การบริหารความเสี่ยงด้านไอซีที

ICT Risk Management

Agenda

- Health Check
  - Threat
  - Organization and process
  - Continuity
- Enterprise Risk management
- ICT Risk Management

ปัญหาที่พบบ่อยๆ

ERM Defined:

"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.
(Committee of Sponsoring Organizations of the Treadway Commission)

WHAT IS COSO ?

COSO = COmmittee of Sponsoring Organizations

- **American Accounting Association (AAA)**
- **American Institute of CPAs (AICPA)**
- **Financial Executives Institute (FEI)**
- **The Institute of Internal Auditors (IIA)**
- **The Institute of Management Accountant (IMA)**

WHAT IS COSO ?

- *ความเป็นมา*
- สืบเนื่องจากวิกฤตทางการเมืองและเศรษฐกิจของสหรัฐอเมริกาในช่วงปี ค.ศ.1970 จนในปีค.ศ.1977 สหรัฐฯได้ประกาศกฎหมายแนวปฏิบัติเกี่ยวกับความไม่สุจริตในการให้สินบนต่างชาติ (the1977 Foreign Corrupt Practices Act – FCPA)ซึ่งส่วนสำคัญส่วนหนึ่งกำหนดให้มีการควบคุมภาย ต่อมาเดือนตุลาคม ค.ศ.1985 มีการจัดตั้งองค์กรอิสระ คือ คณะกรรมการเพื่อการรายงานการทุจริตแห่งชาติ (National Commission on Fraudulent Financial Reporting หรือเรียกย่อ Treadway Commission เพื่อให้เกียรติ Mr.Stephen R Treadway ผู้ก่อตั้งซึ่งตีพิมพ์รายงานครั้งแรกในปี ค.ศ. 1987 ภายใต้การสนับสนุนของคณะกรรมการวิชาชีพอิสระอื่น ๆที่ต่อมาเรียกว่า The Committee of Sponsoring Organization of the Treadway Commission (COSO)

http://en.wikipedia.org/wiki/COSO#Key_concepts_of_the_COSO_framework

Why ERM Is Important

Underlying principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

Why ERM Is Important

ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

ความเสี่ยงเป็นความจำเป็นของทุกองค์กร – เป็นหน้าที่ของทุกคนในองค์กร – ต้องมีความสอดคล้องทั้งแผนกลยุทธ์และแผนบริหารความเสี่ยง – มีความเชื่อมโยงและส่งผลถึงกันในทุกกิจกรรม – วัฒนธรรมองค์กรต้องสอดรับ - ปรับเปลี่ยนตามสภาวะการณ์ที่เปลี่ยนแปลง

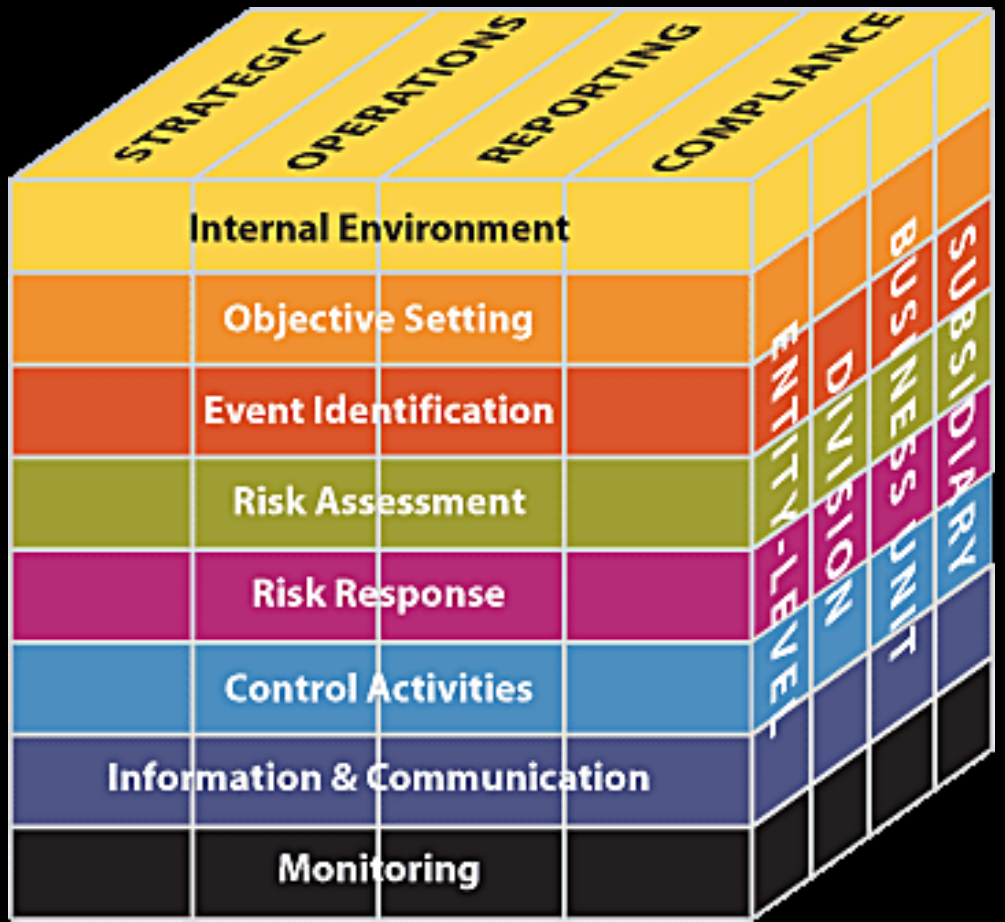
Enterprise Risk Management — Integrated Framework

This COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

Secure by design not accident

The ERM Framework

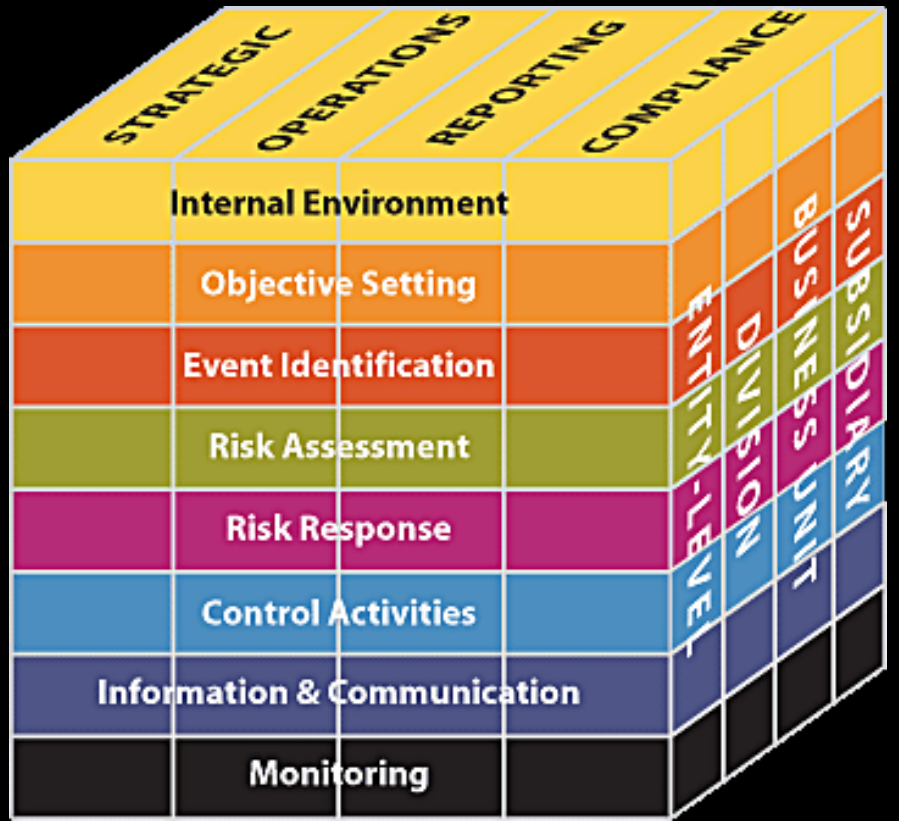
- Entity objectives can be viewed in the context of four categories:
  - Strategic
  - Operations
  - Reporting
  - Compliance



The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes



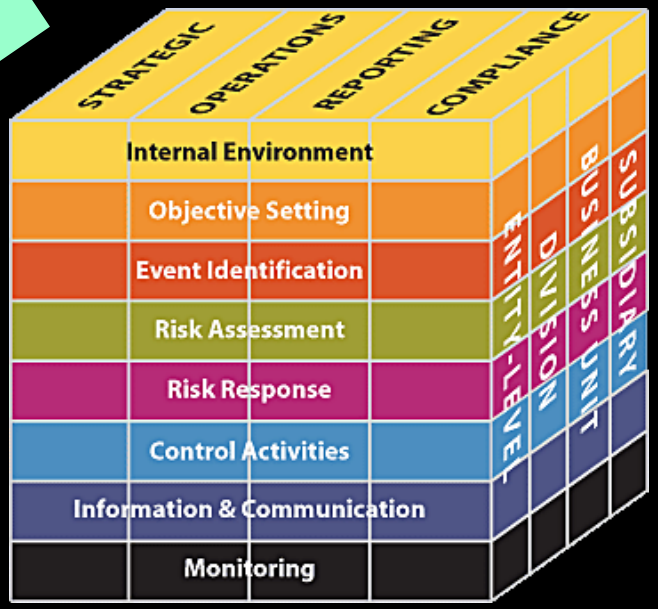
The ERM Framework

Enterprise risk management requires an entity to take a *portfolio view* of risk.

- Management considers how individual risks interrelate.
- Management develops a portfolio view from two perspectives:
  - Business unit level
  - Entity level

The ERM Framework

วัตถุประสงค์
• ระดับกระบวนการ



- สภาพแวดล้อมภายใน
- การกำหนดวัตถุประสงค์
- การระบุเหตุการณ์เสี่ยง
- การประเมินความเสี่ยง
- การจัดการความเสี่ยง
- ออกแบบกิจกรรมควบคุม
- สารสนเทศและการสื่อสาร
- การติดตามผล

The eight components of the framework are interrelated …

วัตถุประสงค์ ระดับองค์กร

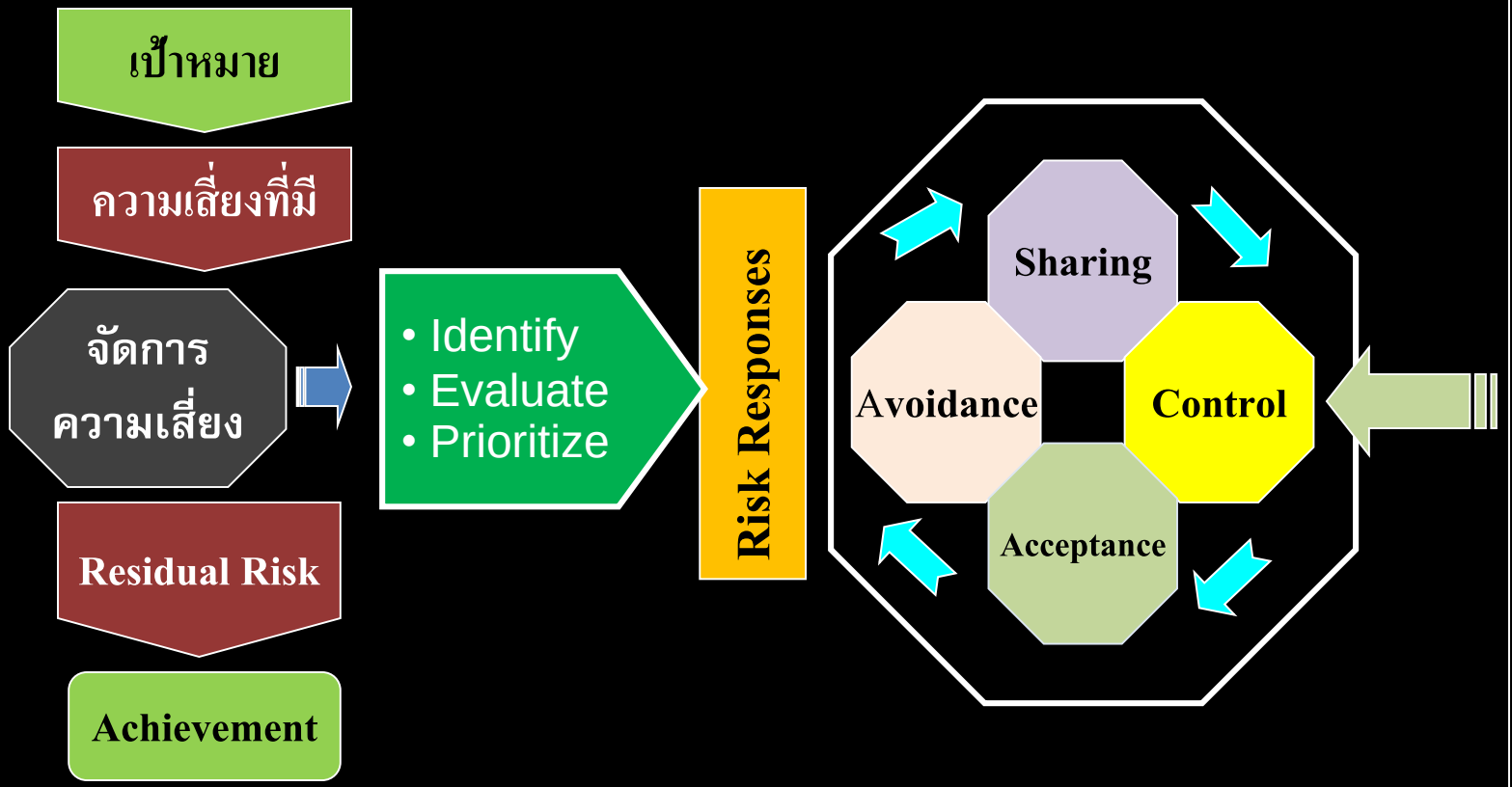
Internal Control

A strong system of internal control is essential to effective ERM.

Key Implementation Factors

- Organizational design of business
- Establishing an ERM organization
- Performing risk assessments
- Determining overall risk appetite
- Identifying risk responses
- Communication of risk results
- Monitoring
- Oversight & periodic review by management

การบริหารความเสี่ยง



Existing COSO ERM Challenges

- ERM Across the enterprise but silo measurements (strategic goals and risk goals)
  - COSO provide little guidance on how to design and execute an effective ERM framework.
  - COSO does not define a methodology for measuring risk.

ERM – "A Methodology for Achieving Strategic Objectives" by Gregory Monahan, SAS Consultant

- Know strategic objectives and metrics
- Know risk profile
- Know methodology
  - Set –metrics
    - Strategic objective metrics
    - Risk driver metrics
      - Key risk indicators (KRIs) –or early warning indicators (EWIs) -leading indicators – เป็น proactive activities เพื่อช่วยลด impact
    - Control metrics
  - Observe metric values
  - Analyze metric values
  - React

Enterprise Risk Management

- Strategic Objectives and Metric
  - Financial / Market / Operational

finanacial	objectives	metric
position	ROA	Profit/assets
	ROE	Profit/equity
	Increase assets	Total assets
performance	Total shareholder return	Growth in share value
	Increase revenue	revenue
	Price/earnings ratio	Share price/earnings per share

Enterprise Risk Management

- Strategic Objectives and Metric
  - Financial / Market / Operational

market	objectives	metric
customers	Increase mkt share	Firm's sales/total mkt sales
	Be rated no 1 in customer service	Customer service survey result
suppliers	Increase supply chain efficiency	Amount saved through revenue-sharing contracts
	On-time delivery	Number of deliveries within n minutes of schedule
competitors	Offer a substantially different product	Points of differentiation
partners	Build strategic partnerships	Monetary value of joint business with partner

Enterprise Risk Management

- Strategic Objectives and Metric
  - Financial / Market / Operational

operational	objectives	metric
Corporate governance	Publish accurate financial statements	Number of negative findings by auditors
	Protect the organization against internal fraud	monetary value of losses due to internal fraud
Human resources	Increase employee satisfaction	Staff satisfaction survey results
Management team	Raise the quality of the management team	Analyst ratings
processes	Reduce process times	Average process time
systems	Operate systems that are more user friendly	User friendliness survey

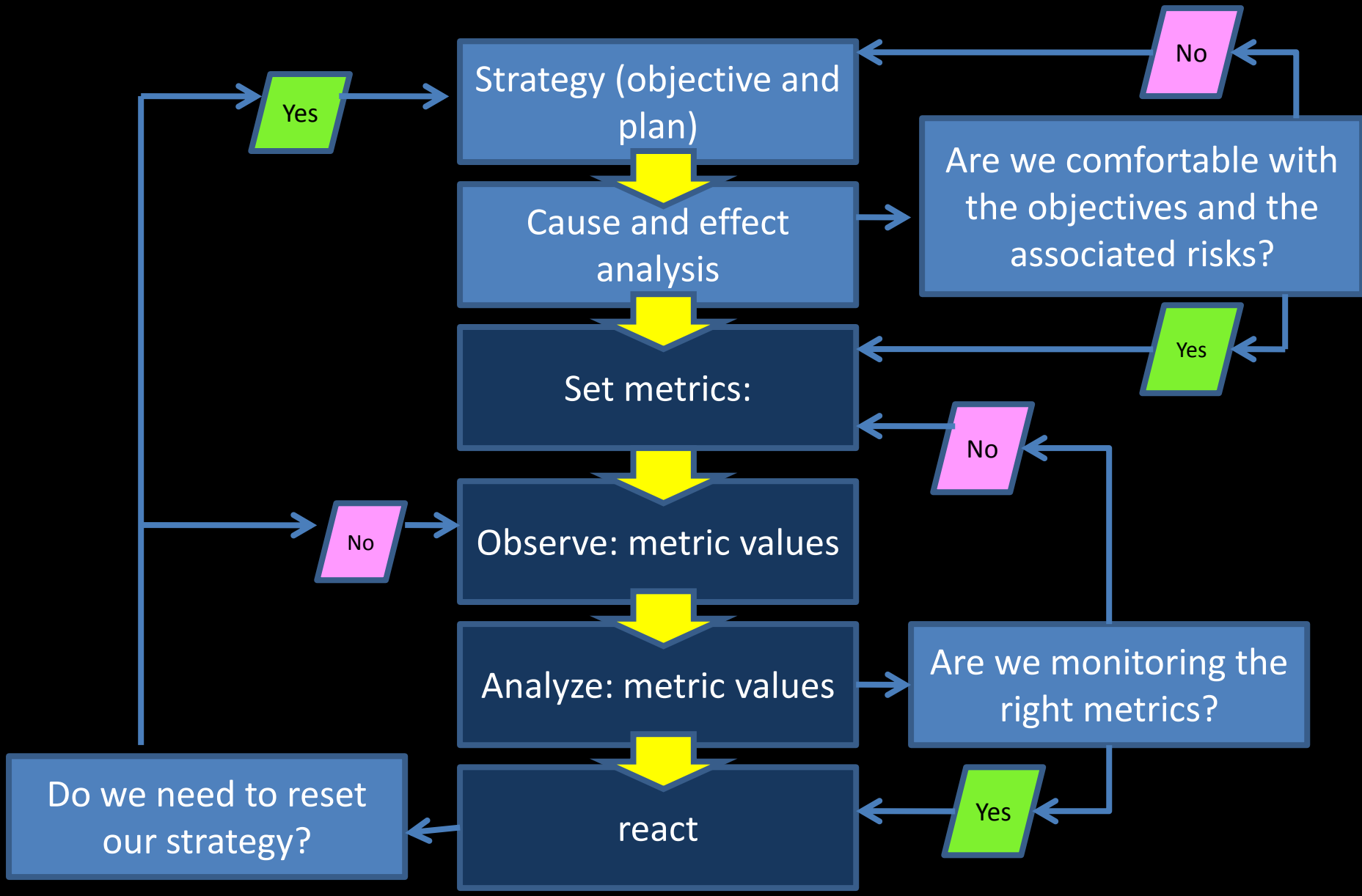
Enterprise Risk Management

- Set –metrics
  - Strategic objective metrics
    - Business outcomes / financial, market and operational
  - Risk driver metrics
    - Key risk indicators (KRIs) –or early warning indicators (EWIs) - leading indicators – เป็น proactive activities เพื่อช่วยลด impact
  - Control metrics
    - Day-to-day guarantee / reduce impact or severity of an event i.e. insurance (well conceived/designed and executed)
    - risk mitigation strategies

ERM – A Methodology for Achieving Strategic Objectives

- Know methodology
  - Set –metrics
    - Strategic objective metrics
    - Risk driver metrics
      - Key risk indicators (KRIs) –or early warning indicators (EWIs) - leading indicators – เป็น proactive activities เพื่อช่วยลด impact
    - Control metrics
  - Observe metric values
  - Analyze metric values
  - React

Strategic Objective At Risk (SOAR) by Gregory Monahan



Risk management Guide for IT Systems

1. Integration of risk management into SDLC
   - Initiation
   - Development or acquisition
   - Implementation
   - Operation or maintenance
   - Disposal
2. Risk management
   - Risk assessment
   - Risk mitigation
   - Evaluation and assessment

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Matrix of Risk Level (Risk Map)

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Matrix of Risk Level (Another Firm)

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

IT Risk

Turning Business Threats into Competitive Advantage

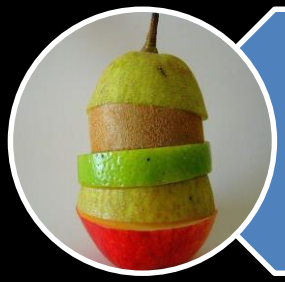
Harvard Business School Press

IT Risk – Turning Business Threats into Competitive Advantage – HBSP

- The 4A Risk Management Framework
  - Availability
    - Keep the systems and business processes running, and recover from interruptions
  - Access
    - Ensure appropriate access
    - Potential for misuse of sensitive information
  - Accuracy
    - Provide correct, timely and complete information that meets stakeholders' requirement
  - Agility
    - Posses the capability to change with managed cost and speed

3 Core Disciplines of IT Risk Management

A well-structured foundation of IT assets



A well-designed and executed risk governance process

A risk-aware culture

Key IT Risk Factors

- Availability
  - High IT staff turnover
  - Infrastructure not standardized
  - Ineffective patch/upgrade management
  - Old technology
  - Poor backup/recovery
  - Poorly understood processes and applications
  - Missing skills for new initiatives
  - Regulators would find deficiencies

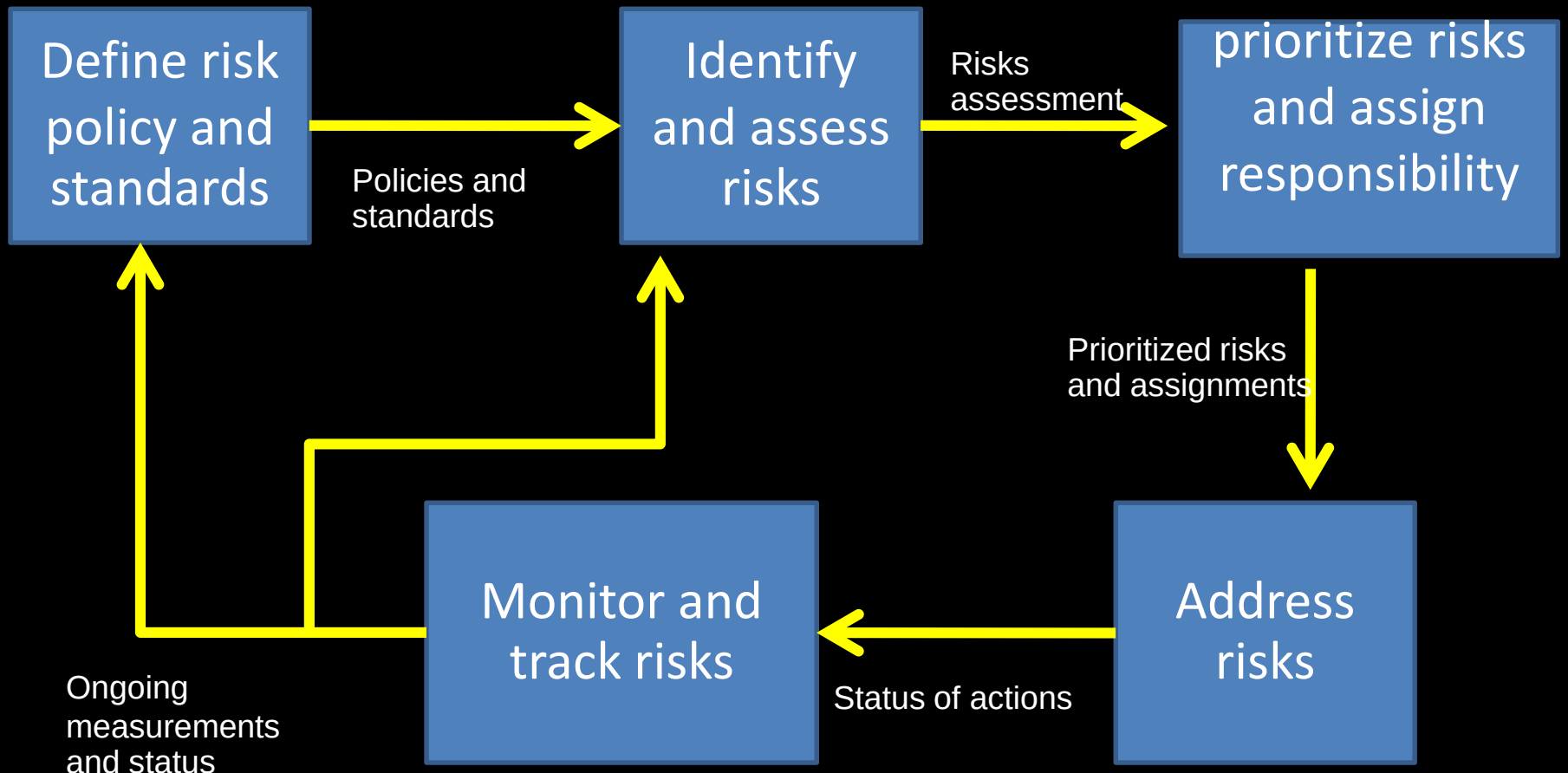
Key IT Risk Factors

- Access
  - Data not compartmentalized
  - Applications need standardization
  - Lack of internal controls in applications
  - Network not reliable at all locations

Key IT Risk Factors

- Accuracy
  - Applications do not meet business requirement
  - Manual data integration required
  - Significant implementation under way or recently completed
- Agility
  - Poor IT-business relations
  - Poor project delivery

IT Risk Governance process



Source: Gartner

ตัวอย่างการดำเนินการ

ของสำนักงาน

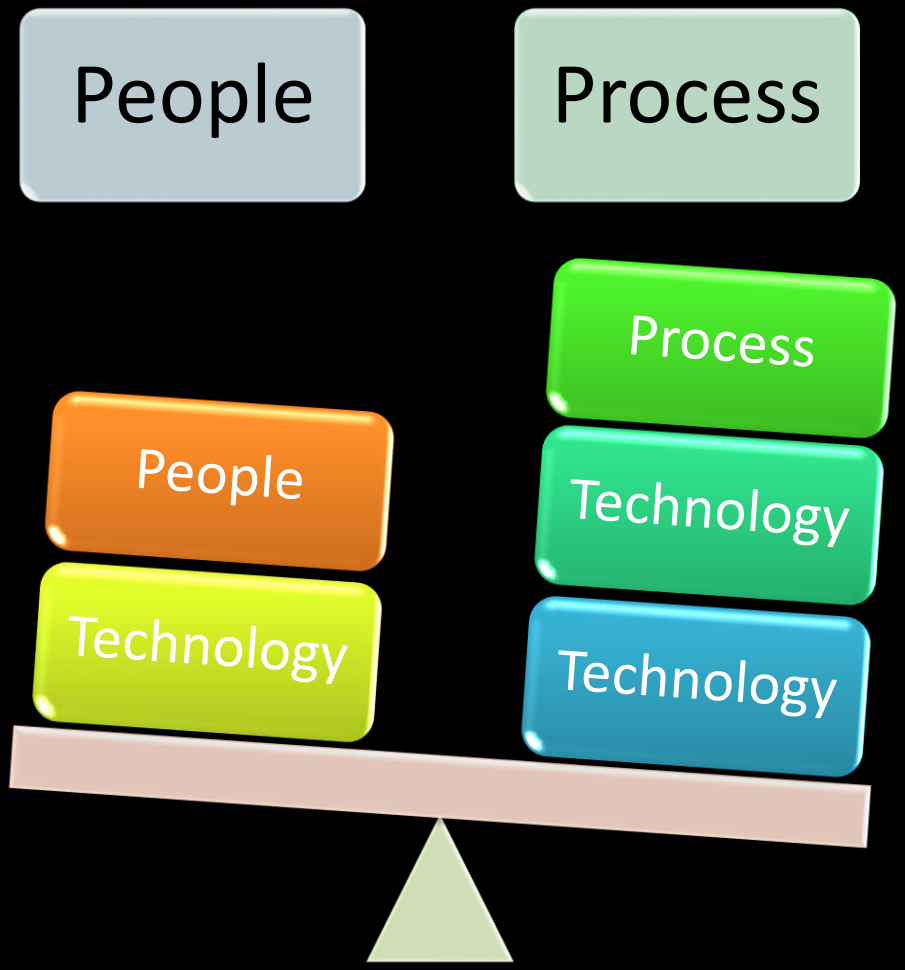
ต้องมีการบริหารจัดการ

People

Process

Technology

ต้องสร้างสมดุล



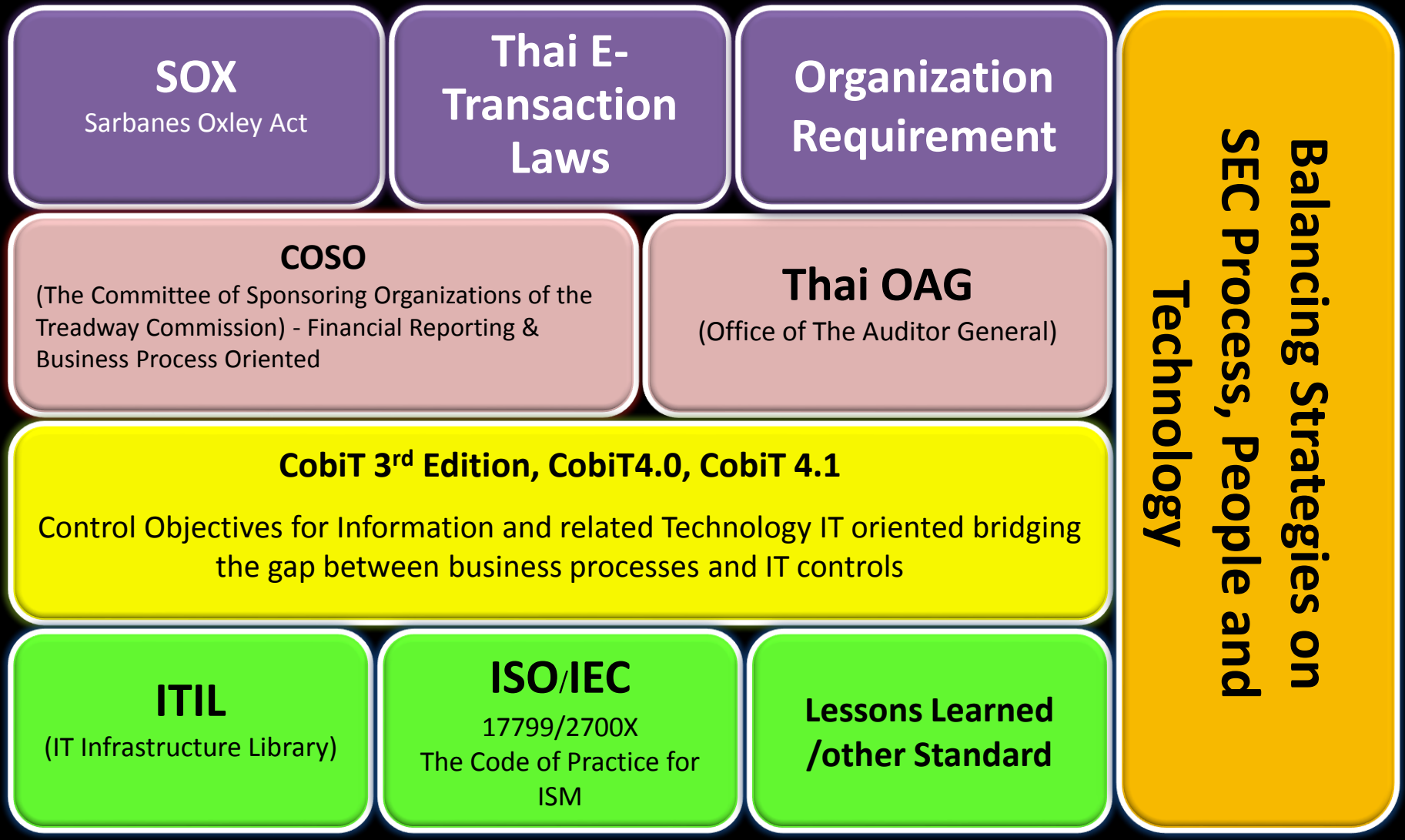
ความคาดหวัง

- สร้างภูมิคุ้มกันให้กับองค์กร ไม่เกะกะระรานระบบคนอื่น
- งานบริการราบรื่น และ **achieve** เรื่อง **CIA**
- ช่วยให้พนักงานรู้เท่าทันภัย ไม่ถูกหลอก
- ช่วยลดค่าใช้จ่ายในการเยียวยาความเสียหาย
- เพิ่ม **productivity** ของคนและองค์กร
- ลดความเสี่ยงจากภัย และการปฏิบัติผิด กม
- สร้างความเชื่อมั่นให้กับองค์กร / พนักงาน

How - ทำอย่างไร

- พัฒนากรอบแนวคิด – **Develop GRC Framework**
- **PDCA – Plan Do Check Act**
  - **Security Assessment**
  - **Develop Policies / Procedures**
  - **Adopt Technology / Streamline Process**
  - **Conduct Self Audit / External Audit**
  - **Review / Improve PPT related**
  - **Repeat PDCA**

SEC IT GRC Framework



Simplified How ?

SEC E-Policy

- Security Policy
- Storage Policy / Information Policy
- Email Policy
- Password Policy
- Net Surfing Policy
- Organizational Policy (Segregation of Duty)
- Social Networking Tools Policy

Work Procedures

- Develop guidelines / check lists / forms / procedures as applicable
- Conduct in-house CobiT training
- Improve internal communication through intranet
- Provide remote / mobile work environment
- Improve process by adopting CobiT Framework
- Built in internal control (adopt risk base approach)

Practicality

Testing : Methodologies and practices

Vulnerability assessment (VA) :regularly perform vulnerability assessments to identify and assess security vulnerabilities in their systems and processes

Scenario-based testing : resumption and recovery plans should be subject to periodic review and testing.

Penetration tests. should carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes.

Red team tests. should challenge their own organisations and ecosystems through the use of so-called red teams to introduce
an adversary perspective in a controlled setting.

Drill Test Scenario

1. หลอกว่าเป็น Email จากคนที่น่าเชื่อถือ
2. เขียนข้อความให้ Click Link โดยซ่อน Hyperlink และให้ไปที่ website ของ Hacker
3. Website Hacker ทำหน้าจอ authen ที่เหมือนกับที่สำนักงานใช้ และหลอกให้ user ใส่ login/password

ตัวอย่าง Drill Test

Scenario #1

ทดการโดยสมมุติว่า Hacker อยู่ในกลุ่มที่คาดว่ารู้เรื่อง Cyber Security เป็นอย่างดี กลุ่มเป้าหมายได้แก่ กลุ่ม IT และกลุ่มที่ทำงานร่วมกับ IT อย่างต่อเนื่อง โดยหลอกใช้ Email ที่กลุ่มมีกิจกรรมร่วม ให้ click Link

Scenario #2

ทดสอบโดยสมมุติว่า Hacker เป็นคนในสำนักงาน โดยจะให้ Email ที่ส่งเวียนทั้งสำนักงาน ส่ง
Email

Scenario #3

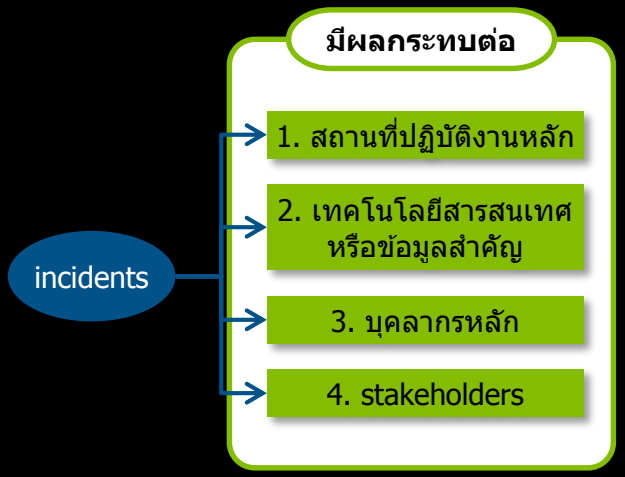
ทดสอบโดยสมมุติว่า Hacker เป็น บุคคลภายนอก ใช้ Email ที่สำนักงานส่งระบบข่าวให้กับบุคคลภายนอก ซึ่งมาจากระบบ E-subscribe

ตัวอย่าง Drill Test

ผลการส่ง Email ไปยังกลุ่มเป้าหมาย 447 คน นับจาก
(ซึ่งจะรวมกลุ่มเป้าหมาย Scenario#1 และ Scenario#2 ด้วย)
ผลของการทดสอบนี้สามารถหลอกให้ป้อน password ได้ 81 คน
สรุปผลการทดสอบตามตารางนี้

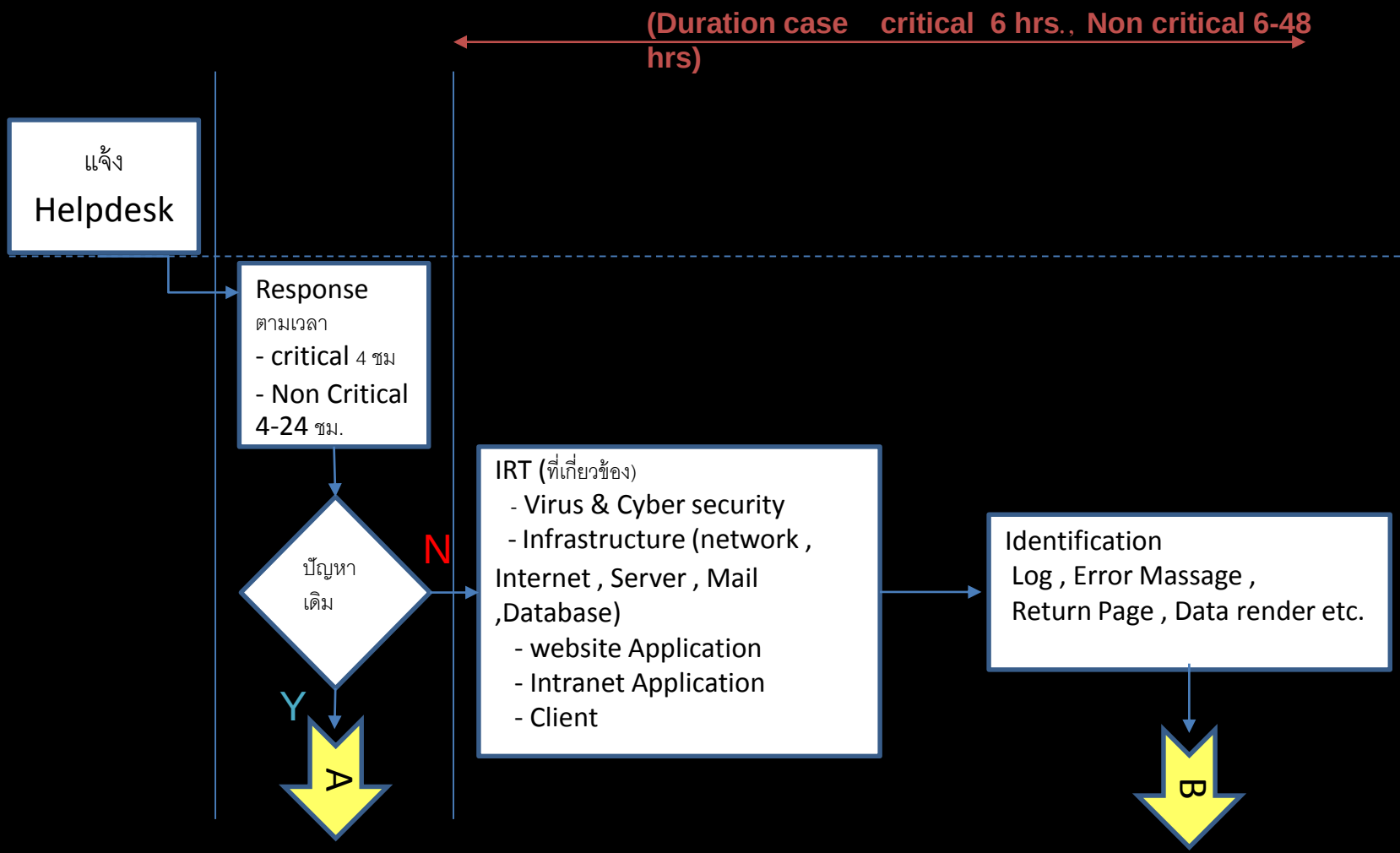
	จำนวน target	ผู้ที่ป้อน
scenario 1	35	10
scenario 2	20	2
scenario 3	447	69
	รวม	81

ตัวอย่างของสำนักงาน กลต.
การประเมินผลกระทบ (จาก บูรณาการ BCM)

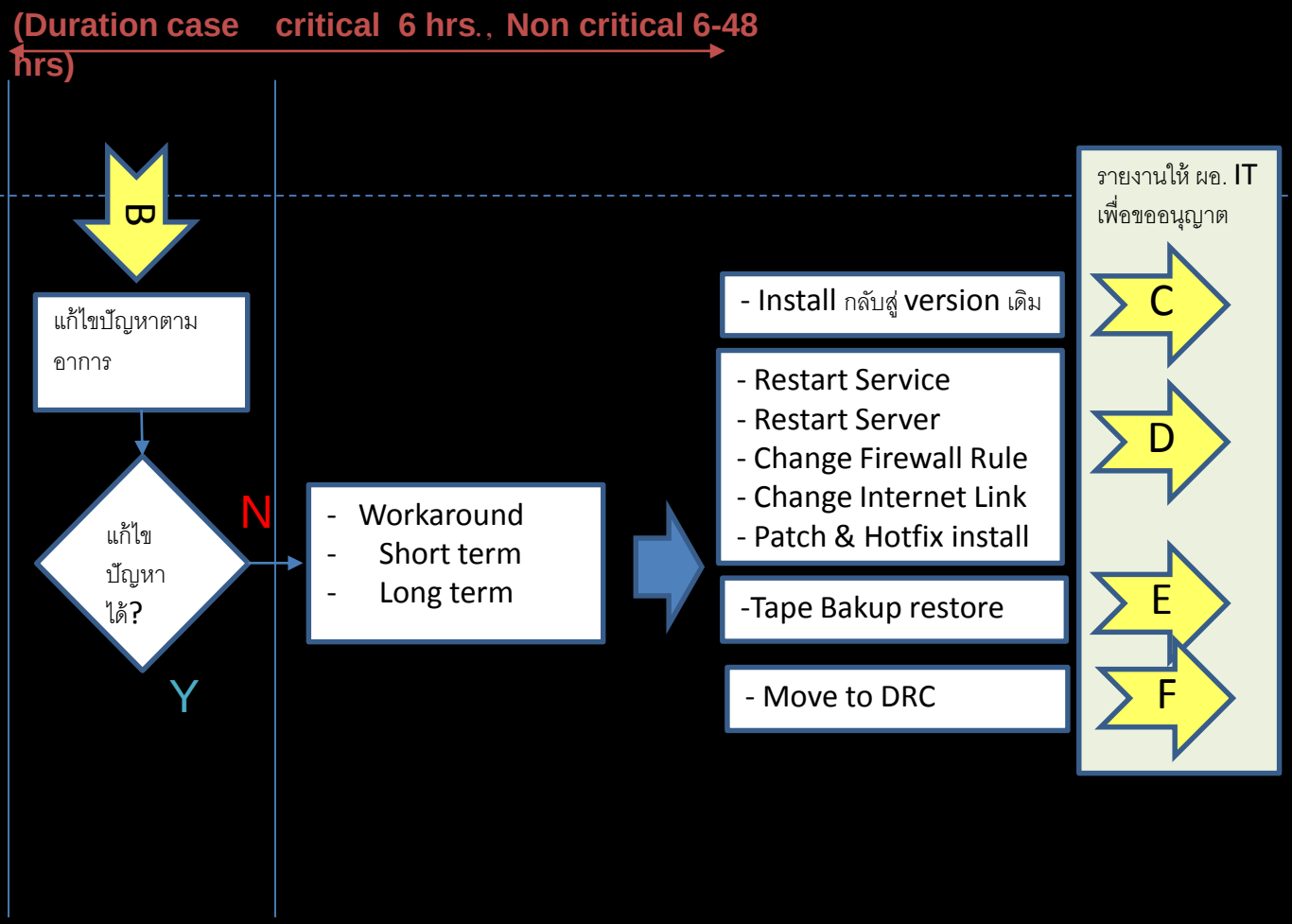


incident	ผลกระทบ			
	สถานที่ปฏิบัติงานหลัก	เทคโนโลยีสารสนเทศหรือข้อมูลสำคัญ	บุคลากรหลัก	stakeholders
อัคคีภัย	✓	✓	✓	
แผ่นดินไหว	✓	✓	✓	✓
อุทกภัย	✓	✓	✓	✓
จลาจลหรือชุมนุมประท้วง	✓	✓	✓	✓
โรคระบาด	✓		✓	✓
ก่อการร้าย			✓	
cyber attack		✓		✓
ข่าวกระทบ market				✓

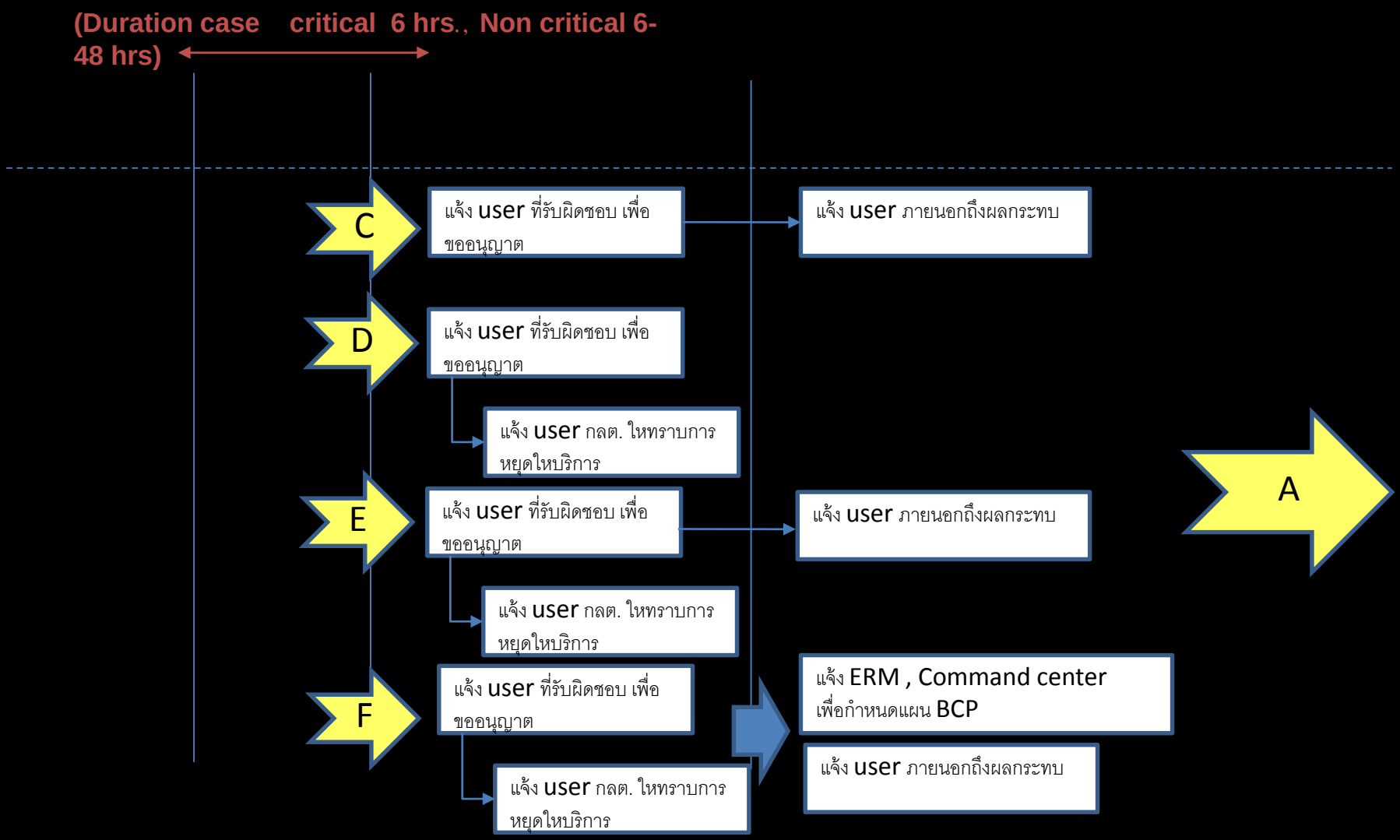
ตัวอย่าง Incident response



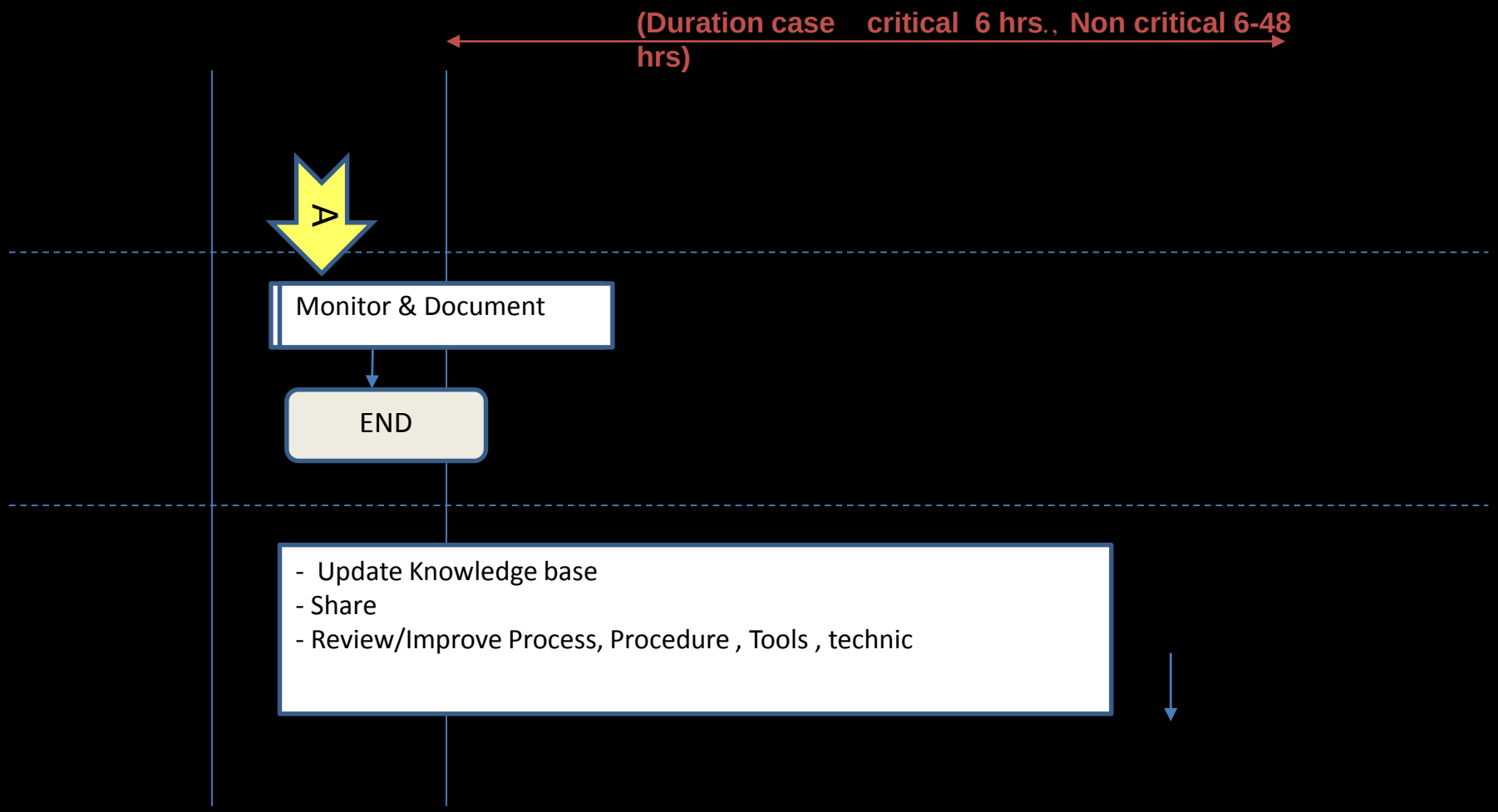
ตัวอย่าง Incident response



ตัวอย่าง Incident response



ตัวอย่าง Incident response




ตัวอย่างการดำเนินการ
กับบริษัทหลักทรัพย์

บทบาทหน้าที่ของ ก.ล.ต.

การกำกับดูแลบริษัทหลักทรัพย์

Risk-Based Approach ของ บล.

ความเสี่ยงของ บล.

- **ความเสี่ยงด้านฐานะการเงิน (prudential risk)**
- **ความเสี่ยงด้านประสิทธิภาพของระบบปฏิบัติงาน ระบบควบคุมภายใน และการป้องกันความเสี่ยง (control risk)**
- **ความเสี่ยงที่ บล. อาจสร้างความเสียหายให้แก่ลูกค้า (consumer relationship risk)**
- **ความเสี่ยงด้าน IT ของ บล. (information technology risk)**
- **ความเสี่ยงที่เกิดจากการประกอบธุรกิจ หรือใช้กลยุทธ์ไม่เหมาะ (business risk)**

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

Access Risk

- บุคคลไม่มีอำนาจสามารถเข้าถึง
- บุคคลมีอำนาจแต่ไม่สามารถเข้าถึง

Integrity Risk

- ความไม่ถูกต้องครบถ้วนของข้อมูล
- ระบบทำงานไม่ถูกต้อง

Availability Risk

- ไม่สามารถใช้งานระบบ/ข้อมูล ได้อย่างต่อเนื่องในเวลาที่ต้องการ

Infrastructure Risk

- ระบบคอมพิวเตอร์/บุคลากร ไม่เพียงพอ
- ขาดระบบการบริหารจัดการที่ดี
- ขาดการควบคุมภายในที่เหมาะสม

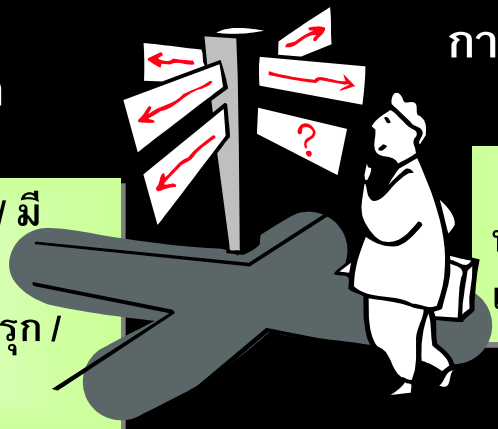
แนวทางการกำกับดูแล บล. ด้านเทคโนโลยีสารสนเทศ

โครงสร้างหน่วยงานและการบริหารจัดการ

แบ่งแยกหน้าที่ให้ชัดเจน เพื่อป้องกันการทุจริต/ทำงานผิดพลาด / กำหนดนโยบาย แผนงาน และขั้นตอนการปฏิบัติงาน / มีการรายงานและการตรวจสอบการปฏิบัติงาน

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์

ควบคุมการเข้าออกศูนย์คอมพิวเตอร์ / มีระบบป้องกันความเสียหายจากภัยต่าง ๆ / กำหนดสิทธิผู้ใช้งาน / ระบบป้องกันการบุกรุก / การตรวจสอบอย่างสม่ำเสมอ



การสำรองข้อมูลและระบบงาน และการจัดทำแผนสำรองฉุกเฉิน

มีระบบการสำรองและทดสอบการนำกลับมาใช้ / จัดทำแผนสำรองฉุกเฉินและทดสอบแผน

การควบคุมการพัฒนา แก้ไข เปลี่ยนแปลงระบบงาน

การพัฒนา แก้ไข เปลี่ยนแปลงระบบต้องได้รับความเห็นชอบ / เน้นการทดสอบก่อนใช้งานจริง / มีการสอบทานว่าเป็นไปตามกฎระเบียบ / มีเอกสารประกอบระบบ

การปฏิบัติงานประจำของศูนย์คอมพิวเตอร์

มีคู่มือขั้นตอนการปฏิบัติงานที่ชัดเจน / กำหนดสิทธิอย่างเหมาะสม / มีระบบการรายงานและตรวจสอบอย่างสม่ำเสมอ


kumpol@secdotordotth