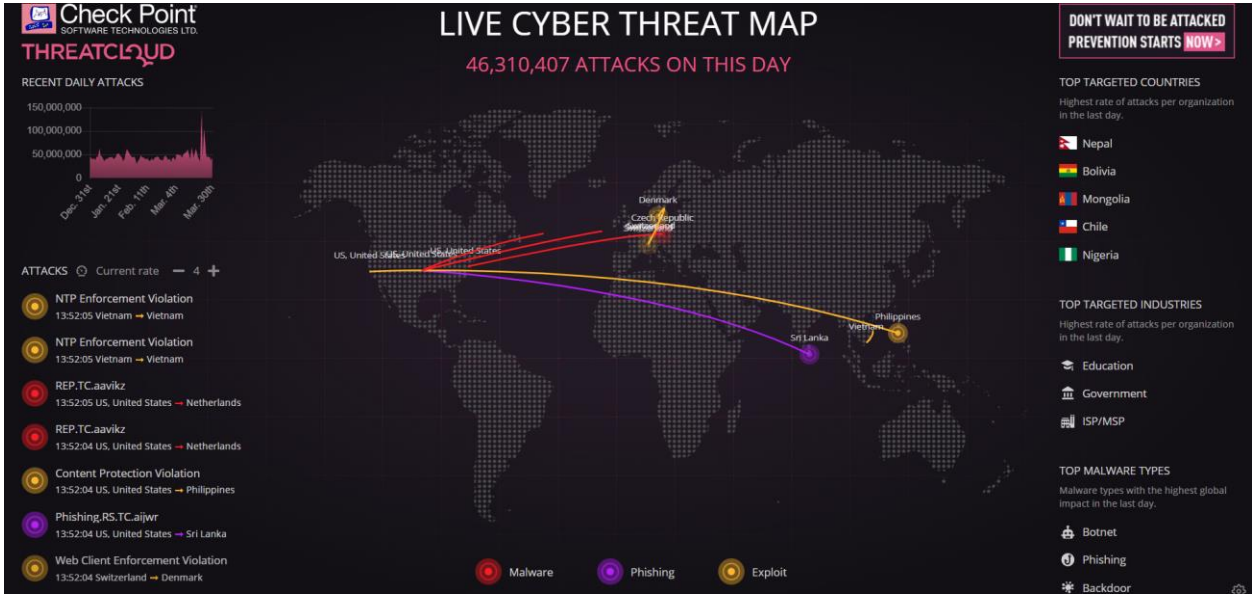
Digital Security for Government Executives

ดร.มัชฌิกา อ่องแตง

Are we under attack !?!

Let's see Live Threat Map

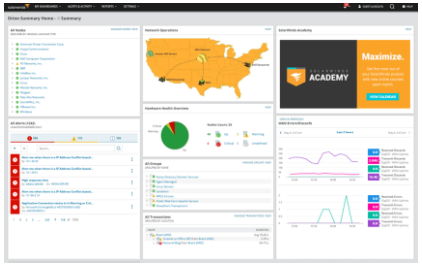


https://threatmap.checkpoint.com/

SolarWinds attack

December 2020: SolarWinds Software Supply Chain Attack

- Attacker ฝัง malware เข้าไปยัง software update ของ SolarWinds' Orion software (ผลิตภัณฑ์ซอฟต์แวร์สำหรับ network and application monitoring)
  - เชื่อว่า Hacker group นี้มีความเชื่อมโยงกับรัฐบาลรัฐเซีย
- Hackers ทำการ compromise infrastructure ของ SolarWinds
  - Access เข้าไปสร้างและแจกจ่าย trojanized updates ไป software users
  - Attacker modify Orion platform plug-in ที่เรียกว่า SolarWinds.Orion.Core.BusinessLayer.dll
  - Orion versions 2019.4 HF 5 ถึง 2020.2.1 (released ระหว่าง March 2020 และ June 2020)
  - Trojanized component บรรจุ backdoor ที่สื่อสารกับ third-party servers ที่ control โดย attacker
- กระทบ software users ทั่วโลก
  - US cybersecurity firm FireEye, US Treasury and Commerce etc.



Costa Rica State of Emergency Declared After Ransomware Attacks

- May 2022 : รัฐบาลประกาศสถานการณ์ฉุกเฉินหลังจากรับมือกับการโจมตีด้วย ransomware ที่มุ่งเป้าไปที่ระบบสำคัญของภาครัฐติดต่อกันหลายสัปดาห์

  - April 2022 : กระทรวงการคลังรายงานว่ามีระบบได้รับผลกระทบ รวมถึงระบบ ระบบจัดเก็บภาษี และ ระบบศุลกากร
    - กระทบการค้าระหว่างประเทศ
    - โลจิสติกส์ทั้งขา import และ export ล่ม

  - การโจมตียังพุ่งเป้าไปที่ ระบบทรัพยากรบุคคลของสำนักงานประกันสังคม และ กระทรวงแรงงาน
    - การโจมตีทำให้ระบบชำระเงินอัตโนมัติหยุดชะงัก ภาครัฐแจ้งแรงงานว่าจะไม่ได้รับค่าจ้างตรงเวลา
  - กลุ่ม Conti gang ซึ่งพูดภาษารัฐเซีย แสดงความรับผิดชอบต่อการโจมตีในครั้งนี้
  - Conti เร่งให้ชาว Costa Ricans กดดันรัฐบาลให้จ่ายเงินค่าไถ่ $20 ล้าน
  - รัฐบาล Costa Rica ปฏิเสธที่จะจ่ายเงิน และพยายามกู้ระบบให้สามารถกลับมาใช้งานได้โดยปกติ

Norwegian government ministries hit by cyberattack

- July 2023 : 12 กระทรวงของรัฐบาลนอร์เวย์ได้รับผลกระทบจาก ICT Platform Hack
  - พบ traffic ที่ผิดปกติบน platform
  - มีการโจมตีผ่าน zero day vulnerability ใน digital platform ที่ใช้งานร่วมกันระหว่างหลายกระทรวง
  - เป็นช่องโหว่ใน third party software ซึ่งถูกปิดในเวลาต่อมา
  - มีการสันนิษฐานว่าเป็นการโจมตีจาก hacker จากรัสเซีย (Source: *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*)

- June 2022: หลายองค์กรในนอร์เวย์ ถูกโจมตีแบบ Distributed-Denial-of-Service (DDoS) ที่ขัดขวางกระบวนการทำงานในองค์กร
  - Norwegian NSM Security กล่าวว่าเป็นการกระทำโดยกลุ่มอาชญากรที่ฝักใฝ่รัสเซีย

Agenda

- (Super) Basic Security Concepts
- Overview of Security Related Standards & Framework
- Common Defenses

Basic Security Concepts

Security Goals

Confidentiality

- รักษาความลับของข้อมูล
- การทำให้ข้อมูลเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ป้องกันการแอบอ่าน
- ปกป้อง Privacy และข้อมูลที่มีเจ้าของ (Proprietary Information)

Integrity

- รักษาความคงสภาพ การทำให้ข้อมูลมีความสมบูรณ์ เชื่อถือได้
- ข้อมูลนั้นไม่ได้ถูกแก้ไข
- ป้องกันการแอบเขียน
- ความน่าเชื่อถือของแหล่งที่มา

Availability

- รักษาความพร้อมใช้งาน
- การให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงระบบและข้อมูลได้ทุกเมื่อที่ต้องการ

Authenticity

- เป็นตัวตนอย่างถ่องแท้ (genuine) โดยสามารถตรวจสอบและสร้างความน่าเชื่อถือได้
- ห้ามปลอม
- ความมั่นใจในความถ่องแท้ของช่องทางการรับส่งข้อมูล ของตัวข้อมูล และของแหล่งข้อมูล

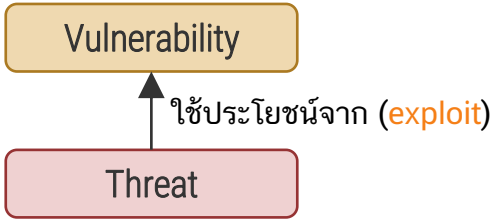
Non-Repudiation

- การป้องกันการปฏิเสธการทำธุรกรรม
- ความสามารถในการรับรองได้ว่าอีกฝ่ายของการทำธุรกรรมหรือการสื่อสารจะไม่สามารถปฏิเสธลายเซ็นบนเอกสาร หรือการส่งข้อมูลที่ฝ่ายนั้นๆส่งมา

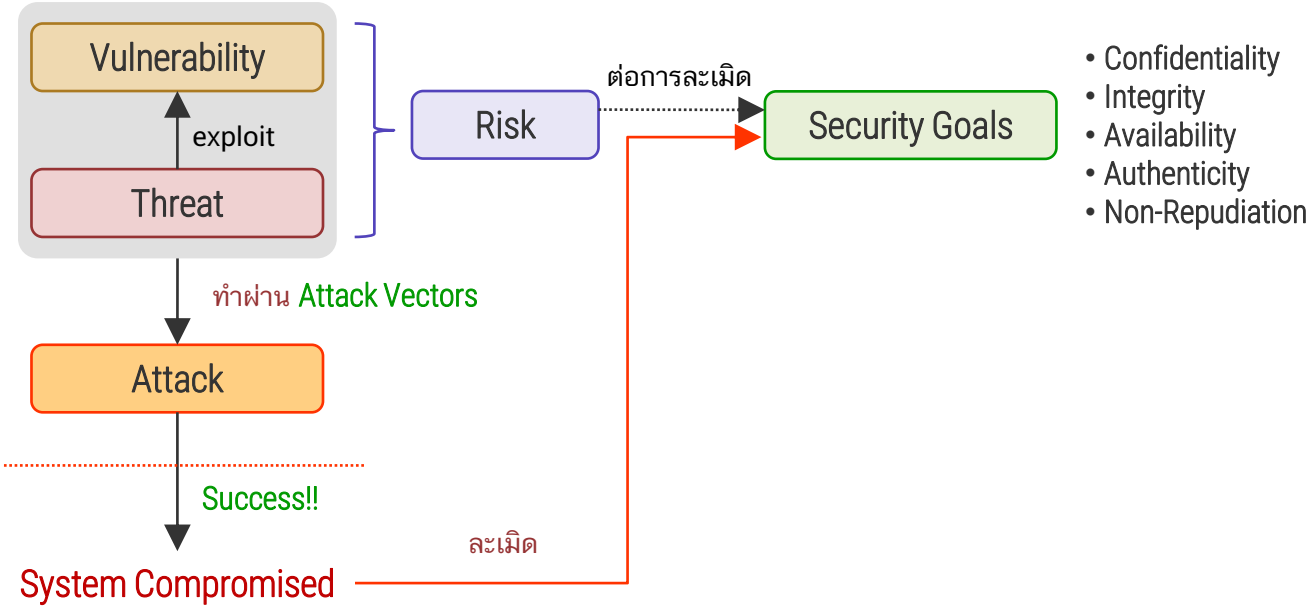
ช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat)

- Vulnerability เป็นสิ่งหนึ่งๆในระบบ ที่เปิดให้ threat สามารถเข้าถึง คน ข้อมูล หรือระบบได้
- ความผิดพลาดหรือจุดอ่อนในการออกแบบระบบ การพัฒนาระบบ การดำเนินการระบบ หรือการบริหารระบบ ที่อาจถูกนำมาใช้ประโยชน์ (exploit) เพื่อละเมิดความมั่นคงของระบบ
  - ต้นเหตุจาก Software หรือ Hardware การออกแบบ การใช้งานระบบในทางที่ผิด (Misuse) ฯลฯ

- Threat หนทาง หรือแนวทาง ที่ผู้โจมตี (Attacker) ใช้ในการทำให้ risk บรรลุผล หรือเป็นจริงขึ้นมา
  - แนวโน้มในการละเมิด Security Goals ของระบบ
  - เกิดขึ้นเมื่อมีเงื่อนไขพฤติการณ์ ความสามารถ การกระทำ หรือเหตุการณ์ที่อาจละเมิดความมั่นคงและทำให้เกิดความเสียหาย
  - Threat หนึ่งๆจะขึ้นอยู่กับสิ่งแวดล้อมของระบบ



Vulnerability – Threat - Attack



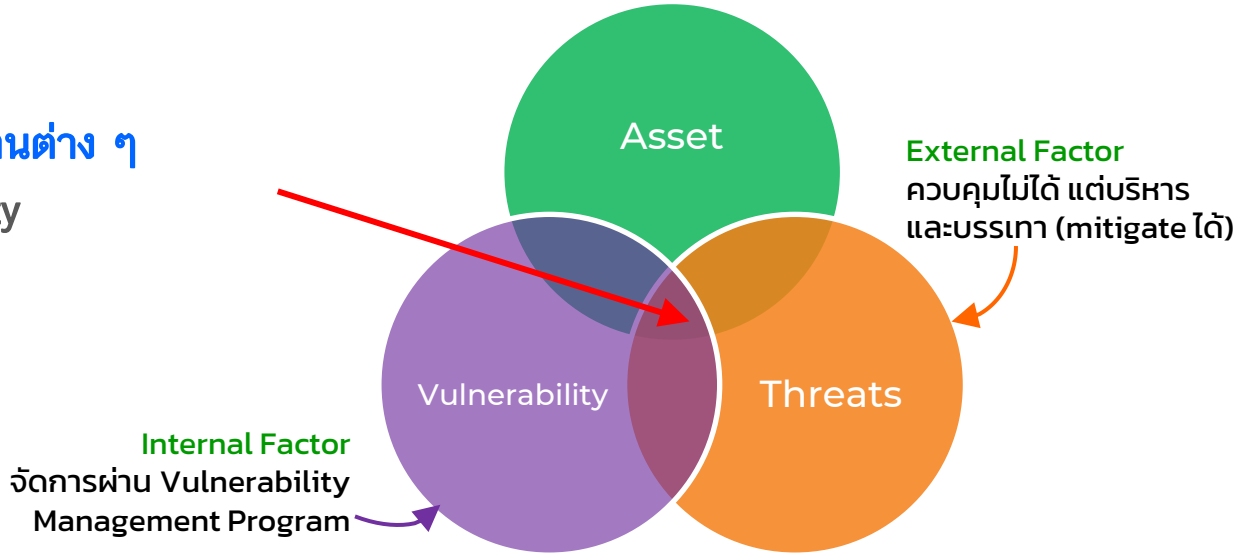
Security Related Standards & Framework

ความเสี่ยง (Risk)

- **แนวโน้ม** ที่ทรัพยากร (resource, assets) ที่มีความสำคัญจะถูกใช้งานในทางที่ผิด (misused) หรือถูกกระทำการใดๆที่จะทำให้เกิดความสูญเสีย

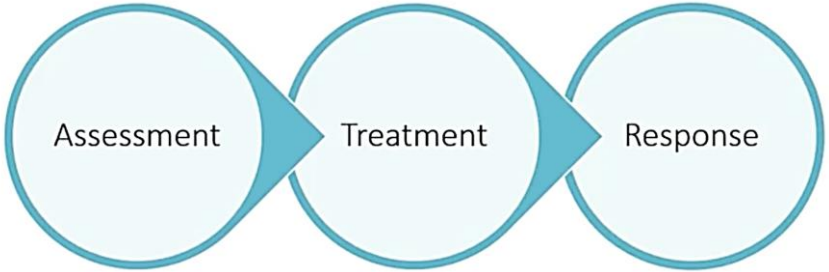
Risk

- **ความเสี่ยงในด้านต่าง ๆ**
  - Confidentiality
  - Integrity
  - Availability



Risk Management

- **Risk Assessment :** ระบุและประเมินนัยสำคัญของแต่ละความเสี่ยง และความน่าจะเป็นที่จะเกิด
- **Risk Treatment :** กำหนดแนวทางการจัดการ
- **Response :** Action ที่กระทำ อ้างอิงจากการตัดสินใจเลือก Risk Treatment



Risk Assessment
- Asset identification and classification
- Threat & Vulnerability Identification
- Risk & Impact Analysis

Risk Treatment
- Risk Mitigation
- Risk Avoidance
- Risk Transfer
- Risk Acceptance

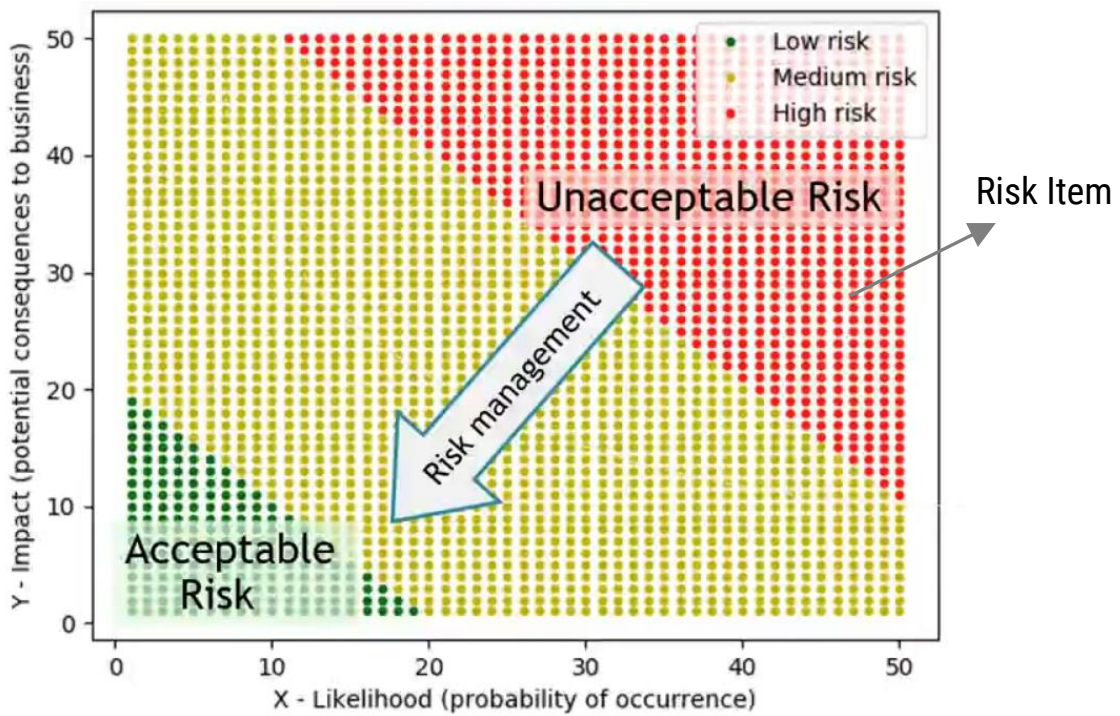
Response
- Make changes or do nothing based on risk treatment decision
- Monitor / Audit

Risk Assessment

- ประเมิน เพื่อระบุ Risk Rating สำหรับแต่ละ Risk Item

Asset-Based

Scenario-Based



Risk Treatment

Risk Mitigation

- Goal ของ Security คือการ ลด risk ให้อยู่ในระดับที่ยอมรับได้ ซึ่งขึ้นกับองค์กร
- ลด Risk โดยการใส่ Risk Control ทั้ง Technical และ Operational Controls
  - ควบคุมบริหารจัดการ Vulnerability
  - ลดผลกระทบที่จะเกิดขึ้นกับ Asset
- ตัวอย่าง ลด Risk จากการที่ Server ถูกโจมตี
  - Patch Server OS, Software จาก Known Vulnerability
  - การติดตั้งและ update Anti-Virus Software

Risk Avoidance

- ถ้า Risk สูงเกินกว่าที่จะยอมรับได้ อาจปรับ design หรือ configuration ของระบบเพื่อหลีกเลี่ยง Risk จาก Vulnerability ที่ทำให้เกิด Threat
- ตัวอย่าง Windows XP มีช่องโหว่ที่อันตราย จึงอัพเดตเป็น Windows 10, Windows 11

Risk Treatment

Risk Acceptance

- องค์กรยอมรับ Risk โดยเฉพาะเมื่อ Risk นั้นน้อยมากจนไม่ต้องการ countermeasures ใดๆ หรือเมื่อมี countermeasures เพียงพอแล้ว
  - เช่น ยอมรับการใช้งาน OS ที่ผ่านการ Patch จน update แล้ว
  - การยอมรับ Risk สำคัญๆ ควรได้รับอนุมัติจาก Executive เช่น CIO

Risk Transference

- ถ้าองค์กรไม่สามารถยอมรับ หรือหลีกเลี่ยง หรือลด Risk ได้ เราสามารถถ่ายโอนไปให้ธุรกิจอื่นได้

ตัวอย่าง

- ทำประกันน้ำท่วม เพื่อลดค่าใช้จ่ายจากเหตุน้ำท่วม
- Data Breach & Cyber Liability Insurance
- Hardware Warrantee, Care Service

ISO 27001

- มุ่งให้มี Systematic Framework ในการบริหารจัดการ risk ที่เกี่ยวข้องกับ Information Security และปกป้อง Information สำคัญ
- เป็น Management System Standard มาตรฐานสำหรับการได้รับ ISO Certification
  - ผูกเข้ากับ Annex A – List ของ Control Objectives และ Controls สำหรับ Information Security ที่ครอบคลุมประเด็นด้าน Security ขององค์กรส่วนมาก
    - ISO 27002 เป็น Guidance ในการ implement controls
- เป็นมาตรฐานสากล ซึ่งใช้ Risk-based Approach

ISO 27001

Information Security Management Systems (ISMS) Requirements

- เป็นมาตรฐานสากล ซึ่งใช้ Risk-based Approach
  - ประกอบด้วย

Process, Approach + 10 Requirements

- Risk Management Process
- Continuous improvement lifecycle processes
- Management Framework
- etc.

+

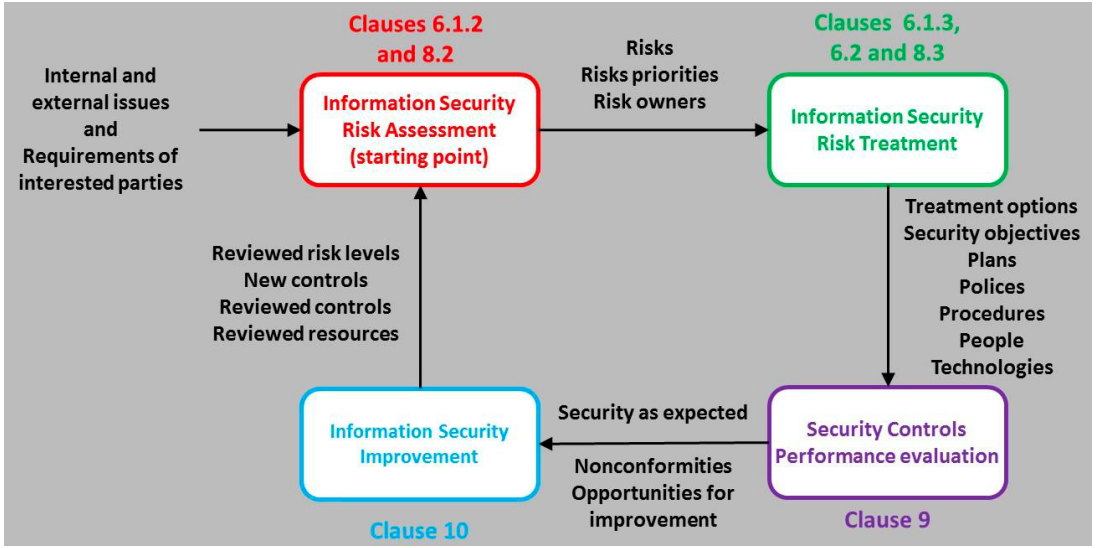
Security Controls

- Baseline Technical Controls (i.e. Annex A of Requirement Specification)
- etc.

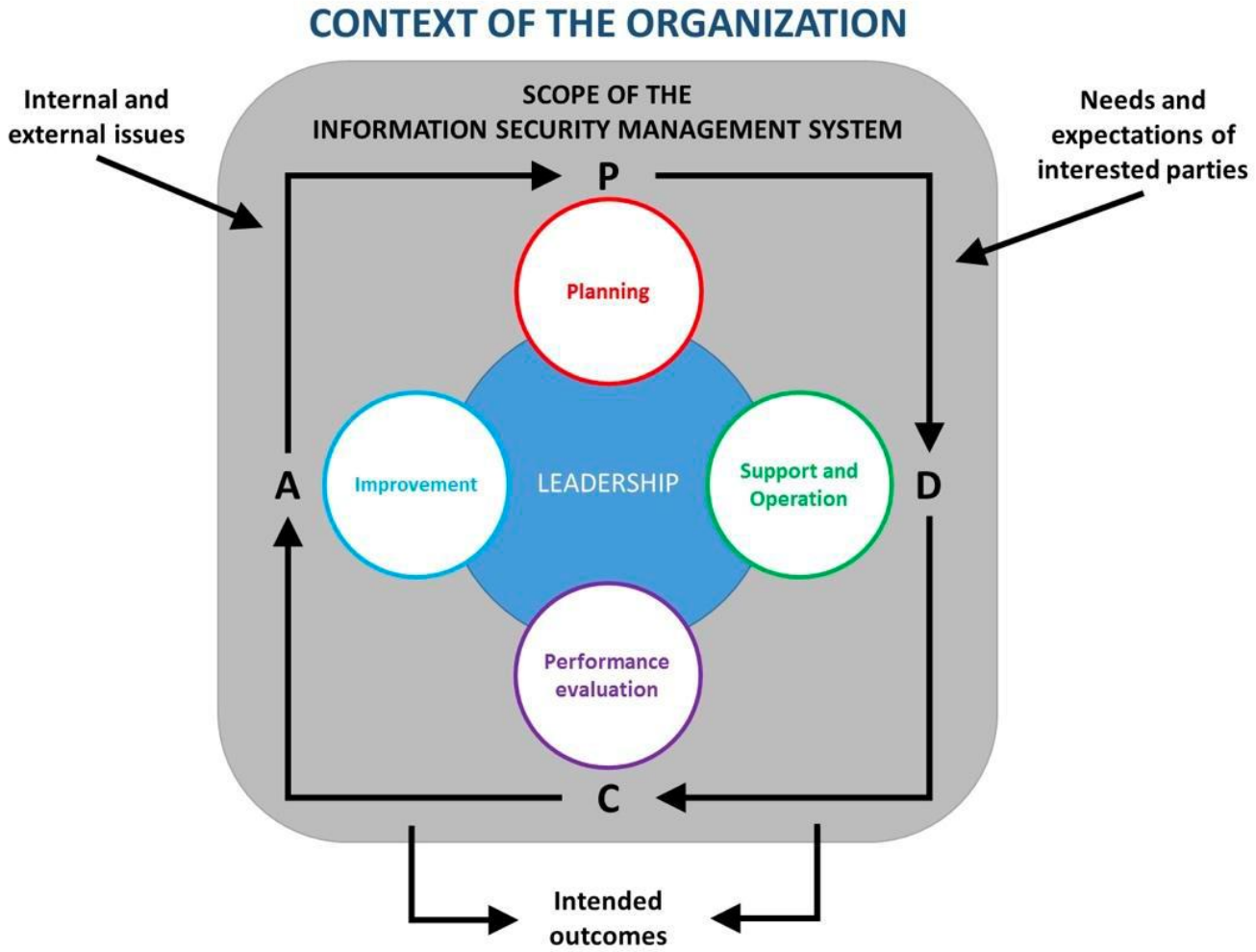
Process and Process Approach

- **Risk:**
  - ความเสี่ยง แนวโน้มผลกระทบของความไม่แน่นอน
- **Risk Assessment (RA):**
  - การประเมินความเสี่ยง เป็นกระบวนการในการระบุ (identify), วิเคราะห์ (analyze), และประเมินผล (evaluate) ความเสี่ยง
- **Risk Treatment Plan (RTP):**
  - ชุดของ procedures, methodologies, และ technologies ที่ประยุกต์ใช้เพื่อจัดการเยียวยาความเสี่ยง
- **Residual Risk:**
  - ความเสี่ยงคงเหลือ **หลัง risk treatment**

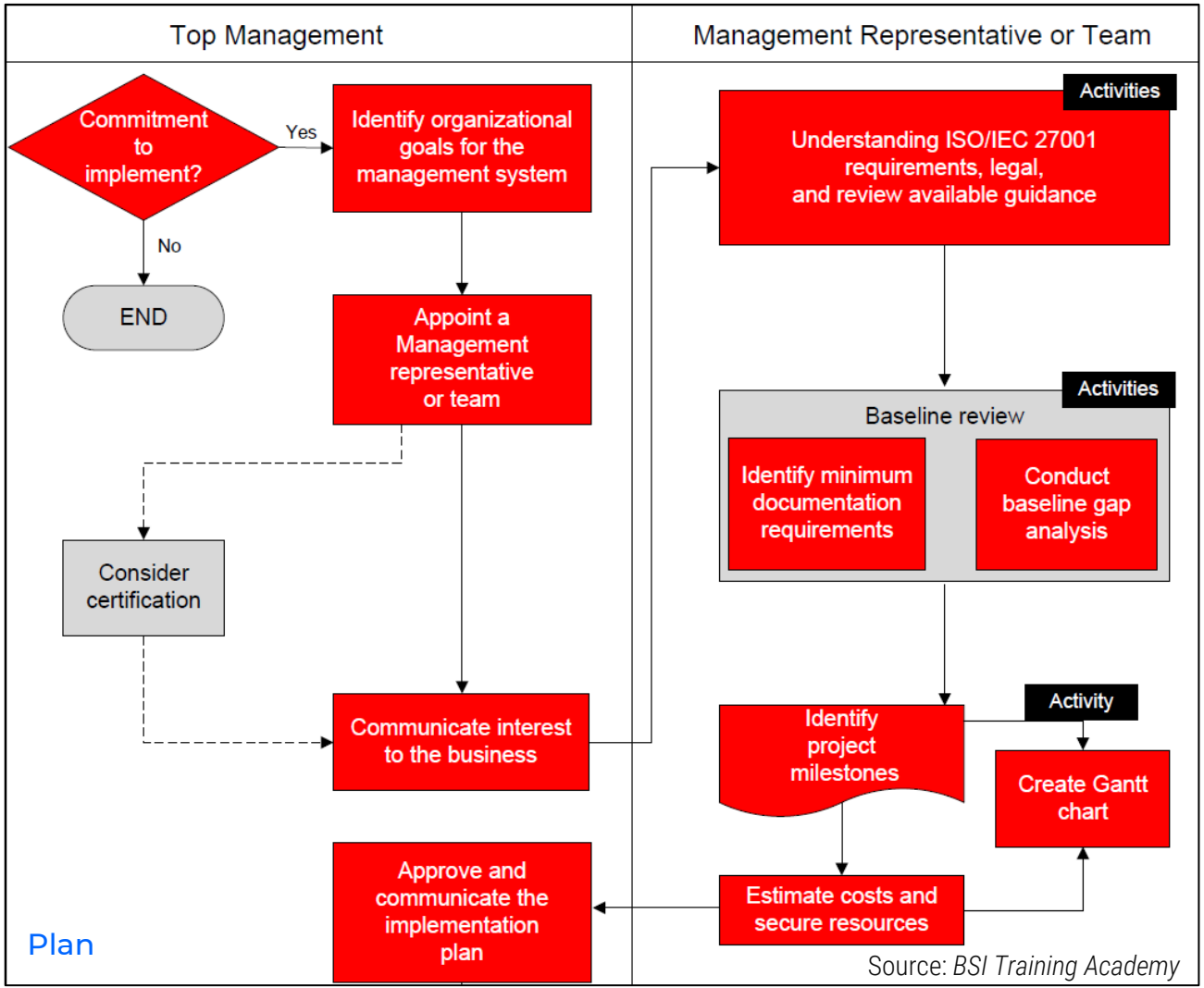
Process Approach Applied to Information Security Management



Plan-Do-Check-Act Cycle

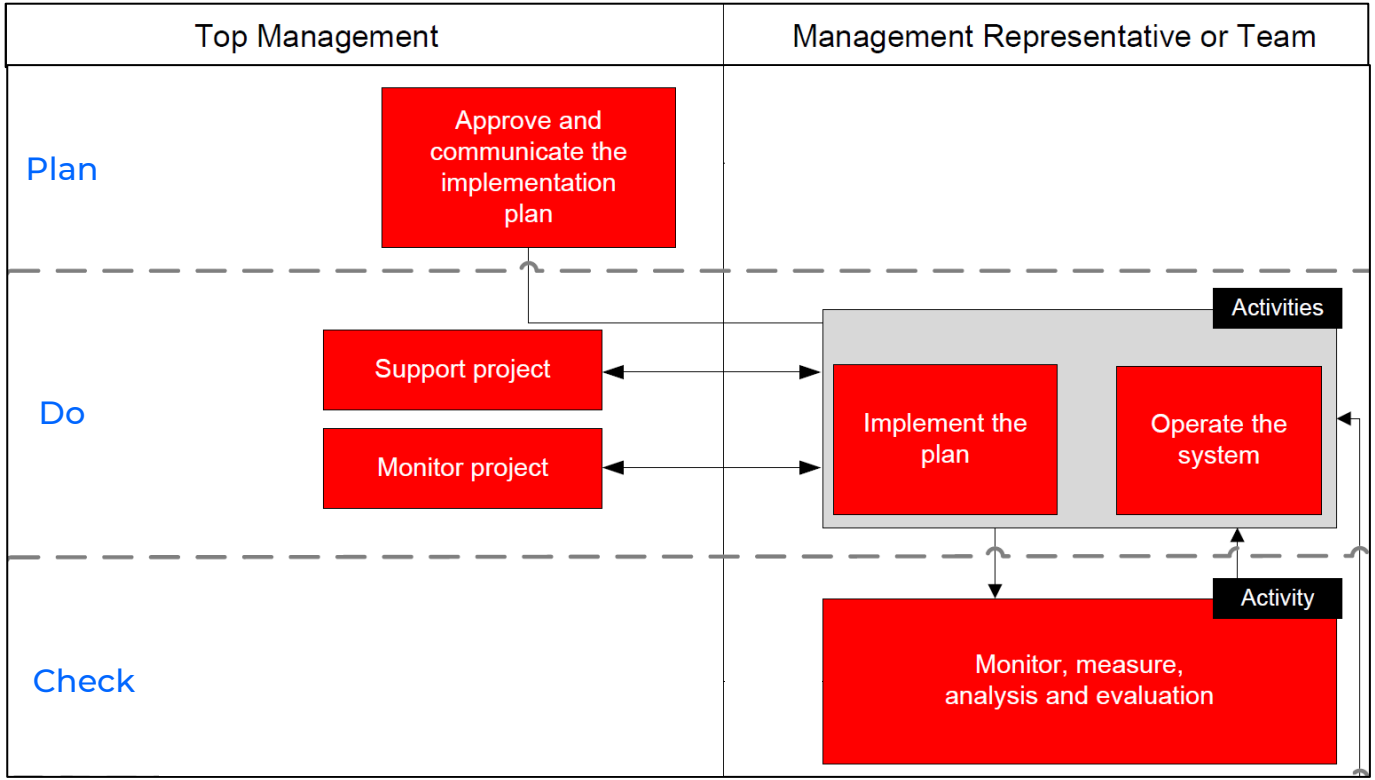


Plan



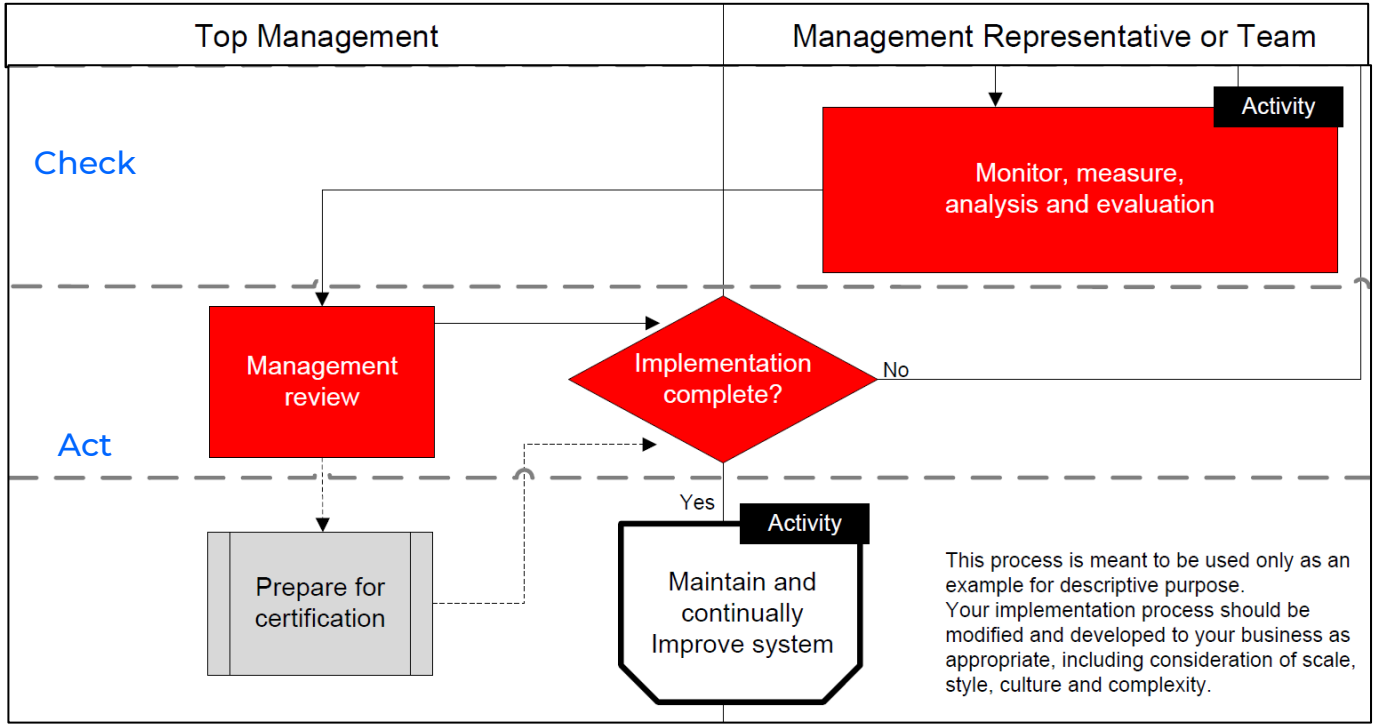
Source: *BSI Training Academy*

Do & Check



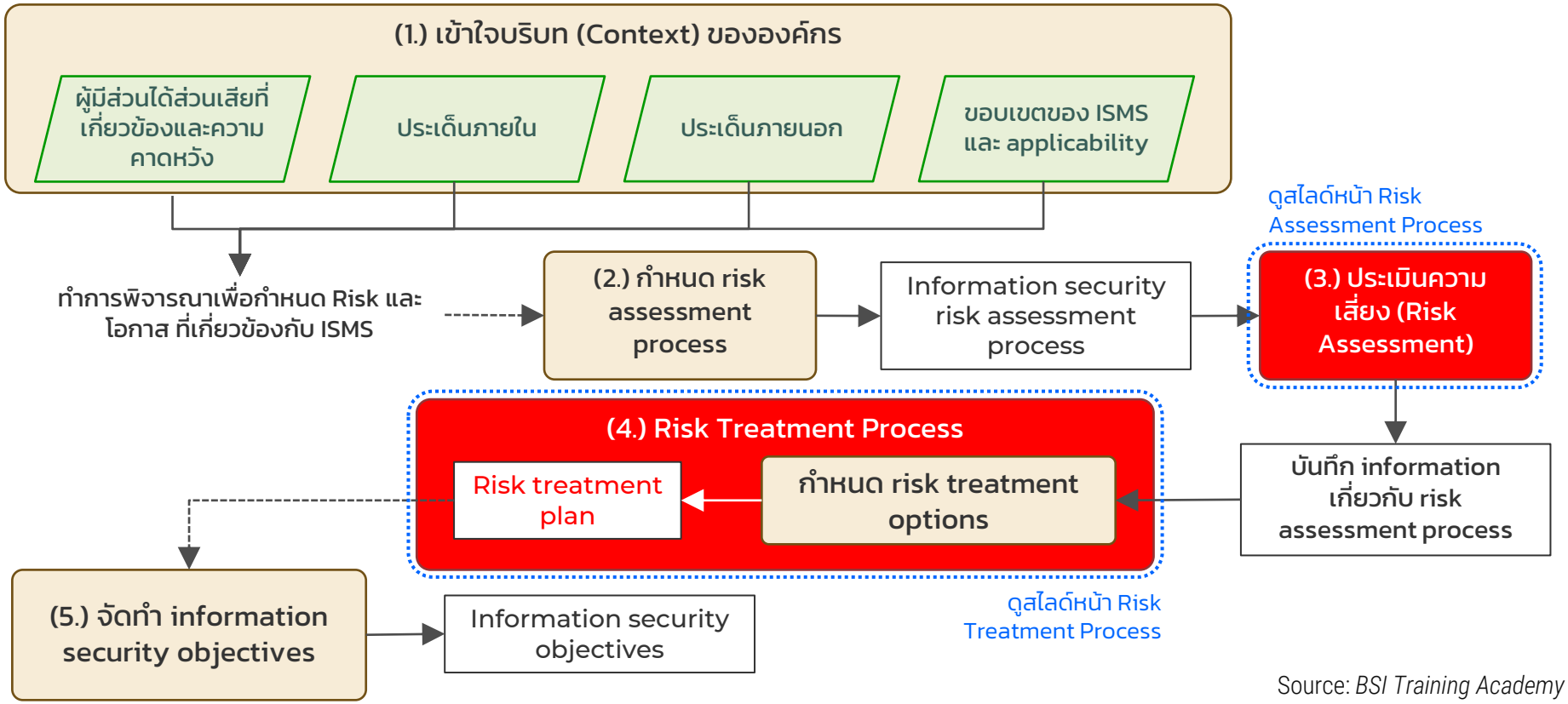
Source: *BSI Training Academy*

Act



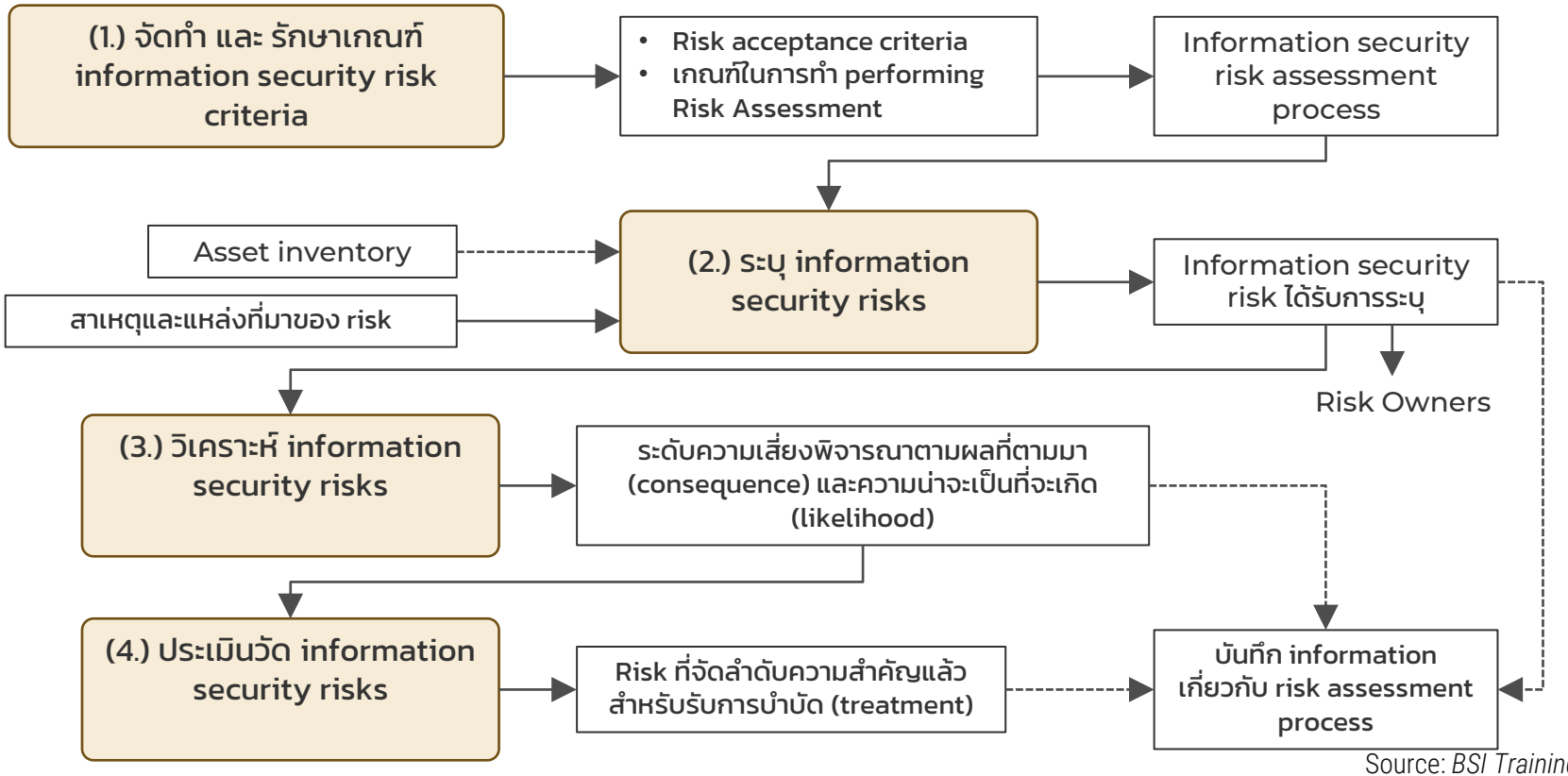
Source: *BSI Training Academy*

Overall Planning Process



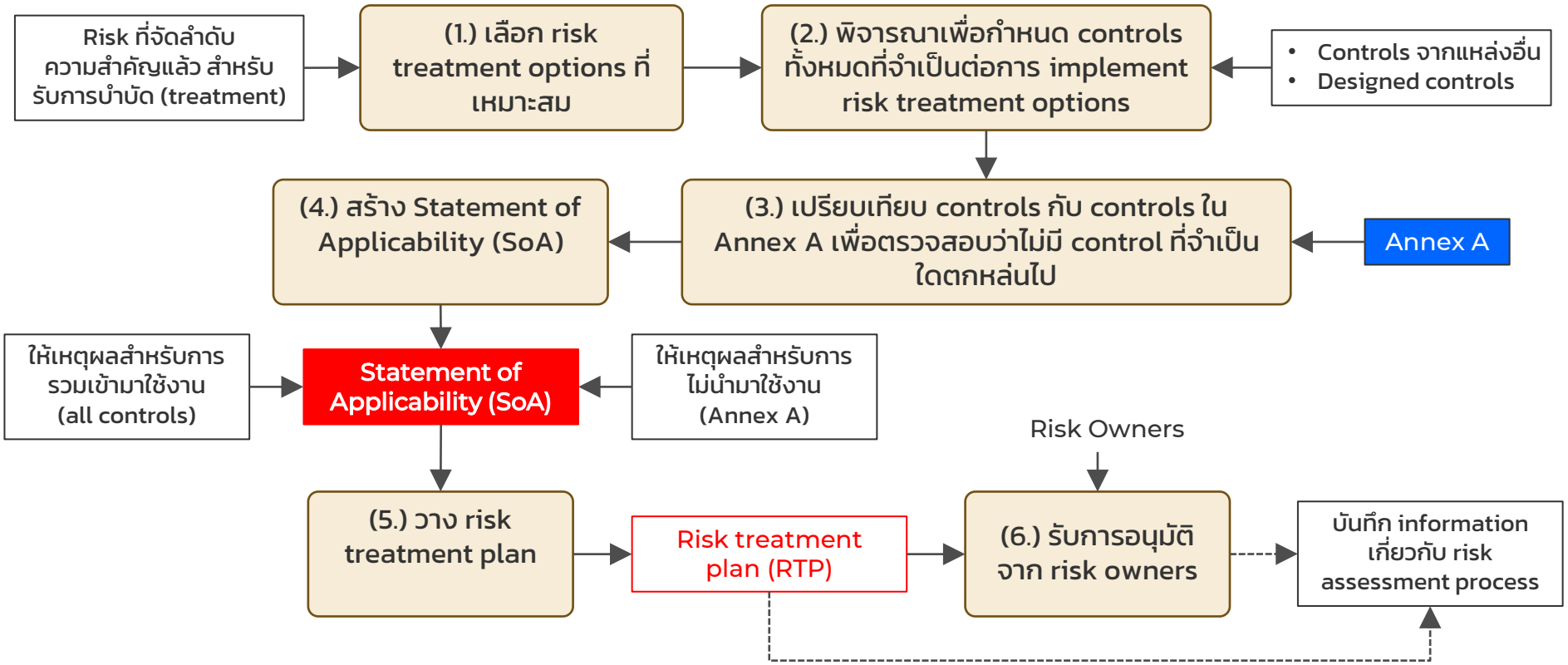
Source: *BSI Training Academy*

Risk Assessment Process



Source: *BSI Training Academy*

Risk Treatment Process



Source: *BSI Training Academy*

Annex A – ISO 27001:2022

- **Information Security specific controls ระบุใน Annex A จัดแบ่งเป็น 4 domains**

1	Clause 5: Organizational controls	37 controls 34 existing in v.2013 + 3 new
2	Clause 6: People controls	8 controls all existing in v.2013
3	Clause 7: Physical controls	14 controls 13 existing in v.2013 + 1 new
4	Clause 8: Technological controls	34 controls 27 existing in v.2013 + 7 new

Organizational controls

A5.1	Policies for information security
A5.2	Information security roles and responsibilities
A5.3	Segregation of duties
A5.4	Management responsibilities
A5.5	Contact with authorities
A5.6	Contact with special interest groups
A5.7	Threat intelligence
A5.8	Information security in project management
A5.9	Inventory of information and other associated assets
A5. 10	Acceptable use of information and other associated assets
A5.11	Return of assets
A5.12	Classification of information
A5.13	Labelling of information
A5.14	Information transfer
A5.15	Access control
A5.16	Identity management
A5.17	Authentication information
A5.18	Access rights
A5.19	Information security in supplier relationships

A5. 20	Addressing information security within supplier agreements
A5.21	Managing information in the ICT supply chain
A5.22	Monitoring, review and change managemnt of supplier services
A5.23	Information security for use of cloud services
A5.24	Information security incident management planning and preparation
A5.25	Assessment and decision on information security events
A5.26	Response to information security incidents
A5.27	Learning from information security incidents
A5.28	Collection of evidence
A5.29	Information security during disruption
A5. 30	ICT readiness for business continuity
A5.31	Legal, statuatory, regulatory and contractual requirements
A5.32	Intellectual property rights
A5.33	Protection of records
A5.34	Privacy and protection of PII
A5.35	Independent review of information security
A5.36	Conformance with policies, rules and standards for information security
A5.37	Documented operating procedures

People controls

A6.1	Screening
A6.2	Terms and definitions of employment
A6.3	Information security awareness, education and training
A6.4	Disciplinary process
A6.5	Responsibilities after termination or change of employment
A6.6	Confidentiality or non-disclosure agreements
A6.7	Remote working
A6.8	Information security event reporting

Physical controls

A7.1	Physical security perimeters
A7.2	Physical entry
A7.3	Securing offices, rooms and facilities
A7.4	Physical security monitoring
A7.5	Protecting against physical and environmental threats
A7.6	Working in secure areas
A7.7	Clear desk and clear screen
A7.8	Equipment siting and protection
A7.9	Security of assets off-premises
A7. 10	Storage media
A7.11	Supporting utilities
A7.12	Cabling security
A7.13	Equipment maintenance
A7.14	Secure disposal or re-use of equipment

Technological controls

A8.1	User endpoint devices
A8.2	Privileged access rights
A8.3	Information access restriction
A8.4	Access to source code
A8.5	Secure authentication
A8.6	Capacity management
A8.7	Protection against malware
A8.8	Management of technical vulnerabilities
A8.9	Configuration management
A8. 10	Information deletion
A8.11	Data masking
A8.12	Data leakage prevention
A8.13	Information backup
A8.14	Redundancy of information processing facilities
A8.15	Logging
A8.16	Monitoring activities
A8.17	Clock syncronization

A8.18	Use of privilaged utility programs
A8.19	Installation of software on operational systems
A8. 20	Networks security
A8.21	Security of network services
A8.22	Segregation of networks
A8.23	Web filtering
A8.24	Use of cryptography
A8.25	Secure development lifecycle
A8.26	Application security requirements
A8.27	Secure system architecture and engineering principles
A8.28	Secure coding
A8.29	Security testing in development and acceptance
A8. 30	Outsourced development
A8.31	Separation of development, test and production environments
A8.32	Change management
A8.33	Test information
A8.34	Protection of information systems during audit testing

NIST Cybersecurity Framework

- กรอบทำงาน (Framework) ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นกรอบการออกแบบและวางกลยุทธ์ให้ระบบรักษาความปลอดภัยทางไซเบอร์ โดยเป็นที่ยอมรับอย่างแพร่หลายในปัจจุบัน ประกอบด้วย

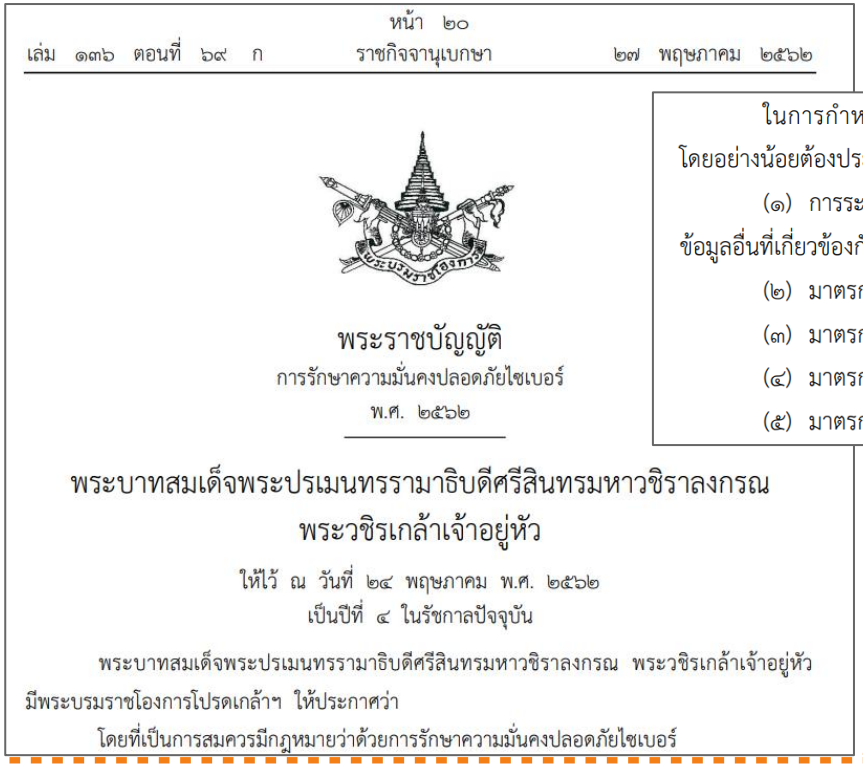
1	IDENTIFY (ID)	ระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง
2	PROTECT (PR)	วางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร
3	DETECT (DE)	กำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ
4	RESPOND (RS)	กำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น
5	RECOVER (RC)	กำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

NIST Cybersecurity Framework 1.1 (2018)

IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND (RS)	RECOVER (RC)
Asset Management (ID.AM)	Identity Management and Access Control (PR.AC)	Anomalies and Events (DE.AE)	Response Planning (RS.RP)	Recovery Planning (RC.RP)
Business Environment (ID.BE)	Awareness and Training (PR.AT)	Security Continuous Monitoring (DE.CM)	Communications (RS.CO)	Improvements (RC.IM)
Governance (ID.GV)	Data Security (PR.DS)	Detection Processes (DE.DP)	Analysis (RS.AN)	Communications (RC.CO)
Risk Assessment (ID.RA)	Information Protection Processes and Procedures (PR.IP)		Mitigation (RS.MI)	
Risk Management Strategy (ID.RM)	Maintenance (PR.MA)		Improvements (RS.IM)	
Supply Chain Risk Management (ID.SC)	Protective Technology (PR.PT)			

NIST Cybersecurity Framework 1.1 (2018)

- **พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ยกมาตรฐานของ NIST มาใช้อ้างอิง**



หน้า ๒๐
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

NIST Cybersecurity Framework 1.1 (2018)

IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND (RS)	RECOVER (RC)
Asset Management (ID.AM)	Identity Management and Access Control (PR.AC)	Anomalies and Events (DE.AE)	Response Planning (RS.RP)	Recovery Planning (RC.RP)
Business Environment (ID.BE)	Awareness and Training (PR.AT)	Security Continuous Monitoring (DE.CM)	Communications (RS.CO)	Improvements (RC.IM)
Governance (ID.GV)	Data Security (PR.DS)	Detection Processes (DE.DP)	Analysis (RS.AN)	Communications (RC.CO)
Risk Assessment (ID.RA)	Information Protection Processes and Procedures (PR.IP)		Mitigation (RS.MI)	
Risk Management Strategy (ID.RM)	Maintenance (PR.MA)		Improvements (RS.IM)	
Supply Chain Risk Management (ID.SC)	Protective Technology (PR.PT)			

พ.ร.บ. ไซเบอร์

การระบุความเสี่ยงที่อาจจะเกิดขึ้น

มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

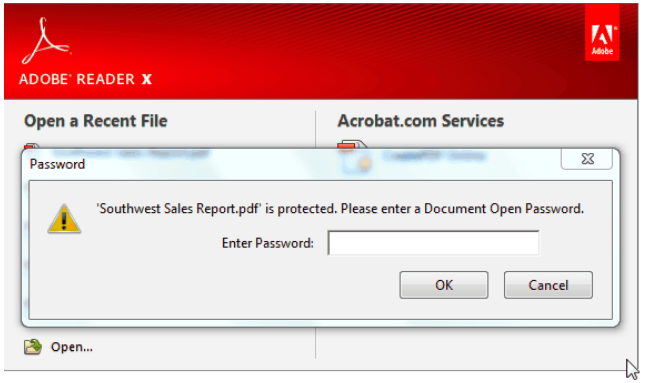
ตัวอย่าง
มาตรการรักษาความมั่นคงปลอดภัยข้อมูล

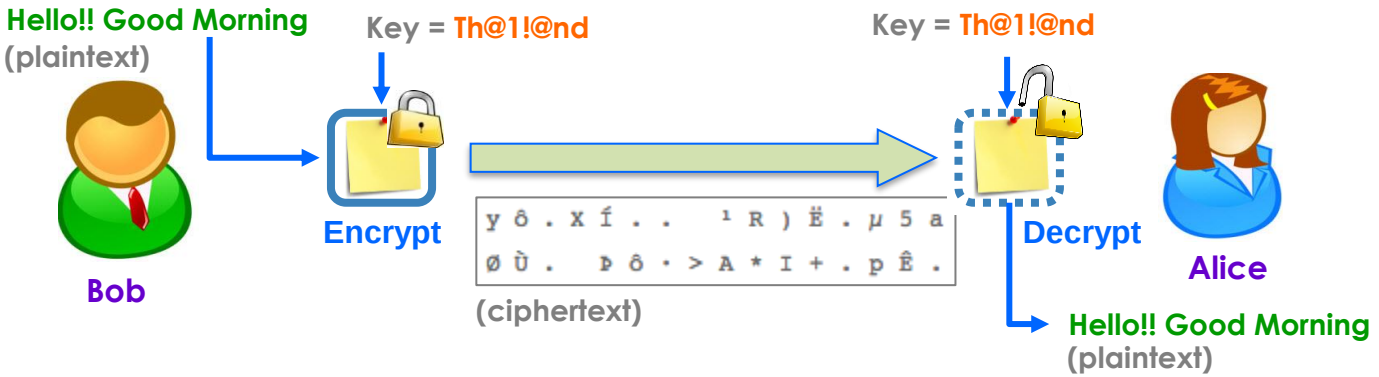
ปกป้องด้วยการเข้ารหัสข้อมูล

- แปลงข้อมูลเพื่อให้ข้อมูลกลายเป็นข้อมูลลับ
  - Encryption การเข้ารหัส

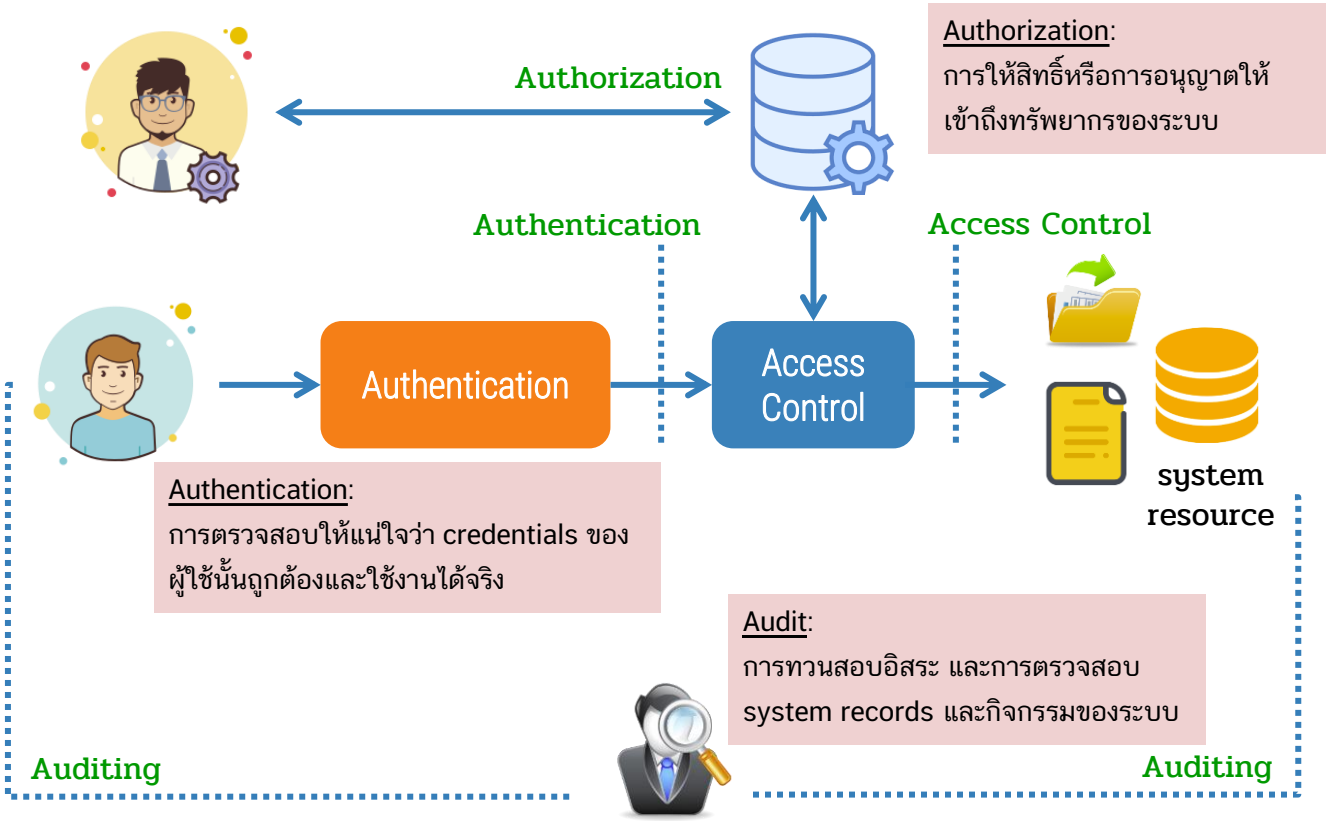
    ใช้ Key ในการ Encrypt เพื่อเปลี่ยน plaintext เป็น ciphertext
  - Decryption การถอดรหัส

    ใช้ Key ในการ Decrypt เพื่อเปลี่ยน ciphertext กลับเป็น plaintext
  - กระบวนการบริหารจัดการ key





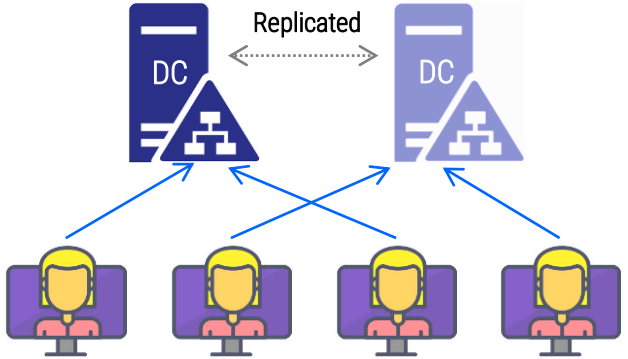
Authentication & Access Control



ตัวอย่างกลไกในองค์กร

- **Active Directory Authentication**
  - AD DS (Active Directory Domain Services) security เป็นกลไกในการพิสูจน์ตัวตนและปกป้อง identity สำหรับ windows environment ที่มี AD-joined clients

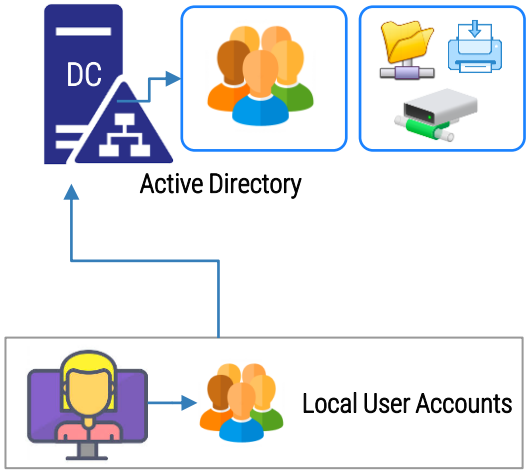
  - ใน Windows Domain เราเรียก Windows Server ที่มี AD DS Role (มีการติดตั้ง AD DS) ว่าเป็น Domain Controller มีหน้าที่พิสูจน์ตัวตนและควบคุมสิทธิ์ของ client ใน Windows Domain นั้นๆ
    - Domain Controller เก็บ Active Directory และ Policy
    - Windows Domain สามารถมีหลาย Domain Controller ได้ (replicate กัน) แต่จะมีเพียง 1 Primary Domain Controller



ตัวอย่างกลไกในองค์กร

- **Active Directory Domain Services (AD DS)**
  - เก็บ Directory Data และกำหนด process ในการเข้าถึง Directory Data
    - User Accounts (names, passwords, contacts, ฯลฯ)
    - Servers, Volumes
    - Printers
    - File Shares, Shared Resources
    - Groups

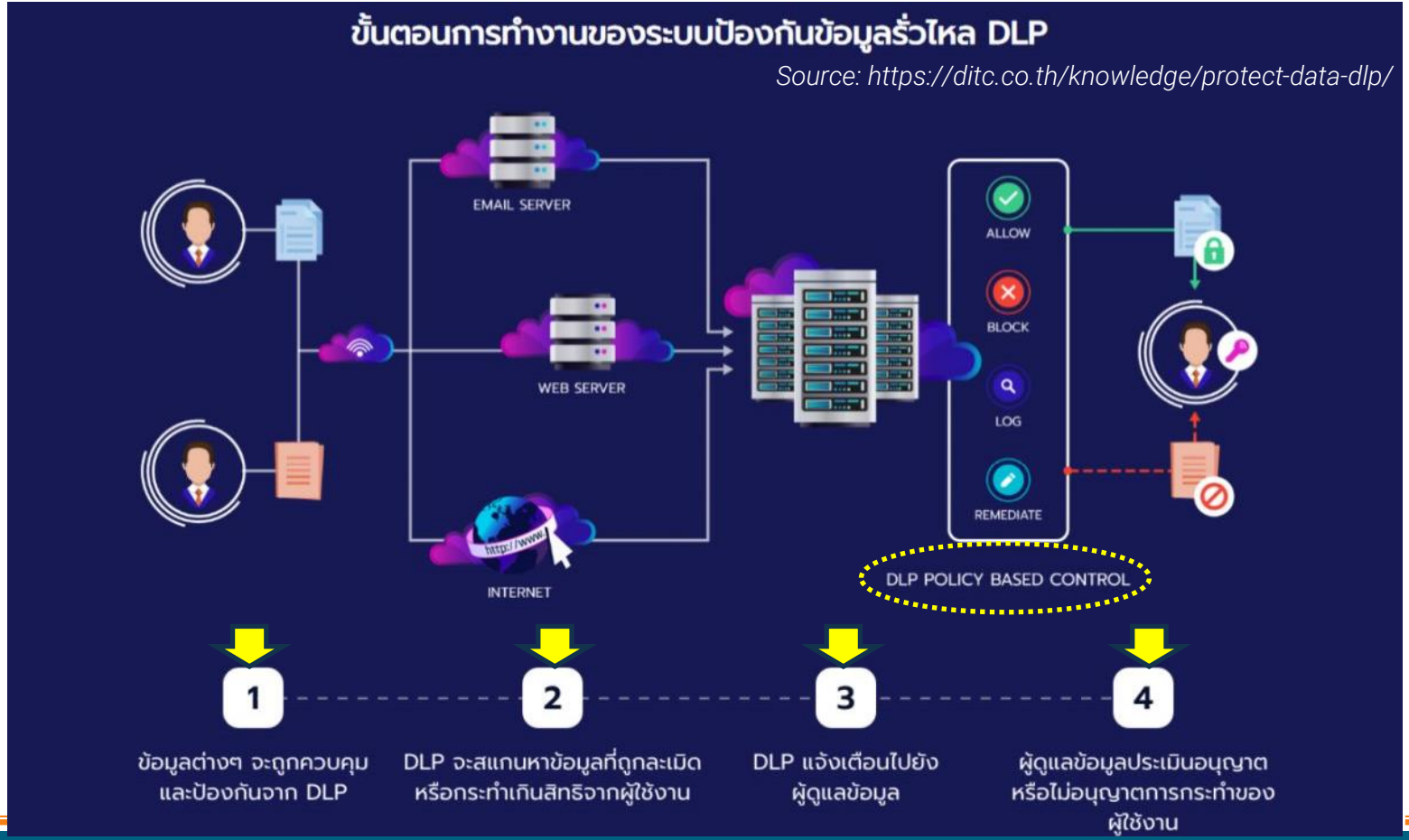
  - เมื่อ user ทำการ log-in บน domain computer เครื่องจะหา user account จาก local computer ก่อน แล้วจึงวิ่งไปหา user account ที่ Active Directory Service



Data Leak Protection (DLP)

- Data Loss Prevention (Data Leak Prevention) เป็นระบบที่ใช้ technologies, process และกลยุทธ์ต่าง ๆ ในการป้องกันไม่ให้บุคคลที่ไม่ได้รับสิทธิ์ เข้าถึง sensitive information ขององค์กรได้
- เป็น tools & techniques ที่ช่วยให้ network administrator สามารถ monitor และบริหารจัดการ data ที่ถูกจัดส่ง
- จำแนกสิทธิ์พร้อมควบคุมการเข้าถึงและส่งข้อมูลของแต่ละบุคคล
- ตรวจจับและป้องกันการรั่วไหลของข้อมูลสำคัญ เพื่อป้องกันไม่ให้บุคคลภายในองค์กรส่งข้อมูลสำคัญหรือ confidential data ออกไปนอกองค์กร เช่น ผ่าน e-mail, web connection เป็นต้น
- วิเคราะห์และคัดแยกความประเภทความสำคัญของข้อมูล

Data Leak Protection (DLP)



ดร.มัชฌิกา อ่องแตง

machigar@gmail.com

LINE ID: machigar