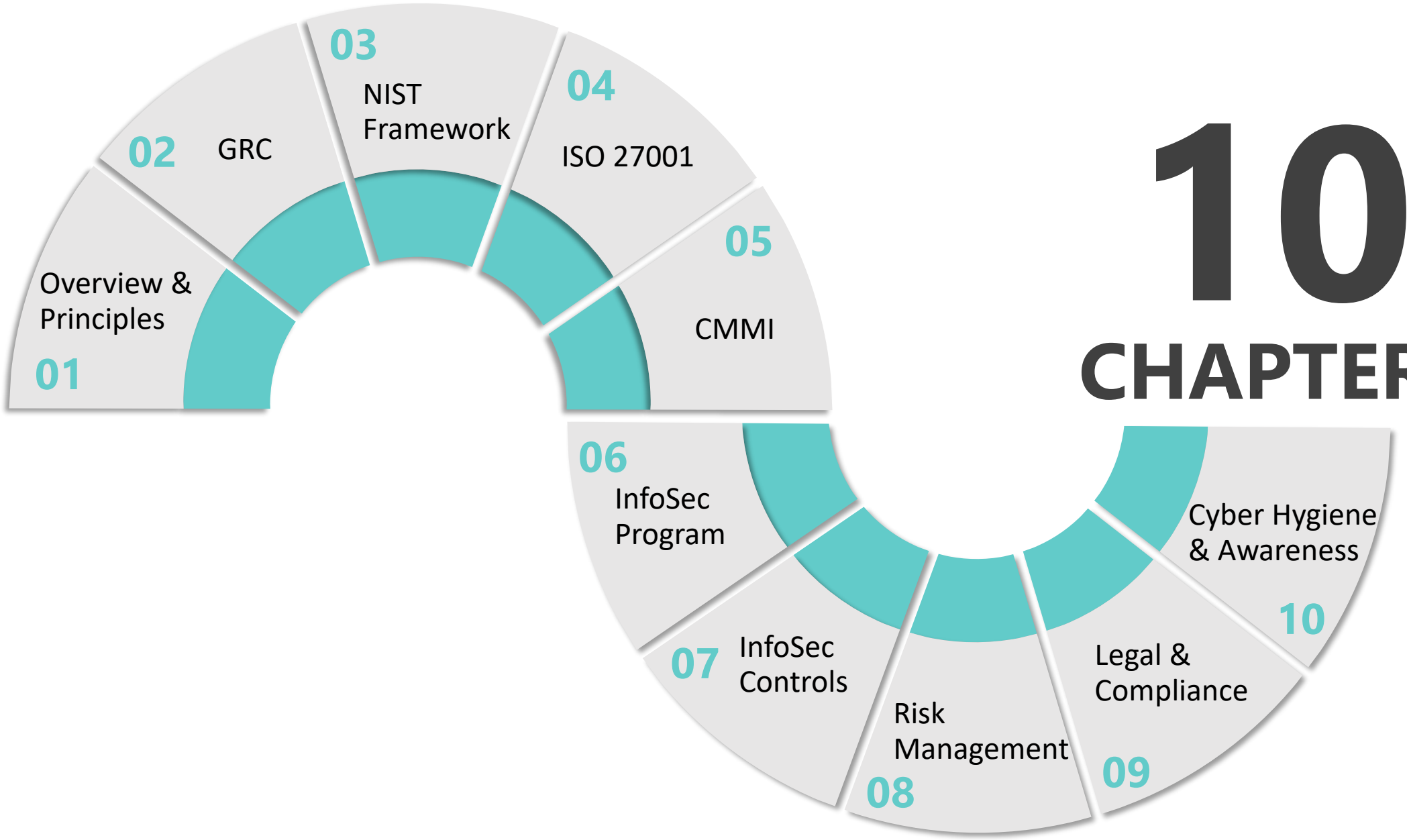
Information Security Governance & Risk Management

Cybersecurity Bootcamp 2024

Disclaimer

This learning material is addressed and used only for Cybersecurity Bootcamp 2024 and should not be used or relied upon for any other purposes. Our learning material is not to be disseminated to or used by any third party in whole or in part without prior consent and permission from Kasikorn Technology Group Secretariat Company Limited (KBTGSec). Accordingly, we will not accept or take any responsibility or liability for any party or any person, whether or not such material is shown, disseminated, obtained, or possessed to such party or person since such material is only for educational purposes. We reserve all of our rights, including but not limited to intellectual property rights in our learning material, such as presentations, spreadsheets, system techniques, ideas, concepts, information, forms, electronic tools, forming parts of the materials, etc.


01
Overview & Principles
02
GRC
03
NIST Framework
04
ISO 27001
05
CMMI
06
InfoSec Program
07
InfoSec Controls
08
Risk Management
09
Legal & Compliance
10
Cyber Hygiene & Awareness

10 CHAPTERs

01

Overview & Principles of Information Security

Key Objectives

Overview & Principles of Information Security

1. Introduction to Information Security
2. Core Principles of Information Security
3. Threats and Vulnerabilities
4. Risk Management in Information Security
5. Best Practices and Frameworks

01

Introduction to Information Security

Definition

Protects information from unauthorized access, use, disclosure, disruption, modification, or destruction.

ทรัพย์สิน
เปิดเผย
หยุดการทำงาน
เปลี่ยนแปลงข้อมูล
ทำลายข้อมูล
เปิดเผยข้อมูล

Objectives [CIA]

- Confidentiality
- Integrity
- Availability

Importance

Essential for protecting data and ensuring business continuity.

*ไม่ว่าจะโดนโจมตีรูปแบบใดก็สามารถทำงานต่อไปได้

01

Core Principles of Information Security

Confidentiality

Ensuring that information is **accessible only** to those authorized to have access.

*อะไรที่เป็นของเราก็ควรเข้าได้แค่เราเท่านั้น

Integrity

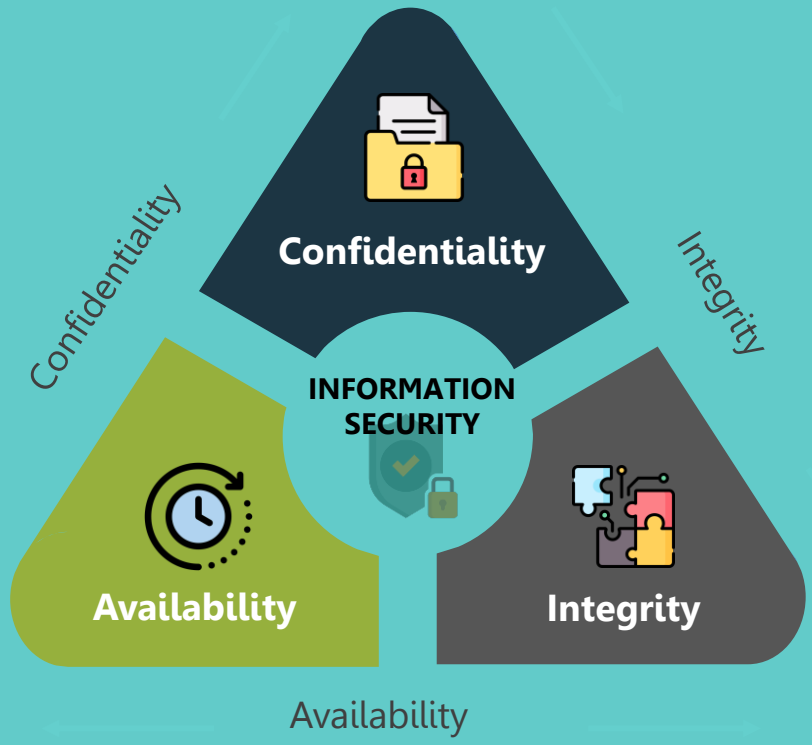
Safeguarding the **accuracy and completeness** of information and processing methods.

*ความถูกต้องของข้อมูลและข้อมูลอยู่ครบ

Availability

Ensuring that authorized users have access to information and associated assets **when required**. *พร้อมใช้งาน คือต้องการใช้ ใช้งานได้

CIA Triad



01

Threats and Vulnerabilities

Threats *ภัยคุกคาม

Potential **cause** of an unwanted incident, which may result in harm to a system or organization.

*สิ่งใดก็ตามทำให้ระบบของเราทำงานต่อไปไม่ได้

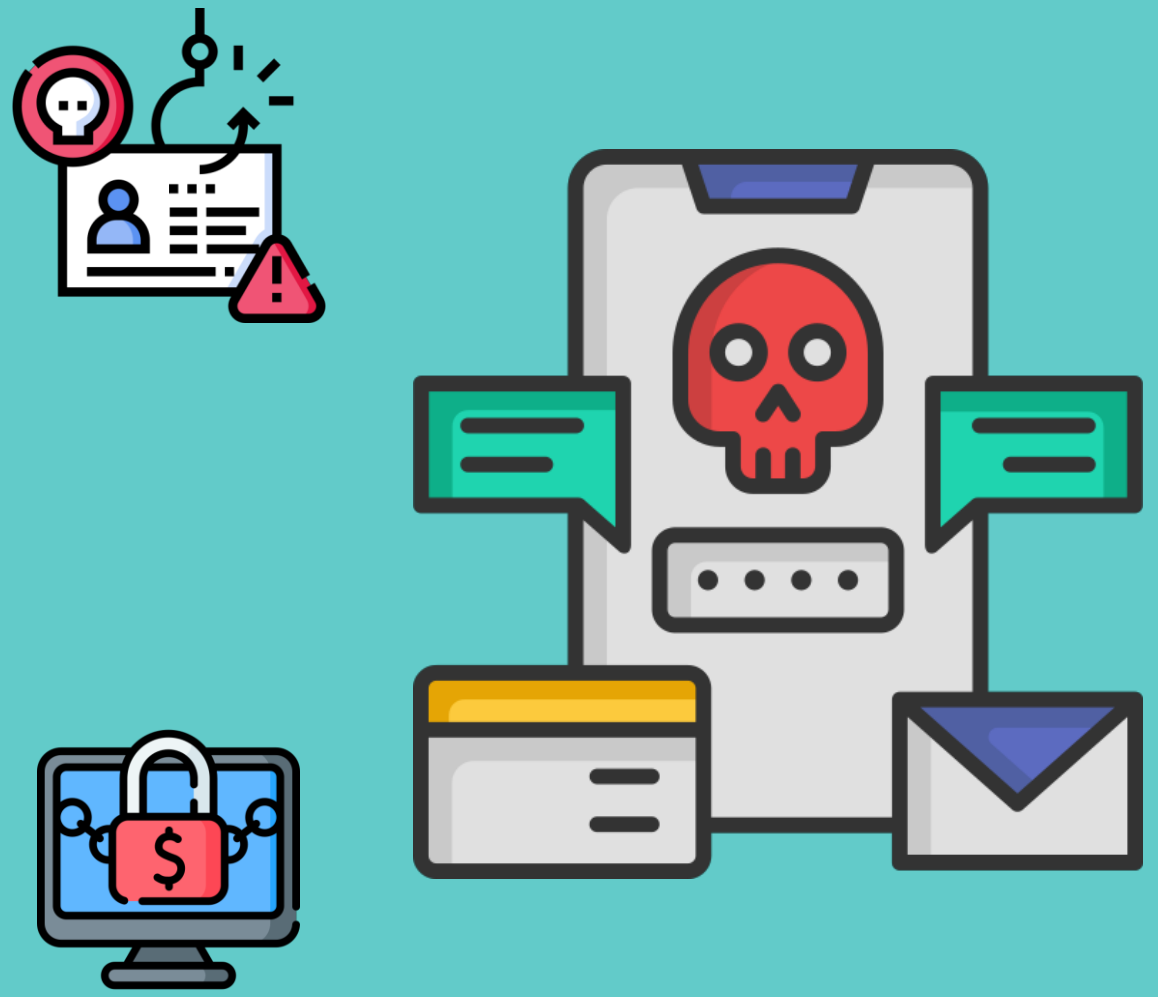
Vulnerabilities *จุดอ่อน

Weaknesses which can be exploited by threats to gain unauthorized access or damage the system.

Examples

เรียกค่าไถ่

Malware, phishing, ransomware, social engineering, zero-day exploits. ใช้ข้อมูลของเรา



01

การจัดการความเสี่ยง

Risk Management in Information Security

Risk Assessment วิเคราะห์ความเสี่ยง

Process of identifying, assessing, and prioritizing risks. หา ประเมินระดับความเสี่ยง จัดลำดับความสำคัญ

Risk Mitigation Strategies ลดความเสี่ยง

Techniques to **manage and reduce** risks (e.g., security policies, training and awareness, technical controls).

ป้องกัน

Continuous Monitoring เฝ้าระวัง

Ongoing assessment of the security posture to identify and respond to new risks.

01

Best Practices and Frameworks

Security Policies & Procedures

Development and implementation of security policies, procedures, and guidelines.

Security Frameworks & Standards

Overview of common frameworks and standards (e.g., ISO 27001, NIST Cybersecurity Framework) that guide information security practices.

*Education & Awareness

Importance of regular training and awareness programs for all employees.

Key Takeaways

Overview & Principles of Information Security

1. The **CIA Triad** is Fundamental to Information Security.
2. Understanding and Managing **Risks** is Essential.
3. A **Proactive** Approach and Awareness are Keys.

02

Governance, Risk & Compliance (GRC)

Key Objectives

Governance, Risk & Compliance (GRC)

1. Introduction to GRC
2. Governance in Information Security
3. Risk Management in GRC
4. Compliance in Information Security
5. Implementation a GRC Framework

02

Introduction to Governance, Risk & Compliance (GRC)

Definition

องค์กรที่มีหลักการและรูปแบบที่ชัดเจนในการจัดการความเสี่ยงในรูปแบบต่างๆ

GRC is an integrated **capability** (ความสามารถ) to ensure an organization reliably achieves objectives, addresses uncertainty (ความไม่แน่นอน), and acts with integrity.

Importance

เราทำธุรกิจต้องทำงานร่วมกับหลายฝ่ายจึงมีการออก กฎเพื่อให้ทุกกลุ่มทำงานร่วมกันได้

GRC helps organizations achieve their business goals, manage risk effectively, and ensure compliance with laws and regulations.

Components

- Governance (strategic leadership and oversight) — ตั้งหน่วยงานขึ้นมากำกับดูแล
- Risk Management (identifying and mitigating risks) — หาและจัดการความเสี่ยง
- Compliance (adhering to standards & regulations) — กฎอะไรก็ตามที่สร้างขึ้นมา ต้องทำตาม

02

Governance in Information Security

Definition ออกนโยบายเพื่อให้ทุกคนปฏิบัตรตามขั้นตอน

The framework of **policies**, **processes**, **and structures** to ensure IT supports and enables the organization's strategies and objectives.

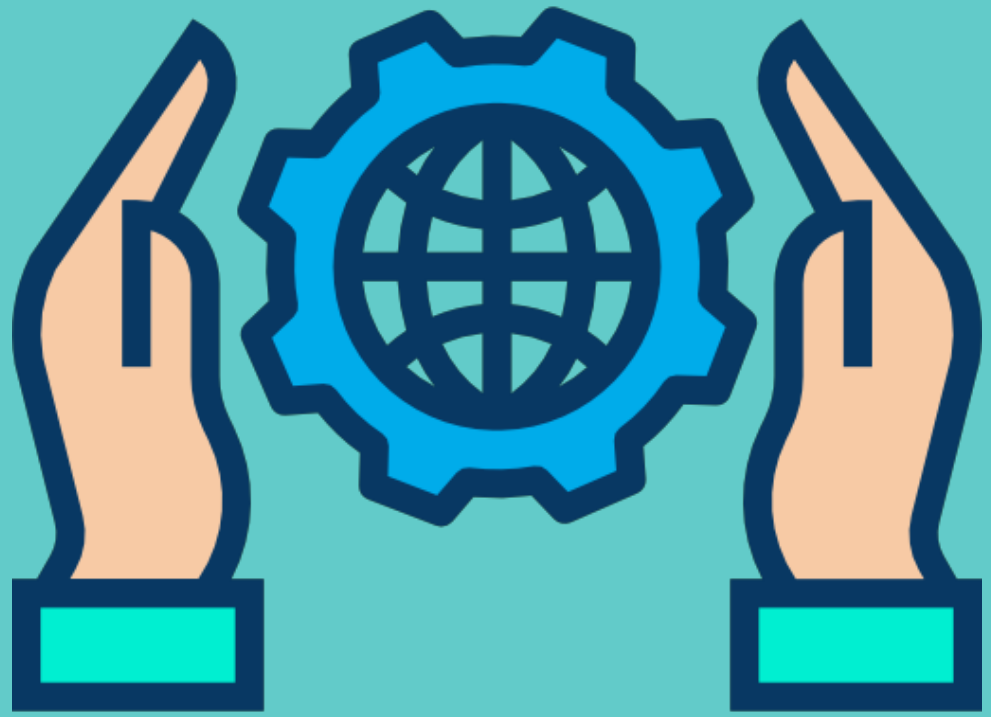
นโยบาย ขั้นตอนการทำงาน

Key Elements

- Strategic Alignment กำหนดเป้าหมายขององค์กร
- Value Delivery มูลค่าที่เราสามารถปกป้องข้อมูลได้
- Resource Management จัดการแหล่งที่มา
- Risk Management
- Performance Measurement วัดผลการทำงาน

Role of Leadership ผู้นำสูงสุดขององค์กร ลงมาจัดการ

Leadership must **actively** define, communicate, and enforce policies and practices, ensuring that governance is not just a concept but an organizational reality.



Risk Management in GRC

Definition

The systematic process of **understanding**, **evaluating**, & **addressing risks** to achieve objectives in a manner consistent with organizational values & the protection of people.

Steps

- 1 Risk Identification — หาความเสี่ยงให้เจอ
- 2 Risk Assessment — ประเมินระดับของความเสี่ยง[สูง,ต่ำ]
- 3 Risk Mitigation — จัดการกับความเสี่ยง
- 4 Monitoring — เฝ้าระวังไม่ให้เกิดขึ้นอีก

Integration with Governance & Compliance

A **bridge** between governance (ensuring risks are considered in decision-making) and compliance (identifying risks of non-compliance and mitigating them). *ทำให้ตัวเองสามารถจัดการกับความเสี่ยงและปฏิบัติตามกฎ

Risk Management

02

Compliance in Information Security

Definition อะไรที่เขาบอกให้เราทำเราต้องทำตามนั้นเปะๆ

Conforming to stated requirements. In an organizational context, it means meeting the laws, regulations, guidelines, and specifications relevant to its business processes.

Challenges

- Keeping up with changing regulations
- Ensuring employee awareness
- Maintaining documentation and evidence of compliance

Best Practices

- Regular compliance audits ประเมินตัวเอง
- Continuous monitoring เช็คข้อมูลให้เป็นไปตามที่กำหนด
- Compliance management processes/systems
  - ตั้งฝ่ายงานเพื่อมาทำกับดูแล 2 ข้อบน

02

Implementing a GRC Framework

เริ่มต้นทำ

Steps for Implementation

- 1 Assess current state — วิเคราะห์ว่าตัวเองเป็นยังไงมีอะไรและยังขาดอะไรบ้าง
- 2 Define strategy and objectives — เราจะทำอะไรบ้างครบแค่ไหนเอาทุกอันหรือบางส่วน [กำหนดขอบเขต]
- 3 Implement processes and tools — เราทำเอง จ้างที่ปรึกษา หรือตั้งทีมมาดูแล
- 4 Continuous improvement → ทำต่อไปเรื่อยๆเพื่อให้ดีขึ้นเรื่อยๆ

Technology's Role

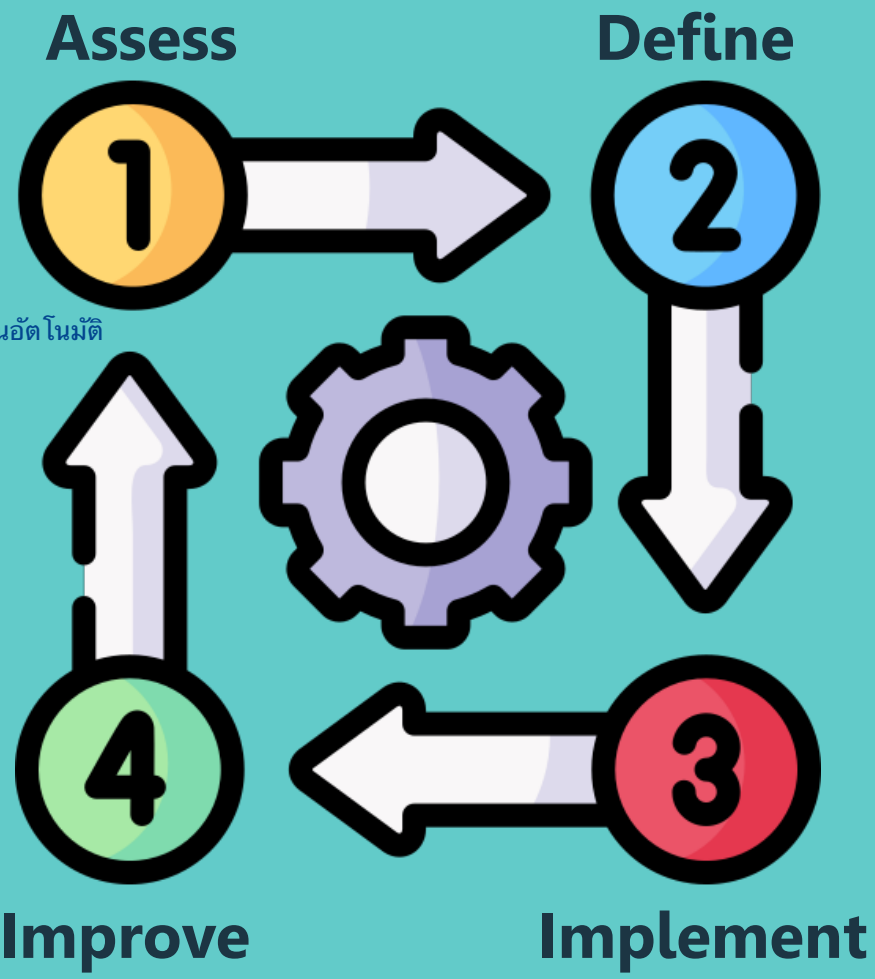
ใช้ Tools เข้ามาช่วยในการจัดการเพื่อให้ทำงานอัตโนมัติ

GRC technology platforms can **automate** many aspects of governance, risk management, and compliance, making these processes **more efficient and less prone** to error.

Benefits

- Enhanced decision-making
- Improved efficiency
- Reduced risk ลดความเสี่ยง

GRC Implementation



Key Takeaways

Governance, Risk & Compliance (GRC)

1. **Integrated approach** enhances organizational resilience.
2. **Proactive risk management** is crucial for security.
3. **Compliance** cultivates trust and ensures business continuity.

03

Information Security Framework:

NIST

Key Objectives

ฐานของทุกสิ่ง

NIST (National Institute of Standards and Technology) Cybersecurity Framework

1. Introduction to NIST CSF
2. Identify & Protect Functions
3. Detect & Respond Functions
4. Recover Function & Continuous Improvement
5. Implementing the NIST CSF

Introduction to NIST CSF

Origin and Purpose

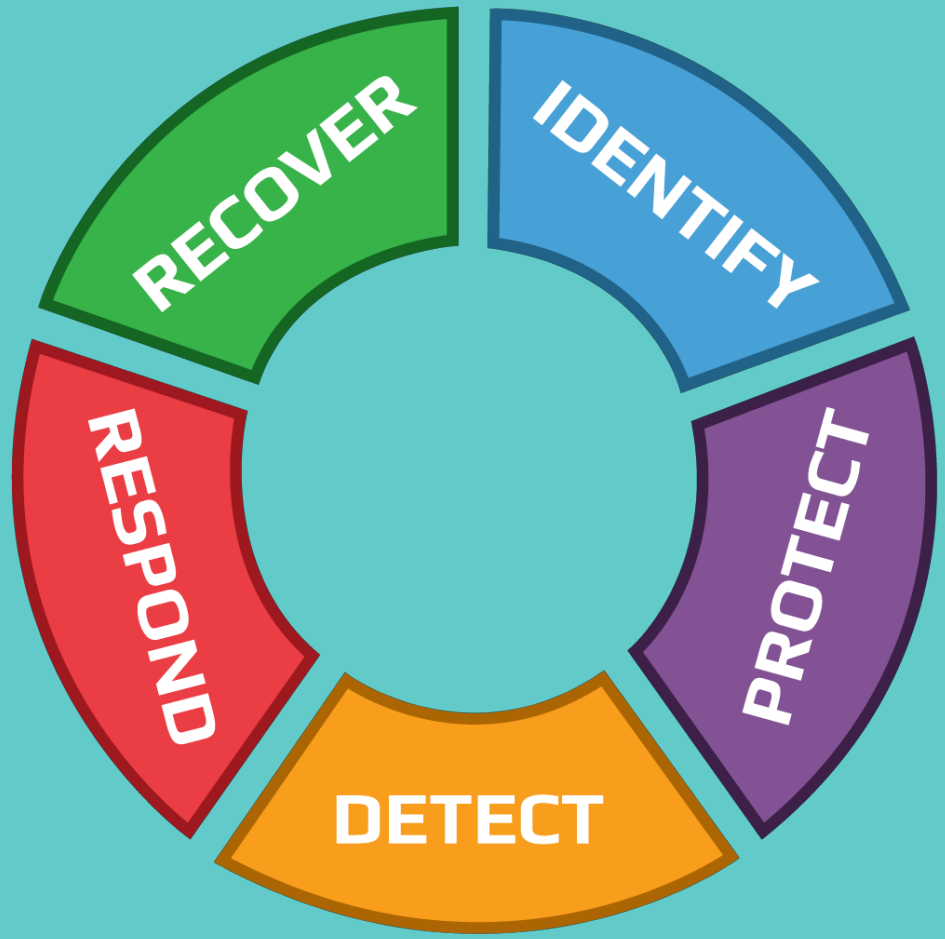
The NIST Cybersecurity Framework was developed to provide organizations with a set of industry **standards and best practices** to help manage cybersecurity risks.

Core Functions

- Identify
- Protect
- Detect
- Respond
- Recover

Benefits

- Help organizations mitigate risk
- Manage cybersecurity incidents
- Align cybersecurity policies with business objectives ยึดหยุ่นต่อธุรกิจ



03

Identify & Protect Functions

Risk Identification ระหาความเสี่ยง

- Understanding business context เข้าใจธุรกิจตัวเอง
- Resources supporting critical functions
- Related cybersecurity risks

Implementing Safeguards ติดตั้งตัวป้องกัน

Protect function: developing and implementing the appropriate **safeguards** to ensure the delivery of critical infrastructure services.

Awareness & Training เทรนคนในบริษัท

Maintaining an informed workforce through ongoing awareness and training programs

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

Source: https://nist.gov

Detect & Respond Functions

Anomaly & Event Detection

Implementing appropriate activities to quickly & continuously **identify a cybersecurity event**.

คอยหาสิ่งที่ผิดปกติ ด้วยวิธีการ monitor (24 x 7)

Response Planning

The response plan outlines protocols and processes to be enacted in the event of a **detected cybersecurity incident**.

เจอความเสี่ยง ต้องวางแผนกับข้อมูลที่ได้มา → communicate → หาแนวทางรับมือ

Incident Mitigation

จัดการความเสี่ยง → เอาบทเรียนมาปรับปรุง

Post-incident, the focus is on containing the impact and moving swiftly to mitigate any damage or disruption caused by the incident.

Source: https://nist.gov

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

03 Recover Functions & Continuous Improvement

Recovery Planning กู้คืนระบบ

Recovery strategies should be put in place to **restore** any capabilities or services that were impaired due to a cybersecurity incident.

Improvement from Incident หมายถึงเกิดอะไรเพื่อ

Following a cybersecurity event, the organization should work on improving its cybersecurity practices based on the **lessons learned**. เรียนรู้สิ่งที่ผิดพลาด → ไม่ให้เกิดซ้ำ

Feedback Loops

- Data Collection of current security program.
- Analysis to identify improvement.
- Action to address any identified issues.
- Reassessment the actions taken.

Source: https://nist.gov

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Process & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Process	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

03

Implementing the NIST CSF

Customization & Integration

- Not a one-size-fits-all solution, need **to be customized** ปรับให้เข้ากับองค์กร
- Integrate with **existing policies** → เข้ากับนโยบายเดิมขององค์กร
- Align with business and regulatory requirements → ไม่ขัดต่อธุรกิจของเรา

Implementation Steps

- Engage stakeholders
- Assess current cybersecurity practices
- Determine goals
- Implement the Framework
- Create a robust cybersecurity program

NIST CSF 2.0

- To be released early 2024
- Add the 6th Core : "**Govern**" Function

NIST CSF 2.0

Key Takeaways

NIST Cybersecurity Framework

1. Comprehensive approach to cybersecurity by **5 key functions**: Identify, Protect, Detect, Respond, and Recover.
2. Customizable & flexible framework regardless of organization' size or sector.
3. Emphasis on **continuous improvement**.

04

Information Security Framework:

ISO 27001

Key Objectives

ISO 27001: Information Security Management System (ISMS)

1. Introduction to ISO 27001 (ความเป็นมา)
2. ISO 27001 Framework Overview (หลักการทำงาน)
3. Structure of ISO 27001:2022 (10 Clauses) (จุดเริ่มการนำ ISO มาใช้)
4. Structure of ISO 27001:2022 (93 Controls) (ต้องทำยังไงบ้างถึงจะปลอดภัย)
5. Implementing ISO 27001:2022 (นำไปใช้จริง)
6. Certification and Beyond (ขอใบรับรอง) (ทำซ้ำตลอด)
7. Affiliated Standards (มีตัวอื่นนอกจาก ISO)

Introduction to ISO 27001

ISO 27001 Overview

International standard for managing and securing sensitive company information, emphasizing the setup and maintenance of an Information Security Management System (**ISMS**). เกิดตอนสงคราม ควบคุมการผลิตลูกปืน ให้มีขนาดเท่ากัน

Benefits

- Enhanced data protection ป้องกันข้อมูล
- Compliance with global regulations
- Demonstrates to stakeholders a commitment to information security ทำให้โลกน่าอยู่

Evolution of ISO 27001

- ISO 27001:2005 (obsoleted)
- ISO 27001:2013 (obsolete in Oct 2025)
- **ISO 27001:2022** (started in Oct 2022) เป็นขั้นต่ำๆ

04

ISO 27001 Framework Overview

Key Components

- 10 Main clauses
- 93 Controls

The PDCA Cycle

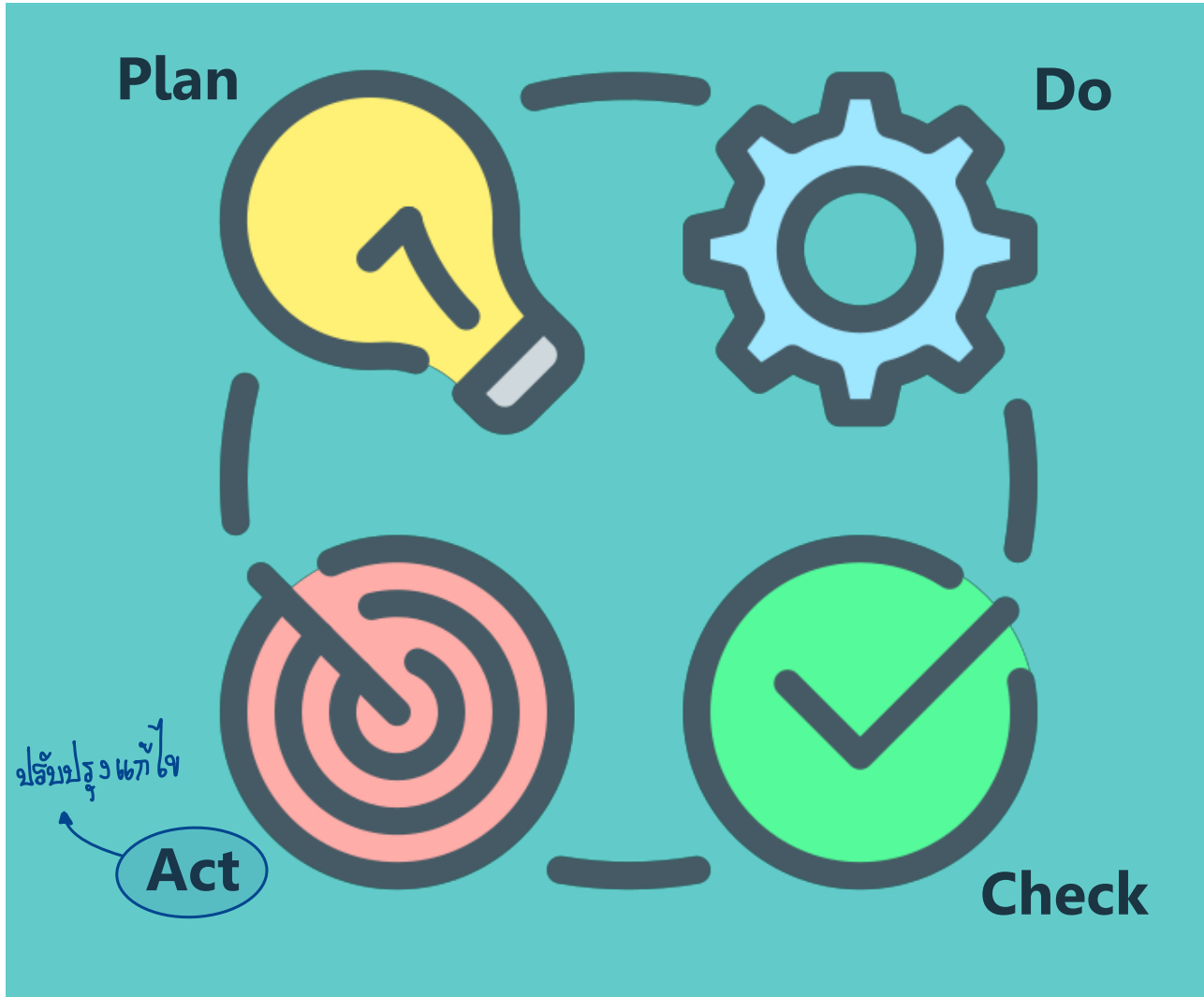
- Plan
- Do
- Check
- Act

Risk-Based Approach

Requiring organizations to **assess and treat information security risks** tailored to their needs.

ใช้ Risk Management ดีกว่า

PDCA



Structure of ISO 27001:2022 [10 Main Clauses]

10 Main Clauses

4. Context of the organization (รู้บริบทขององค์กรตัวเอง)
5. Leadership → ผู้นำสูงสุดต้องลงมา → GRC
6. Planning → ความเสี่ยงอะไร → ทรัพยสินมีอะไร → ทำที่ดีกว่า → ชัดเจนดีขึ้น
7. Support → คนมีความรู้ → สื่อสารและทำงานเป็นทีม → รองรับการเปลี่ยนแปลง
8. Operation → ทำตามแผน → ได้ผลลัพธ์มา
9. Performance evaluation → ใช้ 93 วิธีลดความเสี่ยง (ต้องครบ) หากไม่มีวิธีสามารถเขียนเพิ่มได้ → ต้องมีการทำ internal audit → รายงานผู้บริหาร พร้อมฟังความเห็น
10. Improvement → เก็บ Data → หาทางแก้ไข → ทำไงถึงจะไม่เกิดขึ้นอีก

ISO 27001 Clause 4 - 10

Source: BSI ISO/IEC 27001:2022 Lead Implementer Training Course

Structure of ISO 27001:2022 [93 Controls]

เครื่องมือลดความเสี่ยง

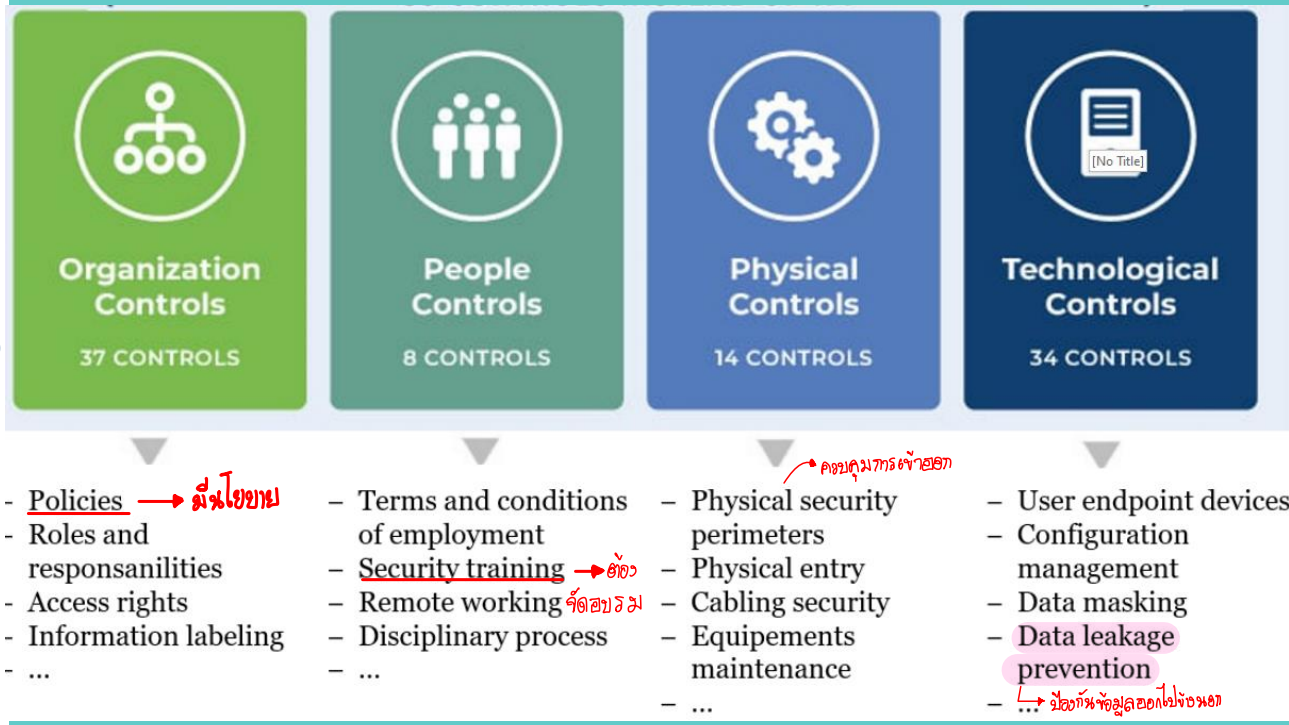
Key Changes in ISO 27001:2022

- Control set revision (From 114 to 93 controls)
- Emphasis on emerging technologies
- Enhance privacy consideration

93 Annex A Controls แบ่งกลุ่ม

- Organizational (37 controls) → องค์กรเป็นคนจัดการ(CEO)
- People (8 controls) → คนในองค์กร
- *Physical (14 controls) → อุปกรณ์หน้างาน(ห้องคอม)
- Technological (34 controls)
  - เขาเครื่องมือมาใช้

4 Themes of ISO 27001:2022



Source: Fatiha D. and Kim N. (2023), *A Comparative analysis of industrial cybersecurity standards*, IEEE Access

Implementing ISO 27001:2022

ใช้ ISO

Implementation Steps

- Define the **scope** กำหนด scope
- Conduct **risk assessments** to identify information security risks → ประเมินความเสี่ยง
- Select appropriate **controls** → หยิบ 93 ข้อมาทำทำทุกข้อ
- **Implement controls** within the organization → เข้ามาดูในชีวิตประจำวัน

Documentation & Record Keeping

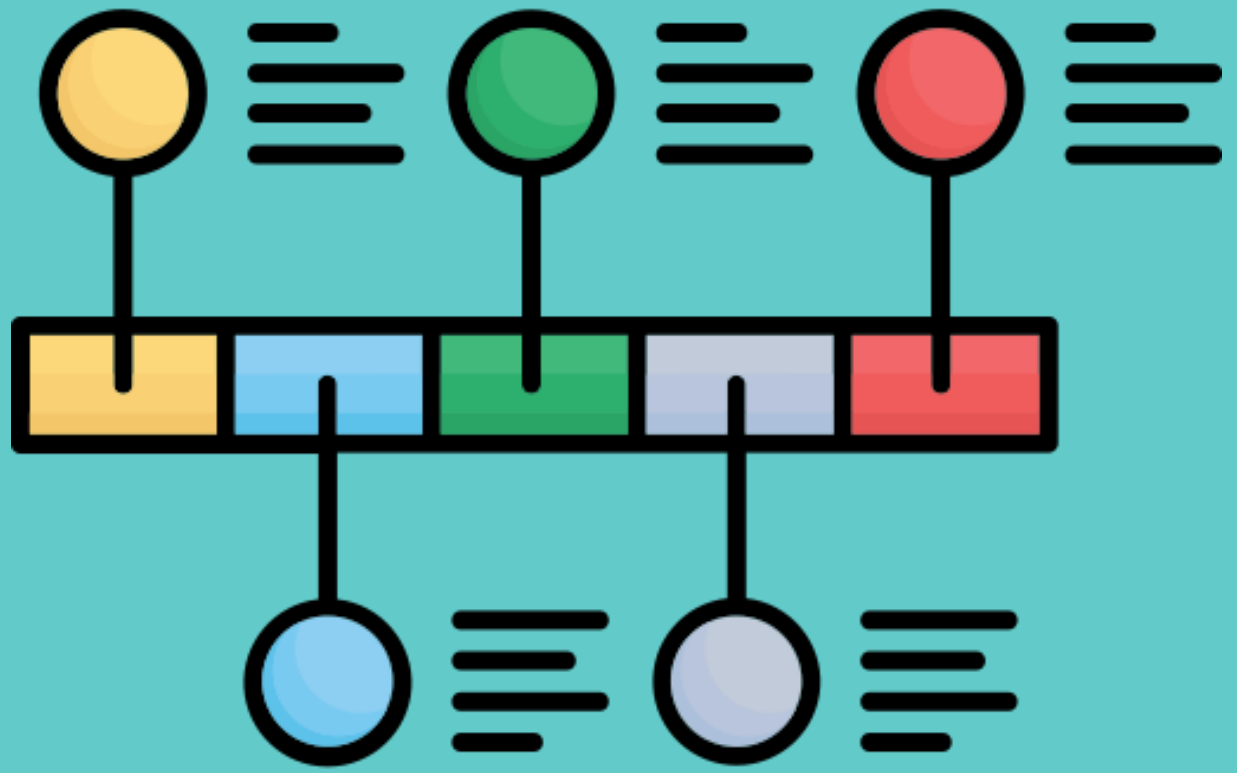
Documents that provide real value to the ISMS are encouraged/mandated to be maintained.

→ ต้องทำเอกสารเป็นทางการ
- กระดาษติดหน้า บ.
- ในสัญญาจ้าง
- ขึ้น web

Employee Involvement & Training

→ อบรมพนักงาน

Organization-wide **awareness and training**, ensuring everyone understands their role in maintaining information security.



Certification and Beyond (การขอใบรับรอง)

Certification Process

- Preparation (เตรียมตัวทำ : 10 Main clauses : 93 Controls)
- Conduct **internal audits** → จ้างภายนอกหรืออีกแผนก
- **Management review** process → รายงานผู้บริหาร
- **External audit** by an accredited body
  - ทำข้อก่อนหน้ามาก่อน → ให้มาตรวจและแก้ไข

Maintaining Certification → ต้องตรวจทุกปี ไปทำ Surveillance

Ongoing compliance and improvement to keep the certification valid, including **regular reviews and updates** to the ISMS.

Surveillance Audits → ถือว่าอายุ 3 ปี → ต้องตรวจทุกปี

Annual periodic audits by the certification body to ensure continued adherence to the standard.

04 Affiliated Standards

KBTG KASIKORN BUSINESS-TECHNOLOGY GROUP

ISO 20001 = ITSMS

- IT Service Management System (ITSMS)
- Ensure efficient and reliable **IT services** delivery and management

ISO 9000 → ชื่นชมหรือชอบให้ได้เหมือนเดิม

ISO 27701 = PIMS → ย่อมาจากนี้ได้ 27001

→ เกี่ยวกับข้อมูล

- Privacy Information Management System (PIMS) → PDPA
- Extension to ISO/IEC 27001
- Enhances controls for the processing and protection of **personal data**

SOC 2 Type 2 นิยมใน cloud

- Systems and Organization Controls 2
- Report on **operational effectiveness** of internal controls over time → วัดการทำหน้างาน
- Focuses: security, availability, processing integrity, confidentiality, and privacy (ไม่ต้องทำหมดก็ได้)

Key Takeaways

ISO 27001: Information Security Management System (ISMS)

1. Comprehensive Information Security Management อาศัยการทำงานร่วมกันทุกกลุ่ม → คน → ผู้บริหาร → resouce
2. **Risk-Based** Approach
   → ความเสี่ยง → เสี่ยงแค่ไหน → จัดการได้หรือไม่
3. Global Recognition and Trust
   ↓
   ทุกคนรู้จัก

05

CMMI Framework

Key Objectives

CMMI (Capability Maturity Model Integration) Framework

1. Introduction to CMMI
2. CMMI Maturity Levels — วัดเป็น Levels
3. CMMI Appraisals — ตรวจประเมินหลายแบบ
4. Benefits of CMMI Implementation
5. Adopting CMMI — การใช้งาน

Introduction to CMMI

CMMI Overview

- **Process level** improvement training and appraisal program
- Administered by the CMMI Institute
- Provides guidelines for developing **better products, services, and software**
- **CMMI Ver 3.0** (released Apr 2023)

CMMI Goals

- Make **process improvement** best practices into an organization's culture
- Decreases risks, errors, and costs
- Improves quality and time to market

CMMI Areas

- CMMI-DEV (for development)
- CMMI-SVC (for services)
- CMMI-ACQ (for acquisition)

CMMI 3.0 Practice Areas

Doing	• Delivering and Managing Services
	• Engineering and Developing Products
	• Ensuring Quality
	• Selecting and Managing Suppliers
		• Delivering and Managing Services
		  • Service Delivery Management
		  • Strategic Service Management
		• Engineering and Developing Products
		  • Product Integration
		  • Technical Solution
			• Ensuring Quality
			  • Peer Reviews
			  • Process Quality Assurance
			  • Requirements Development and Management
			  • Verification and Validation
			• Selecting and Managing Suppliers
			  • Supplier Agreement Management

Managing	• Managing Business Resilience
	• Managing the Workforce
	• Planning and Managing Work
		• Managing Business Resilience
		  • Continuity
		  • Incident Resolution and Prevention
		  • Risk and Opportunity Management
		• Managing the Workforce
		  • Enabling Virtual Work
		  • Organizational Training
		  • Workforce Empowerment
			• Planning and Managing Work
			  • Estimating
			  • Monitor and Control
			  • Planning

Enabling	• Managing Data
	• Managing Security and Safety
	• Supporting Implementation
		• Managing Data
		  • Data Management
		  • Data Quality
		• Managing Security and Safety
		  • Enabling Safety
		  • Enabling Security
		  • Managing Security Threats & Vulnerabilities
			• Supporting Implementation
			  • Casual Analysis and Resolution
			  • Configuration Management
			  • Decision Analysis and Resolution

Improving	• Improving Performance
	• Sustaining Habit and Persistence
		• Improving Performance
		  • Managing Performance and Measurement
		  • Process Asset Development
		  • Process Management
			• Sustaining Habit and Persistence
			  • Governance
			  • Implementation Infrastructure

Source: https://consulting.itgonline.com/cmmi-consulting/cmmi-v3-and-the-transition-from-cmmi-v2/

CMMI Maturity Levels

Maturity Levels Explained

1. Initial : Unpredictable process
2. Managed : Reactive process
3. Defined : Proactive process
4. Quantitatively Managed : Measured and controlled process
5. Optimizing : Continuous improved process

Roadmap for Improvement

These levels provide a **structured path** for organizational process improvement, with each level building on the previous one.

Benchmarking Process Maturity

Organizations use these levels to assess their current process **maturity** against recognized best practices, facilitating targeted improvements.

Source: https://cmmiinstitute.com/

CMMI Maturity Levels

CMMI Appraisals

Purpose of Appraisals

CMMI appraisals are conducted **to evaluate** an organization's adherence to the model and identify areas for process improvement.

SCAMPI Appraisals Method การตรวจประเมิน

- Benchmark Appraisal ตรวจใหญ่ว่าอยู่ใน Levels ไหน
- Sustainment Appraisal ติดตามคะแนนเพื่อให้ได้ตามมาตรฐานเดิม
- Action Plan Reappraisal → ตรวจเรื่องที่สอบตกบางเรื่องเล็กๆ
- Evaluation Appraisal
  → จำลองการตรวจจริง(ไม่เป็นทางการ)

Continuous Improvement Support

With ongoing, incremental enhancements to processes and practices --> process **maturity evolves over time**.

Source: https://cmmiinstitute.com/

CMMI Appraisal Method

05

Benefits of CMMI Implementation

Quality Improvement

Implementation of CMMI practices leads to **higher quality** products and services, enhancing **customer satisfaction**.

เพิ่มความพอใจให้ลูกค้า

Project Management Excellence

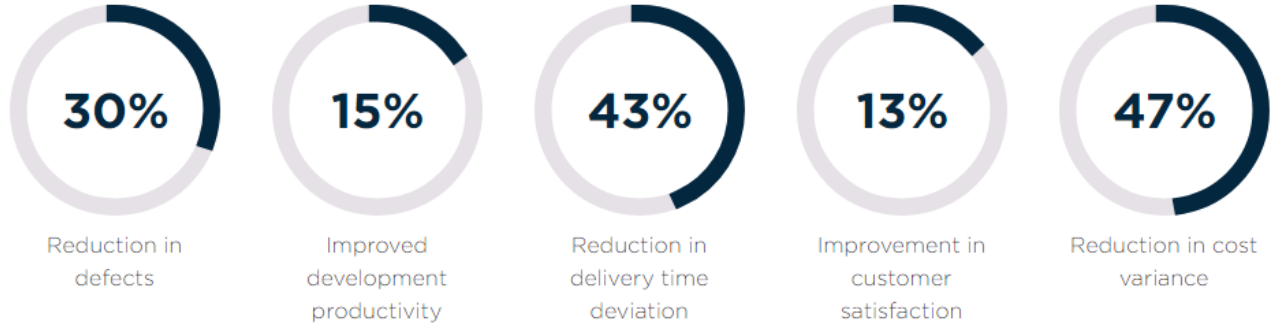
CMMI helps in achieving project goals more **reliably**, in terms of cost, schedule, and quality.

Synergy with Other Methodologies

CMMI complements other methodologies like Agile or Six Sigma, integrating best practices for broader organizational improvement.

CMMI → support Agile

CMMI performance result



Source: https://cmmiinstitute.com/

Adopting CMMI

Adoption Steps

- Gap analysis
- Training
- Process definition
- *Pilot projects
- *Full-scale implementation
- *Appraisal

* ISO ไม่มี

Leadership & Culture

หัวหน้าต้องสนับสนุน

Leadership commitment + Supportive culture = Successful adoption and sustainability of CMMI practices

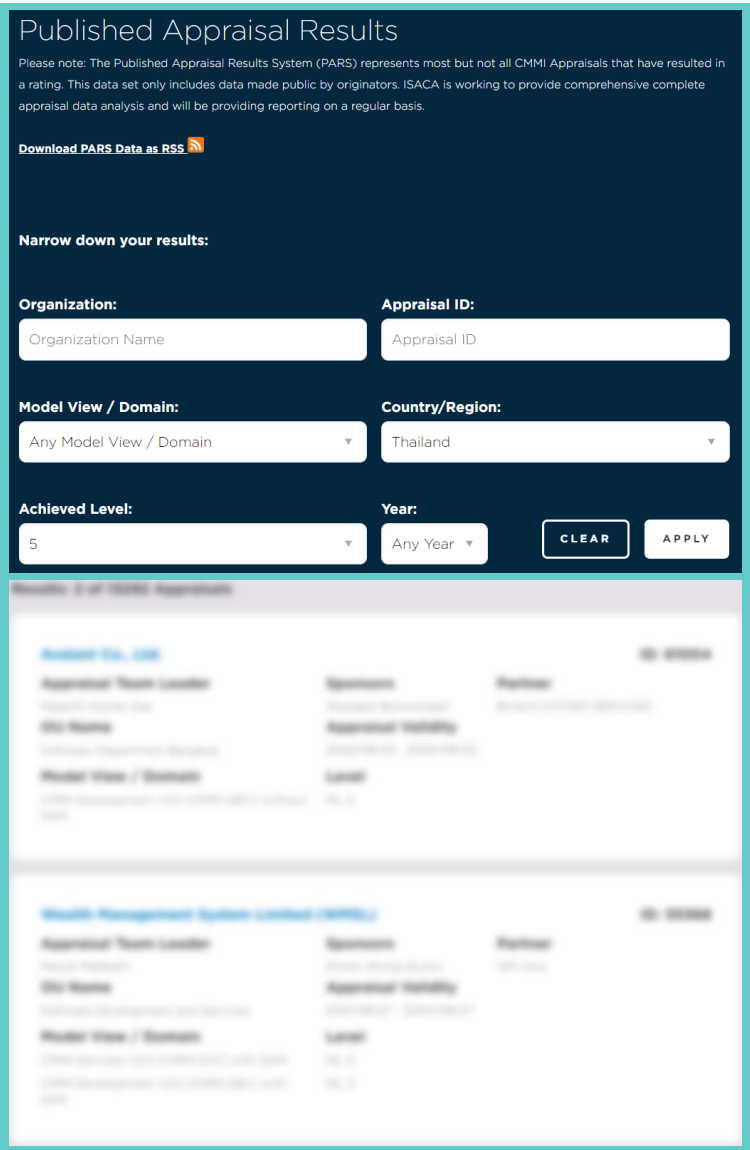
Strategic Benefits

- Long-term benefits
- Enhanced market reputation (**PAR system**)
- Improved competitive edge
- Alignment with industry best practices

เทียบของบริษัทที่ได้ CMMI → BENCHMARK
- ออดทันได้
- สามารถตั้งเป้าหมายตามที่เราอยากได้ ดูได้ว่าเขามีอะไรทำไมเราจะมี
- ลูกค้าสามารถเช็คได้

Source: https://cmmiinstitute.com/

CMMI Published Appraisal Results



Key Takeaways

CMMI Framework

1. Structured approach to **process improvement** เน้น การทำงาน
2. Focus on Maturity & Quality : **5 CMMI Levels**
3. Comprehensive **appraisal and feedback** System
   → ได้รับสิ่งที่ควรปรับให้เหมาะสมกับตน

06 Information Security Program

Key Objectives

Information Security Program

1. Overview
2. Key Components
3. Risk Assessment & Management
4. Incident Response & Recovery
5. Continuous Improvement & Adaptation

06

Overview of an Information Security Program

Definition & Purpose เขียนออกมาให้ชัดเจน

Set of **policies, procedures, processes and technical measures** used to protect the confidentiality, integrity, and availability of information.

Alignment with Business Objective

- Align with & Support organization's overall business objectives สอดคล้องกับธุรกิจ
- Ensure that security measures **do not impede** but rather enable business operations ไม่ block ธุรกิจ

Compliance and Risk Management * หากจำเป็นต้องใช้งาน ต้องขออนุญาต

- Manage **risks** to information assets
- Ensure **compliance** with relevant laws, regulations, and industry standards

ช่วยบริหารตามเสี่ยง

KBTG
KASIKORN BUSINESS-TECHNOLOGY GROUP

Information Security Program

Source: https://er.educause.edu/blogs/2018/5/crafting-an-information-security-program-strategy

06

Key Components of Information Security Program

Policy Framework

- A comprehensive **set of security policies**
- Define the governance structure, roles, responsibilities, and expected behaviors

Technical Controls

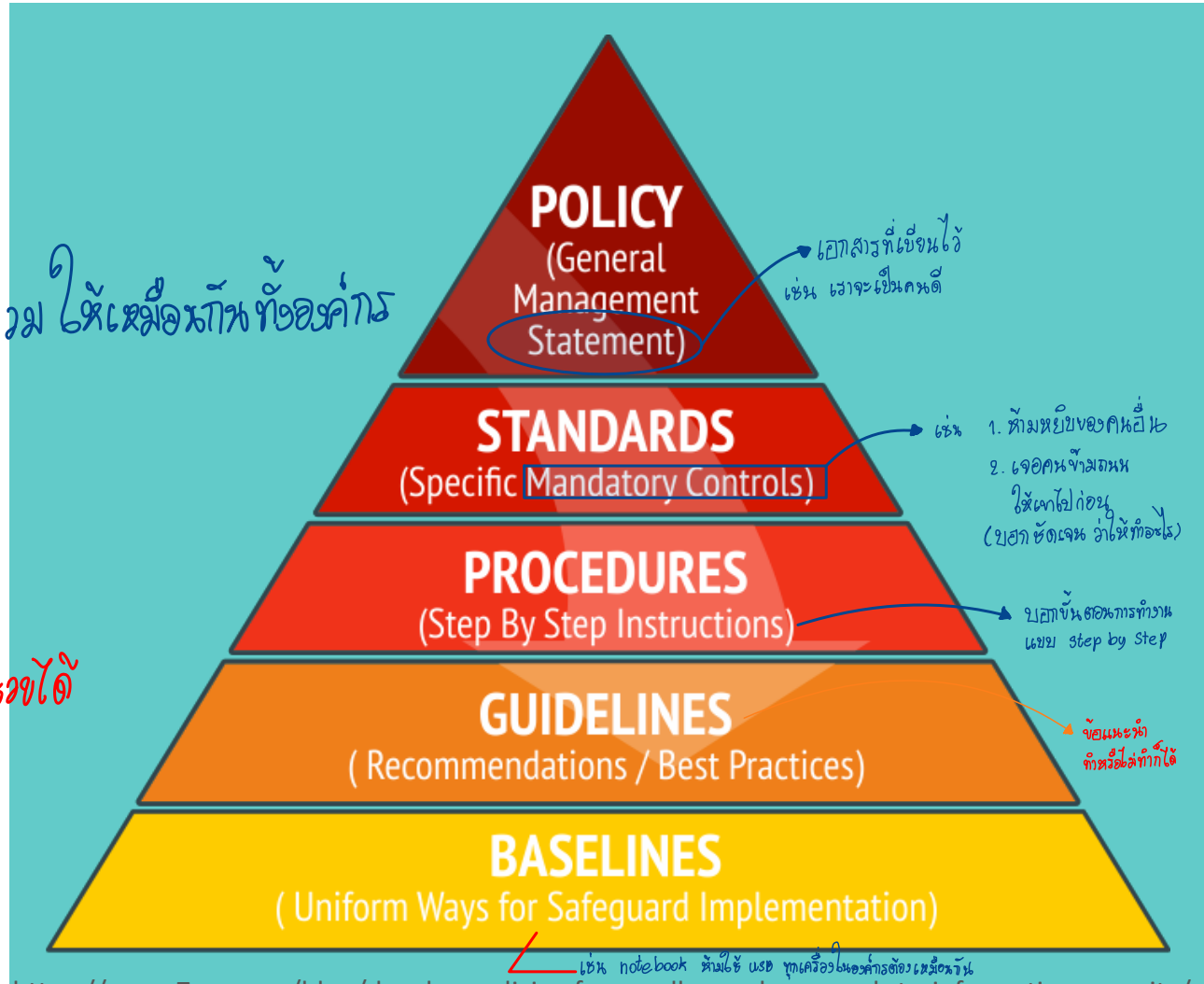
ใช้ควบคุมภาพรวม ให้เหมือนกันทั้งองค์กร

Implementing **technological controls** such as firewalls, encryption, and access controls to protect information assets

* Training & Awareness พนักงานสำคัญสุด เพราะถ้าไม่ทำก็ไม่มีอะไรช่วยได้

- Continuous training programs
- Employees are aware of the security policies
- Employees know **how to respond** to security incidents * เจอ incidents ต้องจัดการถูกต้อง

Rules of Policies Development



Source: https://www.7sec.com/blog/develop-policies-for-an-all-round-approach-to-information-security/

Risk Assessment & Management

Risk Identification

The process of **identifying potential threats** to information assets and vulnerabilities within the organization.

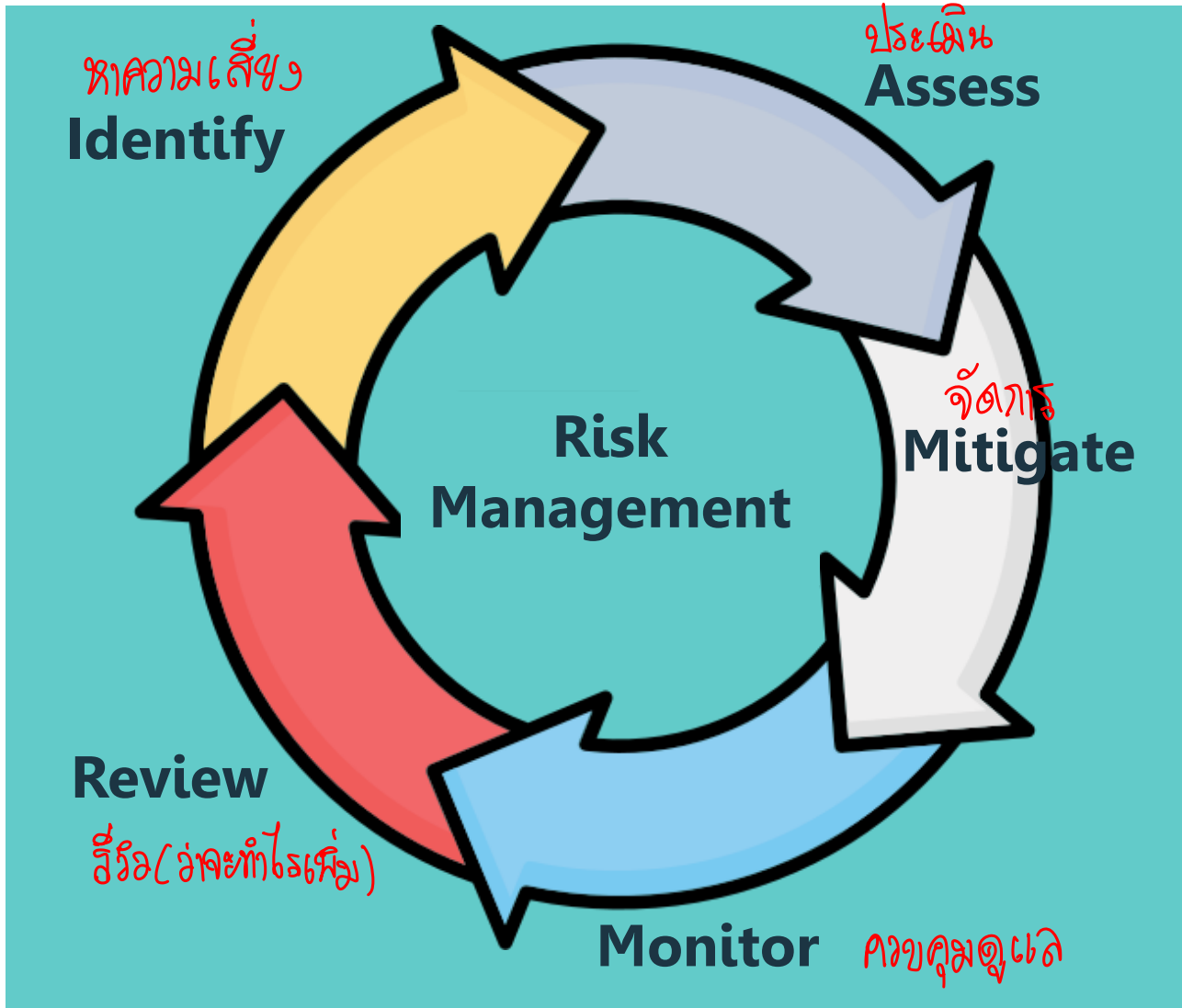
Risk Analysis

Evaluating the **potential impact and likelihood** of identified risks to prioritize response strategies.

Mitigation Strategies

Developing and implementing strategies to **mitigate identified risks**, including preventative controls and incident response plans.

Risk Management Processes



06

Incident Response & Recovery

Incident Response Planning

Preparing detailed plans for **responding to security incidents** to minimize impact and restore operations as quickly as possible.

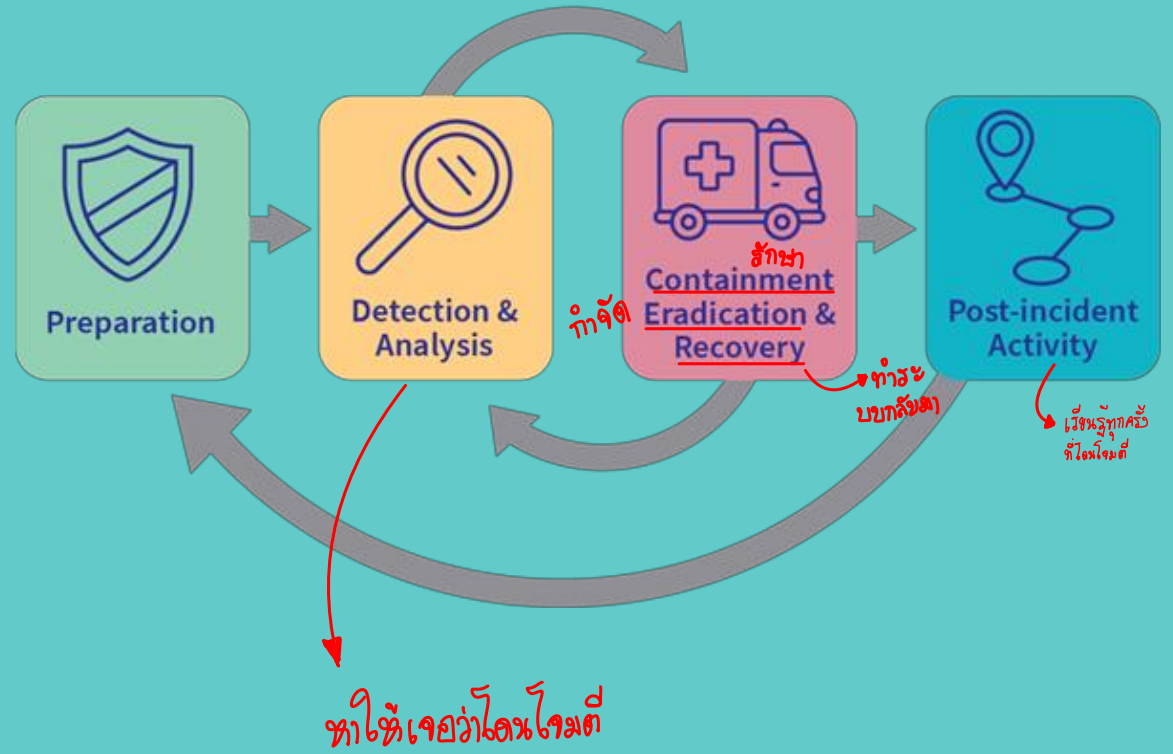
Communication Protocols

- Clear communication channels
- Protocols for reporting incidents
- Protocols for managing incidents

Recovery & Post-Incident Analysis

- Procedures for **recovering** from incidents
- Conduct post-incident analysis
  - Prevent future occurrences
  - Strengthen the security posture

CIRP Cyber Incident Response Cycle



Source: https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle

06

Continuous Improvement & Adaptation

Feedback Loops

- Feedback mechanisms ได้ข้อมูลกลับมาเพื่อวิเคราะห์แก้ไข
- **Learn** from security incidents and the effectiveness of controls
- Fostering a culture of continuous improvement

Technology & Threat Landscape Evolution

Regularly updating the security program to address new technologies and **evolving threats**.

Stakeholder Engagement คนเกี่ยวข้อง

- Employees
- Customers
- Partners
- External parties : Peers (ทำธุรกิจเหมือนกัน), Regulators ผู้กำกับดูแล

Key Takeaways

Information Security Program

ทำงานอย่างเป็นระบบ

1. Holistic approach to Cybersecurity.
2. Risk management = Heart.
3. Continuous improvement is essential.

ทำเสร็จทำต่อไป

07 Information Security Controls

Key Objectives

Information Security Controls

1. Overview
2. Information Security Policy
3. Information Security Standard & Procedures
4. Physical & Technical Controls
5. Roles & Responsibilities
6. Cybersecurity Dream Teams

07

Overview of Information Security Controls

Definition & Purpose

- Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical or digital assets.
- Encompass a range of practices, tools, and policies designed to protect CIA of data.

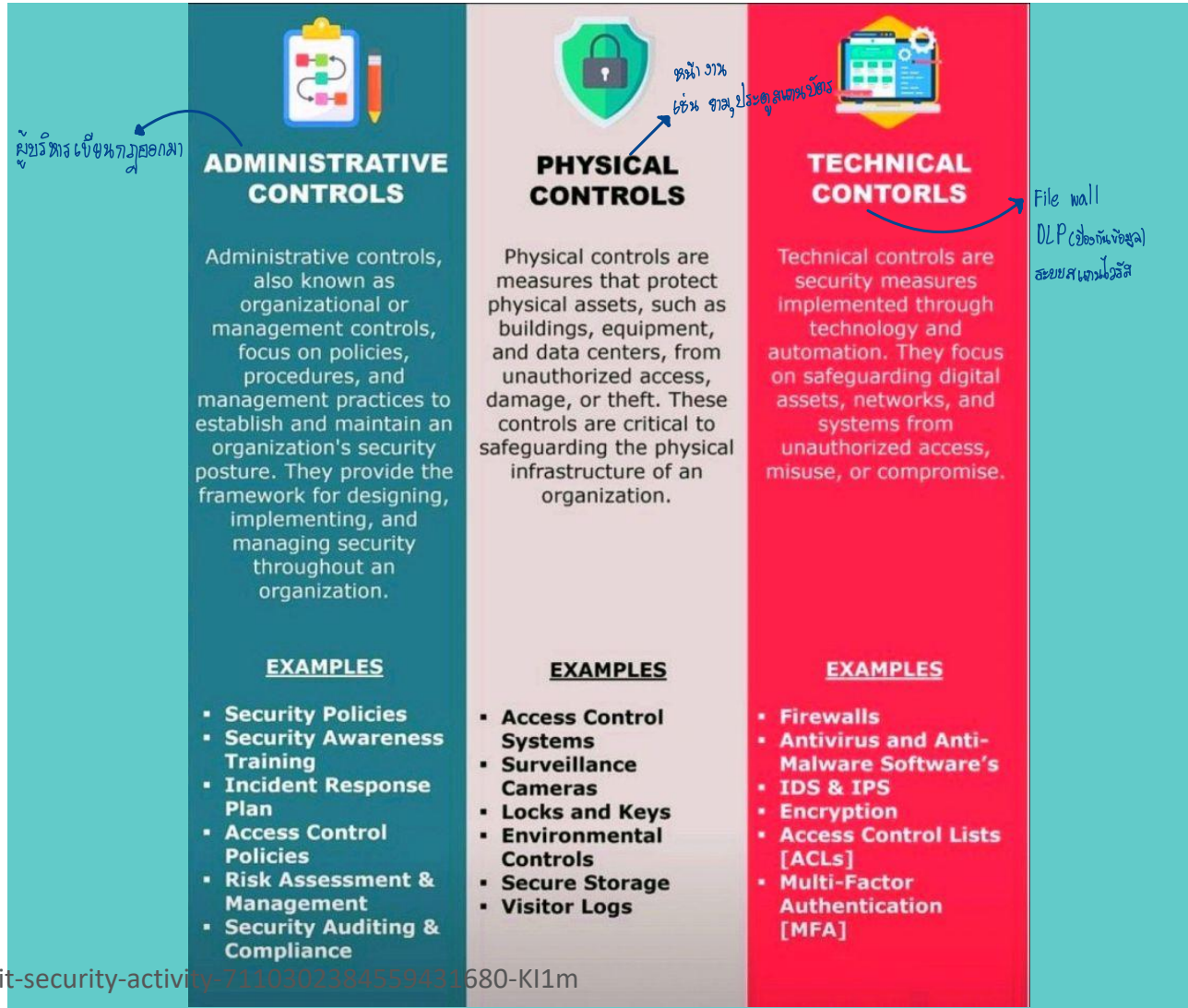
Type of Controls

- Administrative : policies, standards, procedures
- Physical : security guards, access controls
- Technical : firewalls, encryption, DLP, Antivirus

Layered Security Approach

Multi-layered defense strategy (defense in depth), ensuring no single point of failure

3 Types of Information Security Controls



Source: https://www.linkedin.com/posts/hemant-koli-57243035_there-are-three-main-types-of-it-security-activity-7110302384559431680-KI1m

07

Information Security Policies

Foundation of Security Program

Information security policies = backbone of an organization's security program, outlining the management's directives for securing information assets and guiding behavior.

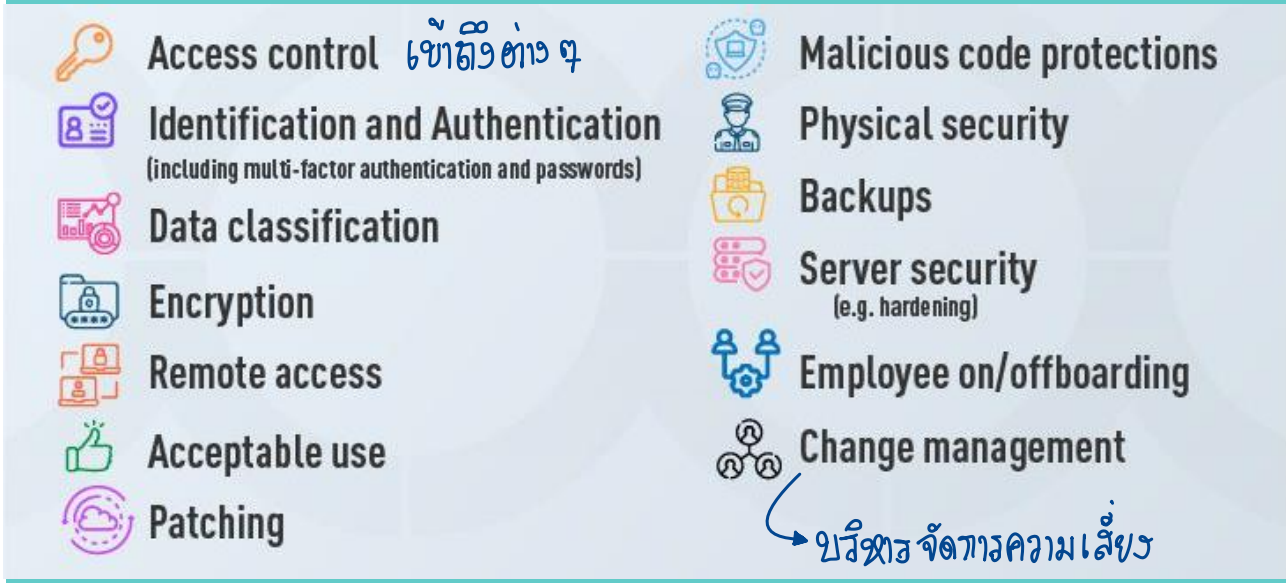
Scope & Objectives

- Define the scope of the security program
- Identify the roles and responsibilities
- Establish the objectives and goals for information protection.

Enforcement & Review

- Enforced through regular training and awareness programs
- Periodic review and updates to address evolving threats and organizational changes.

Information Security Policy Inclusions



Source: https://linfordco.com/blog/information-security-policies/

07

Standards, Procedures, Guidelines & Baseline

Standardization of Practices

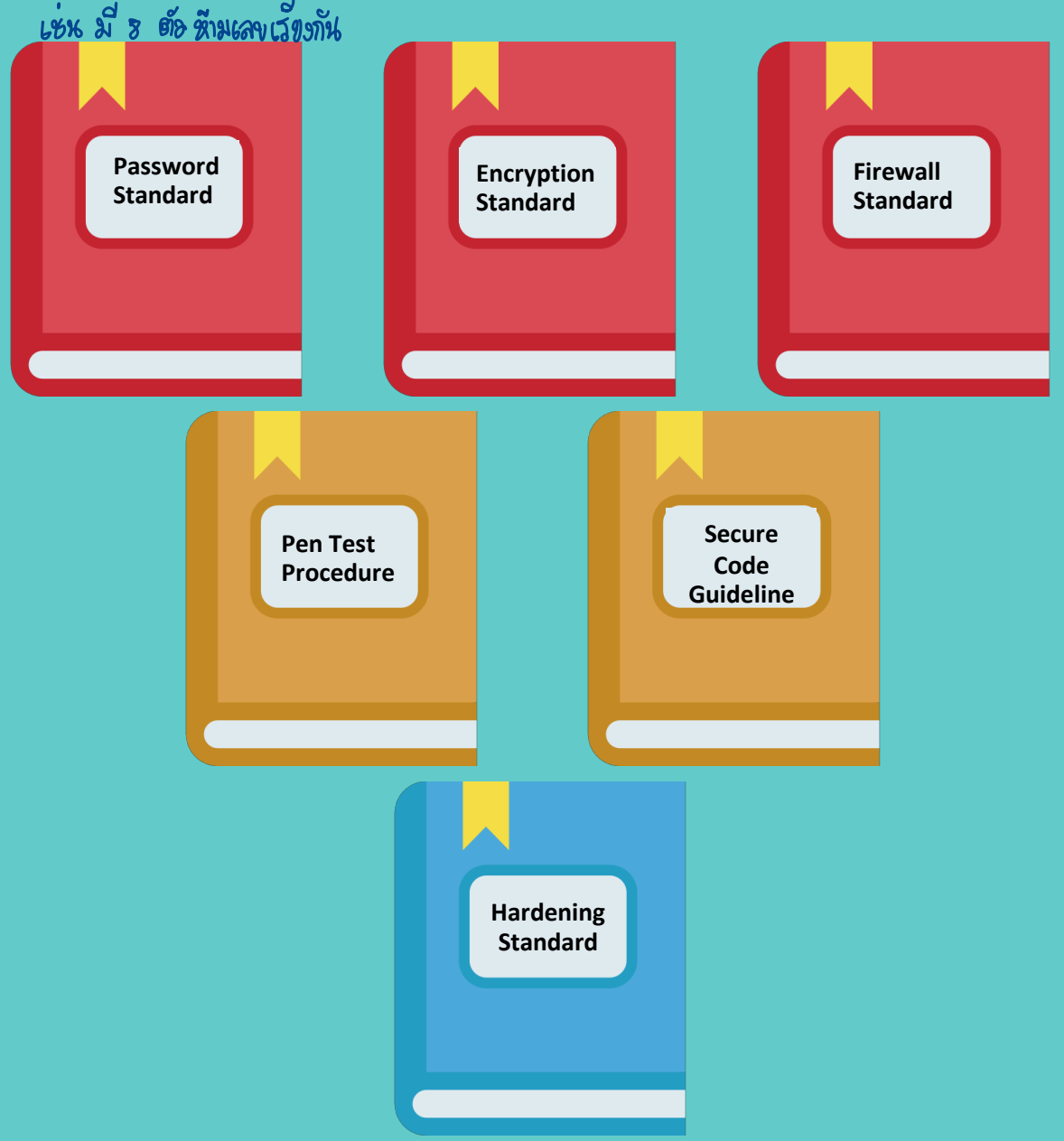
Information security standards provide a benchmark for implementing and measuring security practices, ensuring consistency and compliance with industry and regulatory requirements.

Detailed Implementation

Procedures and guidelines offer detailed, step-by-step instructions and recommendations for implementing the policies/standards, ensuring practical application and operational efficiency.

Security Configuration Baseline

A set of minimum cybersecurity standards for the configuration of systems and software within an organization, ensuring consistency in security posture across all technological assets.



Physical & Technical Controls

Physical Controls

- Access control systems
- Surveillance & Monitoring
- Environmental Controls
- Secure Disposal & Destruction
- Visitor Management

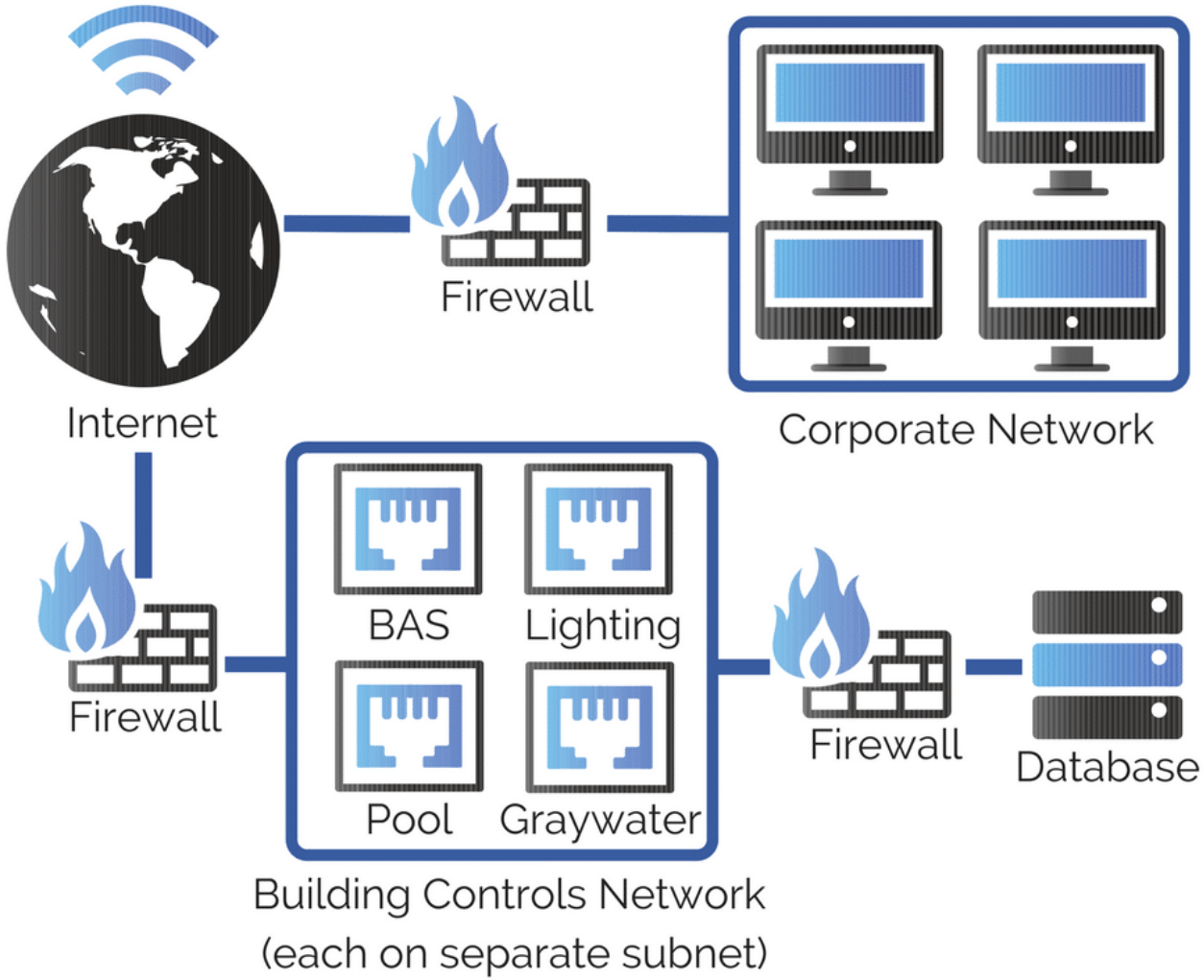
Technical Controls

- Technical mechanism protecting data
- Many are automated :
  - Real-time protection
  - Enhanced detection capabilities
  - Increased responsiveness

Continuous Monitoring

Enabling organizations to detect security breaches or anomalies promptly, facilitating rapid response and mitigation efforts.

Example of Security controls



Source: https://kw-engineering.com/protecting-your-building-cybersecurity-in-building-automation/

07 Roles & Responsibilities

Segregation of Duties แบ่งแยกหน้าที่อย่างชัดเจน

ใครรับผิดชอบหน้าที่อะไร

- Clear accountability
- Maker & Checker คนหนึ่งทำอีกคนเช็ค
- Individuals understand their part.

เข้าใจบทบาทของตัวเองในองค์กร

3 Lines of Defense

- 1st Line: Operational Management
- 2nd Line: Risk & Compliance
- 3rd Line: Internal Audit

คนที่ทำงานหน้างาน

คนอีกกลุ่มมาประเมินความเสี่ยง

ทีมมาตรวจหา Audit issue

Cyber Security Culture

Encouraging a culture of security across all lines of defense.

3 Lines of Defense

Source: https://slideplayer.com/slide/10648605/ = Aron O., "Three Lines of Defense and Business Continuity", February 18, 2016.

Cybersecurity Dream Teams

Technology Risk & Control Governance

- Information Technology Assurance สิ่งที่ต้องทำ ทำยังไง (มาเติมทีหลัง)
- Security Assurance
- Data Protection Office (DPO)
- Cyber Hygiene & Awareness

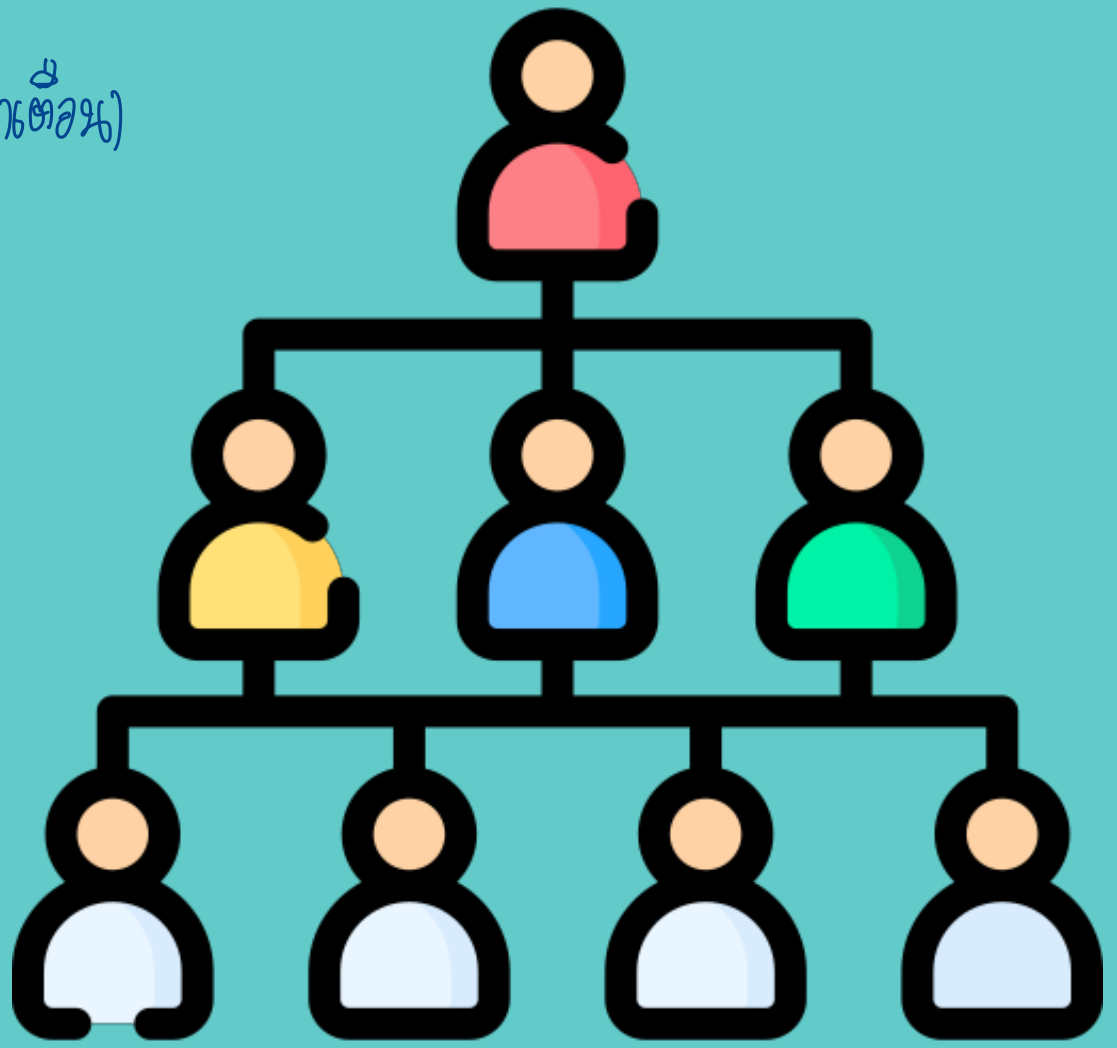
Enterprise Security Architect

- Security Architect → วางโครงสร้างสถาปัตยกรรมขององค์กร
- Security Engineer → กำหนด standard
- Security Advisory
- Regional Security Delivery

Cyber Defense Center CDC

- CyberSecurity Operation Center (CSOC)
- Offensive Security ทำ Red Team
- Security Incident Management → ดูความเสี่ยง → หรือควบคุมดูแล
- Security Access Management → ดูแลสิทธิ์เข้าใช้งาน
- Security Analysis วิเคราะห์ข้อมูล

24 x 7



Key Takeaways

Information Security Controls

1. Controls (administrative, physical, technical) are structured framework for cybersecurity.
2. Foundation is in Policy & Standardization.
3. 3 Lines of Defense provides independent assurance.

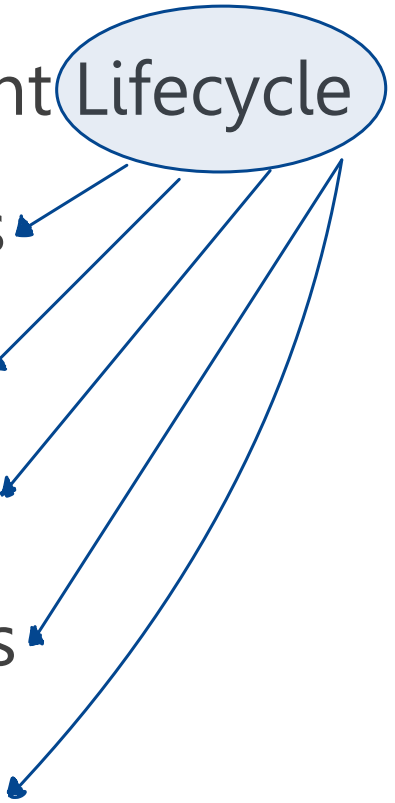
08

Risk Management

Key Objectives

Risk Management

1. Introduction to Information Security Risk Management
2. Risk Management Lifecycle
3. Identifying Risks
4. Assessing Risks
5. Mitigating Risks
6. Monitoring Risks
7. Reviewing Risks
8. Legal & Regulatory Compliance



Introduction to Risk Management

Definition

The process of identifying, analyzing, evaluating, and addressing an organization's cybersecurity risks to protect information assets and ensure business continuity.

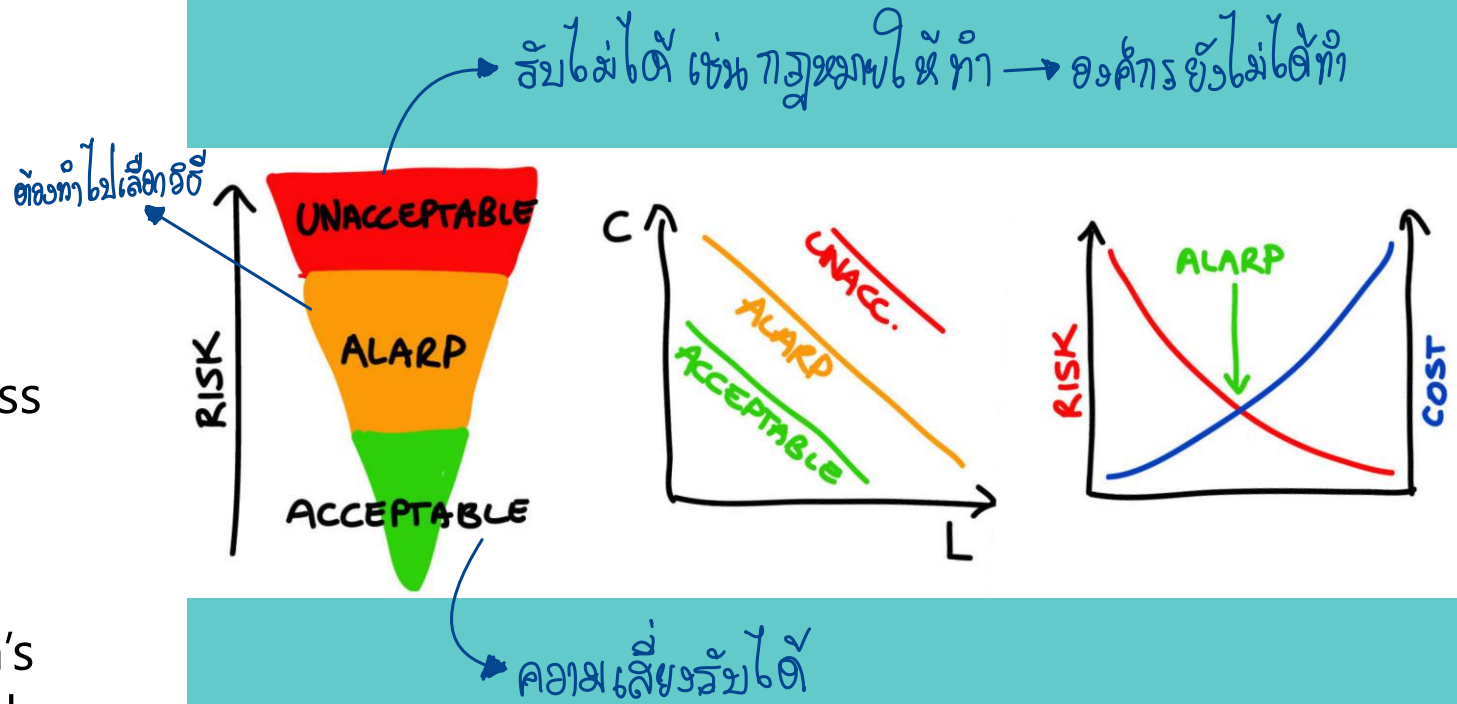
Objective

- Minimize risks to information assets to acceptable levels.
- Align cybersecurity efforts with business goals.

Acceptable Risk Level

A level of residual risk to the organization's operations, assets, or individuals that has been determined to be a reasonable level of potential loss/disruption.

ALARP = As Low As Reasonably Practicable



Source: https://www.therunwaycentreline.com/blog/2012/04/20/as-low-as-reasonably-practicable/

08

Risk Management Lifecycle

Phases

1. Identify หา
2. Assess ประเมิน
3. Mitigate จัดการ
4. Monitor ดูว่าเพิ่มหรือลด
5. Review มีความเสี่ยงใหม่หรือไม่

Cyclical Nature

Risk management is an ongoing process, requiring regular updates and adjustments as threats evolve and organizational priorities change.

Integration with Business Process

Integration of risk management into all levels of organizational planning and decision-making.

Risk Management Processes

1. Identifying Risks (ต่อ)

Asset Identification

ทรัพย์สิน

Cataloging information assets and determining their value to the organization.

Threat & Vulnerability Identification

รัฐศาสตร์ จุดอ่อน

Identifying potential threats (e.g., malware, hackers) and vulnerabilities within systems and processes.

Risk Sources Identification

Understanding the sources of risk, including internal, external, accidental, and deliberate.

2. Assessing Risks ประเมินความเสี่ยง

KBTG KASIKORN BUSINESS-TECHNOLOGY GROUP

Risk Analysis

Evaluating the likelihood and impact of identified risks on information assets.

Risk Evaluation

Prioritizing risks based on their potential impact on organizational objectives.

Tools & Techniques

- Utilizing qualitative and quantitative methods to assess risks accurately
- Risk Matrix --> **High**, **Medium**, **Low**

Example of Risk Matrix

Consequence					Increasing probability			
Severity Rating	People	Assets	Environment	Reputation	A	B	C	D
					Has occurred in Industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero impact	Manage for continued improvement			
1	Slight injury	Slight damage	Slight effect	Slight impact				
2	Minor injury	Minor damage	Minor effect	Limited impact		Incorporate risk-reducing measures		
3	Major injury	Local damage	Local effect	Considerable impact				
4	Single fatality	Major damage	Major effect	Major national impact			Failed to meet screening criteria	
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact				

Source: https://risktec.tuv.com/knowledge-bank/the-matrix-reloaded-our-guide-to-the-risk-assessment-matrix/

3. Mitigating Risks

Risk Treatment Options

1. Avoiding Risks
2. Accepting Risks
3. Transferring Risks
4. **Mitigating Risks**

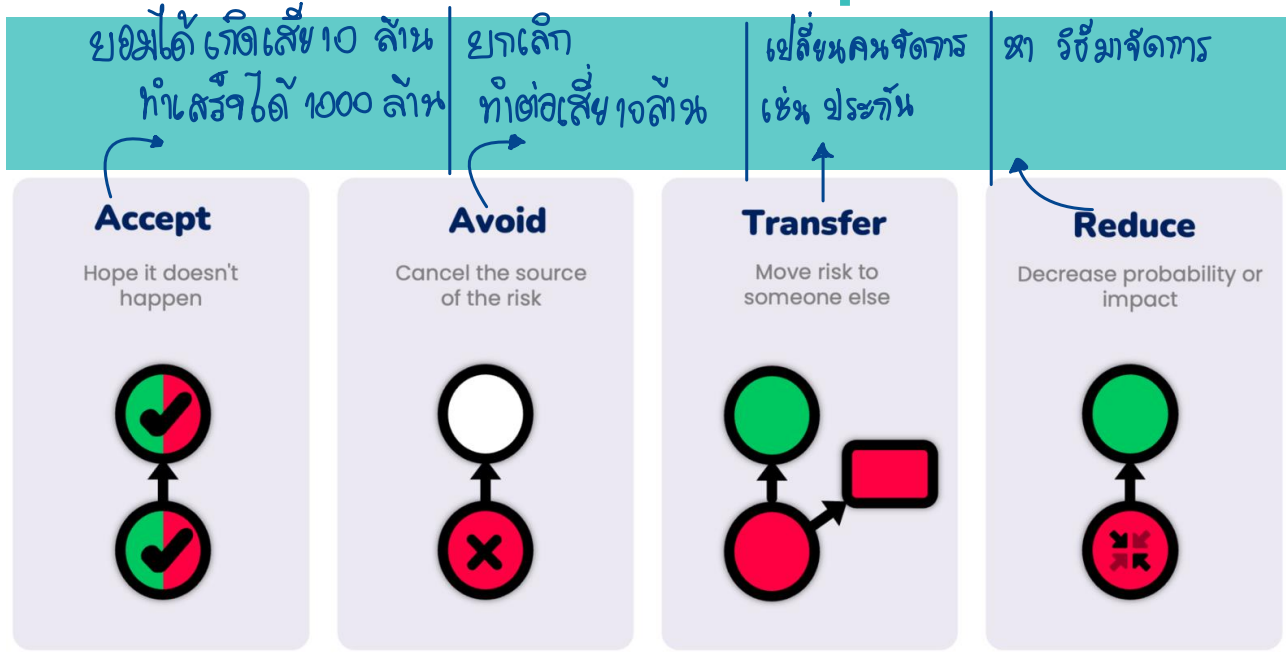
Implementation of Controls

Selecting and implementing appropriate security controls to mitigate identified risks.

Cost-Benefit Analysis

Considering the costs of implementing controls vs. the potential benefits of risk reduction. คุ้มค่าที่จะทำเทียบค่าใช้จ่าย

4 Risk Treatment Options



Source: https://aptien.com/en/kb/articles/what-are-risk-treatment-strategies/

4. Monitoring Risks

Continuous Monitoring

- Tracking Risk Treatment Plan (RTP).
- Establishing processes to continuously monitor risk levels and the effectiveness of controls.

Key Indicators

Developing key risk indicators (KRIs) and key performance indicators (KPIs) to measure risk and control effectiveness.

Adaptation

Adjusting controls as necessary based on monitoring feedback and changes in the risk environment.

Example of Risk Monitoring Tools

Source: https://www.processunity.com/cybersecurity-risk-management/

5. Reviewing Risks

Regular Reviews

Conducting periodic reviews of the risk management process to ensure its effectiveness and alignment with business goals.

Stakeholder Reporting

Communicating risk management activities and findings to stakeholders, including senior management and the board.

Documentation

Maintaining comprehensive documentation of the risk management process, findings, and actions taken.

Top 15 Cybersecurity Threats in 2024

Source: https://www.sprintzeal.com/blog/top-cybersecurity-threats

08

Legal & Regulatory Compliance

Compliance Requirements

Understanding legal, regulatory, and contractual obligations related to information security.

ดูกฎหมายด้วย ว่าต้องทำอะไรบ้าง

Alignment with Risk Management

Aligning compliance efforts with the overall risk management strategy.

Documentation

Using risk management processes to prepare for and facilitate compliance audits.

Regulatory Compliance

Source: https://www.cflowapps.com/process-compliance/

Key Takeaways

Risk Management

1. Risk management is a continuous and comprehensive approach.
2. Key success = Integration of People, Process, & Technology
3. Always align with Business objectives & Compliance * ทำให้ธุรกิจดำเนินต่อไปได้

09

กฎหมาย

Legal & Compliance

ทำตาม

Key Objectives

Legal & Compliance

1. Introduction
2. Key Legal Framework & Regulations
3. Intellectual Property Rights in Information Security ละเมิดลิขสิทธิ์
4. Compliance Strategies & Best Practices
5. Challenges & Future of Legal Compliance

Introduction to Legal & Compliance in Information Security

Purpose of Legal & Compliance

- Framework that organizations must operate
- Protect sensitive data, including personal, financial, and intellectual property
- Protect from unauthorized access or breaches

Impact on Business Operations

- Avoiding penalties
- Maintaining organizational reputation, trust with stakeholders, & competitive advantage

Evolving Landscape

- The legal and regulatory landscape is continuously evolving for new threats
- For examples: AI, Blockchain, IoT

Cybersecurity Compliance & Regulations

Source: https://www.linkedin.com/pulse/cybersecurity-compliance-regulations-you-should-know-safeguarding/

09

Key Legal Framework & Regulations

Country-wide Laws

ข้อมูลส่วนบุคคล

- Personal Data Protection Act (PDPA)
- Cybersecurity Act พรบ cyber
- Cybercrime Act พรบ คอมพิวเตอร์

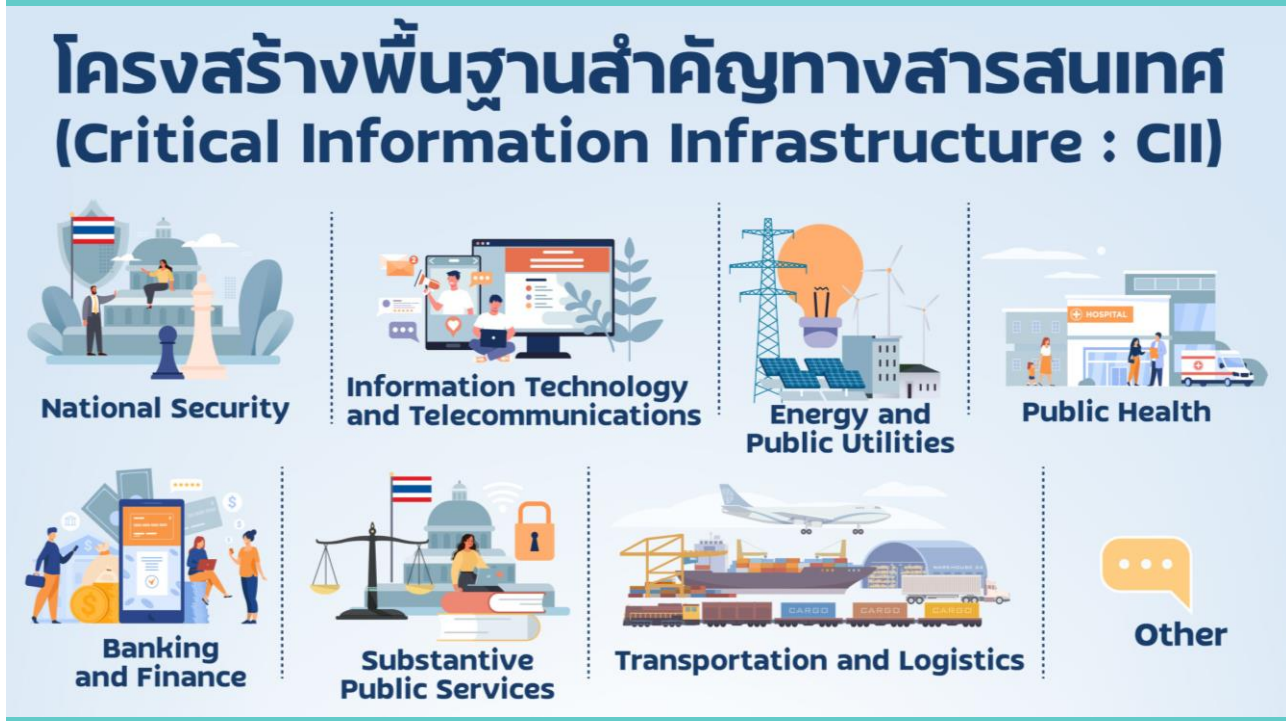
Industry-Specific Regulations บางกลุ่ม(มีผู้กำกับดูแล)

- Bank of Thailand (BOT)
- Securities & Exchange Commission (SEC) กลต
- Office of Insurance Commission (OIC) คปภ(ประกัน)

International Compliance Requirements (ต่างประเทศ)

- SWIFT → ธนาคาร swift
- PCI-DSS → V, master card
- PCI-PIN Security

Critical Information Infrastructure



Source: https://www.thaicert.or.th/en/cii/

09

Intellectual Property Rights in Information Security

ทรัพย์สินทางปัญญา (สำคัญมาก)

Importance of IP Protection

ดูหนังฟรี, อ่านหนังสือฟรี

Intellectual property such as patents, trademarks, and copyrights are vital assets that need protection from theft, infringement, and espionage in the digital realm.

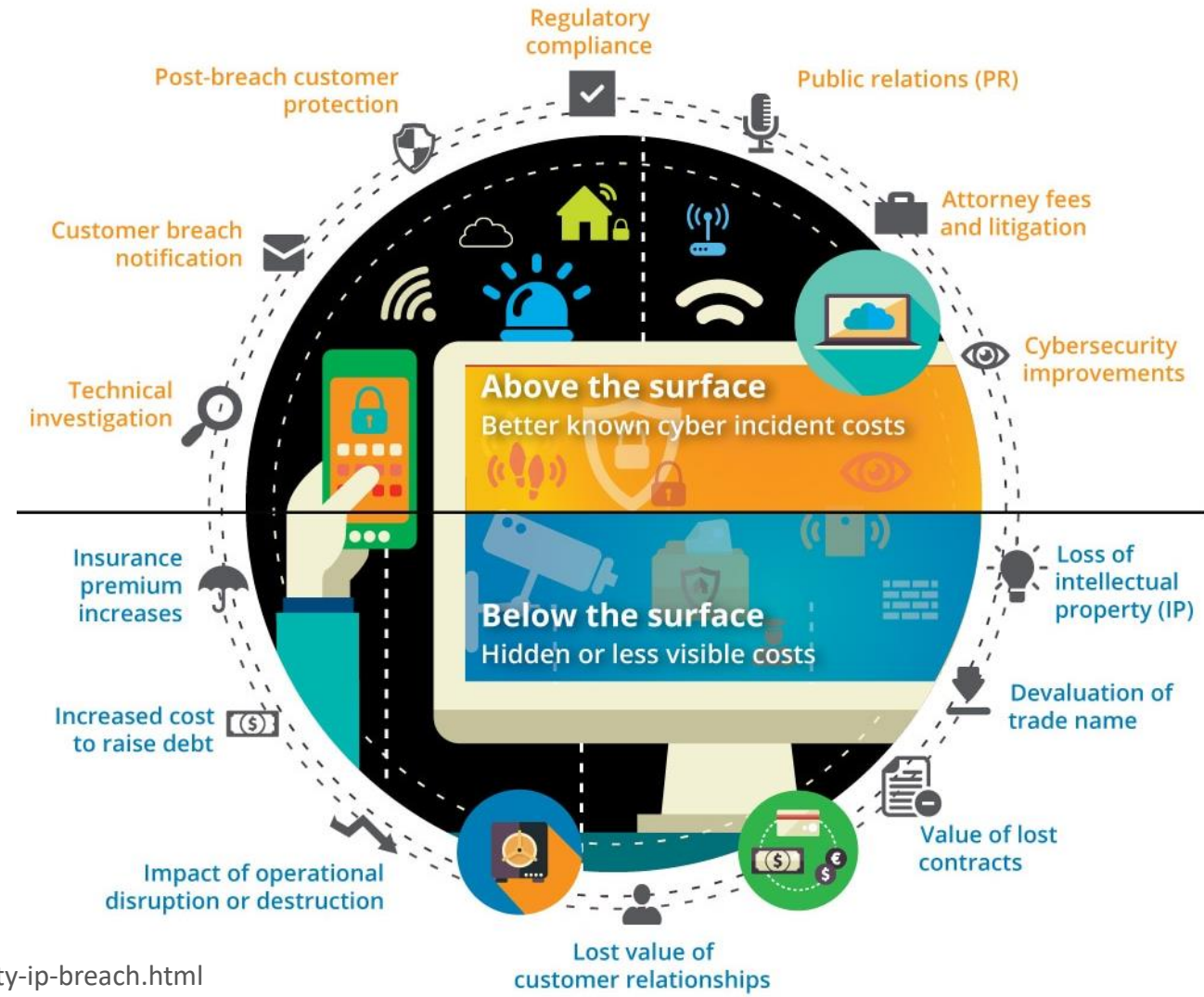
Cybersecurity Measures for IP

- Access controls
- Encryption
- Data loss prevention (DLP)

Legal Recourse and IP Laws

- Digital Millennium Copyright Act (DMCA)

Hidden costs of IP Breach



https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

09

Compliance Strategies & Best Practices

Risk Assessment & Management

Conducting regular risk assessments to identify and mitigate legal and compliance risks associated with information security.

Policy Development & Training

Developing comprehensive policies aligned with legal requirements and conducting regular training to ensure employee awareness and compliance.

Audit & Documentation

Implementing audit trails and maintaining documentation as evidence of compliance with relevant laws and regulations, crucial for legal defenses and audits.

Compliance & Audit

Source: https://steppa.ca/portfolio-view/it-audit-and-compliance/

09

Challenges & Future of Legal Compliance

Keeping Pace with Changes

The challenge of staying updated with rapid changes in legal requirements and cybersecurity threats, requiring ongoing education and adaptation.

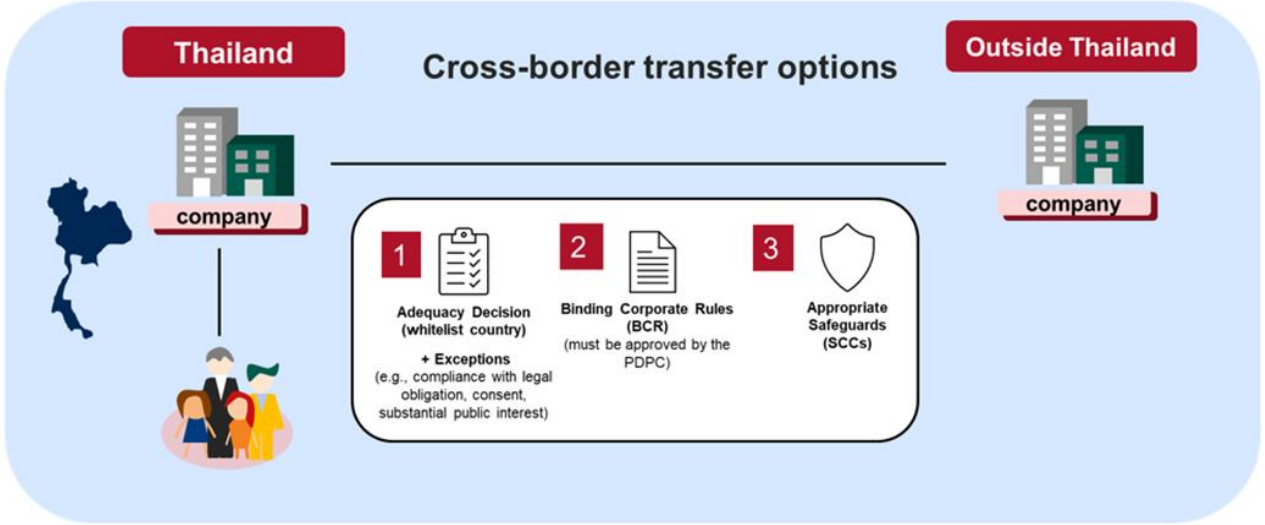
Cross-Border Data Flows * ส่งข้อมูลข้ามประเทศ

Navigating the complexities of cross-border data transfer regulations and ensuring compliance in a globally interconnected digital economy.

Anticipating Future Trends

Anticipate future legal trends: AI IoT, and emerging technologies, to ensure early compliance and strategic advantage.

Thailand Cross-border Data Transfer



Source: https://insightplus.bakermckenzie.com/bm/data-technology/thailand-new-cross-border-data-transfer-rules-officially-published-as-law/

Key Takeaways

Legal & Compliance

ทำเพื่อตอบโจทย์ทุกด้าน

1. Integrated approach to compliance and intellectual property protection

พยายามหาความเสี่ยงตลอด

2. Proactive compliance & Risk management

3. Future-proofing against emerging challenges → มีวิธีการรับมือที่ดี

10

Cyber Hygiene Culture & Awareness

Key Objectives

Cyber Hygiene Culture & Awareness

1. Introduction to Cyber Hygiene Culture
2. Key Elements of Cyber Hygiene
3. Security Awareness Programs
4. Measuring Culture & Awareness Impact
5. Challenges & Solutions in Fostering Cyber Hygiene

Introduction to Cyber Hygiene Culture

Definition & Importance

- Routine security measures
- Critical for risk reduction
- Enhances overall security

Foundation of Cybersecurity Posture

- Culture drives practices
- Affects all operational aspects
- Preventive >> Reactive

มี cost ต้นทางว่า

Benefits

- Minimize vulnerabilities
- Maintain compliance & trust
- Cost-effective security

Source: https://www.linkedin.com/pulse/cyber-hygiene-creating-culture-cybersecurity-your-will

Key Elements of Cyber Hygiene Culture

Secure Password * อนาคต

- Creating strong password
- Not sharing username and/or password
- Use different password for each account

Secure Data * ไม่ทำพังมูลรั่ว

- Aware of sharing sensitive data within/outside organization
- Aware of leaking sensitive data intentionally or unintentionally

Secure Email

สังเกตุและตอบกลับ ให้เหมาะสม

- Identify and respond to phishing email
- Not using organization's email for personal use

Cyber Hygiene Culture

Source: https://news.microsoft.com/wp-content/uploads/prod/sites/439/2019/06/12-Best-Practices-to-Enhance-Organisational-Cybersecurity-Hygiene.pdf

Security Awareness Program

Training & Education ทำกิจกรรม

- Continuous
- Update latest security threats & best practices อัพเดตข่าวสาร ตลอด
- Interactive & engaging training methods
  ↳ เล่นเกมส์ ↳ รับของรางวัล

Phishing Simulations & Security Drills

- Regular simulations and drills
- Reinforce good cyber hygiene habits
- Encourage appropriate respond to suspicious emails

Engagement & Communication

- Newsletter, events ,workshops
- Recognize and reward cyber hygiene practitioners
- Positive reinforcement

Phishing Email Awareness

Measuring Cyber Hygiene & Awareness Impact

Assessment Tools & Surveys

- Assessment tools : Phishing platform
- Surveys
- Statistics of non-compliance incidents

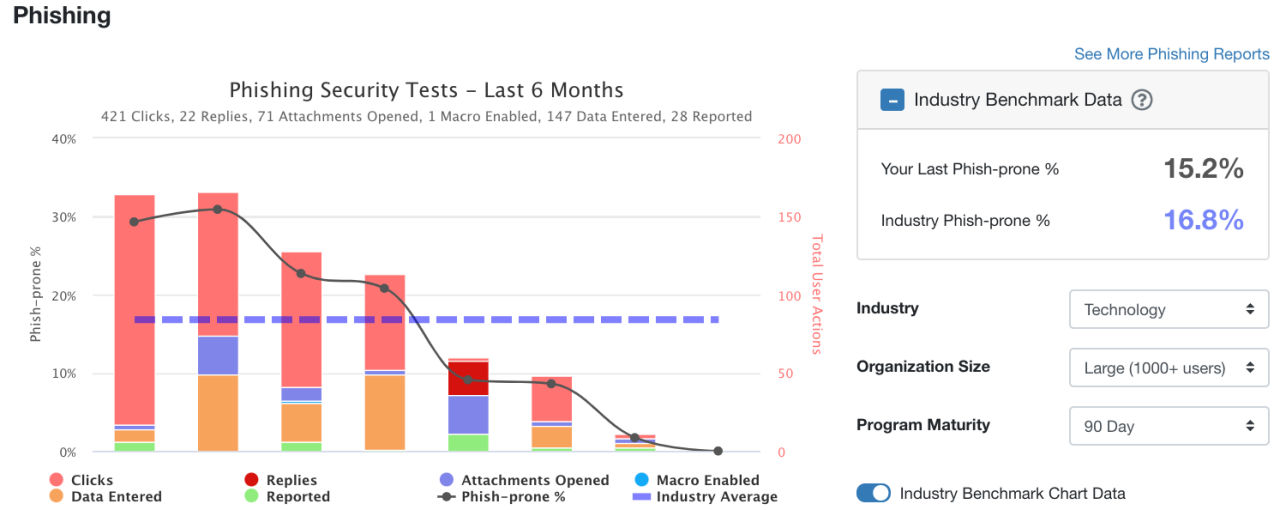
Behavioral Analysis

- Changes in employee behavior
- Short interview
- Cyber hygiene atmosphere

Continuous Improvement

- Learn from feedbacks
- Improve from assessed data
- Refine the program regularly

Benchmarking Phishing Drill Result



Source: https://www.trustradius.com/products/knowbe4/reviews#comparisons

Challenges & Solutions in fostering Cyber Hygiene

Overcoming Complacency

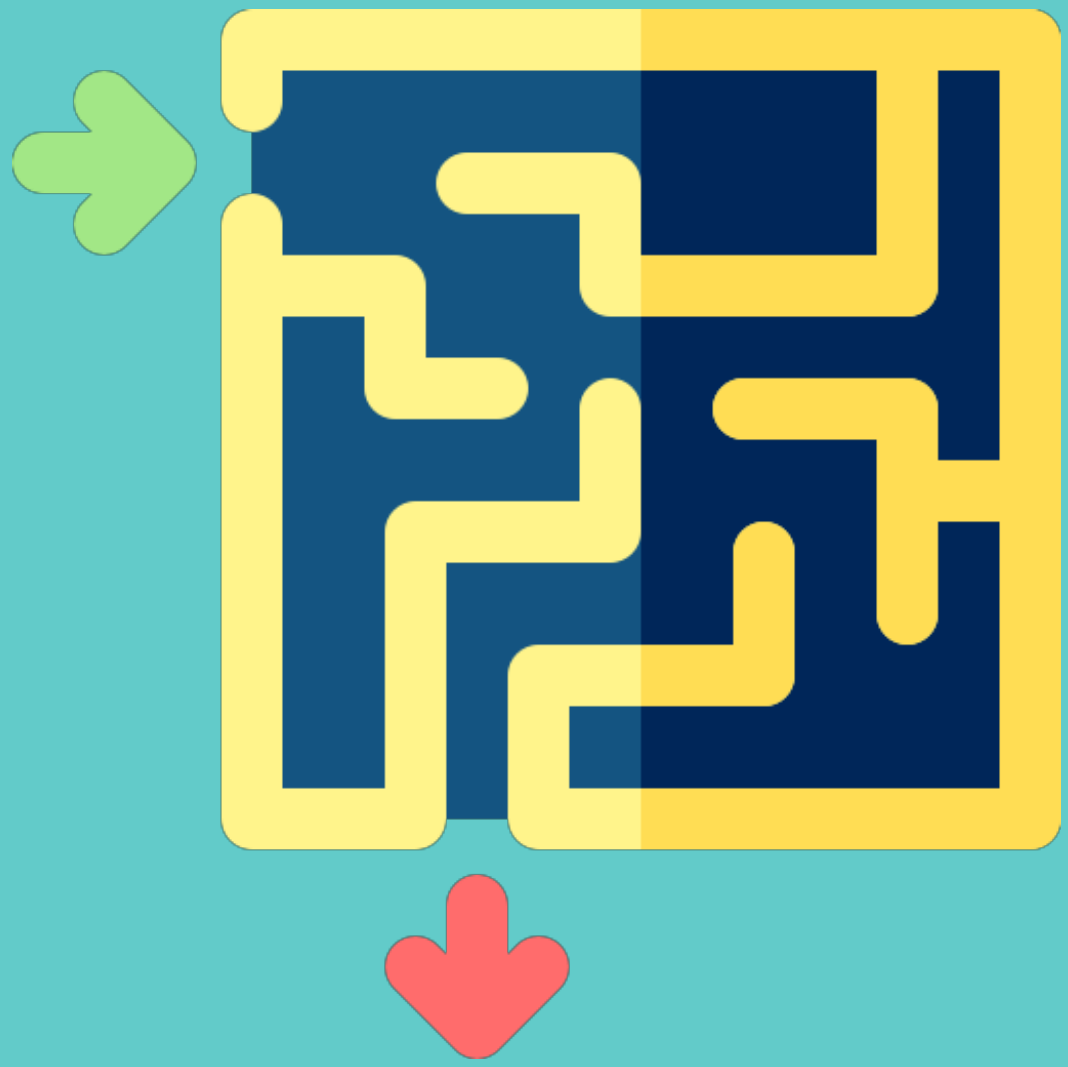
- Make cyber hygiene practice interactive
- Make it relevant to employee's daily tasks
- Incentives and gamification can help

Adapting to Evolving Threats

Ensuring that cyber hygiene practices and awareness programs keep pace with the rapidly changing threat landscape.

Continuous Improvement

Encouraging a sense of personal responsibility and accountability in every employee towards maintaining cyber hygiene.



Key Takeaways

Cyber Hygiene Culture & Awareness

1. Foundation of Cybersecurity : Human Firewalls
2. Continuous education & engagement
3. Adaptability & Personal accountability

10 CHAPTERs

Information Security Governance & Risk Management

Q & A

Cybersecurity Bootcamp 2024