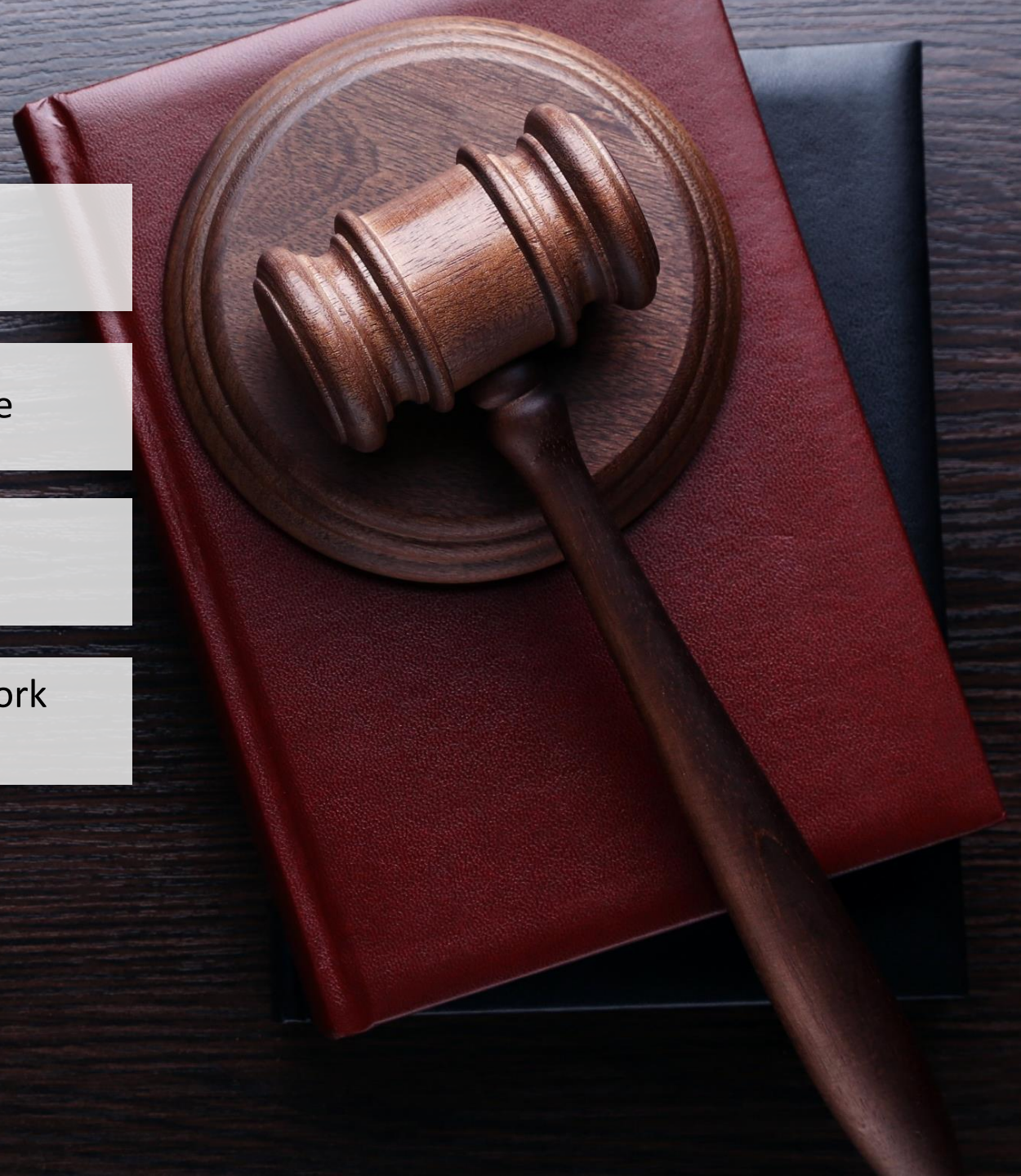
Information Security Compliance Management

Objectives

1. Understanding the Compliance
2. Understanding Why Organizations Need Compliance
3. Understanding the specific types of various local, international regulatory and standards
4. How organization comply to the regulatory framework and standard?



Overview of Different Types of Security Policies

Understanding the compliance

IT compliance is the process by which organizations **ensure** they operate within a specific set of privacy and security requirements, guidelines, and best practices.

Which type of **compliance** shall the organization decided to comply?

There are always **3 types** of compliance which organization **shall comply** are: **Local Regulatory , International Regulatory, Industry Best Practice.**

Why Organizations Need Compliance

Improves Security

- IT security **regulation** and **standards** improve overall security of an organization by meeting regulatory requirements

Minimize Impact

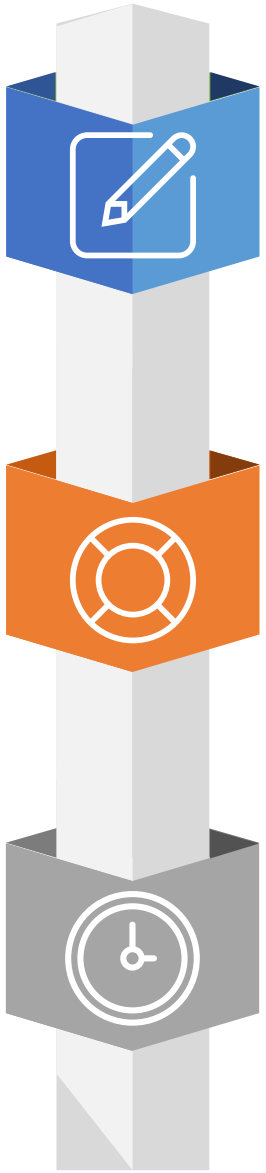
- Improved security, in turn, **prevents** security breaches, which can cost loss to company

Maintain Trust

- Customer trusts the organization in belief that their information is **safe**

Local Regulatory Frameworks, Laws.

Local Regulatory Frameworks Compliance



It is often required for the organizations to comply with some type of **security regulation**

Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary/mandatory **improvements** to cybersecurity

IT security regulatory frameworks contain a set of **guidelines** and **best practices**

Technology Risk Management Guideline (NBC)

- TRMG was released on 26 July 2019 **which cover for all financial and banking institutions.**
- The **TRMG** help BFIs create a secure technology ecosystem base on various security standards and it own control requirements.

TRMG Principles

GOVERNANCE

Information technology governance

IT governance policy and procedures

Information security policy and procedures

IT services outsourcing

Information security audit

Payment card security

Cybersecurity Law (Draft)
Data Protection Law (Draft)
Cyber Crime Offense Law (Draft)

- The purpose of **Cyber Security Law** is to enforce **CII** (Critical Information Infrastructure) to assess the risks regularly and have their own risk mitigations. There are also including incident respond escalation to competent regulatory for coordinates.
- The **Data Protection Law** is enforce everyone to make sure the information is: used fairly, lawfully and transparently.

https://www.copyright.gov

International Regulatory Frameworks, Laws, Acts and Industry Best Practice

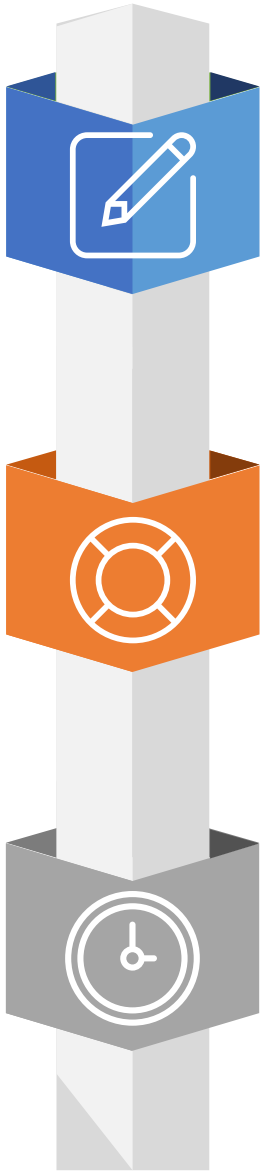
ISO Information Security Standards

Sr. No.	Standards	Objective
1	ISO/IEC 27001	Formal ISMS specification
2	ISO/IEC 27002	Information security controls
3	ISO/IEC 27003	ISMS implementation guide
4	ISO/IEC 27004	Information security metrics
5	ISO/IEC 27005	Information security risk management
6	ISO/IEC 27006	ISMS certification guide
7	ISO/IEC 27007	Management system auditing
8	ISO/IEC TR 27008	Technical auditing
9	ISO/IEC 27010	For inter-organization communication
10	ISO/IEC 27011	Iso27k in telecoms
11	ISO/IEC 27013	ISMS & ITIL/service management
12	ISO/IEC 27014	Information security governance
13	ISO/IEC TR27015	Iso27k in financial services
14	ISO/IEC TR 27016	Information security economics
15	ISO/IEC 27017	Cloud security controls

Sr. No.	Standards	Objective
16	ISO/IEC 27018	Cloud privacy
17	ISO/IEC TR 27019	Process control in energy
18	ISO/IEC 27031	ICT business continuity
19	ISO/IEC 27032	Cybersecurity
20	ISO/IEC 27033-1 to -5	Network security
21	ISO/IEC 27034 -1 & -5	Application security
22	ISO/IEC 27035	Incident management
23	ISO/IEC 27036-1 -2 & -3	ICT supply chain
24	ISO/IEC 27037	Digital evidence [forensics]
25	ISO/IEC 27038	Document reduction
26	ISO/IEC 27039	Intrusion prevention
27	ISO/IEC 27040	Storage security
28	ISO/IEC 27041	Investigation assurance
29	ISO/IEC 27042	Analyzing digital evidence
30	ISO/IEC 27043	Incident investigation
31	ISO 27799 ISO27k	In healthcare

https://www.iso27001security.com

How to comply with regulatory, standards



An **organization** must perform a self-assessment to ascertain the regulatory frameworks that best applies to it.

Compliance **maturity** assessment involves identifying gaps between the existing control environment and an organization’s requirements.

Roadmap, Action Plan, Continue Improving

General Data Protection Regulation (GDPR)

- GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**
- The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

GDPR Data Protection Principles

- **Lawfulness, fairness, and transparency**
- **Purpose limitation**
- **Data minimization**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality**
- **Accountability**

Personal Data Protection Act (PDPA)

- The **PDPA** imposes obligations on the data user to take reasonable steps to protect the personal data being processed from any loss, misuse, unauthorized or accidental access or disclosure, alteration or destruction

There are 4 countries in southeast asia which have their own PDPA :

Singapore PDAP which was released in 2012 and revision in 2014.

Thailand PDPA which was initial at 2019 and fully enforce in 1st June 2022

Malaysia PDPA which was released in June 2010.

Vietnam PDPD which was released in 17 Apr 2023.


Q&A