู้ที่มีส่วนรับผิดชอบอย่างทั่วถึง นอกจากนี้ยังต้องทำงานร่วมกับที่ปรึกษาทางกฎหมายเพื่อระบุขั้นตอนที่จำเป็นในการปฏิบัติตามข้อกำหนดทั้งหมดของกฎหมาย

3. แนวทางในการตรวจสอบสิทธิและหน้าที่ (Audit Guidelines)

PDPA กำหนดแนวทางให้ผู้ตรวจสอบภาครัฐต้องตรวจสอบประเด็นสำคัญ ดังนี้

- **โครงสร้างการบริหารจัดการ:** ตรวจสอบว่ามีการจัดตั้งโครงสร้างเพื่อดูแลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดหรือไม่
- **บทบาทหน้าที่:** ตรวจสอบว่ามีการกำหนดหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษรที่ชัดเจนหรือไม่
- **กระบวนการและแบบฟอร์ม:** ตรวจสอบความถูกต้องของแบบฟอร์มขอความยินยอม (Consent Form) และกระบวนการขอใช้สิทธิต่างๆ ของเจ้าของข้อมูล
- **การรักษาความมั่นคงปลอดภัย:** ตรวจสอบมาตรการทางเทคนิคเพื่อป้องกันข้อมูลรั่วไหล

4. การตรวจสอบหน้าที่ของผู้ควบคุมข้อมูล (Data Controller)

ผู้ตรวจสอบต้องตรวจสอบว่าหน่วยงานในฐานะผู้ควบคุมข้อมูลทำหน้าที่ได้ครบถ้วนตาม **มาตรา 37** หรือไม่ ซึ่งรวมถึง

- การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- การมีระบบตรวจสอบเพื่อลบหรือทำลายข้อมูลเมื่อหมดความจำเป็น
- **การแจ้งเหตุละเมิด:** ต้องมีกลไกที่สามารถแจ้งเหตุข้อมูลรั่วไหลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ได้ **ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุ

5. เครื่องมือในการกำกับดูแลและสร้างความเชื่อมั่น

สำหรับภาครัฐ PDPA ทำหน้าที่เป็นเครื่องมือสำคัญในการกำกับดูแลการดำเนินงาน ช่วยให้สามารถตรวจสอบการทำงานของหน่วยงานรัฐเองและภาคธุรกิจที่เกี่ยวข้องให้มีความถูกต้องเหมาะสม ซึ่งจะช่วยส่งเสริมภาพลักษณ์ที่ดีของประเทศและสร้างความเชื่อมั่นให้กับประชาชนในการรับบริการจากรัฐว่าข้อมูลของเขาจะถูกจัดการอย่างโปร่งใสและตรวจสอบได้

◆ **เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย** หรือ **CAATs (Computer Assist Audit Techniques)** หลักสูตร CGIA ช่วยเพิ่มประสิทธิภาพการตรวจสอบผ่านโอกาสสำคัญ (Opportunities) และเทคนิคเฉพาะด้านต่างๆ ดังนี้

1. เพิ่มผลิตผลและประหยัดต้นทุน (Productivity and Cost Savings)

- **ประมวลผลข้อมูลจำนวนมาก:** ช่วยให้ผู้ตรวจสอบสามารถ**ประมวลผลข้อมูลปริมาณมหาศาลได้คราวละมากๆ** ตามความต้องการ ซึ่งมีประสิทธิภาพสูงกว่าการตรวจสอบด้วยมือ
- **ประหยัดเวลาในการเขียนโปรแกรม:** การใช้ซอฟต์แวร์ตรวจสอบสำเร็จรูป (**Generalized Audit Software - GAS**) ช่วยให้ผู้ตรวจสอบ**ใช้งานได้ทันทีและประหยัดเวลา** โดยไม่ต้องมีความรู้ลึกซึ้งด้านภาษาโปรแกรมมิ่ง (Programming Language)
- **ความสามารถในการนำกลับมาใช้ซ้ำ:** โปรแกรมการตรวจสอบที่สร้างขึ้นสามารถ**นำกลับมาใช้งานซ้ำได้ในคราวต่อๆ ไป** ช่วยลดค่าใช้จ่ายและเวลาในการเตรียมการระยะยาว

2. เพิ่มประสิทธิภาพในการเข้าถึงและวิเคราะห์ข้อมูล (Efficiency in Data Access)

- **การเข้าถึงข้อมูลที่หลากหลาย (Compatibility):** เครื่องมืออย่าง GAS สามารถเชื่อมต่อและเข้าถึงข้อมูลได้หลายประเภท ทำให้ผู้ตรวจสอบทำงานกับระบบงานที่แตกต่างกันได้สะดวกขึ้น
- **ความสามารถในการวิเคราะห์ขั้นสูง:** ช่วยในการคำนวณค่าทางสถิติ, การจัดกลุ่มเพื่อหาแบบแผน (Classification), การตรวจสอบข้อมูลซ้ำ (Duplicate testing) และการตรวจสอบช่องว่างของข้อมูล (Gap testing) ซึ่งช่วยให้พบความผิดปกติที่การตรวจสอบทั่วไปอาจมองข้าม

3. การบริหารความเสี่ยงและการตรวจสอบที่ครอบคลุม (Audit Risk Management)

- **ตรวจสอบได้ครบ 100%:** แทนที่จะสุ่มตรวจเพียงบางส่วน ผู้ตรวจสอบสามารถใช้เครื่องมือ **Data Mining** เพื่อ**ค้นหาจากทุกระเบียนข้อมูล (Every record)** เพื่อระบุรายการที่อาจมีการทุจริตได้อย่างแม่นยำ
- **การจำลองสถานการณ์จริง:** เทคนิค **Parallel Simulation** ช่วยให้ผู้ตรวจสอบสร้างโปรแกรมเลียนแบบการทำงานของระบบจริง เพื่อเปรียบเทียบผลลัพธ์ได้อย่าง**เป็นอิสระจากกระบวนการผลิตปกติ (Production Run)**

4. การตรวจสอบและระบุปัญหาอย่างต่อเนื่องและรวดเร็ว

- **การตรวจสอบอย่างต่อเนื่อง (Continuous Monitoring):** เทคนิคอย่าง **SCARF** (System Control Audit Review File) ช่วยในการติดตามรายการที่เกิดขึ้นและสุ่มตรวจรายการที่ผิดเงื่อนไขได้ตลอดเวลา
- **ระบุปัญหาได้ทันที:** เทคนิคอย่าง **Snapshot** ช่วยให้พบปัญหาและแก้ไขได้อย่างรวดเร็ว โดยการแทรกคำสั่งตรวจสอบไว้ในจุดต่างๆ ของโปรแกรมเพื่อดูการไหลของข้อมูล
- **ทดสอบภายใต้สภาวะจริง:** การใช้ **Integrated Test Facility (ITF)** ทำให้ผู้ตรวจสอบสามารถทดสอบระบบภายใต้สภาวะการทำงานจริงร่วมกับรายการปกติ ทำให้ทราบผลการตรวจสอบและประเมินระบบได้ทันที

สรุปได้ว่า CAATs เป็นเครื่องมือสำคัญที่ตอบโจทย์ความกดดันในปัจจุบันที่หน่วยงานตรวจสอบต้อง **"ทำงานให้ได้มากขึ้นด้วยทรัพยากรที่น้อยลง" (Do more with less)** โดยการนำเทคโนโลยีมาช่วยยกระดับคุณภาพและความทั่วถึงในการตรวจสอบ

◆ **การเลือกใช้เครื่องมือสำหรับทำ Data Analytics ของผู้ตรวจสอบ หลักสูตร CGIA** สามารถแบ่งออกเป็นกลุ่มตามลักษณะการใช้งานและความซับซ้อนของข้อมูลได้ดังนี้

1. เครื่องมือพื้นฐาน (Basic Desktop) เป็นเครื่องมือที่ผู้ตรวจสอบส่วนใหญ่คุ้นเคยและใช้งานได้ในระดับเริ่มต้น

- **Microsoft Excel:** ใช้สำหรับการวิเคราะห์ข้อมูลเบื้องต้น
- **Microsoft Access:** ใช้สำหรับการจัดการฐานข้อมูลในระดับสำนักงาน

2. ซอฟต์แวร์สำหรับการตรวจสอบโดยเฉพาะ (Specialized Auditing Software) เป็นเครื่องมือที่มีฟังก์ชันออกแบบมาเพื่องานตรวจสอบ (GAS) ช่วยให้ประมวลผลข้อมูลได้คราวละมาก ๆ และมีชุดคำสั่งพื้นฐาน เช่น การคำนวณค่าเสื่อมราคาหรือการจัดชั้นลูกหนี้

- **ACL**
- **IDEA**
- **Arbutus**
- **SAS**

3. เครื่องมือวิเคราะห์ข้อมูลและสร้างภาพข้อมูล (Specialized DA Visualization) เน้นการดึงข้อมูลมาวิเคราะห์และนำเสนอในรูปแบบภาพ (Dashboard) เพื่อให้เห็นแนวโน้มหรือความผิดปกติได้ชัดเจน

- **Tableau**
- **Power BI**
- **Qlik**

4. เครื่องมือวิเคราะห์ข้อมูลขั้นสูง (Advance Data Analytic Tools) เหมาะสำหรับงานวิเคราะห์ที่มีความซับซ้อนสูง เช่น การทำ Data Science หรือ AI

Python: ภาษาที่ได้รับความนิยมสูง มี Library รองรับการทำ Data Science, Machine Learning และ AI ได้เป็นอย่างดี

R: เน้นการวิเคราะห์ทางสถิติและประมวลผลข้อมูลขนาดใหญ่ (Big Data)

RapidMiner: โปรแกรมที่ช่วยในการออกแบบ Workflow เพื่อวิเคราะห์ข้อมูล

5. เครื่องมือสืบค้นข้อมูลในระบบงาน (Integrated Query & Report Writers)

Query Tools: ใช้ดึงข้อมูลจากระบบหลักขององค์กรโดยตรง เช่น **SAP, Oracle, PeopleSoft**

Report Writers: ใช้ในการสร้างรายงานจากฐานข้อมูล เช่น **Cognos, Business Objects**

นอกจากนี้ ผู้ตรวจสอบควรมีความรู้ใน **ภาษา SQL** ซึ่งเป็นภาษามาตรฐานในการจัดการและเรียกดูข้อมูลจากระบบฐานข้อมูลเชิงสัมพันธ์ เพื่อให้สามารถเข้าถึงข้อมูลจากแหล่งที่แตกต่างกันได้อย่างอิสระ

◆ **เทคนิค Parallel Simulation** (การประมวลผลคู่ขนาน) เป็นหนึ่งในเทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (**CAATs**) ที่มีความสำคัญในการตรวจสอบความถูกต้องของระบบงาน โดยมีรายละเอียดเพิ่มเติม ดังนี้

- **แนวคิดหลัก:** เป็นการที่ผู้ตรวจสอบ**สร้างโปรแกรมขึ้นมาเพื่อเลียนแบบการทำงาน (Simulate) ของระบบงานจริง (Production Run)** เพื่อทดสอบว่าระบบที่องค์กรใช้งานอยู่นั้นประมวลผลได้ถูกต้องตามเงื่อนไขที่ควรจะเป็นหรือไม่
- **การใช้ข้อมูลจริง:** เทคนิคนี้จะใช้**ข้อมูลที่ผ่านขั้นตอนการปฏิบัติงานจริงมาแล้ว**มาเข้าสู่โปรแกรมจำลองที่ผู้ตรวจสอบสร้างขึ้น เพื่อเปรียบเทียบผลลัพธ์
- **ความเป็นอิสระในการตรวจสอบ:** การตรวจสอบด้วยวิธีนี้สามารถทำได้**โดยอิสระจากกระบวนการผลิตปกติ (Production Run)** และผู้ตรวจสอบสามารถเลือกระดับความละเอียดในการตรวจได้ว่าจะตรวจสอบเพียงบางขั้นตอนหรือครอบคลุมทุกขั้นตอนของระบบงาน
- **ความยืดหยุ่นด้านเวลา:** ผู้ตรวจสอบสามารถพัฒนาระบบตรวจสอบจำลองนี้ขึ้นมาภายหลังจากที่หน่วยงานได้นำระบบงานจริงลงใช้งานแล้วก็ได้
- **เงื่อนไขสำคัญสำหรับผู้ตรวจสอบ**
    - ผู้ตรวจสอบจำเป็นต้อง**มีความเข้าใจในตัวระบบงาน (Application)** นั้น ๆ ดีเพียงพอที่จะเขียนโปรแกรมเลียนแบบเงื่อนไขการประมวลผลได้อย่างถูกต้อง
    - เมื่อได้ข้อมูลจากการประมวลผลของทั้งโปรแกรมจำลองและโปรแกรมจริงแล้ว จะนำผลลัพธ์ทั้งสองมา**เปรียบเทียบความแตกต่างโดยใช้คอมพิวเตอร์**เพื่อระบุจุดผิดปกติ

สรุปได้ว่าเทคนิคนี้ช่วยให้ผู้ตรวจสอบสามารถยืนยันความถูกต้องของตรรกะการประมวลผลในระบบงานจริงได้อย่างมั่นใจ โดยใช้ข้อมูลจริงมาทดสอบในสภาพแวดล้อมที่ควบคุมโดยผู้ตรวจสอบเอง

◆ **เทคนิค Test Data (ข้อมูลทดสอบ)** เป็นวิธีการตรวจสอบความถูกต้องของการทำงานในระบบคอมพิวเตอร์ โดยผู้ตรวจสอบจะจัดเตรียมชุดข้อมูลและคำนวณผลลัพธ์ที่ถูกต้องไว้ล่วงหน้า จากนั้นจึงนำไปประมวลผลด้วยโปรแกรมระบบงานจริงเพื่อเปรียบเทียบผลลัพธ์

สถานการณ์ที่ควรเลือกใช้เทคนิค Test Data มีตัวอย่างดังนี้

1. **การตรวจสอบตรรกะการประมวลผลที่ซับซ้อน:** เมื่อต้องการยืนยันว่าโปรแกรมคำนวณค่าต่างๆ ได้ถูกต้องตามเงื่อนไขทางธุรกิจหรือไม่ เช่น การคำนวณเงินเดือนที่มีเงื่อนไขภาษีและสวัสดิการที่หลากหลาย หรือการจัดชั้นลูกหนี้ตามอายุหนี้ ซึ่งการใช้ Test Data จะช่วยให้สังเกตเห็นข้อบกพร่องในตรรกะของโปรแกรมได้ง่ายกว่าการไปไล่ตรวจจากข้อมูลจริงจำนวนมาก

2. **การทดสอบภายหลังการแก้ไขปรับปรุงระบบ (Regression Testing):** ในกรณีที่ระบบงานมีการแก้ไขโค้ดโปรแกรมหรือเพิ่มฟังก์ชันใหม่ ผู้ตรวจสอบสามารถนำชุดข้อมูลทดสอบชุดเดิมที่เคยใช้มาประมวลผลซ้ำ เพื่อมั่นใจว่าการแก้ไขนั้นไม่กระทบกับส่วนงานเดิมที่เคยทำงานได้ถูกต้องอยู่แล้ว

3. **การตรวจสอบมาตรการควบคุมการนำเข้าข้อมูล (Input Controls):** ใช้เพื่อทดสอบว่าระบบมี "Edit checks" ที่มีประสิทธิภาพหรือไม่ เช่น

- **Limit checks:** ลองป้อนจำนวนเงินที่ติดลบหรือสูงเกินกว่าเพดานที่กำหนดเพื่อดูว่าระบบตัดรายการหรือไม่
- **Check digits:** ลองป้อนเลขที่บัญชีที่ผิดหลักตรวจสอบเพื่อดูว่าระบบตรวจพบความผิดปกติหรือไม่
- **Range tests:** ทดสอบการป้อนข้อมูลที่อยู่นอกช่วงวันที่หรือค่าที่ยอมรับได้

4. **การยืนยันความถูกต้องของระบบงานใหม่ (System Implementation):** ในขั้นตอนการตรวจรับระบบก่อนใช้งานจริง (UAT) ผู้ตรวจสอบสามารถใช้ Test Data เพื่อยืนยันว่าระบบใหม่ทำงานได้ตรงตามความต้องการ (User Requirements) และเงื่อนไขที่ออกแบบไว้

5. **การตรวจสอบความถูกต้องครบถ้วนของฐานข้อมูล (Database Integrity):** ใช้ทดสอบว่าระบบมีการควบคุม Primary Key ไม่ให้ซ้ำกันหรือเป็นค่าว่าง (Null) ตามหลักการ Integrity Controls หรือไม่

ข้อควรระวังสำคัญ: ผู้ตรวจสอบต้องมั่นใจว่าโปรแกรมที่นำมาทดสอบนั้นเป็น **"ตัวเดียวกับที่ใช้ในการปฏิบัติงานจริง"** และต้องระมัดระวังไม่ให้ข้อมูลทดสอบเข้าไปปนเปื้อนหรือทำให้ข้อมูลจริงในระบบเสียหาย

◆ **เทคนิค Integrated Test Facility (ITF)** และ **Test Data** เป็นเทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (CAATs) ที่มีความคล้ายคลึงกันตรงที่ใช้ชุดข้อมูลทดสอบเพื่อตรวจสอบความถูกต้องของระบบงาน แต่มีข้อแตกต่างที่สำคัญในด้านสภาวะแวดล้อมและวิธีการจัดการ ดังนี้

1. สภาวะแวดล้อมในการทดสอบ

Test Data (ข้อมูลทดสอบ): เป็นการนำชุดข้อมูลที่เตรียมไว้ล่วงหน้ามาประมวลผลด้วยโปรแกรมระบบงานจริง เพื่อดูว่าผลลัพธ์ที่ได้ตรงกับที่คาดการณ์ไว้หรือไม่ โดยทั่วไปมักจะทำแยกส่วนจากกระบวนการปฏิบัติงานจริง

ITF (การทดสอบในระบบงานจริง): เป็นการตรวจสอบที่ทำไป **"พร้อม ๆ กับการปฏิบัติงานจริง" (Production Run)** ข้อมูลทดสอบจะไหลเข้าสู่ระบบไปพร้อมกับรายการปกติของหน่วยงาน

2. การแยกข้อมูลและหน่วยรับตรวจ

Test Data: ผู้ตรวจสอบใช้ข้อมูลที่จำลองขึ้นมาเพื่อทดสอบตรรกะของโปรแกรม

ITF: ใช้สิ่งที่เรียกว่า **"Dummy Entity"** (หน่วยจำลองหรือรหัสสมมติ) เข้าช่วย ข้อมูลของ ITF จะถูกบันทึกเข้าระบบจริงแต่จะถูกแยกออกจากรายงานการควบคุม (Control Report) ในงานประจำ เพื่อไม่ให้ไปปะปนกับรายการปกติขององค์กร

3. ระยะเวลาและความสม่ำเสมอ

Test Data: มักทำเป็นครั้งคราว เช่น เมื่อมีการแก้ไขโปรแกรมหรือต้องการยืนยันความถูกต้องเฉพาะจุด

ITF: สามารถ**ตรวจสอบได้อย่างสม่ำเสมอ**และต่อเนื่องโดยไม่มีกำหนดการล่วงหน้า เหมาะสำหรับระบบงานที่มีการแก้ไขเพิ่มเติมบ่อยๆ

4. การกำจัดข้อมูลหลังการตรวจสอบ

Test Data: เนื่องจากมักทำในสภาพแวดล้อมทดสอบ จึงไม่มีประเด็นเรื่องข้อมูลตกค้างในบัญชีจริง

ITF: มีความยุ่งยากกว่า เพราะรายการทดสอบที่ส่งเข้าไปพร้อมระบบงานจริง**ต้องถูกนำออกจากบัญชี** โดยการลงรายการปรับปรุงด้วยมือหรือใช้โปรแกรมช่วย หากขจัดข้อมูล (ITF Data) ออกไม่หมดจะเสี่ยงต่อความผิดพลาดของข้อมูลในระบบบัญชีจริง

5. ต้นทุนและประสิทธิภาพ

Test Data: ผู้ตรวจสอบต้องเสียเวลามากในการจัดเตรียมข้อมูลและคำนวณผลลัพธ์ที่คาดหวัง

ITF: มี**ต้นทุนในการประมวลผลต่ำ**เพราะข้อมูลถูกประมวลผลไปพร้อมกับรายการปกติ แต่จะมีต้นทุนสูงหากต้องแก้ไขโปรแกรมเพื่อขจัดผลรายการทดสอบออกไป

สรุปสั้นๆ: Test Data คือการเอาข้อมูลปลอมไปใส่โปรแกรมจริงเพื่อดูผลลัพธ์ (มักทำแยกส่วน) ในขณะที่ **ITF** คือการสร้าง "ลูกค้าปลอม" ไว้ในระบบจริง แล้วส่งรายการเข้าไปประมวลผลร่วมกับลูกค้าคนอื่นๆ เพื่อทดสอบระบบภายใต้สภาวะการทำงานจริง

◆ **แนวทางการตรวจสอบหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีรายละเอียดที่ผู้ตรวจสอบต้องประเมินและพิจารณาดังนี้

1. โครงสร้างและการบริหารจัดการ (Management Structure)

ผู้ตรวจสอบควรดำเนินการตรวจสอบการจัดทำ**โครงสร้างการบริหารจัดการ**ให้เป็นไปตามกฎหมาย ซึ่งรวมถึง

- **การกำหนดบทบาทและหน้าที่:** ต้องมีการระบุหน้าที่ความรับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร
- **การแต่งตั้งตัวแทน:** ในกรณีที่มีความจำเป็นต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทนนั้นต้องอยู่ในราชอาณาจักรและได้รับการมอบอำนาจเป็นหนังสือ
- **การจัดทำนโยบาย:** ตรวจสอบว่ามีการจัดทำนโยบายที่จำเป็น เช่น **นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)** และนโยบายการรักษาความมั่นคงปลอดภัย

2. มาตรการรักษาความมั่นคงปลอดภัย (Security Measures)

ผู้ควบคุมข้อมูลมีหน้าที่จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** โดยผู้ตรวจสอบต้องพิจารณาองค์ประกอบ 3 ด้าน (CIA Triad) ดังนี้

- **ความลับ (Confidentiality):** ป้องกันการเข้าถึงข้อมูลโดยมิชอบ
- **ความถูกต้องครบถ้วน (Integrity):** ป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ
- **สภาพพร้อมใช้งาน (Availability):** เพื่อให้สามารถเรียกใช้งานข้อมูลได้เมื่อต้องการ
- **การป้องกันเมื่อต้องให้ข้อมูลแก่ผู้อื่น:** หากมีการส่งข้อมูลให้บุคคลอื่นหรือผู้ประมวลผลข้อมูล ต้องมีมาตรการป้องกันการใช้ข้อมูลโดยมิชอบ

3. กระบวนการและแบบฟอร์ม (Processes and Forms)

ผู้ตรวจสอบต้องประเมินความถูกต้องของกระบวนการต่าง ๆ ได้แก่

- **การขอความยินยอม (Consent):** ตรวจสอบแบบฟอร์มขอความยินยอม (Consent Form) และกระบวนการจัดการความยินยอม (Consent Management Procedure) ให้เป็นไปตามเงื่อนไขทางกฎหมาย เช่น การใช้ภาษาที่อ่านง่ายและเข้าถึงได้ง่าย
- **การแจ้งรายละเอียด (Notification):** ตรวจสอบว่ามีการแจ้งวัตถุประสงค์ ระยะเวลาการเก็บรักษาและรายละเอียดการติดต่อให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูล
- **สิทธิของเจ้าของข้อมูล:** ตรวจสอบแบบฟอร์มและกระบวนการขอใช้สิทธิต่าง ๆ (Data Subject Request Form/Procedure) เช่น สิทธิการเข้าถึงข้อมูล หรือสิทธิการขอให้ลบข้อมูล

4. การจัดการวงจรชีวิตข้อมูล (Data Lifecycle Management)

- **การตรวจสอบการลบหรือทำลาย:** ตรวจสอบว่าหน่วยงานมีระบบการตรวจสอบเพื่อดำเนินการ**ลบหรือทำลายข้อมูล** เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อข้อมูลนั้นเกินความจำเป็น
- **การจัดการข้อมูลเอกสารและสารสนเทศ:** ตรวจสอบการบริหารจัดการข้อมูลทั้งในรูปแบบสิ่งพิมพ์และระบบเทคโนโลยีสารสนเทศ

5. การจัดการเมื่อเกิดเหตุละเมิด (Data Breach Management)

ผู้ตรวจสอบต้องยืนยันว่าหน่วยงานมีกลไกในการ**แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล**ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

- ต้องแจ้งโดยไม่ชักช้า**ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุเท่าที่จะทำได้
- ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล ต้องแจ้งเหตุให้เจ้าของข้อมูลทราบพร้อม**แนวทางการเยียวยา**ด้วย

6. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross Border Transfer)

ตรวจสอบว่ามีการกำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ สำหรับการส่งหรือโอนข้อมูลไปยังต่างประเทศ ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

ความแตกต่างระหว่าง Risk Governance กับ Risk Management

หัวข้อ	Risk Governance (การกำกับดูแลความเสี่ยง)	Risk Management (การบริหารความเสี่ยง)
นิยาม	กระบวนการกำหนดทิศทาง นโยบาย โครงสร้าง และการกำกับติดตามการบริหารความเสี่ยง	กระบวนการระบุ ประเมิน ตอบสนอง และติดตามความเสี่ยง
เป้าหมาย	เพื่อให้มั่นใจว่าองค์กรมีระบบการจัดการความเสี่ยงที่เหมาะสม และสอดคล้องกับเป้าหมายและนโยบาย	เพื่อลดผลกระทบและความน่าจะเป็นของความเสี่ยงต่อการดำเนินงาน
ผู้รับผิดชอบหลัก	คณะกรรมการ ผู้บริหารระดับสูง เช่น นายก อบจ. หรือ ปลัด อบจ.	เจ้าหน้าที่ หน่วยงานภายใน ผู้ตรวจสอบภายใน
กรอบแนวทาง	กำหนดนโยบาย Framework เช่น COSO ERM / ISO 31000	ใช้เครื่องมือ เทคนิค เช่น Risk Register, Heatmap, Internal Control
การมีส่วนร่วมของ Stakeholder	สูงมาก เนื่องจากเกี่ยวข้องกับการตัดสินใจเชิงนโยบาย	ปานกลาง ถึงสูง ขึ้นอยู่กับระดับของความเสี่ยง
ผลลัพธ์ที่คาดหวัง	การมีระบบบริหารความเสี่ยงที่โปร่งใส รับผิดชอบได้ (accountable)	การลดเหตุการณ์ไม่พึงประสงค์ และเพิ่มโอกาสในการบรรลุเป้าหมาย

การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Audit Specialist)
วิชา ความเสี่ยงและการควบคุมด้าน IT

วิทยากร : อาจารย์พัทยา ปานสุวรรณ

สรุปองค์ความรู้เรื่อง **"ความเสี่ยงและการควบคุมด้าน IT"** โดยครอบคลุมตั้งแต่การเชื่อมโยงกลยุทธ์ไอทีกับธุรกิจ ไปจนถึงเทคนิคการตรวจสอบสมัยใหม่และกฎหมายที่เกี่ยวข้อง ดังนี้

1. การเชื่อมโยง IT กับธุรกิจ (IT-Business Alignment)

แนวคิดหลัก: IT ต้องสนับสนุนองค์กรใน 3 ระดับ ได้แก่ **ระดับกลยุทธ์ (Strategic Objectives)**, **ระดับกระบวนการทางธุรกิจ (Business Processes)** และ**ระดับปฏิบัติการ (Operational Efficiency)**

ความเสี่ยงหากไม่สอดคล้องกัน: จะทำให้การลงทุนไม่คุ้มค่า ระบบไม่ตอบโจทย์ผู้ใช้ และเกิด **Shadow IT** (การที่พนักงานนำซอฟต์แวร์/Cloud มาใช้เองโดยไม่ผ่านการอนุมัติ) ซึ่งเพิ่มความเสี่ยงด้านความปลอดภัย

การกำกับดูแล: ควรใช้กรอบการทำงานอย่าง **COBIT**, **IT Balanced Scorecard** และมีการตั้งคณะกรรมการ **IT Steering Committee** เพื่อกำกับดูแล

2. โอกาสและความเสี่ยงจากเทคโนโลยี

โอกาส: ช่วยในด้าน **Automation** (ลดความผิดพลาดจากมนุษย์), **Data Analytics** (ช่วยในการตัดสินใจและคาดการณ์) และ **Digital Transformation** (สร้างมูลค่าเพิ่มให้องค์กร)

ความเสี่ยง: ประกอบด้วยภัยคุกคามทางไซเบอร์ (Phishing, Ransomware), ระบบล่ม (System Failure), ปัญหาความถูกต้องของข้อมูล (Data Integrity) และการเข้าถึงโดยไม่ได้รับอนุญาต

การบริหารจัดการ: ต้องสร้างความสมดุลระหว่าง **นวัตกรรม (Innovation)** กับ **การควบคุม (Control)** และระหว่าง **ความเร็ว (Speed)** กับ **ความปลอดภัย (Security)**

3. การบริหารความเสี่ยงด้าน IT (IT Risk Management)

ขั้นตอน: เริ่มจากการค้นหา (Discover), ประเมิน (Assess), รับมือ (Respond) และติดตามผล (Monitor)

เครื่องมือ: ใช้ **Risk Matrix** (Likelihood x Impact) เพื่อจัดลำดับความสำคัญ และใช้ **Risk Register** เพื่อบันทึกความเสี่ยงทั้งหมด รวมถึงกำหนด **KRI (Key Risk Indicator)** เป็นสัญญาณเตือนภัยล่วงหน้า

ประเภทความเสี่ยง: แบ่งเป็น Inherent Risk (ความเสี่ยงก่อนมีมาตรการควบคุม) และ Residual Risk (ความเสี่ยงที่เหลืออยู่หลังควบคุมแล้ว)

4. การควบคุมด้าน IT (IT Controls)

ประเภทหลัก:

- **IT General Controls (ITGC):** การควบคุมระดับโครงสร้างพื้นฐาน เช่น การเข้าถึง (Access Control), การบริหารการเปลี่ยนแปลง (Change Management) และการปฏิบัติงาน (IT Operations)
- **Application Controls:** การควบคุมเฉพาะระบบงาน ครอบคลุมขั้นตอนการนำข้อมูลเข้า (Input), ประมวลผล (Processing) และแสดงผล (Output)

วัตถุประสงค์การควบคุม: แบ่งเป็น **Preventive** (ป้องกัน), **Detective** (ตรวจจับ) และ **Corrective** (แก้ไข)

5. การแบ่งแยกหน้าที่ (Segregation of Duties: SoD)

หลักการ: ไม่มีใครสามารถควบคุมกระบวนการสำคัญได้เพียงคนเดียว เพื่อป้องกันการทุจริตและข้อผิดพลาด

ตัวอย่าง: ผู้พัฒนา (Developer) ต้องไม่ใช่คนเดียวกับผู้ทดสอบ (Tester) หรือผู้ปฏิบัติงาน (Operator)

มาตรการชดเชย: หากแบ่งแยกหน้าที่ไม่ได้สมบูรณ์ ต้องมีการตรวจสอบ Log หรือการกำกับดูแลจากฝ่ายบริหาร (Management Oversight) เข้ามาช่วย

6. การตรวจสอบแบบ IT-Driven Audit

ความเปลี่ยนแปลง: เปลี่ยนจากการตรวจสอบแบบเดิม (สุ่มตรวจเอกสาร) มาเป็นการใช้ข้อมูล 100% ผ่านเครื่องมืออย่าง **Data Analytics**, **CAATs** และการตรวจสอบอย่างต่อเนื่อง (**Continuous Auditing**)

ทักษะที่จำเป็น: ผู้ตรวจสอบต้องมีความรู้ด้านไอที, การวิเคราะห์ข้อมูล, ความตระหนักด้าน Cybersecurity และการเรียนรู้อย่างต่อเนื่อง

7. กฎหมาย IT และการทุจริต (Fraud)

กฎหมายหลัก 4 ฉบับ: PDPA (คุ้มครองข้อมูลส่วนบุคคล), **พ.ร.บ. ไซเบอร์**, **พ.ร.บ. คอมพิวเตอร์** และ **พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์**

ประเด็นสำคัญของ PDPA: การกำหนดนโยบายความเป็นส่วนตัว, การขอความยินยอม และการแจ้งเหตุละเมิดข้อมูลภายใน **72 ชั่วโมง**

ทฤษฎีทุจริต (Fraud Triangle): ประกอบด้วย **แรงกดดัน (Pressure)**, **โอกาส (Opportunity)** และ **การหาข้ออ้าง (Rationalization)** โดย IT มักจะเป็นตัวขยาย "โอกาส" หากขาดการควบคุมที่ดี

◆ **Shadow IT** คือ การที่พนักงานนำซอฟต์แวร์ แอปพลิเคชัน หรือบริการ Cloud ภายนอกมาใช้ในการทำงานโดย**ไม่ได้รับการอนุมัติจากฝ่าย IT** ขององค์กร เช่น การใช้ Google Drive ส่วนตัวส่งข้อมูลลูกค้าแทนระบบที่องค์กรกำหนด

จากการวิเคราะห์ตามแหล่งที่มา ความเสี่ยงของ Shadow IT มีประเด็นสำคัญดังนี้

- **ความเสี่ยงด้านความปลอดภัย (Security Risk):** เนื่องจากการใช้เครื่องมือภายนอกไม่ได้ผ่านการตรวจสอบหรืออนุมัติจากฝ่าย IT จึงอาจไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอตามมาตรฐานองค์กร
- **การละเมิดนโยบายและกฎหมาย (Non-compliance):** การนำข้อมูลออกไปไว้นอกระบบที่ควบคุมได้ อาจทำให้องค์กร**ละเมิดนโยบายความปลอดภัย**ภายใน และ**ผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA)** หากมีการรั่วไหลของข้อมูลลูกค้า
- **คุณภาพและประสิทธิภาพของข้อมูล (Data Integrity & Efficiency):** เมื่อพนักงานหลีกเลี่ยงไปใช้ระบบอื่น จะส่งผลกระทบโดยตรงต่อ**คุณภาพของข้อมูล**ที่องค์กรจัดเก็บ และทำให้ประสิทธิภาพการทำงานในภาพรวมลดลงเนื่องจากข้อมูลกระจัดกระจาย
- **สัญญาณเตือนความไม่สอดคล้อง (IT-Business Misalignment):** การแพร่หลายของ Shadow IT ในองค์กรถือเป็น**สัญญาณเตือน (Warning Signal)** ว่าระบบไอทีปัจจุบันที่องค์กรจัดหาให้นั้น**ไม่ตอบโจทย์การใช้งานจริง**ของพนักงาน

สรุปได้ว่า Shadow IT ไม่ได้เป็นเพียงปัญหาทางเทคนิค แต่เป็นความเสี่ยงเชิงกลยุทธ์ที่สะท้อนถึงช่องว่างระหว่างความต้องการของธุรกิจกับระบบไอทีที่องค์กรมีอยู่

◆ **ความเสี่ยงด้าน IT ที่สำคัญได้ 4 ประเภทหลัก** ซึ่งเป็นประเด็นที่ผู้ตรวจสอบต้องให้ความสำคัญและจัดการอย่างจริงจัง ดังนี้

1. **Cyber Attack (การโจมตีทางไซเบอร์):** เป็นภัยคุกคามจากภายนอกที่มุ่งเป้าทำลายระบบหรือขโมยข้อมูล เช่น **Phishing, Ransomware และ DDoS** ซึ่งส่งผลกระทบต่อความมั่นคงปลอดภัยและความน่าเชื่อถือขององค์กร
2. **System Failure (ระบบล่มหรือทำงานผิดพลาด):** ความเสี่ยงที่ระบบและโครงสร้างพื้นฐานหยุดชะงักหรือไม่สามารถทำงานได้ตามปกติ ทำให้การดำเนินธุรกิจต้องหยุดชะงักและขาดความต่อเนื่อง
3. **Data Integrity Issue (ปัญหาความถูกต้องครบถ้วนของข้อมูล):** ความเสี่ยงที่ข้อมูลจะสูญหาย ถูกแก้ไข หรือมีความผิดพลาดในกระบวนการประมวลผล ทำให้ข้อมูลที่ได้ขาดความแม่นยำและไม่สามารถนำไปใช้ตัดสินใจได้อย่างถูกต้อง
4. **Unauthorized Access (การเข้าถึงโดยไม่ได้รับอนุญาต):** การที่บุคคลที่ไม่มีสิทธิ์หรือไม่มีอำนาจหน้าที่สามารถเข้าถึงระบบหรือข้อมูลสำคัญขององค์กรได้ ซึ่งอาจนำไปสู่การทุจริตหรือข้อมูลรั่วไหล

หมายเหตุเพิ่มเติม : ในหัวข้อถัดไปของเอกสาร (หัวข้อ 4.1) มีการขยายความเสี่ยงด้าน IT ออกเป็น **5 ประเภท** ตามผลกระทบต่อเป้าหมายองค์กร ได้แก่ **Strategic Risk** (ความเสี่ยงเชิงกลยุทธ์), **Operational Risk** (ความเสี่ยงด้านปฏิบัติการ), **Compliance Risk** (ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย เช่น PDPA), **Cybersecurity Risk** (ความเสี่ยงไซเบอร์) และ **Data Risk** (ความเสี่ยงด้านข้อมูล)

◆ **หลักการ Principle of Least Privilege (PoLP)** หรือการกำหนดสิทธิขั้นต่ำที่จำเป็น เป็นแนวคิดพื้นฐานสำคัญในการบริหารจัดการสิทธิของผู้ใช้งาน ซึ่งมีรายละเอียดดังนี้

1. **นิยามและความหมาย:** คือการ**กำหนดสิทธิการเข้าถึงข้อมูลและระบบให้เหมาะสม** โดยมอบสิทธิให้แก่ผู้ใช้งาน**เท่าที่จำเป็น**ต่อการปฏิบัติงานตามหน้าที่เท่านั้น เพื่อไม่ให้ผู้ใช้งานมีอำนาจในระบบเกินความจำเป็น
2. **บทบาทในโครงสร้างการควบคุม:** หลักการนี้ถือเป็นส่วนหนึ่งของ **การควบคุมการเข้าถึง (Access Control)** ซึ่งจัดเป็นหนึ่งในเสาหลักของ **การควบคุมทั่วไปด้านไอที (IT General Controls - ITGC)** ที่เป็นรากฐานความปลอดภัยของทั้งองค์กร
3. **ประเภทของการควบคุม:** ถูกจัดอยู่ในกลุ่ม **การควบคุมเชิงป้องกัน (Preventive Control)** ซึ่งเป็นการออกแบบมาเพื่อปิดกั้นหรือป้องกันไม่ให้เกิดข้อผิดพลาด หรือการเข้าถึงข้อมูลโดยมิชอบตั้งแต่เริ่มต้น
4. **ความสำคัญต่อความปลอดภัยขององค์กร:**
    - **ลดโอกาสการเข้าถึงโดยมิชอบ (Unauthorized Access):** ช่วยป้องกันไม่ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้าถึงระบบหรือข้อมูลสำคัญได้
    - **ลดโอกาสในการทุจริต (Fraud):** การจำกัดสิทธิช่วยลด "โอกาส" (Opportunity) ซึ่งเป็นหนึ่งในองค์ประกอบของ **Fraud Triangle** โดยป้องกันไม่ให้พนักงานคนใดคนหนึ่งมีสิทธิเหนือกระบวนการสำคัญมากเกินไปจนสามารถกระทำการทุจริตได้โดยไม่มีใครตรวจสอบ
    - **สนับสนุนการแบ่งแยกหน้าที่ (Segregation of Duties - SoD):** หลักการ PoLP ช่วยให้การแบ่งแยกหน้าที่เป็นไปอย่างมีประสิทธิภาพ เช่น การแยกสิทธิระหว่างผู้พัฒนา (Developer), ผู้ทดสอบ (Tester) และผู้ปฏิบัติงาน (Operator) ออกจากกันอย่างชัดเจน

5. **จุดที่ผู้ตรวจสอบต้องให้ความสำคัญ:** ผู้ตรวจสอบควรระวังกลุ่มผู้ใช้งานที่มีสิทธิสูง เช่น **Admin Account** หรือ **Privileged User** เพราะหากบุคคลเหล่านี้มีสิทธิกว้างขวางโดยไม่มีการตรวจสอบซ้ำ (Secondary Review) หรือไม่ปฏิบัติตามหลักสิทธิขั้นต่ำ จะถือเป็นจุดที่มีความเสี่ยงสูงสุดต่อองค์กร

สรุปได้ว่า หลักการนี้คือการทำให้มั่นใจว่า **"ไม่มีใครควบคุมหรือเข้าถึงได้ทุกอย่าง"** เพื่อสร้างระบบการตรวจสอบและถ่วงดุลที่มีประสิทธิภาพภายในองค์กร

◆ **แนวทางการป้องกัน Shadow IT** ในหน่วยงานภาครัฐตามที่ระบุในแหล่งข้อมูล มุ่งเน้นไปที่การแก้ปัญหาที่ต้นเหตุและการสร้างระบบกำกับดูแลที่เข้มแข็ง ดังนี้

1. การสร้างความสอดคล้องระหว่าง IT และภารกิจขององค์กร (IT-Business Alignment)

หัวใจสำคัญของการป้องกัน Shadow IT คือการทำให้ระบบที่หน่วยงานจัดหาให้สามารถ**ตอบโจทย์การใช้งานจริง**ของบุคลากรได้

การออกแบบระบบตามความต้องการ: ต้องพัฒนาหรือจัดหาไอทีที่สนับสนุนกระบวนการทางธุรกิจ (Business Processes) และเพิ่มประสิทธิภาพในการปฏิบัติงาน (Operational Efficiency) อย่างแท้จริง

การพิจารณาร่วมกัน: โครงการไอทีควรได้รับการพิจารณาร่วมกันระหว่างฝ่ายไอทีและฝ่ายที่ต้องใช้งานจริง เพื่อให้มั่นใจว่าระบบจะถูกนำไปใช้งานและไม่ถูกหลีกเลี่ยง

2. การกำกับดูแลและการบริหารจัดการ (IT Governance & Structures)

การมีโครงสร้างการกำกับดูแลที่ชัดเจนจะช่วยลดช่องว่างที่ทำให้เกิดการลักลอบใช้เครื่องมือภายนอก

คณะกรรมการกำกับดูแล (IT Steering Committee): จัดตั้งคณะกรรมการเพื่อดูแลนโยบายไอทีในภาพรวมและตรวจสอบว่าการลงทุนไอทีคุ้มค่าและตอบโจทย์องค์กรหรือไม่

การใช้กรอบมาตรฐานสากล: นำกรอบการทำงานอย่าง **COBIT** มาใช้เป็นแนวทางในการกำกับดูแลและบริหารจัดการไอทีอย่างเป็นระบบ

แผนกลยุทธ์ไอที: ต้องมีแผนกลยุทธ์ไอทีที่เป็นลายลักษณ์อักษรและผ่านการอนุมัติจากผู้บริหารระดับสูง เพื่อให้ทิศทางปฏิบัติเป็นไปในทางเดียวกัน

3. การกำหนดนโยบายและมาตรการควบคุม (Policies & Access Controls)

นโยบายความมั่นคงปลอดภัย: จัดทำนโยบายการรักษาความปลอดภัยด้านสารสนเทศที่ชัดเจน ครอบคลุมถึงแนวปฏิบัติในการใช้ซอฟต์แวร์และบริการ Cloud ภายนอก

การควบคุมการเข้าถึง (Access Control): ใช้หลักการ **Principle of Least Privilege** เพื่อกำหนดสิทธิการเข้าถึงข้อมูลและระบบให้เหมาะสมกับหน้าที่ความรับผิดชอบ

การระบุตัวตนที่เข้มงวด: นำการยืนยันตัวตนหลายปัจจัย (**MFA**) มาใช้เพื่อเพิ่มความปลอดภัยในการเข้าถึงระบบงานของรัฐ

4. บทบาทของผู้ตรวจสอบ (Auditor's Perspective) ผู้ตรวจสอบภายในมีบทบาทสำคัญในการเป็น "สัญญาณเตือนภัย" เมื่อพบว่ามีการใช้ Shadow IT ในหน่วยงาน

การเฝ้าระวังสัญญาณเตือน: หากพบพนักงานใช้เครื่องมือนอกระบบจำนวนมาก (Shadow IT แพร่หลาย) ให้สันนิษฐานว่าระบบไอทีปัจจุบันอาจไม่ตอบโจทย์การทำงาน

การตรวจสอบ Risk Register: ตรวจสอบรายการความเสี่ยงว่ามีการระบุความเสี่ยงที่เกิดจากการใช้เทคโนโลยีภายนอกที่ไม่อนุมัติไว้หรือไม่ และมีแผนรับมืออย่างไร

การใช้ Data Analytics: ใช้การวิเคราะห์ข้อมูลเพื่อตรวจจับความผิดปกติในการรับ-ส่งข้อมูลไปยังบริการภายนอกที่ไม่ได้กำหนดไว้

5. การปฏิบัติตามกฎหมาย (Compliance) หน่วยงานต้องตระหนักว่า Shadow IT เพิ่มความเสี่ยงต่อการผิดกฎหมายสำคัญ โดยเฉพาะ **PDPA**

การป้องกันข้อมูลรั่วไหล: การใช้เครื่องมือที่ไม่อนุมัติอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล ซึ่งหากเกิดเหตุต้องแจ้งต่อหน่วยงานกำกับดูแลภายใน **72 ชั่วโมง**

การควบคุมความปลอดภัย: ต้องมั่นใจว่ามาตรการควบคุม (Security Control) ครอบคลุมถึงทุกช่องทางที่มีการประมวลผลข้อมูลส่วนบุคคลของประชาชน

สรุปได้ว่า แนวทางป้องกันที่ดีที่สุดคือการทำให้ไอทีของภาครัฐ**ทำงานได้ง่ายและปลอดภัยพอ**ที่พนักงานไม่จำเป็นต้องแสวงหาเครื่องมือภายนอกมาใช้เอง

◆ **ความแตกต่างระหว่าง Inherent Risk** และ **Residual Risk** ตามที่ระบุในเอกสารประกอบการเรียนมีรายละเอียดดังนี้

- **Inherent Risk (ความเสี่ยงที่มีอยู่แต่เดิม):** หมายถึง **ระดับความเสี่ยงที่ประเมินได้ก่อนที่จะมีการนำมาตรการควบคุมใดๆ เข้ามาใช้**, เป็นความเสี่ยงโดยธรรมชาติของกิจกรรมหรือระบบนั้นๆ หากไม่มีการป้องกันเลย
- **Residual Risk (ความเสี่ยงที่เหลืออยู่):** หมายถึง **ระดับความเสี่ยงที่ยังคงเหลืออยู่หลังจากที่องค์กรได้นำมาตรการควบคุม (Controls) มาใช้จัดการแล้ว**,

ประเด็นสำคัญที่ผู้ตรวจสอบต้องพิจารณา: เป้าหมายของการบริหารความเสี่ยงคือ การใช้มาตรการควบคุมต่างๆ เพื่อลดระดับความเสี่ยงจาก Inherent Risk ลงมาให้เป็น Residual Risk โดยที่องค์กรจะต้องดูแลให้ **Residual Risk อยู่ในระดับที่ยอมรับได้ (Acceptable level)**

ทั้งนี้ ในการประเมินความเสี่ยงทั้งสองรูปแบบ จะใช้สูตรพื้นฐานเดียวกันคือการพิจารณาจาก **โอกาสที่จะเกิด (Likelihood)** คูณกับ **ผลกระทบ (Impact)** แล้วนำผลลัพธ์ที่ได้ไปจัดลำดับความสำคัญบน **Risk Matrix** เพื่อเลือกแนวทางการตอบสนองต่อความเสี่ยงที่เหมาะสมต่อไป

◆ **ความแตกต่างระหว่าง ITGC (IT General Controls)** และ **Application Controls** สรุปได้ดังนี้

1. IT General Controls (ITGC) - การควบคุมทั่วไปด้านไอที

นิยาม: เป็นการควบคุมในระดับ**โครงสร้างพื้นฐาน (Infrastructure)** ของเทคโนโลยีสารสนเทศ

ขอบเขต: มีลักษณะครอบคลุมกว้างขวาง**ทั้งองค์กร** เพื่อสร้างรากฐานความมั่นคงปลอดภัยให้กับทุกระบบงาน

องค์ประกอบหลัก:

- **การควบคุมการเข้าถึง (Access Control):** การกำหนดสิทธิตามหลักการสิทธิขั้นต่ำที่จำเป็น (Principle of Least Privilege)
- **การบริหารจัดการการเปลี่ยนแปลง (Change Management):** การควบคุมการแก้ไขระบบผ่านกระบวนการอนุมัติที่ชัดเจน
- **การปฏิบัติงานด้านไอที (IT Operations):** การดูแลระบบให้มีความเสถียรและพร้อมใช้งานตลอด 24 ชั่วโมง

2. Application Controls - การควบคุมระบบงาน

นิยาม: เป็นการควบคุมที่ออกแบบมา**เฉพาะเจาะจงภายในแอปพลิเคชัน**หรือซอฟต์แวร์นั้นๆ

ขอบเขต: เน้นไปที่การสนับสนุน**กระบวนการทางธุรกิจเฉพาะอย่าง** เพื่อให้มั่นใจในคุณภาพของข้อมูล

วงจรการควบคุม: ครอบคลุมการทำงานของข้อมูลใน 3 ขั้นตอนหลัก คือ

- **การนำข้อมูลเข้า (Input):** ตรวจสอบความถูกต้องตั้งแต่จุดเริ่มต้น
- **การประมวลผล (Processing):** มั่นใจว่าระบบคำนวณและจัดการข้อมูลได้ถูกต้อง
- **การแสดงผล (Output):** ข้อมูลที่ออกมามีความครบถ้วนและแม่นยำ

ตารางสรุปความแตกต่าง

ประเด็นเปรียบเทียบ	IT General Controls (ITGC)	Application Controls
ระดับการควบคุม	ระดับโครงสร้างพื้นฐาน (Infrastructure)	ระดับซอฟต์แวร์/ระบบงาน (Application)
ขอบเขตพื้นที่	ครอบคลุมทั้งองค์กร	เฉพาะเจาะจงรายกระบวนการธุรกิจ
เป้าหมายหลัก	สร้างรากฐานความปลอดภัยโดยรวม	ดูแลความถูกต้องครบถ้วนของข้อมูล
ตัวอย่าง	การตั้งรหัสผ่าน, การอนุมัติแก้โค้ดระบบ	การตรวจสอบยอดรวม, การดักจับข้อมูลผิด

โดยสรุป **ITGC** เปรียบเสมือนการสร้างบ้านให้แข็งแรงและปลอดภัยในภาพรวม ส่วน **Application Controls** เปรียบเสมือนการตรวจสอบความถูกต้องของกิจกรรมหรืองานแต่ละชิ้นที่เกิดขึ้นภายในบ้านหลังนั้น

◆ **กลยุทธ์การตอบสนองต่อความเสี่ยง (Risk Response)** ในการบริหารจัดการไอที ประกอบการเรียน มี 4 รูปแบบหลักที่องค์กรสามารถเลือกใช้ได้ตามความเหมาะสม ดังนี้

1. **Avoid (หลีกเลี่ยง):** เป็นการตัดสินใจ**ยกเลิกหรือปรับเปลี่ยนกิจกรรม**ที่เป็นต้นเหตุซึ่งก่อให้เกิดความเสี่ยงนั้นๆ เพื่อไม่ให้ความเสี่ยงเกิดขึ้นเลย

2. **Reduce (ลดความเสี่ยง):** เป็นการ**ใช้มาตรการควบคุม (Controls)** เข้ามาจัดการเพื่อลดโอกาสที่จะเกิด (Likelihood) หรือลดระดับความรุนแรงของผลกระทบ (Impact) ที่จะเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้

3. **Transfer (โอนย้าย):** เป็นการ**โอนความเสี่ยงไปยังบุคคลที่สาม** เพื่อช่วยรับภาระหากเกิดความเสียหายขึ้น ตัวอย่างที่ชัดเจนคือ **การทำประกันภัยไซเบอร์ (Cyber Insurance)**

4. **Accept (ยอมรับ):** เป็นการที่องค์กร**ยินยอมรับความเสี่ยง**นั้นไว้ มักใช้ในกรณีที่ความเสี่ยงมีระดับต่ำมาก หรือเมื่อพิจารณาแล้วพบว่า**ค่าใช้จ่ายในการจัดการความเสี่ยงนั้นสูงกว่ามูลค่าของผลกระทบ**ที่จะได้รับ

การเลือกใช้กลยุทธ์เหล่านี้ ฝ่ายบริหารจะพิจารณาจากผลการประเมินใน **Risk Matrix** เพื่อตัดสินใจเลือกมาตรการที่ให้ประสิทธิภาพสูงสุดต่อองค์กร

◆ **กลยุทธ์การตอบสนองต่อความเสี่ยง (Risk Response)** ประกอบการเรียน มี 4 รูปแบบหลักที่องค์กรสามารถเลือกใช้เพื่อให้เหมาะสมกับระดับความเสี่ยงและบริบทขององค์กร ดังนี้

1. **Avoid (หลีกเลี่ยง):** เป็นการตัดสินใจ**ยกเลิกหรือปรับเปลี่ยนกิจกรรม**ที่เป็นต้นเหตุสำคัญซึ่งก่อให้เกิดความเสี่ยงนั้น เพื่อป้องกันไม่ให้ความเสี่ยงเกิดขึ้นตั้งแต่แรก

2. **Reduce (ลดความเสี่ยง):** เป็นการ**นำมาตรการควบคุม (Controls) เข้ามาใช้** เพื่อลดโอกาสที่จะเกิด (Likelihood) หรือลดความรุนแรงของผลกระทบ (Impact) ที่อาจเกิดขึ้นให้อยู่ในระดับที่องค์กรยอมรับได้

3.**Transfer (โอนย้าย):** เป็นการ**โอนความเสี่ยงไปยังบุคคลที่สาม**ให้ช่วยรับภาระแทนในกรณีที่เกิดความเสียหายขึ้น ตัวอย่างเช่น **การทำประกันภัยไซเบอร์ (Cyber Insurance)**

4. **Accept (ยอมรับ):** เป็นการที่องค์กร**ยินยอมรับความเสี่ยง**นั้นไว้ มักใช้กับความเสี่ยงที่มีระดับต่ำหรือพิจารณาแล้วว่า**ค่าใช้จ่ายในการจัดการความเสี่ยงนั้นสูงกว่ามูลค่าความเสียหาย**ที่จะได้รับหากเกิดเหตุการณ์จริง

การเลือกใช้กลยุทธ์เหล่านี้จะช่วยให้องค์กรสามารถจัดการความเสี่ยงด้านไอทีได้อย่างเป็นระบบและมีประสิทธิภาพภายใต้ทรัพยากรที่มีอยู่จำกัด

◆ **ตัวอย่างของการควบคุมแบบ Preventive** (เชิงป้องกัน) และ **Detective** (เชิงตรวจจับ) มีรายละเอียดและตัวอย่างที่สำคัญดังนี้

1. การควบคุมเชิงป้องกัน (Preventive Control) เป็นการออกแบบมาเพื่อ **"ป้องกัน"** ไม่ให้เกิดข้อผิดพลาดหรือเหตุการณ์ที่ไม่พึงประสงค์ขึ้นตั้งแต่เริ่มต้น

- **นโยบายความปลอดภัยสารสนเทศ:** กำหนดแนวทางที่ชัดเจนในการใช้งานและปกป้องข้อมูล
- **การแบ่งแยกหน้าที่ (Segregation of Duties - SoD):** ป้องกันไม่ให้บุคคลใดบุคคลหนึ่งมีอำนาจควบคุมกระบวนการสำคัญทั้งหมดเพียงคนเดียว เพื่อลดความเสี่ยงการทุจริต
- **การควบคุมการเข้าถึง (Logical Access Controls):** เช่น การใช้รหัสผ่านที่ซับซ้อน, การยืนยันตัวตนหลายปัจจัย (MFA) และการกำหนดสิทธิเข้าถึงตามหลักสิทธิขั้นต่ำที่จำเป็น (Least Privilege)
- **การอนุมัติรายการ (Approval):** ต้องมีการอนุมัติก่อนดำเนินกิจกรรมสำคัญ เช่น การขอแก้ไขระบบงาน

2. การควบคุมเชิงตรวจจับ (Detective Control) เป็นการออกแบบมาเพื่อ **"ตรวจพบ"** ข้อผิดพลาดหรือเหตุการณ์ที่ผิดปกติหลังจากที่เกิดขึ้นแล้ว

- **ร่องรอยการตรวจสอบ (Audit Trails):** การบันทึกรายละเอียดกิจกรรมต่างๆ ในระบบเพื่อให้สามารถย้อนกลับมาตรวจสอบได้
- **การตรวจสอบ Log (Log Monitoring):** การเฝ้าสังเกตและวิเคราะห์บันทึกการใช้งานระบบเพื่อค้นหารูปแบบการทำงานที่ผิดปกติ เช่น การพยายามล็อกอินผิดพลาดซ้ำๆ หรือการล็อกอินนอกเวลาทำการ
- **รายงานรายการผิดปกติ (Exception Report):** รายงานที่ระบุถึงธุรกรรมหรือพฤติกรรมที่เบี่ยงเบนไปจากค่ามาตรฐาน เพื่อให้ผู้บริหารหรือผู้ตรวจสอบติดตามได้ทันที
- **การวิเคราะห์ข้อมูล (Data Analytics):** การใช้เทคนิคทางสถิติหรือซอฟต์แวร์เพื่อค้นหารูปแบบการทุจริตที่ซ่อนอยู่ เช่น การตรวจพบการจ่ายเงินซ้ำ (Duplicate Payment) หรือการตรวจสอบตามกฎของ Benford
- **การตรวจนับพัสดุหรือทรัพย์สิน:** เพื่อเปรียบเทียบจำนวนที่มีอยู่จริงกับข้อมูลในระบบ

ข้อสรุปเพิ่มเติม : นอกจากการควบคุมสองแบบข้างต้นแล้ว เอกสารยังกล่าวถึง **Corrective Control** (การควบคุมเชิงแก้ไข) ซึ่งเน้นที่การกู้คืนและแก้ไขความเสียหาย เช่น **การสำรองข้อมูล (Backup and Recovery)** และการแก้ไขข้อผิดพลาดของโปรแกรม (Bug Fixing) เพื่อไม่ให้เกิดปัญหาเดิมซ้ำอีก

◆ **แนวทางการตรวจสอบ Application Controls ในขั้นตอนการนำข้อมูลเข้า (Input)**

"ความเสี่ยงและการควบคุมด้าน IT" เน้นไปที่การสร้างความมั่นใจว่าข้อมูลที่เข้าสู่ระบบมีความถูกต้องครบถ้วน และได้รับอนุญาต โดยมีแนวทางที่สำคัญดังนี้

1. การประเมินประสิทธิผลของการออกแบบ (Design Effectiveness) ผู้ตรวจสอบต้องประเมินว่ามาตรการควบคุมในขั้นตอน Input ถูกออกแบบมาอย่างเหมาะสมเพื่อรับมือกับความเสี่ยงหรือไม่

- **ความชัดเจนของนโยบาย:** ตรวจสอบว่ามีกระบวนการและขั้นตอนการนำเข้าข้อมูลที่ชัดเจน ครอบคลุม และมีการสื่อสารให้ผู้ปฏิบัติงานทราบหรือไม่
- **ความเหมาะสมของเทคโนโลยี:** พิจารณาว่าเครื่องมือที่ใช้ในการบันทึกข้อมูลมีฟังก์ชันป้องกันข้อผิดพลาดที่ตอบโจทย์ความถูกต้องของข้อมูล (Data Integrity) หรือไม่
- **การแบ่งแยกหน้าที่ (SoD):** ตรวจสอบว่ามีการแยกหน้าที่ระหว่าง **"ผู้บันทึกข้อมูล" (Requester)** และ **"ผู้อนุมัติรายการ" (Approver)** เพื่อป้องกันการนำข้อมูลที่ผิดพลาดหรือการทุจริตเข้าสู่ระบบ

2. การประเมินประสิทธิผลของการดำเนินงาน (Operating Effectiveness) เป็นการตรวจสอบว่าในทางปฏิบัติจริง มาตรการควบคุมขั้นตอน Input ทำงานได้อย่างถูกต้องสม่ำเสมอ:

- **การทดสอบการควบคุม (Test of Control):** สุ่มตรวจสอบตัวอย่างรายการที่ถูกบันทึกเข้าระบบ เพื่อดูว่ารายการเหล่านั้นผ่านการตรวจสอบความถูกต้องและได้รับการอนุมัติจากผู้มีอำนาจตามที่กำหนดไว้หรือไม่
- **การทดสอบแบบ Walkthrough:** ผู้ตรวจสอบควรใช้วิธีการติดตามกระบวนการตั้งแต่จุดเริ่มต้นที่ข้อมูลถูกนำเข้า (Input) ไหลไปสู่การประมวลผล เพื่อยืนยันว่าการทำงานจริงสอดคล้องกับคู่มือหรือขั้นตอนที่บันทึกไว้

3. การใช้เทคนิคการวิเคราะห์ข้อมูล (Data Analytics) ผู้ตรวจสอบสามารถใช้เครื่องมือวิเคราะห์ข้อมูล (Data Analytics) เพื่อตรวจสอบความผิดปกติในขั้นตอน Input ได้ครอบคลุม 100% ของรายการทั้งหมด

- **Duplicate Detection:** ตรวจสอบการบันทึกรายการซ้ำซ้อน เช่น การจ่ายเงินซ้ำ (Duplicate Payment)
- **Gap & Sequence Analysis:** ตรวจสอบความต่อเนื่องของเลขที่เอกสารนำเข้า เพื่อหาว่ามีรายการใดสูญหายหรือถูกข้ามไปหรือไม่
- **Exception Report:** ตรวจสอบรายงานรายการที่ผิดปกติ ซึ่งระบุธุรกรรมที่มีพฤติกรรมเบี่ยงเบนไปจากค่ามาตรฐานที่กำหนดไว้ในขั้นตอนการนำเข้า

4. การตรวจสอบร่องรอยและบันทึกกิจกรรม (Log Monitoring)

- **Authentication Log:** ตรวจสอบบันทึกการเข้าใช้งานเพื่อดูว่าใครเป็นผู้นำข้อมูลเข้าสู่ระบบ มีการเข้าใช้งานนอกเวลาทำการที่ผิดปกติ หรือใช้รหัสผ่านของผู้อื่นหรือไม่
- **Change Log:** ติดตามการแก้ไขข้อมูลสำคัญ เช่น การแก้ไขข้อมูลเงินเดือน หรือข้อมูลลูกค้า ว่าใครเป็นคนทำ และได้รับอนุญาตหรือไม่

การตรวจสอบที่ได้ผลลัพธ์ดีที่สุดคือการรวบรวมหลักฐานทั้งในรูปแบบเอกสาร (Documentary Evidence) และหลักฐานจากการปฏิบัติงานจริง (Operational Evidence) เพื่อยืนยันว่าระบบควบคุมขั้นตอน Input มีความแข็งแกร่งเพียงพอ

◆ **การควบคุมระบบงาน (Application Controls)** ถูกออกแบบมาเพื่อดูแลความถูกต้องของข้อมูลตลอดทั้ง**วงจรข้อมูล** โดยแบ่งออกเป็น 3 ขั้นตอนหลักตามลักษณะการทำงาน ดังนี้

1. การควบคุมการนำข้อมูลเข้า (Input Control)

- **จุดเน้น:** มุ่งเน้นไปที่ขั้นตอนแรกสุดคือ **"การรับข้อมูลเข้าสู่ระบบ"**
- **วัตถุประสงค์:** เพื่อให้มั่นใจว่าข้อมูลที่ถูกป้อนเข้าสู่ระบบมีความถูกต้อง ครบถ้วน และเป็นรายการที่ได้รับอนุญาตจริง
- **บทบาท:** ทำหน้าที่เป็นด่านแรกในการคัดกรองข้อมูลก่อนจะถูกนำไปประมวลผลต่อ

2. การควบคุมการประมวลผล (Processing Control)

- **จุดเน้น:** มุ่งเน้นไปที่ขั้นตอนการทำงานภายในของซอฟต์แวร์หรือระบบงาน
- **วัตถุประสงค์:** เพื่อให้มั่นใจว่าระบบมีการ**คำนวณและจัดการข้อมูล**ได้อย่างถูกต้องแม่นยำตามตรรกะ (Logic) หรือเงื่อนไขที่โปรแกรมกำหนดไว้
- **บทบาท:** ดูแลความถูกต้องในระหว่างที่ข้อมูลกำลังถูกเปลี่ยนแปลงหรือจัดกระทำโดยระบบ.

3. การควบคุมการแสดงผล (Output Control)

- **จุดเน้น:** มุ่งเน้นไปที่ขั้นตอนสุดท้ายคือ **"ผลลัพธ์หรือรายงาน"** ที่ได้จากระบบ
- **วัตถุประสงค์:** เพื่อให้มั่นใจว่าข้อมูลหรือรายงานที่แสดงผลออกมานั้นมีความ**ถูกต้องและครบถ้วน** ก่อนจะนำไปใช้งานต่อ
- **บทบาท:** ตรวจสอบความแม่นยำของผลผลิตสุดท้ายที่ระบบสร้างขึ้น
-

สรุปความแตกต่าง: การควบคุมทั้ง 3 ประเภทนี้ทำงานร่วมกันเป็นลำดับขั้น

- **Input** คุมที่ "ต้นทาง" (ข้อมูลดิบ)
- **Processing** คุมที่ "ตัวเครื่องจักร" (กระบวนการคำนวณ)
- **Output** คุมที่ "ปลายทาง" (ผลลัพธ์/รายงาน)

ทั้งหมดนี้มีเป้าหมายร่วมกันคือการรักษาความถูกต้องครบถ้วนของข้อมูล (**Data Integrity**) ตั้งแต่ต้นจนจบกระบวนการ

◆ **การตรวจสอบ Log Monitoring** เพื่อค้นหาการทุจริต เป็นกระบวนการตรวจสอบเชิงตรวจจับ (**Detective Control**) ที่สำคัญอย่างยิ่งในการระบุพฤติกรรมผิดปกติที่อาจนำไปสู่การทุจริตในระบบไอที โดยข้อมูลจากแหล่งข้อมูลได้ให้รายละเอียดแนวทางการตรวจสอบอย่างมีประสิทธิภาพไว้ดังนี้:

1. ประเภทของ Log ที่ต้องให้ความสำคัญเป็นพิเศษ

เพื่อให้การตรวจสอบครอบคลุมโอกาสในการทุจริต ผู้ตรวจสอบควรเน้นไปที่ Log 3 กลุ่มหลัก

- **Authentication Log:** ตรวจสอบการล็อกอินเพื่อหาความผิดปกติ เช่น การพยายามล็อกอินผิดพลาดซ้ำๆ หลายครั้ง (ซึ่งอาจเป็นการพยายามเดาสุ่มรหัสผ่าน), การล็อกอินจาก **IP Address ที่ไม่รู้จัก**, หรือการเข้าใช้งาน**นอกเวลาทำการ** (เช่น ช่วงกลางคืนหรือวันหยุด) ซึ่งเป็นหนึ่งในสัญญาณเตือนภัย (Warning Signal) ของการทุจริต
- **Change Log:** ใช้สำหรับติดตามการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญในระบบ โดยต้องระบุได้ว่า **"ใคร เปลี่ยนอะไร เมื่อไหร่ และเปลี่ยนจากค่าเดิมเป็นค่าอะไร"** โดยเฉพาะข้อมูลทางการเงิน ข้อมูลเงินเดือน หรือข้อมูลส่วนบุคคล ซึ่งอาจถูกลักลอบแก้ไขเพื่อผลประโยชน์ส่วนตัว

- **Privileged Access Log:** เป็นจุดที่มีความเสี่ยงสูงสุด จึงต้องเฝ้าระวังการใช้งานของกลุ่ม **Admin หรือ Privileged User** อย่างเข้มงวด เนื่องจากกลุ่มนี้มีสิทธิในการเข้าถึงและจัดการระบบในระดับสูง หากขาดการตรวจสอบซ้ำ (Secondary Review) อาจทำให้สามารถกระทำการทุจริตและลบหลักฐานทิ้งได้ง่าย

2. เทคนิคการตรวจสอบเพื่อตรวจจับการทุจริต

- **การใช้เป็นมาตรการชดเชย (Compensating Control):** ในกรณีที่องค์กรไม่สามารถแบ่งแยกหน้าที่ (**SoD**) ได้อย่างสมบูรณ์ การหมั่นตรวจสอบ Log (Review Log) จะทำหน้าที่เป็นมาตรการชดเชยเพื่อป้องกันไม่ให้บุคคลเพียงคนเดียวใช้อำนาจเหนือกระบวนการสำคัญไปในทางที่ผิด
- **การวิเคราะห์พฤติกรรมผิดปกติ (Anomaly Detection):** ตรวจสอบธุรกรรมที่มีพฤติกรรมเบี่ยงเบนไปจากมาตรฐาน เช่น การทำรายการด้วยจำนวนเงินเล็กน้อยแต่บ่อยครั้ง (Salami Attack) หรือการทำรายการที่มียอดเงินสูงผิดปกติ
- **Audit Trails:** ต้องมั่นใจว่าระบบมีการบันทึกกิจกรรมทุกอย่างโดยอัตโนมัติ ครบถ้วน และที่สำคัญที่สุดคือ **"ต้องไม่สามารถแก้ไขได้"** เพื่อให้ใช้เป็นหลักฐานในการตรวจสอบย้อนหลังได้เสมอ

3. การบูรณาการร่วมกับ Data Analytics ในยุคปัจจุบันที่ข้อมูลมีมหาศาล ผู้ตรวจสอบควรใช้เทคนิค **Data Analytics** เข้ามาช่วยในการตรวจสอบ Log

- **Exception Report:** การตั้งค่าระบบให้สรุปรายงานรายการที่ผิดปกติออกมาโดยเฉพาะ เพื่อให้ผู้ตรวจสอบสามารถมุ่งเป้าไปที่จุดเสี่ยงได้ทันที แทนการไล่ตรวจ Log ทั้งหมด,
- **การตรวจสอบแบบ 100%:** การใช้เครื่องมืออย่าง ACL, IDEA หรือ Python ช่วยให้สามารถวิเคราะห์ Log ได้ครบทุกระเบียนข้อมูล (100%) เพื่อหาความสัมพันธ์หรือรูปแบบการทุจริตที่ซับซ้อน ซึ่งการสุ่มตรวจแบบเดิมอาจมองข้าม

4. ข้อกำหนดและการเก็บรักษา (Log Retention) ตามกฎหมายและมาตรฐานสากล องค์กรมีหน้าที่ต้องเก็บรักษา Log ไว้เพื่อการตรวจสอบ

- **พ.ร.บ. คอมพิวเตอร์ฯ:** กำหนดให้ต้องเก็บรักษา Log ไว้ไม่น้อยกว่า **90 วัน**
- **มาตรฐานอื่นๆ:** เช่น ระเบียบธนาคารอาจกำหนดให้เก็บ 5-7 ปี หรือตามมาตรฐาน ISO 27001 แนะนำที่ 1 ปี เพื่อให้เพียงพอต่อการตรวจสอบย้อนหลังหากพบเหตุทุจริตในภายหลัง

◆ **แนวทางการตรวจสอบหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)**

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มุ่งเน้นไปที่การตรวจสอบว่าหน่วยงานปฏิบัติตามกฎหมายและมาตรการรักษาความปลอดภัยที่กำหนดไว้ในฐานะผู้ประมวลผล โดยมีประเด็นสำคัญดังนี้

1. การกำกับดูแลและโครงสร้างหน้าที่ (Governance & Compliance)

- **การกำหนดบทบาทหน้าที่:** ตรวจสอบว่ามีการระบุหน้าที่และความรับผิดชอบระหว่างผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผลข้อมูล (Processor) อย่างชัดเจนเป็นลายลักษณ์อักษรตามข้อกำหนดของกฎหมาย
- **นโยบายความเป็นส่วนตัว (Privacy Policy):** ตรวจสอบว่ามีนโยบายหรือกระบวนการปฏิบัติงานที่สอดคล้องกับวัตถุประสงค์ที่ผู้ควบคุมข้อมูลกำหนด โดยต้องไม่มีการประมวลผลนอกเหนือจากที่ได้รับมอบหมาย

2. มาตรการรักษาความมั่นคงปลอดภัย (Security Controls)

ผู้ประมวลผลมีหน้าที่หลักในการดูแลความปลอดภัยของข้อมูล ซึ่งผู้ตรวจสอบควรประเมินดังนี้:

• **การควบคุมการเข้าถึง (Access Control):** ตรวจสอบการกำหนดสิทธิเข้าถึงข้อมูลตามหลักสิทธิขั้นต่ำที่จำเป็น (**Principle of Least Privilege**) และการยืนยันตัวตนหลายปัจจัย (**MFA**).

• **การปกป้องข้อมูล (Data Protection):** ประเมินการใช้เทคโนโลยีเพื่อป้องกันข้อมูล เช่น **การเข้ารหัสข้อมูล (Encryption)** เพื่อลดความเสี่ยงจากการรั่วไหล.

• **การทดสอบระบบ:** ตรวจสอบว่ามีการทดสอบและประเมินความมั่นคงปลอดภัยของระบบงานที่ใช้ประมวลผลข้อมูลอย่างสม่ำเสมอ

3. การบันทึกและติดตามร่องรอย (Log Monitoring & Audit Trails)

• **ร่องรอยการตรวจสอบ (Audit Trails):** ต้องมีระบบการบันทึกกิจกรรม (**Log**) ที่เกิดขึ้นกับข้อมูลส่วนบุคคลอย่างครบถ้วนและไม่สามารถแก้ไขได้ เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่า "ใคร ทำอะไรกับข้อมูลใด เมื่อไหร่"

• **การตรวจสอบการเข้าถึง (Authentication Log):** ตรวจติดตามการล็อกอินที่ผิดปกติ เช่น การพยายามเข้าถึงนอกเวลาทำการ หรือจาก IP Address ที่ไม่รู้จัก เพื่อป้องกันการทุจริตหรือการเข้าถึงโดยมิชอบ

• **การเก็บรักษา Log (Log Retention):** ตรวจสอบว่ามีการเก็บรักษา Log ไว้ตามระยะเวลาที่กฎหมายกำหนด (เช่น ขั้นต่ำ 90 วันตาม พ.ร.บ. คอมพิวเตอร์ฯ)

4. การจัดการวงจรชีวิตข้อมูลและการแจ้งเหตุ (Data Management)

• **การจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization):** ตรวจสอบว่ามีการจัดเก็บและประมวลผลข้อมูลเฉพาะที่จำเป็นตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น

• **กระบวนการแจ้งเหตุละเมิด:** ตรวจสอบความพร้อมของกระบวนการแจ้งเหตุเมื่อพบการละเมิดข้อมูลส่วนบุคคล เพื่อให้ผู้ควบคุมข้อมูลสามารถดำเนินการรายงานต่อหน่วยงานกำกับดูแลได้**ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุ

5. การตรวจสอบความสอดคล้องในทางปฏิบัติ (Effectiveness Testing)

• **Design Effectiveness:** ตรวจสอบว่ามาตรการที่วางไว้ถูกออกแบบมาให้รับมือกับความเสี่ยงด้านข้อมูล (Data Risk) ได้จริง

• **Operating Effectiveness:** ใช้วิธีการสุ่มตรวจสอบรายการ (**Test of Control**) หรือการเดินดูหน้างานจริง (**Walkthrough**) เพื่อยืนยันว่ามาตรการเหล่านั้นถูกนำไปปฏิบัติอย่างสม่ำเสมอ

สรุปได้ว่า ผู้ตรวจสอบต้องยืนยันให้ได้ว่าผู้ประมวลผลข้อมูลมี**เกราะป้องกัน (IT Controls)** ที่แข็งแกร่งพอ และมี**ร่องรอยการทำงาน (Audit Trails)** ที่โปร่งใส เพื่อลดความเสี่ยงทั้งด้านปฏิบัติการและด้านกฎหมาย

นางสาวศุภลักษณ์ สมโภชน์ ตำแหน่งนักตรวจสอบภายใน ชำนาญการ

นางสาววราภรณ์ คล้ามสถิต ตำแหน่งนักตรวจสอบภายใน

ผู้สรุปรายงานการอบรม