แนวทางตรวจสอบระบบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบระบบเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์

สมภพ เตชเสนสกุล

ผู้อำนวยการฝ่ายตรวจสอบระบบเทคโนโลยีสารสนเทศ

ธนาคารอาคารสงเคราะห์

หัวข้อการบรรยาย :

1. ความจำเป็นของงานตรวจสอบระบบเทคโนโลยีสารสนเทศ
2. หลักการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Auditing)
3. กระบวนการตรวจสอบระบบเทคโนโลยีสารสนเทศ
4. ระบบฐานข้อมูลเพื่อการตรวจสอบ (Audit Analysis Database)
5. ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Auditor)
6. การบริหารจัดการความเสี่ยงด้านระบบงานเทคโนโลยีสารสนเทศ

ความหมาย/คำนิยามของการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Defining IT Audit)

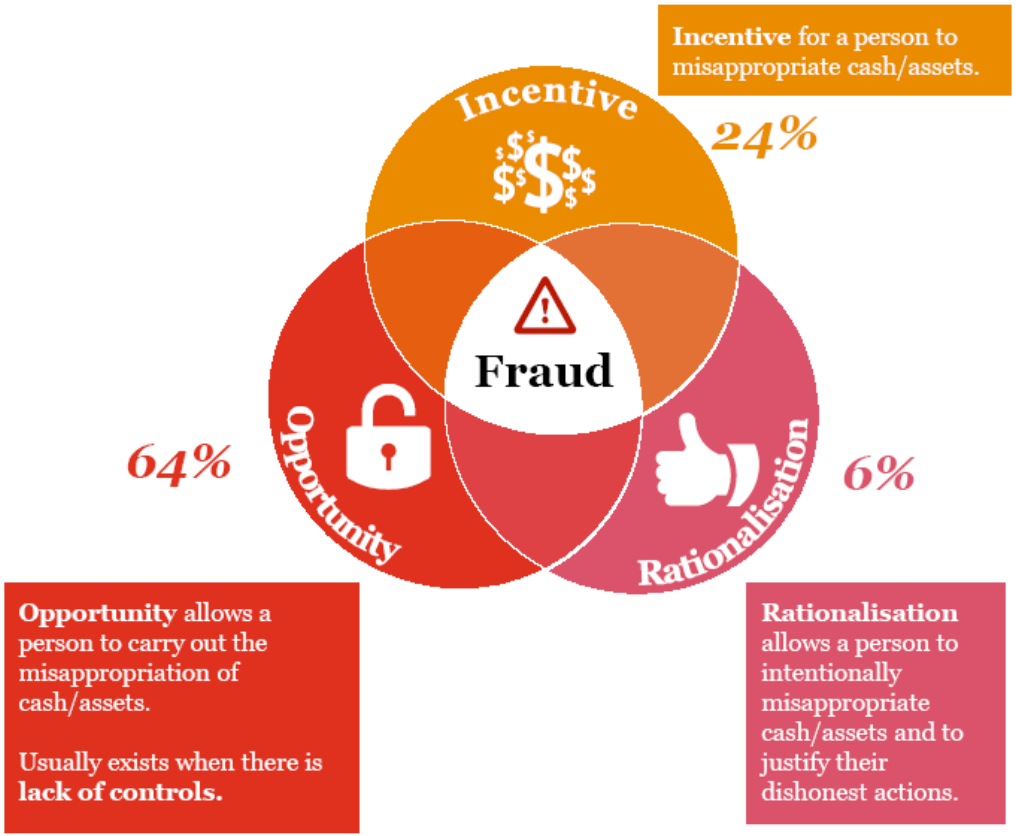
- การตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Auditing) หมายถึง

  การค้นหาหลักฐานสำหรับสิ่งผิดปกติที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ (IT) โดยมีวัตถุประสงค์เพื่อประเมินความเพียงพอของการควบคุมภายในด้าน IT และการจัดการความเสี่ยงด้าน IT

ความจำเป็นของงานตรวจสอบ ระบบเทคโนโลยีสารสนเทศ

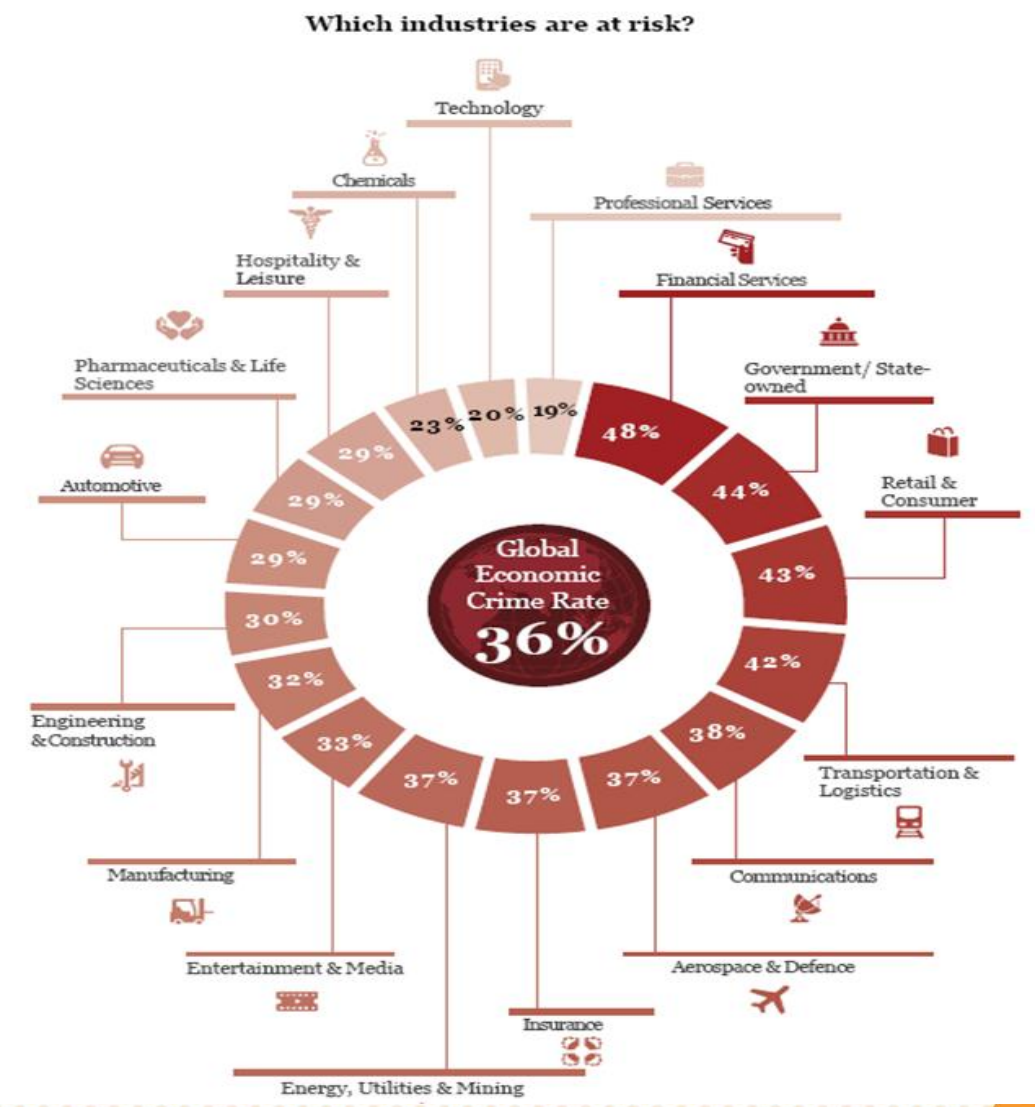
ความจำเป็นของงานตรวจสอบ :

Perceived factors that contribute to fraud



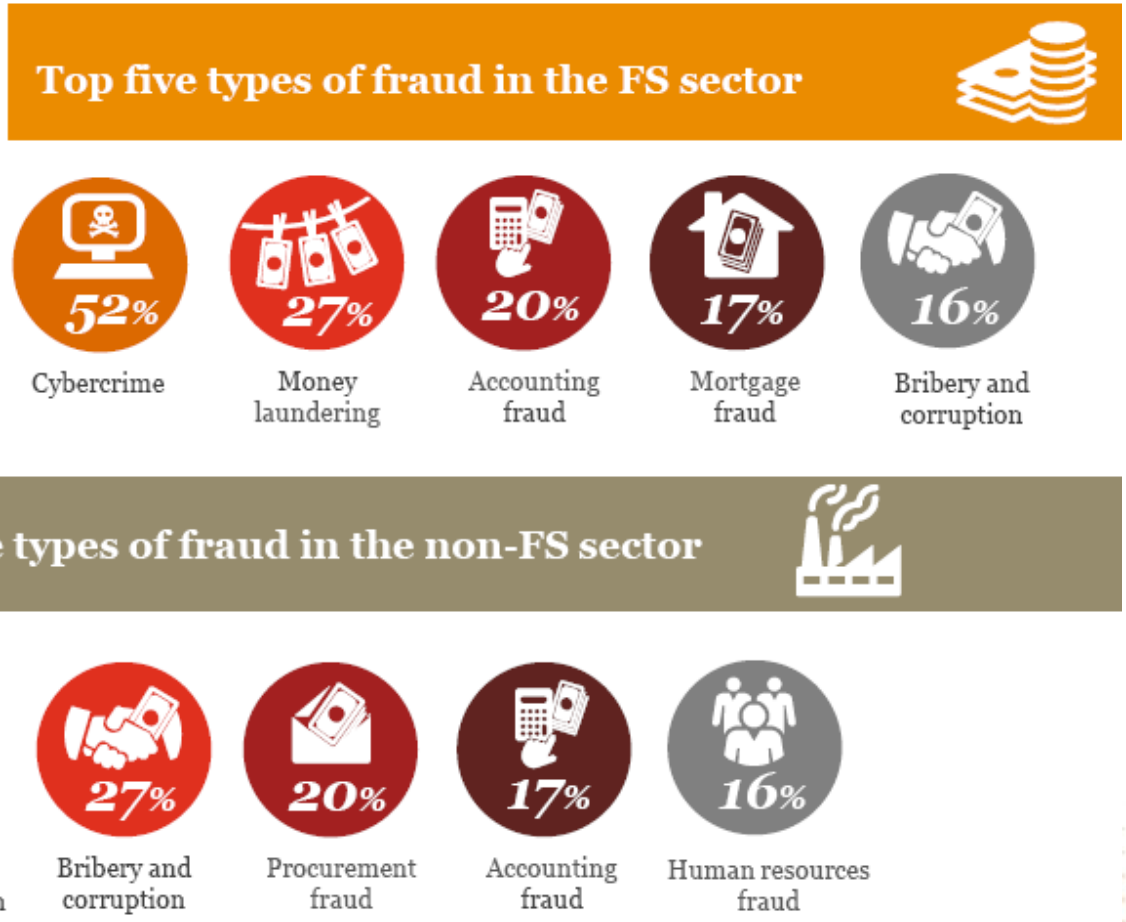
PwC's 2016 Global Economic Crime Survey, "Economic Crime in Thailand" P.8

ผลงานวิจัยการเกิด Fraud :



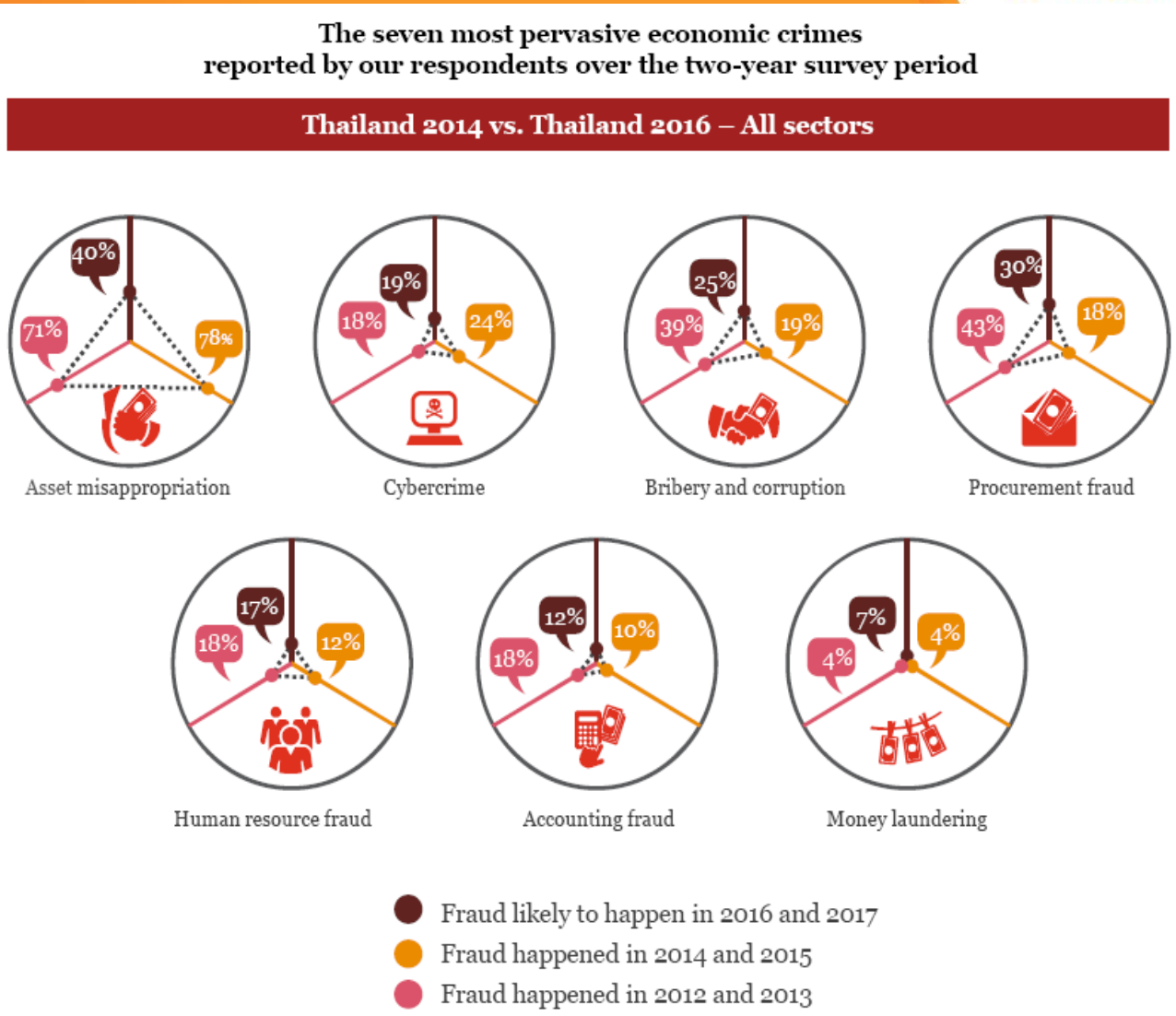
PwC's 2016 Global Economic Crime Survey, "Economic Crime in Thailand" P.9

ผลงานวิจัยการเกิด Fraud (ตามประเภทธุรกิจ) :



PwC's 2016 Global Economic Crime Survey, "Economic Crime in Thailand" P.10

ผลการเปรียบเทียบการเกิด Fraud :



PwC's 2016 Global Economic Crime Survey, "Economic Crime in Thailand" P.11

หลักการตรวจสอบระบบเทคโนโลยีสารสนเทศ

หลักการตรวจสอบระบบเทคโนโลยีสารสนเทศ

การตรวจสอบระบบเทคโนโลยีสารสนเทศ จะเป็นการตรวจสอบการควบคุมภายในด้านคอมพิวเตอร์ ที่แบ่งออกได้เป็น 2 ลักษณะ คือ

1. การควบคุมภายในทั่วไป (General Controls)

เป็นการควบคุมที่อาศัยนโยบาย และระเบียบปฏิบัติงาน เป็นหลักในการควบคุมกิจกรรมของหน่วยงานคอมพิวเตอร์

2. การควบคุมภายในเฉพาะงาน (Application Controls)

เป็นการควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูลเป็นแนวทางในการกำหนดขอบเขตการควบคุม

3. การตรวจสอบโครงการเทคโนโลยีสารสนเทศ (Quality Assurance IT Project)

เป็นการเข้าร่วมสังเกตการณ์ ให้ข้อเสนอแนะโครงการ ตั้งแต่เริ่มโครงการ

การตรวจสอบระบบเทคโนโลยีสารสนเทศ

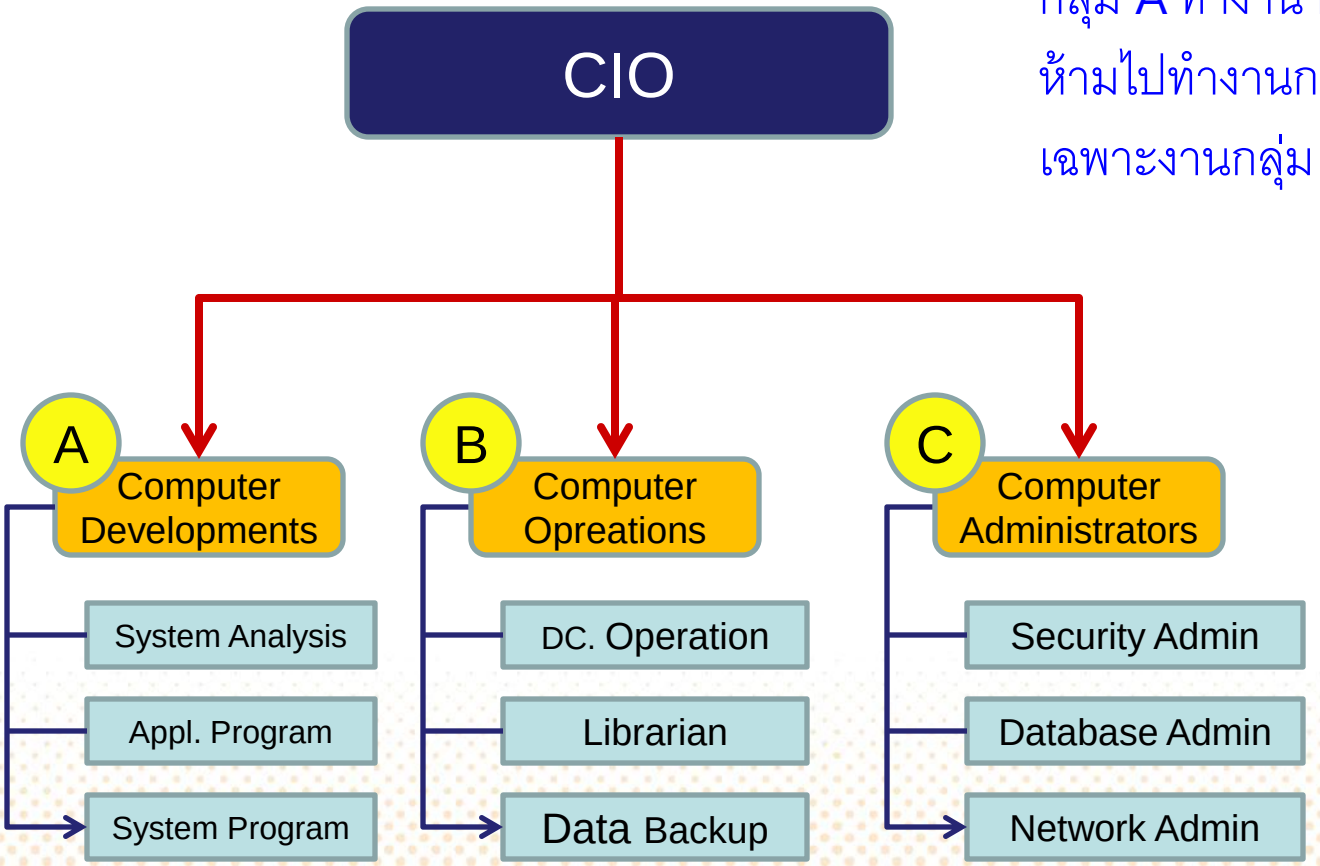
1. การควบคุมภายในทั่วไป(General Controls)

- **IT Planning and Organization**
  - **IT Steering Committee**
    - กำหนดนโยบายด้านเทคโนโลยีสารสนเทศ
    - พิจารณาโครงการและงบประมาณ IT
    - ติดตามผลการดำเนินการด้านสารสนเทศขององค์กร

- **IT Organization Control**

Audit Concern

กลุ่ม A ทำงาน Programmer ห้ามไปทำงานกลุ่มอื่นด้วย โดยเฉพาะงานกลุ่ม B



- **Development and Implementation Control**

  - Business Requirement
  - Feasibility Study (User agree & signoff)
  - System Analysis and Design (Documentation & User signoff)
  - Coding Program
  - Program Testing (Test Scenario , UAT , User Signoff)
  - Data Conversion (Data Reconciliation & User signoff)
  - Implementation (System doc. & Training Manual)
  - Post Implementation Review

    (Problem logging & Change Procedure)

การตรวจสอบระบบเทคโนโลยีสารสนเทศ

- **Information Security Control**
  - IT security Policy and Procedure
    - นโยบายด้านความปลอดภัยและระเบียบปฏิบัติ
    - จัดความสำคัญของระบบและข้อมูล
    - มีการกำหนดหน้าที่รับผิดชอบ
  - User Access Control Feature
    - Password Policy
    - User Authorized Matrix
  - Logging and Monitoring
    - ระยะเวลาการเก็บ Log
  - Physical Security
    - การควบคุมการเข้าออก , **Room Environment**

- **Maintenance of Existing System Control**
  - ตรวจการปฏิบัติตามระเบียบการพัฒนาระบบ **(SDLC)**
  - Change Management
    - Changed Detection Program
    - Changed Request Form

ทุกการเปลี่ยนแปลงในระบบ จะต้องมี **Request Form**

การตรวจสอบระบบเทคโนโลยีสารสนเทศ

- **Computer Operation Control**
  - Operation Schedule/Time table/Control Procedure
    - ต้องทำงานตามคู่มือและขั้นตอนการปฏิบัติงาน
  - Service Level Agreement: SLA
  - Data Backup Procedure
  - Disaster and Recovery Plan: DRP
    - การเขียนแผน การทดสอบแผน และการปรับปรุงแผน

2. การควบคุมภายในเฉพาะงาน (Application Controls)

วัตถุประสงค์

- **C**ompleteness (ให้ความมั่นใจในความสมบูรณ์ของข้อมูล)
- **A**ccuracy (ความถูกต้องตรงกันทุกประการของข้อมูล)
- **V**alidity (ความสมเหตุสมผลของข้อมูล)
- **R**estricted Access to Data and Physical asset

  (การจำกัดการเข้าถึงข้อมูลและสินทรัพย์)

C A V R

CAVR ทำได้โดยการควบคุมข้อมูล

- ข้อมูลนำเข้า **(Input Control)** วิธีการ ที่มา ความถูกต้อง
- การประมวลผล **(Processing Control)**
- ข้อมูลผลลัพธ์ **(Output Control)**

- **ตัวอย่างการควบคุมความถูกต้องของรายการข้อมูล**
  - Check digit validation (การคำนวณเลขหลักสุดท้ายของเลขบัญชี)
  - Range Check (เช่น ข้อมูลช่วงอายุของลูกค้า)
  - Limit Check (เช่น จำกัดวงเงินในการถอนจากตู้ ATM)
  - Sequence Check (เช่นเลขที่เอกสารไม่ซ้ำกัน)

การตรวจสอบระบบเทคโนโลยีสารสนเทศ

- **เทคนิคการใช้ระบบคอมพิวเตอร์ช่วยในการตรวจสอบ เพื่อหาสาระในเชิงลึก** (Substantive Test) ไม่มีความเชื่อถือในระบบการควบคุมภายใน และต้องทำการทดสอบความถูกต้องของรายการ

  – Generalized Audit Software: GAS เช่น ACL software

  – Custom Audit Software: เขียนหรือพัฒนาขึ้นมาเอง เพื่อเปรียบเทียบ Output กับรายงาน User

  – Test Data โดยการสร้าง Test script และนำ Program ของ User มา Run กับ Data test

  – Concurrent Auditing Techniques การตรวจสอบหาความผิดปกติของข้อมูลที่เกิดขึ้นในระบบ

การตรวจสอบระบบเทคโนโลยีสารสนเทศ

ธอส GH BANK
ธนาคารอาคารสงเคราะห์

- **Concurrent Auditing Techniques**

  เป็นการตรวจสอบข้อมูลในระบบเพื่อหา ข้อผิดพลาด ความผิดปกติของข้อมูลที่ส่อในทางทุจริต หรือความบกพร่องของระบบควบคุมภายในและระเบียบ

ผลที่จะได้

-พบว่าไม่ปฏิบัติตามระเบียบ
-ข้อมูลส่อในทางทุจริต
-พบข้อบกพร่องของระบบ IT
-พบข้อบกพร่องของการควบคุมภายใน
-ได้ทราบถึงพฤติกรรมของผู้ปฏิบัติงาน
-ฯลฯ

ตัวอย่างการนำเทคนิคทางด้าน IT มาใช้ตรวจสอบเพื่อหาความผิดปกติ

ธอส GHBANK ธนาคารอาคารสงเคราะห์

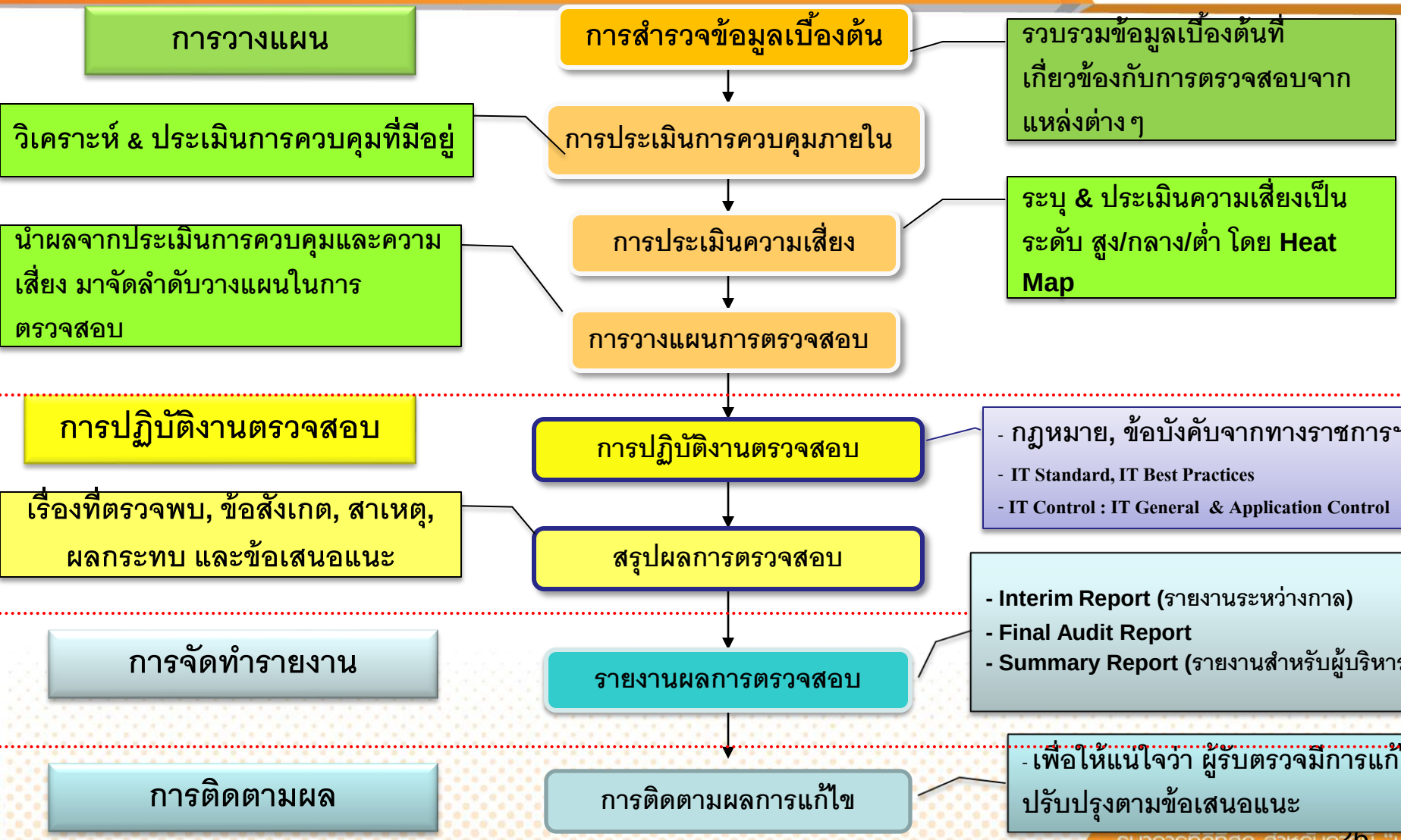
- **การตรวจสอบความถูกต้องของอัตราดอกเบี้ยในระบบเปรียบเทียบกับผลิตภัณฑ์**
  - กวาดข้อมูลตามผลิตภัณฑ์ ดูว่ามีรายใดที่มีอัตราดอกเบี้ยไม่ตรงตามข้อกำหนด
  - เปรียบเทียบดอกเบี้ยสะสมประจำเดือน ว่ามีรายใดที่มีการเปลี่ยนแปลงสูง
  - ดู Audittrail Log ที่แก้ไขอัตราดอกเบี้ย
- **การตรวจข้อมูลการจ่ายเงินเดือน ค่ารักษาพยาบาล**
  - ดูยอดเบิกจ่ายที่สูงและมีความถี่สูง และดูความสัมพันธ์ของผู้ทำรายการกับผู้เบิก
- **การดูการเคลื่อนไหวของรายการที่สูงผิดปกติ หรือการเกิดซ้ำ เกิดนอกเวลาทำการ**
  - ดูจากบัญชีเงินฝากที่มีเงินเข้าแต่ละเดือนสูงกว่ารายรับที่ควรจะเป็น และเกิดต่อเนื่อง
  - มีการทำรายการทางการเงิน นอกเวลาทำการ

3. การตรวจสอบโครงการเทคโนโลยีสารสนเทศ (Quality Assurance IT Project)

- **<u>วัตถุประสงค์</u>**
  - การสร้างความมั่นใจและให้คำปรึกษาในการทำงานโครงการที่ยังไม่เสร็จสิ้น เพื่อให้ได้โครงการประสบความสำเร็จ
- **<u>ระยะเวลาการตรวจสอบ</u>**
  - ช่วงการวางแผนโครงการ คือการตรวจสอบในช่วงที่เริ่มวางแผนว่าจะดำเนินโครงการว่าได้จัดทำข้อกำหนดครบถ้วนหรือไม่
  - ในช่วงการจัดหาบริษัทที่ปรึกษา คือการตรวจสอบว่าได้จัดหาบริษัทที่ปรึกษามาอย่างถูกต้องตามหลักเกณฑ์หรือไม่
  - ในช่วงการดำเนินโครงการ คือการตรวจสอบการทำโครงการว่าถูกต้องหรือไม่
  - ในช่วงหลังการติดตั้งใช้งานผลของโครงการ คือการตรวจสอบว่าโครงการได้ผลตามที่ต้องการหรือไม่

วิธีการตรวจสอบระบบเทคโนโลยีสารสนเทศ
(Steps of an IT Audit)

วิธีการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Steps of an IT Audit)



วิธีการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Steps of an IT Audit)

การวางแผน (Planning)	→	แนวการตรวจสอบ (Audit Program)
การปฏิบัติงานภาคสนาม (Field Work)	→	สิ่งที่ตรวจพบ (Audit Findings)
การรายงานผลงาน (Communicating Results)	→	รายงานการตรวจสอบ (Audit Report)
การติดตามผล (Follow-Up)	→	รายงานผลการเสนอแนะ (Report of Recommendation)

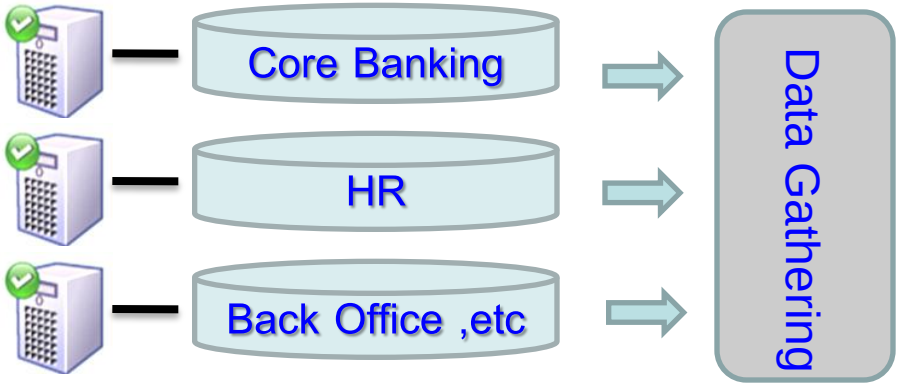
ระบบฐานข้อมูลเพื่อการตรวจสอบ

Audit Analysis Database

ระบบฐานข้อมูลเพื่อการตรวจสอบ

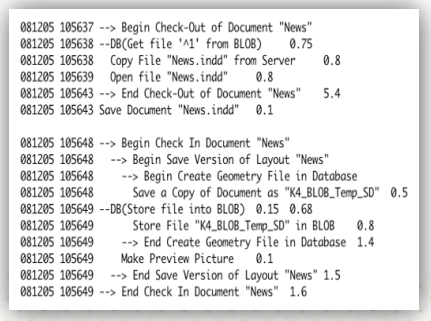
(Audit Analysis Database)

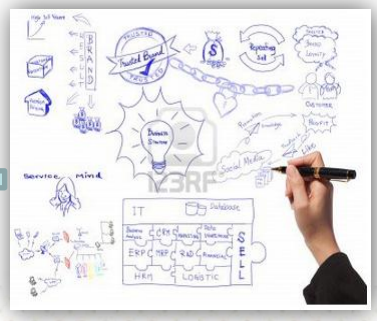
ธอส GH BANK
ธนาคารอาคารสงเคราะห์



Audit Analysis Database

- Master Data
- Transaction Data
- Configurations Data
- Logs





Analysis

IT Auditor

ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Auditor)

1. ทักษะด้านการตรวจสอบ

- ผ่านงานผู้ตรวจสอบ
- มี **Certificated** ผู้ตรวจสอบ **IT**

2. ทักษะด้าน IT

- ผ่านงานด้าน **IT**
- จบการศึกษาด้าน **IT**

3. ทักษะด้านธุรกรรมหลักของธนาคาร

- ผ่านงานด้านธุรกรรมหลักขององค์กร ในระดับ **Supervisor**

6. สมาคมผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ (Information Technology Auditor)

ธอส GHBANK ธนาคารอาคารสงเคราะห์

- Internal Auditor ->

The Institute of Internal Auditors Thailand

Certified Internal Auditor® Professionalism Defined

- Information Technology Auditor ->

ISACA® Trust in, and value from, information systems

CISA Certified Information Systems Auditor® An ISACA® Certification

- Information Security Auditor ->

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

CISSP® Certified Information Systems Security Professional

การบริหารจัดการความเสี่ยง ด้านระบบงานเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์

อัครเดช ภาพน้ำ

หัวหน้าส่วนตรวจสอบการปฏิบัติงานด้าน IT

ธนาคารอาคารสงเคราะห์

2. การบริหารจัดการความเสี่ยงด้าน IT (IT Risk Management)

ธอส GH BANK
ธนาคารอาคารสงเคราะห์

2.1 IT Risk

2.2 กระบวนการบริหารความเสี่ยง

(ความเสี่ยง – ปัจจัยเสี่ยง – ประเมินความเสี่ยง – จัดการความเสี่ยง)

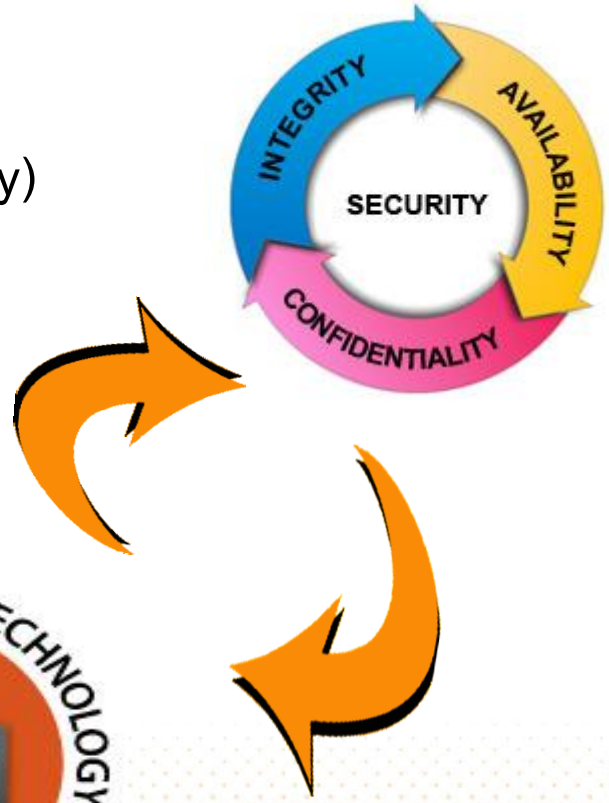
2.3 กรณีตัวอย่าง- การประเมินความเสี่ยงด้าน IT ของ ธอส.

2. การบริหารจัดการความเสี่ยงด้าน IT
(IT Risk Management)

ธอส GH BANK
ธนาคารอาคารสงเคราะห์

2.1 IT Risk -> ความเสี่ยงที่องค์กรนำ IT มาใช้ในการขับเคลื่อนองค์กร

- ความไม่พร้อมของระบบ IT (Available)
- การเข้าถึงข้อมูลในระบบ IT (Confidentiality)
- ความถูกต้องข้อมูลในระบบ IT (Integrity)



2.2 กระบวนการบริหารความเสี่ยง

(ความเสี่ยง – ปัจจัยเสี่ยง – ประเมินความเสี่ยง – จัดการความเสี่ยง)

หลักเกณฑ์ประเมินความเสี่ยงเพื่อจัดทำแผนตรวจสอบ

ธอส GH BANK
ธนาคารอาคารสงเคราะห์

ปัจจัยความเสี่ยง ด้านการบริหารและการปฏิบัติการเทคโนโลยีสารสนเทศ

1. การวางแผนกลยุทธ์ นโยบายและแผนการปฏิบัติงานด้าน IT
2. นโยบายและคุณภาพการรักษาความปลอดภัย
3. ความเหมาะสมของโครงสร้างระบบ IT และเครือข่ายการสื่อสารเพื่อรองรับระบบ IT
4. จุดอ่อนของระบบการควบคุมภายในและการรักษาความปลอดภัย
5. ข้อผิดพลาดของข้อมูลและรายงานที่ออกจากระบบ
6. การเชื่อมโยง แก้ไข หรือเปลี่ยนแปลงระบบงานที่ก่อให้เกิดความผิดพลาด
7. การจัดทำแผนรองรับการดำเนินธุรกิจต่อเนื่องและการกู้คืนระบบ

ผลกระทบ (1 - 5)	โอกาสเกิด (1 - 5)	คะแนนรวม	ระดับความเสี่ยง

คะแนนรวม	ระดับความเสี่ยง	การตรวจสอบ
1-3	ต่ำ	ตรวจทุก 3 ปี
4 – 8	ปานกลาง	ตรวจทุก 2 ปี
9 – 15	สูง	ตรวจ ปี เว้น ปี
16 – 25	สูงมาก	ตรวจทุกปี

Back

หลักเกณฑ์ประเมินความเสี่ยงเพื่อจัดทำแผนตรวจสอบ (ต่อ)

ธอส GHBANK
ธนาคารอาคารสงเคราะห์

ปัจจัยความเสี่ยง ด้านระบบงานเทคโนโลยี

1. นโยบายและคุณภาพของการรักษาความปลอดภัยระบบงาน (กระทบต่อการให้บริการลูกค้า)
2. ปริมาณ ประเภท และ ความซับซ้อนของรายการ/ธุรกรรม ผลิตภัณฑ์และการบริการ (ผลกระทบทางการเงิน)
3. ความเหมาะสมของโครงสร้างระบบ IT และเครือข่ายเพื่อรองรับการให้บริการ
4. ความผิดพลาด บกพร่องและการทุจริตที่เกิดสภาพแวดล้อมความปลอดภัย (การเปลี่ยนแปลงแก้ไขระบบงาน)
5. จุดอ่อนของระบบการควบคุมภายในและการรักษาความปลอดภัย (จุดอ่อนที่พบจากการตรวจสอบ)
6. ความสำคัญและความถูกต้องของข้อมูล
7. การจัดทำแผนรองรับการดำเนินธุรกิจ/การกู้คืน

ผลกระทบ (1 - 5)	โอกาสเกิด (1 - 5)	คะแนนรวม	ระดับความเสี่ยง

คะแนนรวม	ระดับความเสี่ยง	การตรวจสอบ
1-3	ต่ำ	ตรวจทุก 3 ปี
4 – 8	ปานกลาง	ตรวจทุก 2 ปี
9 – 15	สูง	ตรวจ ปี เว้น ปี
16 – 25	สูงมาก	ตรวจทุกปี

Next

Q & A