**การตรวจสอบเทคโนโลยีสารสนเทศ : Information Technology Audit by อ.บุญเกียรติ เดชะวรานนท์**

## 1. เทคโนโลยีสารสนเทศ กับผลกระทบต่องานตรวจสอบ

ตัวอย่างของเทคโนโลยีสารสนเทศ ที่มีผลกระทบต่องานตรวจสอบ

1. Distributed Data Processing: การประมวลผลเชิงกระจาย
   - Audit Implication: (Access to Data Program, Client / Server)
   - Limit access to System: การจำกัดการเข้าถึงระบบตามความจำเป็น
   - Transaction Completeness: ความครบถ้วนสมบูรณ์ของรายการข้อมูล
2. Networking: เครือข่าย (Lan , Wireless Lan)
   - Limit access to the Network (as need basic) ต้องมีมาตรการจำกัดการข้าใช้งานในเครือข่ายตามความจำเป็นเท่านั้น
3. Real-time Systems: ระบบการประมวลผลทันที

   ลดภาระงานเอกสารและได้ผลลัพธ์ที่รวดเร็ว เช่นระบบ JIT, Auto ordering, POS – Point of sale
   - No batch-type Control: ไม่รองรับการสอบทานผลรวมรายการทั้งหมด
   - Transactions Authorization Control: การควบคุมอำนาจอนุมัติรายการ
   - Entity's Access Control: จำกัดการใช้ Real time ให้หน่วยงานต่าง ๆ ที่เกี่ยวข้องตามความจำเป็นเท่านั้น
   - More Continuous Audit ต้องมีการตรวจสอบอย่างต่อเนื่อง (การฝากและถอนเงินมาก ๆ ในเวลาใกล้เคียงกัน คือการฟอกเงิน)
4. End-User Computing: ผู้ใช้งานพัฒนาระบบงานขึ้นใช้เอง (High-Level computer language, Packaged software)
   - Safeguarding of data Integrity: ความถูกต้องครบถ้วนของข้อมูล
   - Unauthorized Access from the various work of control at user department: การเข้าถึงระบบโดยไม่ได้รับอนุญาตจากช่องทางต่าง ๆ ที่ไม่ได้รับการควบคุมโดยผู้ใช้งาน
5. Internet: e-Commerce: อินเตอร์เน็ต (WWW, Web Application , Web Server)
   - Unauthorized Access to the entity's network: การเข้าถึงเครือข่าย
   - Need More Technology access controls form external, such as router & Firewall : ต้องใช้เทคโนโลยีควบคุมการเข้าถึงเครือข่ายที่เพียงพอ
   - Need transaction Validation ความสมเหตุสมผลของรายการข้อมูลที่บันทึกเข้าระบบ
   - Need Transaction Authorization control จำกัดอำนาจการอนุมัติรายการ
   - Need transaction Completeness ความครบถ้วนสมบูรณ์ของรายการข้อมูล

## 2. กฎหมายด้านเทคโนโลยีสารนเทศ

### 1. พรฎ.ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

ในเรื่อง พรฎ.มีเรื่องที่เกี่ยวข้อง “หลักเกณฑ์การเก็ฐรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ.2550” ซึ่งพูดถึงการ forward ข้อมูลใด ๆ ที่เป็นการทำให้ผู้อื่นเสียหาย....จะมีความผิดทางกฎหมายด้วย

### 2. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

มีเนื้อหาที่น่าสนใจในส่วนดังนี้

- ★ มาตรา ๙ ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ
- ★ มาตรา ๑๐ กระทำให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ จนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ
- ★ มาตรา ๑๒ การกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลหรือระบบคอมพิวเตอร์ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ของสาธารณะ ในทางเศรษฐกิจของประเทศ หรือกระทำต่อข้อมูลหรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

(๓) การกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

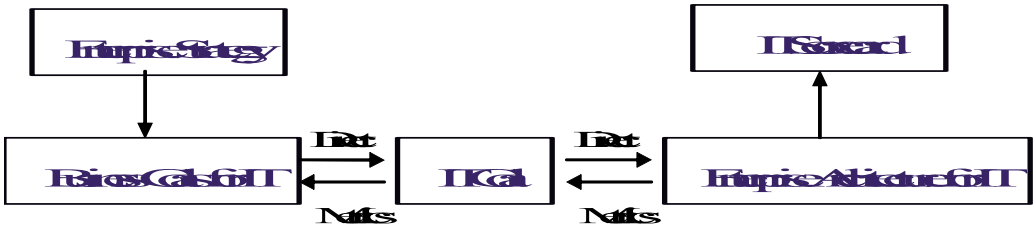
## 3. กรอบงานด้านการควบคุมเทคโนโลยีสารสนเทศ IT Control Framework “COBIT”

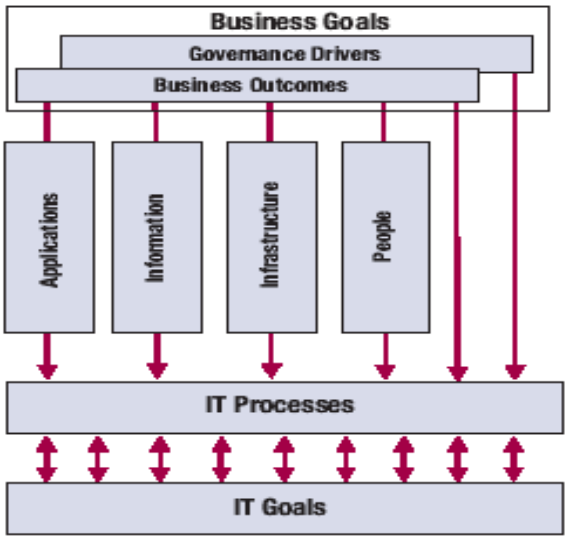
**“COBIT” ⇨ Control Objective Information & Related Technology**

1. General Information on COBIT
   - What is COBIT? การเชื่อมโยงกระบวนการทำงานไปยังความต้องการหรือเป้าหมายทางธุรกิจ มี Good Practices ของกลุ่มงาน และกระบวนการที่เป็นเลิศฝังตาม Domain ทั้ง 4 Domains, มุ่งที่ Control and less on execution, ช่วยด้านการลงทุนระบบ IT และการส่งมอบ สามารถวัดและตัดสินสิ่งที่ผิดพลาด
   - Who does COBIT serve? Stakeholders และ ผู้ที่สนใจทั่วไปใน Value From IT Investments, Internal & External, Stakeholders who provide the IT Services, Who have a control / risk responsibility

2. Main Characteristics of COBIT V.4.1

- Business Focus ความต้องการทางธุรกิจเป็นตัวกำหนดให้มี IT Goals และ IT Enterprise Architecture ให้สอดคล้องกัน



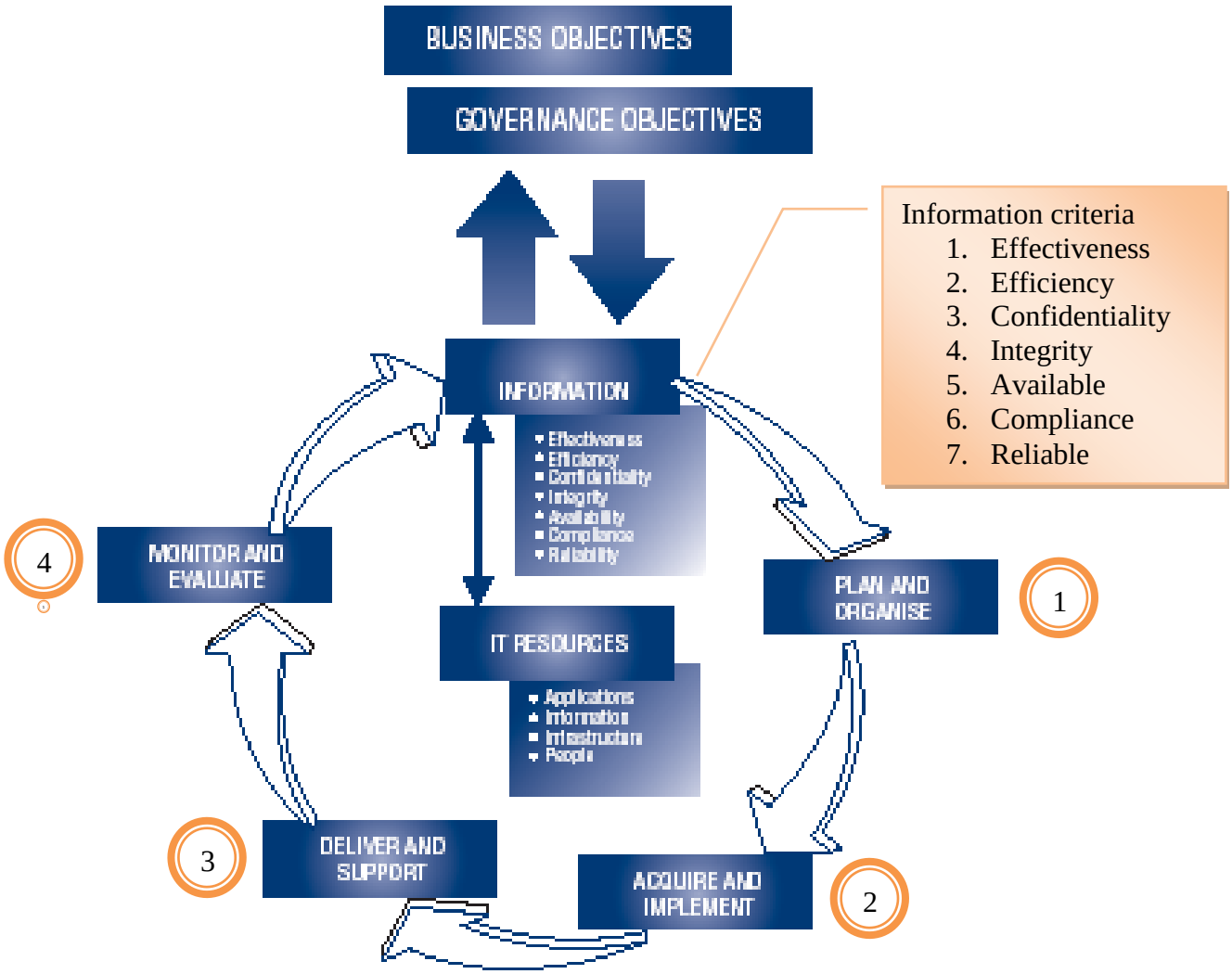



IT Processes มี 34 กระบวนการ

IT Goals ต้องสอดคล้องกับ Business Goals

- Process – Oriented ประกอบด้วย 4 Domain , 34 Process (**4 Domains = Plan, Build, Run and Monitor)**

| | | |
|---|---|---|
| 1 | PLAN AND ORGANISE (PO) (10 Process) | Strategy aligned? (กลยุทธ์ของ IT สอดคล้องกับกลยุทธ์ของธุรกิจหรือไม่), optimum use of its resources? , IT objectives? , IT risks? , quality of IT systems? |
| 2 | ACQUIRE AND IMPLEMENT (AI) (7 Processes) กระบวนการสร้างและนำไปใช้ | Deliver solutions that meet business needs? , delivered on time and within budget?, work properly, changes be made without upsetting |
| 3 | DELIVER AND SUPPORT (DS) (13 Processes) | In line with business priorities? , costs optimized? , productively and safely? , confidentiality, integrity and availability in place? |
| 4 | MONITOR AND EVALUATE (ME) (4 Processes) | Performance measured? , manage internal controls? , linked back to business goals? , risk, control, compliance and performance measured and reported |




1

| Plan and Organise Domain Mapping | Information Criteria: Effectiveness | Efficiency | Confidentiality | Integrity | Availability | Compliance | Reliability |
|---|---|---|---|---|---|---|---|
| PO1 Define a strategic IT plan. | P | S | | | | | |
| PO2 Define the information architecture. | S | P | S | P | | | |
| PO3 Determine technological direction. | P | P | | | | | |
| PO4 Define the IT processes, organisation and relationships. | P | P | | | | | |
| PO5 Manage the IT investment. | P | P | | | | | S |
| PO6 Communicate management aims and direction. | P | | | | | S | |
| PO7 Manage IT human resources. | P | P | | | | | |
| PO8 Manage quality. | P | P | | S | | | S |
| PO9 Assess and manage IT risks. | S | S | P | P | P | S | S |
| PO10 Manage projects. | P | P | | | | | |

2

| Acquire and Implement Domain Mapping | Information Criteria: Effectiveness | Efficiency | Confidentiality | Integrity | Availability | Compliance | Reliability |
|---|---|---|---|---|---|---|---|
| AI1 Identify automated solutions. | P | S | | | | | |
| AI2 Acquire and maintain application software. | P | P | | S | | | S |
| AI3 Acquire and maintain technology infrastructure. | S | P | | S | S | | |
| AI4 Enable operation and use. | P | P | | S | S | S | S |
| AI5 Procure IT resources. | S | P | | | | S | |
| AI6 Manage changes. | P | P | | P | P | | S |
| AI7 Install and accredit solutions and changes. | P | S | | S | S | | |

3

| Deliver and Support Domain Mapping | Information Criteria: Effectiveness | Efficiency | Confidentiality | Integrity | Availability | Compliance | Reliability |
|---|---|---|---|---|---|---|---|
| DS1 Define and manage service levels. | P | P | S | S | S | S | S |
| DS2 Manage third-party services. | P | P | S | S | S | S | S |
| DS3 Manage performance and capacity. | P | P | | | S | | |
| DS4 Ensure continuous service. | P | S | | | P | | |
| DS5 Ensure systems security. | | | P | P | S | S | S |
| DS6 Identify and allocate costs. | | P | | | | | P |
| DS7 Educate and train users. | P | S | | | | | |
| DS8 Manage service desk and incidents. | P | P | | | | | |
| DS9 Manage the configuration. | P | S | | | S | | S |
| DS10 Manage problems. | P | P | | | S | | |
| DS11 Manage data. | | | | P | | | P |
| DS12 Manage the physical environment. | | | | P | P | | |
| DS13 Manage operations. | P | P | | S | S | | |

4

| Monitor and Evaluate Domain Mapping | Information Criteria: Effectiveness | Efficiency | Confidentiality | Integrity | Availability | Compliance | Reliability |
|---|---|---|---|---|---|---|---|
| ME1 Monitor and evaluate IT performance. | P | P | S | S | S | S | S |
| ME2 Monitor and evaluate internal control. | P | P | S | S | S | S | S |
| ME3 Ensure regulatory compliance. | | | | | | P | S |
| ME4 Provide IT governance. | P | P | S | S | S | S | S |

- Control -Based

  ☑ PO1 Process Owner ⟶Assign an owner that responsibility is clear.

  ☑ PO2 Repeatability ⟶Define process repeatable.

  ☑ PO3 Goals and Objectives ⟶Establish clear goals and objectives

  ☑ PO4 Roles and Responsibilities ⟶Define unambiguous roles

  ☑ PO5 Process Performance ⟶Measure the performance

  ☑ PO6 Policy, Plan and Procedures ⟶Document, review, keep up to date, sign off and communicate

  **The enterprise's system of internal controls impacts IT at 3 levels:**

  - **At the executive management level**⟶business objectives, policies, overall approach to governance and control
  - **At the business process level** ⟶combination of manual controls operated by the business
  - **At IT services level** ⟶IT general controls (เกี่ยวกับ COBIT)

  COBIT IT Processes จะมองภาพในลักษณะเป็น General IT controls ไม่ได้เกี่ยวข้องกับ Application control

- Measurement-driven ถือว่ายากที่สุด เป็นการวัด performance ของ IT มี 6 ระดับ คือ

  0 Non-exist - Mgt. Processes are not applied at all (ไม่มีการใช้เทคโนโลยีสารสนเทศ)

  1 Initial - Processes are ad-hoc and disorganized (มีบ้างแต่ยังยุ่งเหยิง ไม่ Update ไม่มี Standard)

  2 Repeatable - Processes follow a regular pattern (มีการทำและ Update แต่ไม่มีเอกสาร)

  3 Defined - Processes are documented and communicated (มีการจัดทำเป็นเอกสาร มี Standard และมีการสื่อสาร)

  4 Managed - Processes are monitored and measured (สามารถวัดและติดตามผล มีการ monitor รวมถึงพัฒนาอยู่ตลอดเวลา)

  5 Optimized - Best practices are followed and automated (กระบวนการ IT ต่าง ๆ มีขั้นตอนชัดเจนอย่างดีที่สุดเหมาะที่สุดสำหรับองค์กร สามารถเป็นแบบอย่างให้ในอุตสาหกรรมได้ มีคู่มือมี workflow ชัดเจน มีเครื่องมือต่าง ๆ ที่มีประสิทธิภาพ, คุณภาพ และมีประสิทธิผลอย่างดีเยี่ยม)

## 4. การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ IT Risk Management Guideline

### 1. Enterprise Risk Management


**คุณลักษณะของการกำหนดวัตถุประสงค์ที่ดี..... SMART**

- **Specific** ระบุได้เฉพาะเจาะจงและชัดเจน
- **Measurable** สามารถวัดได้
- **Actionable** สามารถทำได้หรือปฏิบัติได้จริง
- **Reality** สมเหตุสมผล
- **Timely** มีการกำหนดระยะเวลา

**ความเสี่ยง คือ** ปัจจัยต่างๆ ที่ส่งผลกระทบต่อความสามารถในการบรรลุเป้าหมายขององค์กร ซึ่งมีโอกาสเกิด และส่งผลให้เกิดความเสียหายในระดับที่แตกต่างกันไปตามสภาพแวดล้อม และวิธีการดำเนินกิจการ และการบริหารงานขององค์กร

อีก wording เพื่อให้เข้าใจง่าย....

**"อะไรก็ตามที่เกิดขึ้นแล้วเป็นภัยคุกคามต่อการบรรลุเป้าหมายขององค์กร..เรียกว่า "ความเสี่ยง"**

**ต้องประเมินอย่างน้อยปีละครั้ง เนื่องจาก ความเสี่ยงจะเปลี่ยนตามเป้าหมายของธุรกิจที่เปลี่ยนไป**

**การบ่งชี้ความเสี่ยง** ต้องคุยกับเบอร์หนึ่งของบริษัทนั้นจึงจะได้ข้อมูลที่น่าจะดีที่สุด

- ข้อมูลจากผู้บริหารระดับต่างๆ ที่มีความเข้าใจในเป้าหมายขององค์การ หรือหน่วยงาน
- กระบวนการหรือกิจกรรม ที่ใช้สนับสนุนการบรรลุวัตถุประสงค์
- อุปสรรคต่าง ๆ ที่มีผลกระทบต่อกระบวนการ หรือกิจกรรมที่ใช้ในการบรรลุวัตถุประสงค์องค์กร หรือหน่วยงาน

**การประเมินความเสี่ยง - มาจาก 2 ทาง**

1. ผลกระทบ (Impact) – ระดับความรุนแรง ความเสียหายต่อการอยู่รอด การแข่งขัน สภาพคล่อง ชื่อเสียง บุคคลากร
2. โอกาสที่จะเกิดขึ้น (Likelihood) – โอกาสที่จะเกิดเหตุการณ์ ความน่าจะเป็น หรือความถี่

**การจัดการความเสี่ยง (ความเสี่ยง - การควบคุม = ความเสียหายในส่วนที่เหลือ)**

**การควบคุมที่เพียงพอและเหมาะสมจะช่วยให้กิจการบรรลุวัตถุประสงค์ได้จริง**

**Internal Audit ช่วยให้บริษัทบรรลุวัตถุประสงค์ได้จริง**

**เป้าหมายเปลี่ยนไป ความเสี่ยงเปลี่ยนไป การควบคุมต้องเปลี่ยนตาม**

**การควบคุม เหมือนการติดเบรคของรถ รถก็เหมือนบริษัทเรานั่นแหล่ะ ใครวิ่งได้แรงกว่า เร็วกว่า ใครก็ชอบ แต่ถ้ารถไม่มีเบรคเลยหล่ะ ...ใครจะกล้าขับรถคันนั้น**

**ทำอย่างไรก็ได้ ให้ความเสี่ยงในส่วนที่เหลือเป็นความเสี่ยงที่เราสามารถยอมรับได้....Acceptable risk**

โดยการควบคุมมีดังนี้

- AVOID คือการหลีกเลี่ยงความเสี่ยง โดยการยุติกิจกรรม หรือการลดขนาดของกิจกรรม เป็นต้น
- TRANSFER คือการโอนความเสี่ยงให้กับบุคคลอื่น เช่นการประกัน การทำ Forward หรือ Hedging และการ Outsource
- CONTROL คือการจัดให้มีกิจกรรมการควบคุมต่าง ๆ เช่นการรักษาความปลอดภัย การสอบทาน เป็นต้น
- ACCEPT คือการยอมรับความเสี่ยง แต่มีการวางมาตรการรองรับเมื่อความเสี่ยงต่าง ๆ เหล่านั้นเกิดขึ้น

**5. การนำ COBIT มาใช้ในการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือการ Mapping Process ในแต่ละ Domain ให้เข้ากับ IT Requirement ทั้ง 7 ข้อ**

**กระบวนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

1. IT Risk Assessment ประเมินระดับความเสี่ยงเทคโนโลยีสารสนเทศ
2. IT Control Evaluation ประเมินระดับการควบคุม
3. Gap Analysis วิเคราะห์ช่องว่างของระดับความเสี่ยงกับการควบคุม
4. Implementation Plan การวางแผนจัดการความเสี่ยง

**1. IT Risk Assessment (Objective): 7 Information Criteria (effectiveness, efficiency, integrity availability, confidentiality, compliance, reliability)**

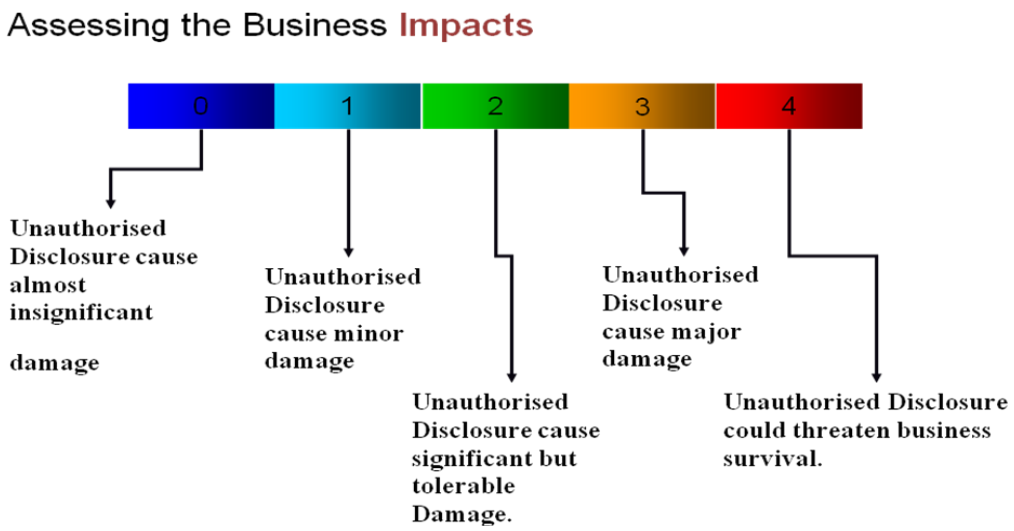
- **Risk Identification ในแต่ละ Criteria**

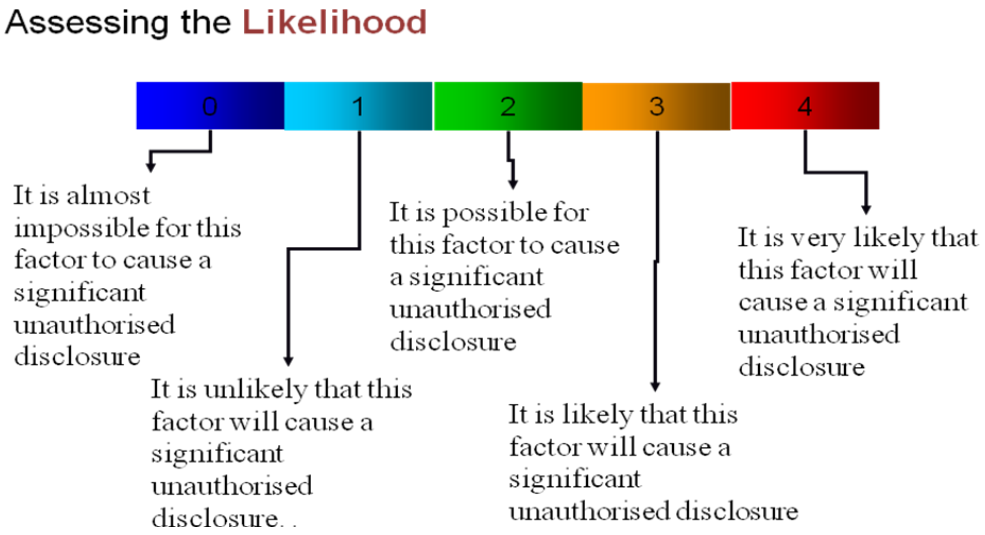
| **Effectiveness &Efficiency** | **Confidentiality** | **Availability** | **Reliability & Integrity** | **Compliance** |
|---|---|---|---|---|
| -Poor management (Planning & Policy)<br>-System (H/W & technology)<br>- Skill of IT & non IT<br>- Processing management (design & executions) | -Security management (Policy & Procedure)<br>-System (H/W & Technology & network)<br>- User awareness<br>- Hacker, Virus | -System & Network design<br>- Hardware fails<br>- External sabotage<br>- Viruses & Attack<br>- No BCP, backup & Recovery | - System design (Input, Process, Output)<br>- Error | -Unaware or not understand<br>-No monitoring |

- **Assessment** > Overall Business impacts & likelihood

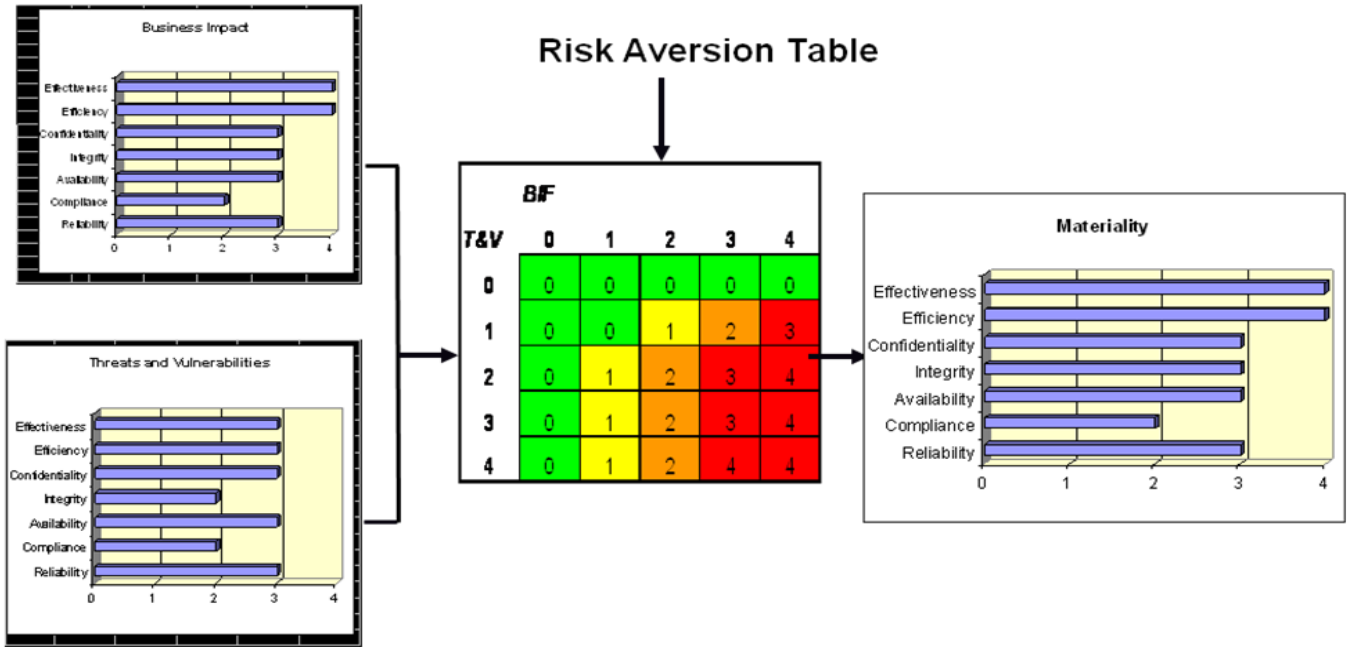
| **Overall Business Impact** | **Overall Likelihood** |
|---|---|
| Financial Impacts | Network of business (Industry) |
| Damage to Reputations, due to unsecured systems | Organization Structure & culture |
| Interception to business operations | Network of the system (open or close new or outdate technology) |
| Lost of valuable assets (system & data) | Etc. |
| Delay in decision Making process | |

ให้คะแนน Impact และ Likelihood (0-4 หรือ 1-5) แล้วนำมารวมกัน โดย Link กับ 7 criteria .(หากใช้จุดทศนิยม ต้องตัดสินให้ได้เป็นจำนวนเต็มว่า Criteria นั้นๆ มีความเสี่ยง(Impacts &Likelihood) ออกมาเท่าไร



**Combine impact & likelihood**




ข้อมูลดังกล่าวต้องได้จากผู้บริหารสูงสุดของบริษัท เพราะผู้บริหารของบริษัทจะเป็นคนที่ทราบดีที่สุดว่าอะไรจะ impact ต่อธุรกิจของบริษัท

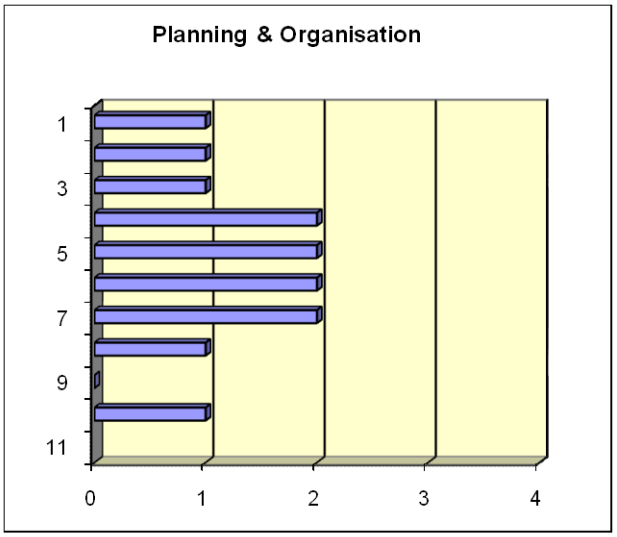
2. **IT Control Evaluation ดูตามที่ mapping process ต่างๆ แต่การประเมินตาม COBIT จะมีคะแนน 0-5 แต่ในการประเมินการควบคุม ต้องตัดให้เหลือ 0-4 โดยรวม 3 และ 4 ไว้ด้วยกัน และให้ 5 มาเป็น 4**


**Legends for Ranking used**

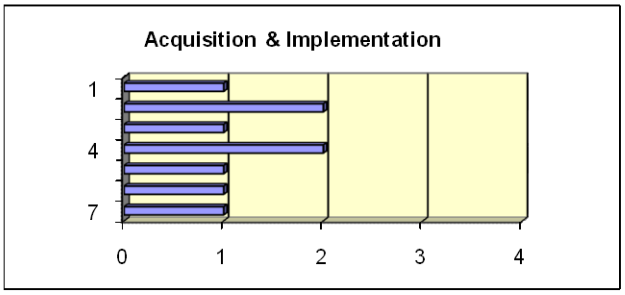
| | |
|---|---|
| 0 Non-exist | - Mgt. Processes are not applied at all |
| 1 Initial | - Processes are ad-hoc and disorganized |
| 2 Repeatable | - Processes follow a regular pattern |
| 3 Defined & Managed | - Processes are documented and communicated<br>- Processes are monitored and measured |
| 4 Optimised | - Best practices are followed and automated |

ตัวอย่าง :

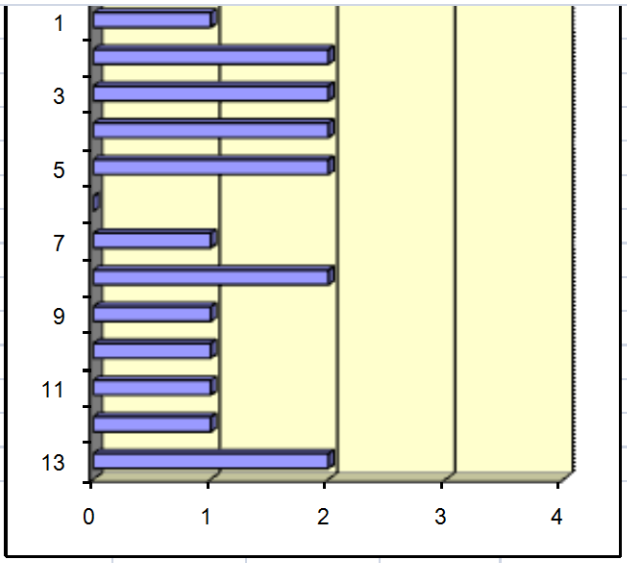
| Plan and Organise | | |
|---|---|---|
| PO 1 | Define a strategic IT plan | 1 |
| PO 2 | Define the information architecture | 1 |
| PO 3 | Determine technological direction | 1 |
| PO 4 | Define IT process, organisation & relationships | 2 |
| PO 5 | Manage the investment | 2 |
| PO 6 | Communicate management aims and direction | 2 |
| PO 7 | Manage IT human resources | 2 |
| PO 8 | Manage quality | 1 |
| PO 9 | Assess and manage IT risks | 0 |
| PO 10 | Manage projects | 1 |



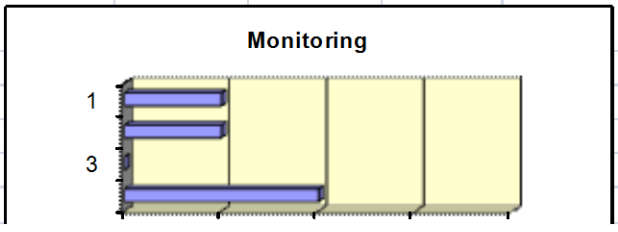

| Acquire and Implement | | |
|---|---|---|
| AI 1 | Identify automated solutions | 1 |
| AI 2 | Acquire and maintain application software | 2 |
| AI 3 | Acquire and maintain technology infrastructure | 1 |
| AI 4 | Enable operation and use | 2 |
| AI 5 | Procure IT resource | 1 |
| AI 6 | Managing changes | 1 |
| AI 7 | Install and accredit solutions and changes | 1 |




| Delivery and support | | |
|---|---|---|
| DS 1 | Define and manage service levels | 1 |
| DS 2 | Manage third-party services | 2 |
| DS 3 | Manage performance and capacity | 2 |
| DS 4 | Ensure continuous service | 2 |
| DS 5 | Ensure systems security | 2 |
| DS 6 | Identify and allocate costs | 0 |
| DS 7 | Educate and train users | 1 |
| DS 8 | Manage service desk and incidents | 2 |
| DS 9 | Manage the configuration | 1 |
| DS 10 | Manage problems | 1 |
| DS 11 | Manage data | 1 |
| DS 12 | Manage the physical ew nvironment | 1 |
| DS 13 | Manage operations | 2 |




| Monitor and Evaluate | | |
|---|---|---|
| ME 1 | Monitor and evaluate IT performance | 1 |
| ME 2 | Monitor and evaluate internal control | 1 |
| ME 3 | Ensure regulatory compliance | 0 |
| ME 4 | Provide IT governance | 2 |



### 3. Gap Analysis

**From assessment of Impacts & Likelihood**

**E2 Control Risk**

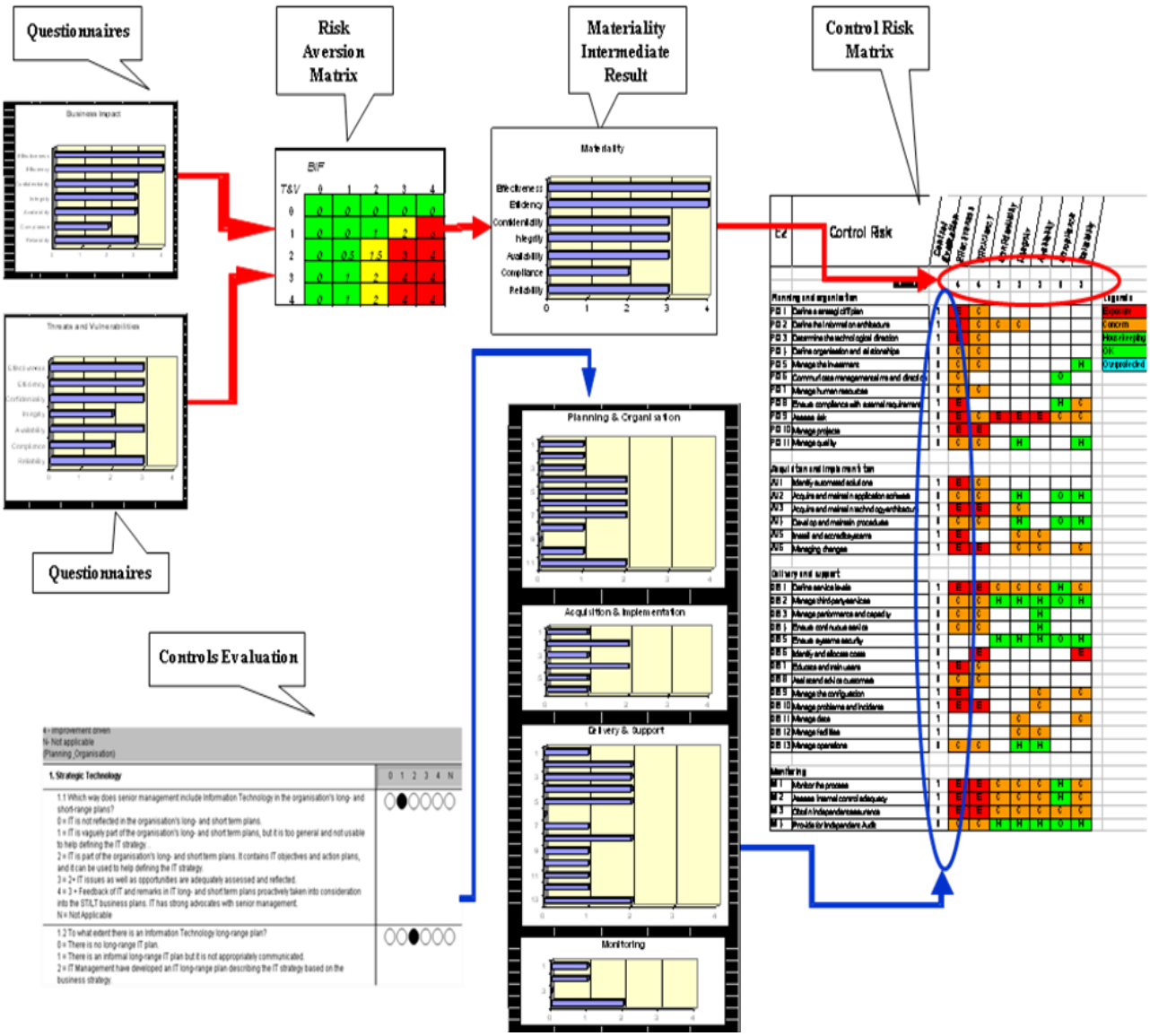
| | | Control Evaluation | Effectiveness | Efficiency | Confidentiality | Integrity | Availability | Compliance | Reliability |
|---|---|---|---|---|---|---|---|---|---|
| | *Materiality* | | 4 | 4 | 3 | 3 | 3 | 2 | 3 |
| **Planning and organisation** | | | | | | | | | |
| PO 1 | Define a strategic IT plan | 1 | E | C | | | | | |
| PO 2 | Define the information architecture | 1 | C | E | C | C | | | |
| PO 3 | Determine technological direction | 1 | E | E | | | | | |
| PO 4 | Define IT process, organisation &relationships | 2 | C | C | | | | | |
| PO 5 | Manage the IT investment | 2 | C | C | | | | | H |
| PO 6 | Communicate management aims and direction | 2 | C | | | | | O | |
| PO 7 | Manage IT human resources | 2 | C | C | | | | | |
| PO 8 | Manage quality | 1 | E | E | | C | | | C |
| PO 9 | Assess and manage IT risk | 0 | C | C | E | E | E | C | C |
| PO 10 | Manage projects | 1 | E | E | | | | | |
| **Acquisition and implementation** | | | | | | | | | |
| AI 1 | Identify automated solutions | 1 | E | C | | | | | |
| AI 2 | Acquire and maintain application software | 2 | C | C | | H | | O | H |
| AI 3 | Acquire and maintain technology instruction | 1 | E | E | | C | | | |
| AI 4 | Enable operation and use | 2 | C | C | | H | | O | H |
| AI 5 | Procure IT resources | 1 | E | | | C | C | | |
| AI 6 | Managing changes | 1 | E | E | | C | C | | C |
| AI 7 | Install and accredit solutions and changes | 1 | E | C | | C | C | | |

**Gap Analysis for P: Primary**

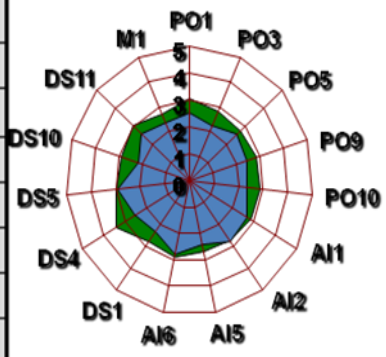
| R-C | Legends |
|---|---|
| 3 | Exposure |
| 2 | Concern |
| 1 | Housekeeping |
| 0 | OK |
| >0 | Overprotected |

**Gap Analysis for S: Secondary**

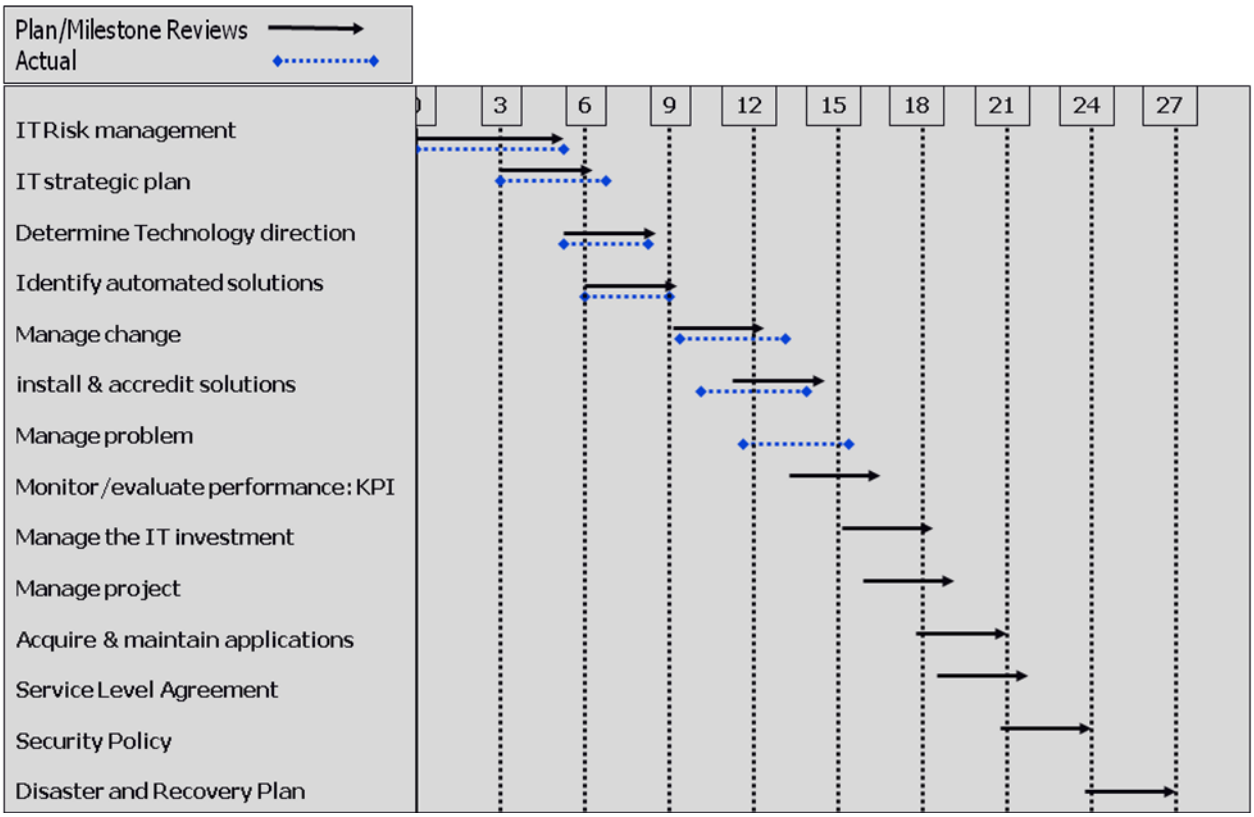
| R-C | Legends |
|---|---|
| 3 | Concern |
| 2 | Concern |
| 1 | Housekeeping |
| 0 | OK |
| >0 | Overprotected |



| CobiT's Key Controls | Control Level | | | | |
|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 |
| PO1 define a strategic IT plan | | | | | |
| PO3 determine technological direction | | | | | |
| PO5 manage the IT investment | | | | | |
| PO9 assess risks | | | | | |
| PO10 manage projects | | | | | |
| AI1 identify automated solutions | | | | | |
| AI2 acquire & maintain applications | | | | | |
| AI6 manage changes | | | | | |
| AI7 install & accredit solutions/changes | | | | | |
| DS1 define and manage service levels | | | | | |
| DS4 ensure continuous service | | | | | |
| DS5 ensure system security | | | | | |
| DS10 manage problems | | | | | |
| DS11 manage data | | | | | |
| M1 monitor and evaluate IT performance | | | | | |


**4. Implementation Plan**



**บทสรุป:** **Concept : คิดอย่างเจ้าของธุรกิจ** คิดอย่างผู้เป็น consult เพื่อต้องการให้ลดความเสี่ยงอย่างไรให้มากที่สุด แต่การจะเสนอแนะว่าบริหารความเสี่ยงให้พัฒนาการควบคุมมากขนาดไหนนั้น ต้องดูว่าบริษัทแต่ละบริษัทมีลักษณะการบริหารแบบ Aggressive หรือ Conservative ขนาดไหน Risk appetite รับได้ขนาดไหน เพราะบางอย่างการมี control มากหรือน้อยไปก็ไม่ดีขึ้นอยู่กับลักษณะของบริษัทด้วย....

**วิธีการจัดลำดับแผนก็คือเลือกทำตัวที่มี Gap เยอะ ๆ ก่อน และอันไหนที่ใช้ความพยายาม (Effort) น้อยที่สุให้เลือกทำอย่างนั้นก่อน ....High risk effort low**

**บริษัทใดจะประเมินความเสี่ยงได้ดี แผนก Risk Management ควรต้องให้ความรู้และความเข้าใจต่อ MD ให้เข้าใจอย่างถ่องแท้ เพราะสิ่งที่น่ากลัวอย่างหนึ่งก็คือผู้บริหารอาจจะเข้าใจ Risk Framework ได้ไม่ถ่องแท้**.....งานนี้เรื่องใหญ่.....สามารถหาข้อมูลเพิ่มเติมได้ที่ website ของ ISACA ได้

## 6. การตรวจสอบควบคุมเทคโนโลยีสารสนเทศ

### 1. IT Audit Approach & Strategy: แนวทางและกลยุทธ์ การตรวจสอบเทคโนโลยีสารสนเทศ

- **Decision Process for IT Auditing** *****

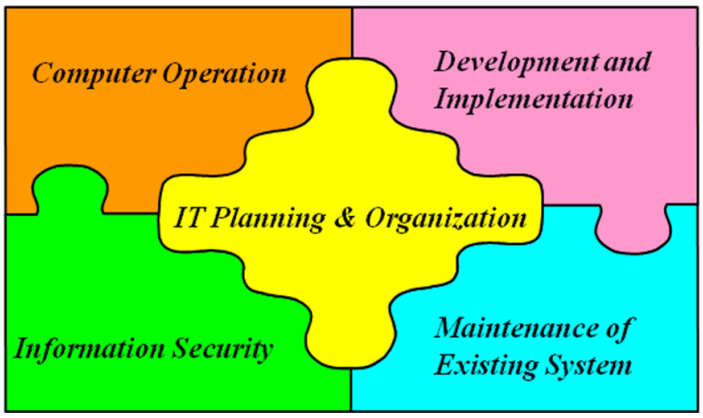
1. Review general control ให้ตรวจตาม COBIT
   - Assess general control (walk through)
   - Test of Controls ทดสอบการควบคุมที่มี หรือถ้าไม่มีแล้วมีอะไรชดเชย ให้คะแนน
   - Are general control reliable? ตกลงแล้วการควบคุมทั่วไปเชื่อถือได้หรือไม่

   ต้อง update ข้อมูลก่อนตรวจว่าปีนี้มีอะไรที่เปลี่ยนแปลงไปหรือไม่ ซึ่งต้อง update ใน Audit program ด้วย finding ปีที่แล้วแก้ไขหรือยัง ไปทดสอบในส่วนที่เขาทำเพิ่มด้วย
2. Review application control : (การควบคุมงานเฉพาะอย่าง เช่น จัดซื้อ , บัญชี)
   - Assess application control เช่น การจำกัดอำนาจการอนุมัติ ลองทำเกินอำนาจว่าระบบยอมหรือไม่ หรือถ้ายอมต้องมี Approve
   - Test of Controls
   - Are application controls reliable?
3. Design Substantive test หาค่าความเสียหายที่ทำผิดไปแล้ว มีกี่ครั้ง มูลค่าเท่าไร หน้าที่ IA โดยตรง

- *** หน้าที่ของฝ่าย IT คือ ข้อ 1) + 2)**
- **ถ้าข้อ 1) ไม่ผ่าน (ไม่น่าเชื่อถือ) ไม่ต้องทำข้อ 2) ทำข้อ 3) เลย**

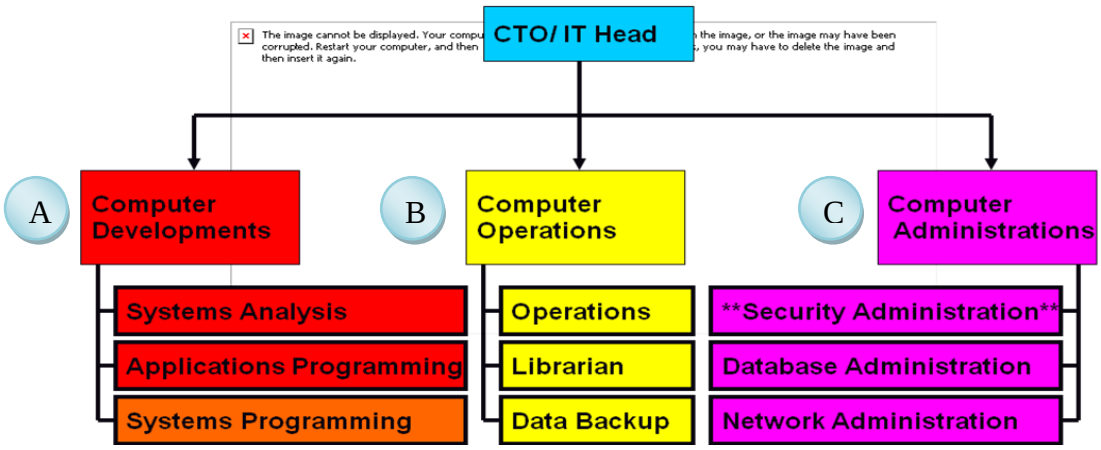
**ความหมายคือถ้า General control เละมาก ไม่มีประโยชน์ที่จะ test Application control หยุดเลยไปทำ Substantive test ดีกว่า**

**2. IT General Controls มี 5 องค์ประกอบ**




- **IT Planning and organization**


1. IT Planning มี IT Steering Committee มีหน้าที่กลั่นกรองงาน IT เพื่อพัฒนาระบบให้สามารถสนับสนุนบริษัทได้อย่างเต็มประสิทธิภาพ และคณะกรรมการควรประกอบด้วยเบอร์ 1 ของ business unit ที่ใช้ computer หรือสารสนเทศเยอะ ๆ, วาง IT Strategic Plan โดยฝ่ายบริหาร, วาง IT Strategic ขึ้นมาให้รองรับ Business Plan , มีแผนระยะสั้นระยะยาว, มีงบประมาณในการลงทุน IT Budget, มีการสื่อสารวัตถุประสงค์ และติดตามผลทั้งนี้การติดตามผลแบบไม่มี paper ไม่มีลายลักษณ์อักษรแบบพูดปากเปล่า....น่ากลัว!!!! เพราะจินตนาการของแต่ละคนไม่เหมือนกัน ไม่มีความชัดเจน ดังนั้นควรต้องมีการติดตามผลแบบมีลายลักษณ์อักษร
2. IT Organization control



คนกลุ่ม A เป็นประเภท programmer ซึ่งต้องให้ทำงาน programmer อย่างเดียว ห้ามไปทำงานที่อื่น โดยเฉพาะงานกลุ่ม B เพราะเป็นงาน operation โดยตรงของบริษัท ต้องแบ่งแยกหน้าที่ระหว่างกลุ่ม A และ B อย่างชัดเจนไม่อย่างนั้น ...อันตราย !!!!!!

Operations เช่น งาน Day end processing

Librarian = บรรณาธิการ Tap back up

Operations, Librarian, Data backup เป็นคนเดียวกันก็พอได้อยู่

Security admin กำหนดค่า parameter ต่าง ๆ ในระบบ

Database admin เป็นคนควบคุมค่าความปลอดภัยของ data

- **Development and Implementation Controls**


1. **Business Requirement** (Completely & Clearly)

**งานพัฒนาระบบสารสนเทศ สิ่งที่น่าเป็นห่วงมาก ๆ คือพัฒนาแล้วไม่ตรงกับความต้องการของ user ....เพราะฉะนั้นต้องควบคุมเรื่อง Business Requirement .ให้ดีจริง ๆ ดังนั้นต้องครบถ้วนและชัดเจน ระหว่าง user กับคนพัฒนาระบบต้องให้เข้าใจตรงกัน**

**Project manager ควรเป็น user ที่ต้องการ program นั้น ๆ ต้องการเปลี่ยนระบบอย่างไร user จะเป็นคนบอกความต้องการของตัวเองได้ดีที่สุด ....แต่ถ้าถามแล้วปรากฏว่า Project manager เป็น programmer เอง....X ผิดตั้งแต่แรกเลย**

**Audit Concern ⟶Prototyping เหมือนแบบบ้าน คือการเชิญ vendor มา present ถึงคุณสมบัติต่าง ๆ ของ program ใหม่ของเขา ว่าของเขามีดีอะไร แล้วสิ่งดีส่วนใดที่จูงใจให้บริษัทเราเปลี่ยนไปใช้ของเขา**

**⟶User Signoff ....ยืนยัน ...ไม่มีไม่ได้**

2. Feasibility Study : ศึกษาความเป็นไปได้ต่างๆ (Cost VS Benefit, Scoring, Agree Signoff)

**Audit Concern ⟶User agree and Signoff ⟶รับรองทางเลือกและลงนาม**

3. System Analysis and Design : พิมพ์เขียว ,Output Design(Screen/Report), Input Design, Process Design

**Audit Concern ⟶Documentation + User Signoff**

4. Coding Program ⟶ เป็นเรื่องของทีมพัฒนา

5. **Program Testing** (Unit Test, System Test, **User Acceptance Test - UAT**) ต้องทดสอบทุกหัวข้อที่ร้องขอไว้

**Audit Concern- ⟶UAT + User Signoff ...user ต้อง test ทุก scenario ให้ครบทุกเงื่อนไข และต้องมี test scrip ของการทดสอบตั้งแต่ข้อที่ 1 – 100 ของทุก ๆ Business requirement**

**User อาจจะดูแค่เรื่องประสิทธิภาพและประสิทธิผล แต่ auditor ต้องดูเรื่อง control, security และเรื่อง confidentiality บรรดา vendor มัดไม่ได้คิดเรื่อง control design แต่เราในฐานะ auditor ต้องดูเรื่อง control design ด้วย**

**Program ใดไม่ทำ UAT …….Finding ได้เลย**

6. Data Conversion

Audit Concern ⟶Reconciliation/Hash total Control (User จะต้องทำ Reconciliation เอง) Hash total control คือเวลาเขียน program จะใช้เลขฐาน 2 คือ 0, 1 โดยวิธีการคือของเดิมรวม Hash ได้เท่าไหร่ sum ยอดออกมาแล้วของระบบเก่าต้องได้เท่ากันกับเลขฐาน 2 ของระบบใหม่

⟶User Signoff

7. System Implementation

Audit Concern ⟶System Documentation

- Entities Relationship Diagram = ความสัมพันธ์การส่งข้อมูลแต่ละหน่วยงาน
- DFD : Data flow Diagram = ทางเดิน input-Process-output
- Data Dictionary = คู่มือบอกว่า Data 1 Record ประกอบไปด้วยอะไรบ้าง (แต่ละ field อยู่ตรงไหน)

⟶Training and Manual

8. Post Implementation Review :

**IT จะมีการบันทึกว่ามีปัญหาอะไรเกิดขึ้นบ้าง จะได้รวบรวมและแก้ไขต้นเหตุของปัญหา ในกรณีที่พบว่ามี change request เป็จำนวนมาก แล้วเป็นการขอในส่วนที่ user ต้องขออะไรใหม่ ๆ อยู่เสมอ มันน่าจะเป็นสัญญาณบอกว่าอาจจะมีปัญหาที่ user requirement เพราะขอไม่หยุดซะที ตอนเขียน BR ตอนแรกอาจจะเขียนไม่ครบตั้งแต่แรก ถ้า change request เจอ bug เยอะ ๆ แสดงว่ามีปัญญาตอน UAT**

**ทั้ง 8 ข้อที่ผ่านมาจะต้องเป็นระดับระเบียบปฏิบัติการพัฒนาระบบสารสนเทศ เวลาตรวจสอบถ้าดูแล้วไม่มีข้อใด....ให้ comment ได้เลย.....**

- **Maintenance of Existing System Control**


1. ตรวจโดยขอดูระเบียบปฏิบัติในการพัฒนาระบบสารสนเทศ
2. Changed detection program เป็นสิ่งที่ตรวจจับว่า program ใดมีการเปลี่ยนแปลงบ้าง ถ้า program เปลี่ยนจะรู้ทันที
3. หากมี program เพิ่มเติม, มีการเปลี่ยนแปลง program หรือมีการเปลี่ยนแปลงระบบอย่างมีสาระแล้วต้องมี change request เช่น ถ้ามีใครมาเตะระบบหรือ program ที่เกี่ยวกับเงิน ๆ ทอง ๆ การคำนวณดอกเบี้ย การโอนเงิน....ใครมาเตะต้องมีเหตุผล
4. ถ้ามีการเปลี่ยนแปลงเรื่องใดก็ตามต้องมีการทำ Change Request โดยเฉพาะอย่างยิ่งกรณีการเปลี่ยน program เป็นเรื่องสำคัญมากๆ เสี่ยงมากๆ ให้เทียบ source code ที่ละ record เลย

   **"All change to the source code should be related to the change request"**

   ⟶ต้องมีฟอร์ม change Request

   ⟶มีกระบวนการเขียน change Request (มี 4 ขั้นตอนละเอียด)

   ⟶Changed detection program – Update Data

   – Update Time

   – Update Size.

ธุรกิจธนาคาร แม้ว่าจะมีการแบ่งแยกหน้าที่ชัดเจนขนาดไหน..แต่ถ้า Programmer เล่นบอล Liverpool ...คนหน้าบ้านก็เล่นบอล Liverpool เหมือนกัน...อาจจะเกิดการฮั้วกันได้....

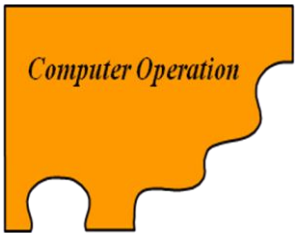
- **Information Security Control**


1. IT Security Policy and Procedure ต้องมีนโยบายความปลอดภัยและระเบียบปฏิบัติอย่างชัดเจน ควรทำเป็น checklist เพื่อกำหนดเรื่องที่ต้องมี ..ไม่มีไม่ได้ ...ทุกระบบงานต้องระบุความเป็นเจ้าของและหน้าที่ความรับผิดชอบอย่างชัดเจน, แจงลำดับชั้นความสำคัญของข้อมูล ระบุผู้ทำหน้าที่รักษาความปลอดภัยและความรับผิดชอบ, ผู้ใช้ได้รับการฝึกด้านความปลอดภัย, ลิขสิทธิ์, ไวรัส, ทักษะของผู้ใช้

2. User Access Control Feature (การเข้าถึงข้อมูลระบบงาน) กำหนด 1 user : 1 ID, Password Control (0-8 หลัก, อายุ 30 – 90 วัน, Invalid sign-on 3-5 ครั้ง, การสแกนม่านตาหรือนิ้วมือ, การกำหนดสิทธิ์ใช้งานเท่าที่จำเป็น (Based on as need basis)


3. ผู้ใช้ request form on procedure
4. การเก็บ Logging and Monitoring : บางระบบจะต้องตั้งไว้ว่าถ้า user ไม่เข้าระบบเกิน 90 วัน แล้วให้ temporary distribute และควรออกรายงานด้วย หรือกรณีใครพยายาม sign in ระบบแล้วผิดบ่อย ๆ ...ควรรายงาน
5. ความปลอดภัยทางด้านกายภาพ เช่น ห้องคอม, สถานที่ = Low Profile, เข้าได้เฉพาะ Staff ที่ทำงานในนั้นเท่านั้น. ตรวจจับควัน, ความร้อน, ไฟ, ยกพื้นสูง (ใช้เดินสายไฟและแอร์) พริ้นเตอร์ไม่ควรอยู่ในห้อง, ถังดับเพลิง สาร FM200 (แทนฮารอน ซึ่งทำลายสิ่งแวดล้อม)

- **Computer Operation Control**




1. **Key :** คู่มือและขั้นตอนปฏิบัติ, Operation Schedule / Timetable, การ Control Procedure ไม่ให้ข้ามหรือทำซ้ำ

**Concern: การทำงานต้อง run on schedule เท่านั้น การควบคุมคือมีใครคอย monitor หรือไม่ว่า process ทั้งหมดยังคง run ไปตาม schedule ที่ควรเป็น**

2. Define Service Level Agreement (SLA), Data back-up procedure (วัน, เดือน, สัปดาห์)
3. การ Recovery from Operation Failure, กำหนดแผนกู้ระบบ IT : Disaster and Recovery Plan (DRP) – เขียนแผนทดสอบ , ทดสอบ (Test) อย่างน้อยปีละ 1 ครั้ง และแผนปรับปรุงให้ทันกาล (update)

**Concern: DRP เขียนเป็นลายลักษณ์อักษรหรือยัง จะคิดว่าเป็นอับดุลตลอดเวลาไม่ได้นะคะ ต้องเขียนเป็น paper ชัดเจน ...เวลาเกิดความเสียหาย..อับดุล..ไม่อยู่ตอบคำถามหรอกนะ**

**ถ้ามีแผนแต่ไม่ Test….ไร้ประโยชน์....สำหรับการ test ถ้าไม่ full test บริษัทจะต้องรับผิดชอบความเสี่ยงเอง..คำถามต่อ..บริษัทจะรับต้นทุนได้ไหม**

**3. Application Control มีวัตถุประสงค์ 4 ประการ คือ (CAVR)**

1. **C**ompleteness ⟹ ให้ความมั่นใจในความสมบูรณ์ของข้อมูลที่วิ่งไป
2. **A**ccuracy ⟹ ถูกต้องตรงกันทุกประการ
3. **V**alidity ⟹ ความสมเหตุสมผล
4. **R**estricted Access to Date and Physical Assets ⟹ จำกัดการเข้าถึงข้อมูลและสินทรัพย์

**CAVR ทำโดยการควบคุมข้อมูล** ⟹ ข้อมูลนำเข้า (Input Control) วิธีการ ที่มา และความถูกต้อง
⟹ การประมวลผล (Processing Control)
⟹ ข้อมูลผลลัพธ์ (Output Control)

**คำถาม: การควบคุมใดที่สามารถทดแทนได้ด้วย General control….ตอบ.Process control**

**คำถาม: ระหว่าง input, process, output สิ่งใดสำคัญที่สุด...ตอบ Input สำคัญสุด**

****เจ้าหน้าที่ print cheque สามารถเปลี่ยนแปลงแก้ไขข้อมูลได้หรือไม่....ลองไปตรวจสอบดู

ควบคุมความผิดพลาดในการป้อนข้อมูล (นับวัน, จำนวนเงิน), ใช้แบบฟอร์มที่กำหนด (ไม่ซ้ำ, การยกเลิกและปรับปรุง)

ตัวอย่างการควบคุมความถูกต้องของรายการข้อมูลโดยทั่วไป ได้แก่

- Limit Check – จำกัดวงเงินในการถอนจากตู้ ATM
- Range Check – ข้อมูลอายุของลูกค้าที่ตั้งไว้ เช่น 15 – 80 ปี
- Sequence Check – เลขที่ใบเอกสารที่ไม่ควรซ้ำหรือว่างไว้ได้
- Check digit verification – การเช็คคำนวณตัวเลขหลักสุดท้ายบัญชีธนาคาร

**7. Computer Assist Audit Techniques (CAATs) เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ ใช้ในการตรวจเพื่อหาสาระในเชิงลึก (Substantive Test) มี 5 เทคนิค**

1. GAS หรือ Generalized Audit Software : เช่น ACL การใช้โปรแกรมประยุกต์ช่วยในการตรวจ การใช้ GAS มีข้อดี เช่น ประหยัดเวลา, โปรแกรมไม่ซับซ้อน, มีชุดคำสั่งประมวลแบบพื้นฐาน เช่น การจัดชั้นลูกหนี้ สินค้าคงคลัง และการคิดค่าเสื่อมราคาสะสม เป็นต้น ประมวลผลข้อมูลได้ครั้งละมาก ๆ ตามที่ต้องการ เหมือนรถบรรทุก บรรทุกได้คราวละมาก ๆ แต่ขับเร็วไม่ได้, นำกลับมาใช้ได้ อ่านข้อมูลได้หลายแบบ แต่การคำนวณที่ซับซ้อนทำไม่ได้
2. Custom Audit Software : IA เขียนหรือพัฒนาขึ้นเอง เพื่อนำมาเปรียบเทียบกับ รายงานที่ประมวลผลโดยระบบตามที่ต้องการทดสอบ หมายถึง นำ input มาใส่ใน program ตรวจสอบแล้วเปรียบเทียบผลกับรายงานของ user
3. Test Data : เป็นการตรวจ program โดยใช้ data ของเราใส่เข้าไปใหม่ เพื่อยืนยันว่า program ถูกหรือไม่ หรือมีจุดผิดตรงที่ใดของ program การใส่ข้อมูลเข้าไปในระบบงานจริง แล้วรอดูว่าระบบจะประมวลผลออกมาอย่างไร (ผิด หรือ ถูก), Test Script ทำได้ทีละคำสั่ง IA ควรศึกษาระบบงานให้

เข้าใจโดยละเอียด, การ Test Data มักใช้เมื่อมีการเปลี่ยนแปลงแก้ไขโปรแกรม, ข้อมูลที่นำไปทดสอบต้องไม่นำไปปนกับข้อมูลจริงที่องค์กรใช้งานอยู่ (Production), ไม่จำเป็นต้องใช้ข้อมูลทดสอบมาก, เพื่อความรวดเร็วในการวิเคราะห์ผล สรุปผลรวมทั้งข้อเสนอแนะต่าง ๆ เช่น Three way matching ลองใส่ข้อมูล invoice ที่ผิดแล้วลองดูว่าใส่เข้าไปแล้วมี exception report ออกมาหรือไม่

ทั้งนี้การทดสอบดังกล่าวต้องขึ้นอยู่กับความสามารถของผู้ตรวจสอบด้วยว่าเก่งในการคิด scenario ที่แปลก ๆ ได้ขนาดไหน

4. Integrated Test Facility (ITF) ทำบน Production Environment เป็นการตรวจการปฏิบัติการงานของ Functions ต่าง ๆใน Computer Application โดย IA ต้องจัดเตรียม Test Data และผลลัพธ์ไว้ล่วงหน้า, การตรวจทำไปพร้อมกับ Production Run โดยใช้ Dummy Entity และ ITF Data จะถูกแยกจาก Control Report ในงานประจำ สามารถทำได้ตลอดเป็นปี ๆ ก็ได้, เหมาะกับระบบงานที่ IA มีส่วนร่วมในการพัฒนาก่อนใช้งานจริง, ใช้ตรวจรับระบบงานจริงที่ใช้อยู่แต่มีการแก้ไข

5. Concurrent Auditing Techniques (ตรวจข้อมูลที่เกิดขึ้นในระบบงาน โดยเราเขียน Script เข้าไปในระบบ)

- เขียน Script คำสั่งเข้าไปในระบบ (แต่เมื่อ Test เสร็จต้องออกจากระบบด้วย) ⇨ Snapshot
  เช่น ถ้ามีการถอนเงินเยอะ ๆ ในช่วงเลือกตั้ง..หรือแลกเงินแบงก์พันเป็นแบงก์ร้อยเยอะ ๆ ให้ดึงข้อมูลออกมา
- ต้องมีการตั้งเงื่อนไขให้มากขึ้น จนกระทั่งมั่นใจว่าเป็นข้อมูลที่ผิดปกติจึงมีการ Report หรือ Warning ⇨ SCARF
- เป็นระบบขนาดใหญ่ที่มีความฉลาดสามารถตัดสินใจได้ ⇨ Expert System
  เช่น ดูพฤติกรรมการบริโภคแปลก ๆ เช่น บัตรเครดิต ถ้าปกติลูกค้าคนนี้ใช้ซื้อของ Lotuses Big C เป็นปกติ อยู่มาวันหนึ่งไปซื้อทองซื้อเพชร...reject รายการก่อน...ทั้งนี้จะ reject ทันทีหรือไม่ขึ้นอยู่กับนโยบายของบริษัทด้วย เพราะบางทีอาจจะทำให้ลูกค้าไม่ปลื้มก็ได้...