

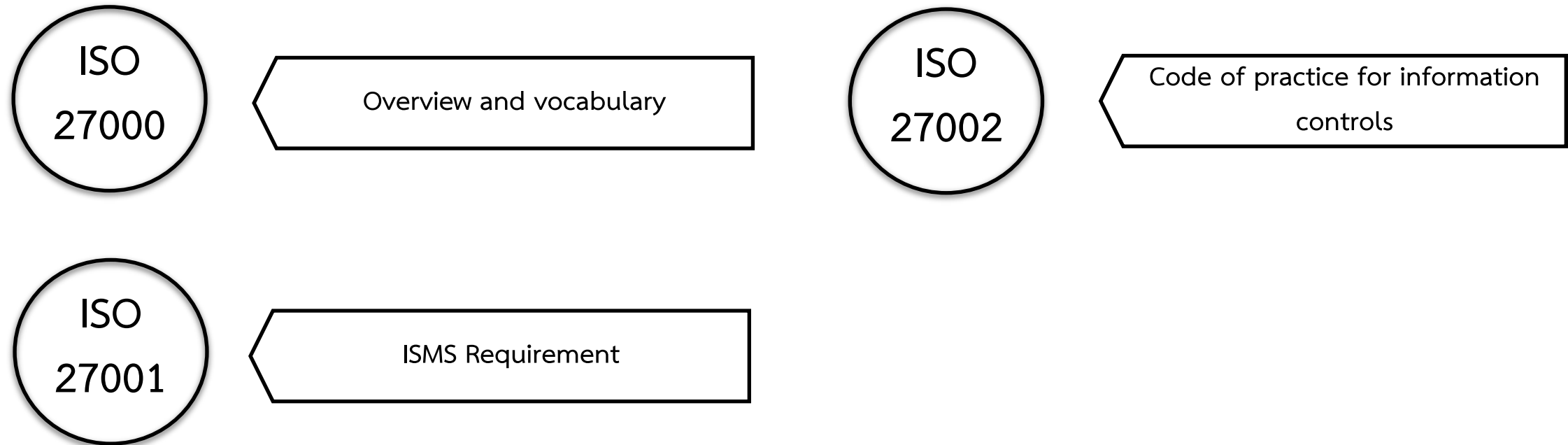


Information Security Management System  
ISO/IEC 27001:2013  
Intensive training  
22 June 2021

# Topic Covered

- Overview of Management
- Requirements Structure
  - Clause 4 Context of the organization
  - Clause 5 Leadership
  - Clause 6 Planning
  - Clause 7 Support
  - Clause 8 Operation
  - Clause 9 Performance and evaluation
  - Clause 10 Improvement
- Annex A control objectives and controls (A.5 – A.18)

# ISO/IEC 27000 and Members



# Information security Properties : C I A Model

## C = Confidentiality

การรักษาความลับของข้อมูล  
ข้อมูลจะต้องไม่ถูกเปิดเผยโดยผู้  
ไม่มีสิทธิ์หรือผู้ไม่ได้รับอนุญาต



## I = Integrity

การรักษาความครบถ้วนสมบูรณ์  
ของข้อมูล ข้อมูลจะต้องคงความ  
ครบถ้วน ไม่ถูกแก้ไขเปลี่ยนแปลง

## A = Availability

ความพร้อมใช้ของข้อมูล สำหรับผู้ที่  
มีสิทธิ์และผู้ได้รับอนุญาตที่จะ  
สามารถเข้าถึงข้อมูลได้เมื่อต้องการ

# ISO/IEC 27001 : Requirements Structure (Clauses 4 - 10)

# High Level Structure – Annex SL

0 Introduction

1 Scope

2 Normative references

3 Terms and conditions

4 Context of the organization

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance evaluation

10 Improvement

# ISO/IEC 27001 : PDCA Model

## PLAN

- Clause 4 Context of the organization
- Clause 5 Leadership
- Clause 6 Planning
- Clause 7 Support

## DO

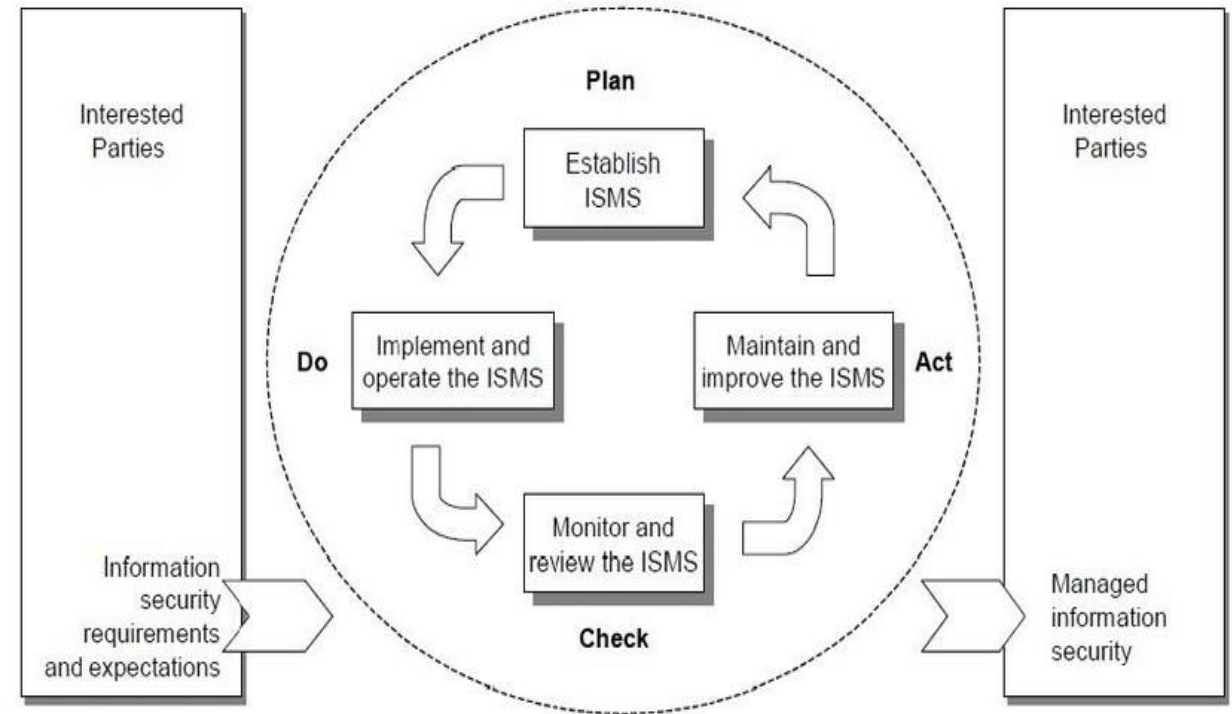
- Clause 8 Operation

## CHECK

- Clause 9 Performance evaluation

## ACT

- Clause 10 Improvement



## 4 Context of the organization

### 4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.



## 4 Context of the organization

### External Issue

- Political
- Economic
- Social / culture
- Technology
- Environment
- Regulatory /Legal
- Financial

### Internal Issue

- Organizational structure
- Policies, Objectives , Strategies
- The organization's culture
- Capabilities, understood in terms of resources and knowledge
- Standards, guidelines and models adopted by the organization

## 4 Context of the organization

### 4.2 Understanding the needs and expectations of interested parties

The organization shall determine.

- a) Interested parties that are relevant to information security management systems; and
- b) The requirement of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligation.

## 4 Context of the organization

### 4.3 Determining the scope of the information security management system

The organization shall determine boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

- a) The external and internal issues referred to in 4.1
- b) Requirement referred to in 4.2
- c) Interface and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.★

## 4 Context of the organization

### 4.4 Information security management system.

The organization shall establish, implement, maintain and continual improvement an information security management system. In accordance with the requirements of this international standard.

# 5 Leadership

## 5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by.

- a) Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
- b) Ensuring the integration of the information security management system requirements into the organization's process;
- c) Ensuring that the resources needed for the information security management system are available;
- d) Communicating the importance of effective information security management and of conforming to the information security management system requirement;
- e) Ensuring that the information security management system achieve its intended outcome(s)
- f) Direction and supporting persons to contribute to the effectiveness of the information security management system;
- g) Promoting continual improvement; and
- h) Support other relevant management roles to demonstrate to their leadership as it applies to their areas of responsibility.


# 5 Leadership

## 5.2 Policy

Top management shall establish an information security policy that:

- a) Is appropriate to the purpose of the organization
- b) Includes information security objectives or provides the framework for setting information security objective;
- c) Includes a commitment to satisfy applicable requirements related to information security; and
- d) Includes a commitment to continual improvement of the information security management system.

The information security policy shall:

- e) Be available as documented information; 
- f) Be communicate within the organization; and
- g) Be available to interested parties, as appropriate.

# 5 Leadership

## 5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for the roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

- a) Ensuring that the information security management system conforms to the requirements of this International Standard; and
- b) Reporting on the performance of the information security management system to top management.

# 6 Planning

## 6.1 Actions to address risks and opportunities

### 6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in [4.1](#) and the requirement referred to in [4.2](#) and determine the risks and opportunities that need to be addressed to:

- a) Ensure the information security management system can achieve its intended outcome(s);
- b) Prevent, or reduce, undesired effects; and
- c) Achieve continual improvement.

The organization shall plan:

- d) Actions to address these risks and opportunities; and
- e) How to
  - 1) Integrate and implement the actions into its information security management system processes; and
  - 2) Evaluate the effectiveness of these actions.



# 6 Planning

## 6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

- a) Establishes and maintains information security risk criteria that include:
  - 1) The risk acceptance criteria; and
  - 2) Criteria for performing information security risk assessments;
- b) Ensures that repeated information security risk assessments produce consistent, valid and comparable results;
- c) Identifies the information security risks:
  - 1) Apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
  - 2) Identify the risk owners;

## 6 Planning

### 6.1.2 Information security risk assessment (ต่อ)

- d) Analyses the information security risks:
  - 1) Assess the potential consequences that would result if the risks identified in [6.1.2 c\)](#) 1) were to materialize;
  - 2) Assess the realistic likelihood of the occurrence of the risks identified in [6.1.2 c\) 1\)](#); and
  - 3) Determine the levels of risk;
- e) Evaluates the information security risks:
  - 1) Compare the results of risk analysis with the risk criteria established in [6.1.2 a\)](#); and
  - 2) Prioritize the analyzed risks for risk treatment.

The organization shall retain documented information  about the information security risk assessment process.

# 6 Planning

## 6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

- a) Select appropriate information security risk treatment option, taking account of the risk assessment results;
- b) Determine all control that are necessary to implement the information security risk treatment option(s) chosen;

NOTE Organizations can design controls as required, or identify them from any source.

- c) Compare the controls determined in [6.1.3 b\)](#) above with those in [Annex A](#) and verify that no necessary controls have been omitted;

## 6 Planning

### 6.1.3 Information security risk treatment (ต่อ)

- d) Produce a Statement of Applicability<sup>★</sup> that contains the necessary controls (See 6.1.3 b) c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
- e) Formulate an information security risk treatment plan; and
- f) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain document information<sup>★</sup> about the information security risk treatment process.

## 6 Planning

### 6.2 Information security objectives and planning to achieve them.

The organization shall establish information security objectives as relevant functions and levels. The information security objectives shall:

- a) Be consistent with the information security policy;
- b) Be measurable (if practicable);
- c) Take into account applicable information security requirement, and results from risk assessment and risk treatment;
- d) Be communicated; and
- e) Be updated as appropriate.

## 6 Planning

### 6.2 Information security objectives and planning to achieve them. (ต่อ)

The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objective, the organization shall determine:

- f) What will be done;
- g) What resources will be required;
- h) Who will be responsible;
- i) When it will be completed; and
- j) How the results will be evaluated.

# 7 Support


## 7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the security management system.

# 7 Support

## 7.2 Competence

The organization shall:

- a) Determine the necessary competence of person(s) doing work under its control that affects its information security performance;
- b) Ensure that these persons are competent on the basis of appropriate education, training or experience;
- c) Where applicable, take actions to acquire to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- d) Retain appropriate documented information  as evidence of competence.



# 7 Support

## 7.3 Awareness

Person doing work under the organization's control shall be aware of:

- a) The information security policy;
- b) Their contribution to the effectiveness of the information security management system. Including the benefits of improved information security performance; and
- c) The implications of not conforming with the information security management system requirements.

# 7 Support

## 7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

- a) On what to communicate;
- b) When to communicate;
- c) With whom to communicate;
- d) Who shall communicate; and
- e) The process by which communication shall be effected.

# 7 Support

## 7.5 Documented information

### 7.5.1 General

The organization's information security management system shall include:

- a) Documented information required by this International Standard; and
- b) Documented information determined by the organization as being necessary for the effectiveness of the information security management system.
  - 1) The size of organization and its type of activities, processes, products and services;
  - 2) The complexity of processes and their interactions; and
  - 3) The competence of persons.

# 7 Support

## 7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate;

- a) Identification and description (e.g. a title, author, or reference number);
- b) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
- c) Review and approval for suitability and adequacy.

# 7 Support

## 7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

- a) It is available and suitable for use, where and when it is needed; and
- b) It is adequately protected (e.g. from loss of confidentiality, improper use, or loss integrity).

For the control of documented information, the organization shall address the following activities, as applicable;

- c) Distribution, access, retrieval and use;
- d) Storage and preservation , including the preservation of legibility;
- e) Control of changes (e.g. version control); and
- f) Retention and disposition.

## 8 Operation

### 8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in [6.1](#). The organization shall also implement plans to achieve information security objectives determined in [6.2](#).

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.


The organization shall control planned changes and reviews the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled

## 8 Operation

### 8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in [6.1.2 a\)](#)

The organization shall retain documented information  of the results of the information security risk assessments.

## 8 Operation

### 8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information<sup>★</sup> of the results of the information security risk treatment.



## 9 Performance evaluation

### 9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:


- a) What needs to be monitored and measured, including information security processes and controls;
- b) The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results:

NOTE The Methods selected should produce comparable and reproducible to be considered valid.

## 9 Performance evaluation

### 9.1 Monitoring, measurement, analysis and evaluation (ต่อ)

- c) When the monitoring and measuring shall be preformed;
- d) Who shall monitor and measure;
- e) When the results from monitoring and measurement shall be analysed and evaluated; and
- f) Who shall analyse and evaluate these results.

The organization shall retain appropriate documented information  as evidence of the monitoring and measurement results.

## 9 Performance evaluation

### 9.2 Internal audit

The organization shall conduct internal audit at planned intervals to provide information on whether the information security management system:

- a) Conforms to
  - 1) The organization's own requirements for its information security management system; an
  - 2) The requirement of this International Standard;
- b) Is effectively implemented and maintained.

## 9 Performance evaluation

### 9.2 Internal audit (ต่อ)

- c) Plan, establish, implement and maintain as audit programme(s), including the frequency, methods, responsibilities, planning requirements and reported The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
- d) Define the audit criteria and scope for each audit;
- e) Select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
- f) Ensure that the results of the audits are reported to relevant management; and
- g) Retain documented information as evidence of the audit programme(s) and the audit results.

## 9 Performance evaluation

### 9.3 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability and effectiveness.

The management review shall include consideration of :

- a) The status of actions from previous management reviews;
- b) Changes in external and internal issues that are relevant to the information security management system;
- c) Feedback on the information security performance, including trends in:
  - 1) Nonconformities and corrective actions;
  - 2) Monitoring and measurement results;
  - 3) Audit results; and
  - 4) Fulfilment or information security objectives;

## 9 Performance evaluation

### 9.3 Management review (ต่อ)

- d) Feedback from interested parties;
- e) Result of risk assessment and status of risk treatment plan; and
- f) Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information  as evidence of the result of management review

# 10 Improvement

## 10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

- a) React to the nonconformity, and as applicable:
  - 1) Take action to control and correct it; and
  - 2) Deal with the consequences;
- b) Evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
  - 1) Reviewing the nonconformity;
  - 2) Determining the causes of the nonconformity; and
  - 3) Determining if similar nonconformity exist, or could potentially occur;

# 10 Improvement

## 10.1 Nonconformity and corrective action (ต่อ)

- c) Implement any action needed;
- d) Review the effectiveness of any corrective action taken; and
- e) Make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information  as evidence of:

- f) The nature of the nonconformities and any subsequent actions taken, and
- g) The result of any corrective action.



# 10 Improvement

## 10.2 Continual improvement

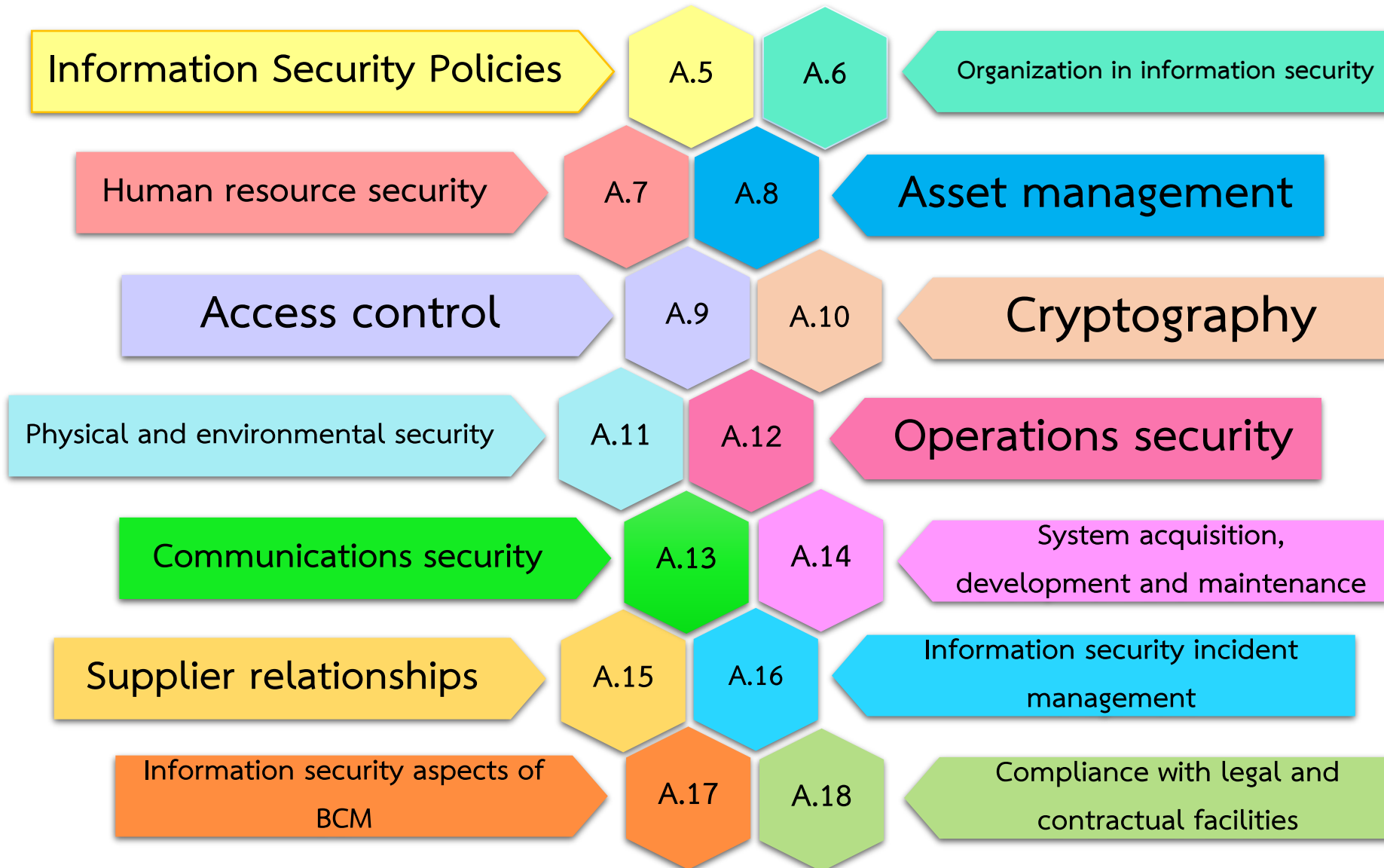
The organization shall continually the suitability, adequacy and effectiveness of the information security management system.

# ISO/IEC 27001 : Annex A control objectives and controls (Annex A.5 – A.18)

# Annex A : Domains, Control Objectives, Controls



# Annex A – 14 Control Domains



## A.5 Information security policies

### A.5.1 Management direction for information security

Objective : To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Policies for information security

A.5.1.2 Review of the policies for information Security

## A.6 Organization of information security

### A.6.1 Internal Organization

Objective : To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1 Information security roles and responsibilities

A.6.1.2 Segregation of duties

A.6.1.3 Contact with authorities

A.6.1.4 Contact with special interest groups

A.6.1.5 Information security in project management

## A.6 Organization of information security

### A.6.2 Mobile devices and teleworking

Objective : To ensure the security of teleworking and use of mobile devices.

A.6.2.1 Mobile device policy

A.6.2.2 Teleworking

## A.7 Human resource security

### A.7.1 Prior to Employment

Objective : To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A.7.1.1 Screening

A.7.1.2 Terms and conditions of employment



## A.7 Human resource security

### A.7.2 During Employment

Objective : To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A.7.1.1 Screening

A.7.1.2 Terms and conditions of employment

## A.7 Human resource security

### A.7.3 Termination or change of employment

Objective : To protect the organization's interests as part of the process of changing or terminating employment.

A.7.3.1 Termination or change of employment responsibilities

## A.8 Asset management

### A.8.1 Responsibility for Assets

Objective : To identify organizational assets and define appropriate protection responsibilities.

A.8.1.1 Inventory of assets

A.8.1.2 Ownership of assets

A.8.1.3 Acceptable use of assets

A.8.1.4 Return of assets

## A.8 Asset management

### A.8.2 Information classification

**Objective :** To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

A.8.2.1 Classification of information

A.8.2.2 Labelling of information

A.8.2.3 Handling of assets

## A.8 Asset management

### A.8.3 Media handling

Objective : To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

A.8.3.1 Management of removable media

A.8.3.2 Disposal of media

A.8.3.3 Physical media transfer

## A.9 Access Control

### A.9.1 Business Requirement for Access Control

Objective : To limit access to information and information processing facilities.

A.9.1.1 Access control policy

A.9.1.2 Access to networks and network services

## A.9 Access Control

### A.9.2 User Access Management

**Objective :** To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1 User registration and de-registration

A.9.2.2 User access provisioning

A.9.2.3 Management of privileged access rights

A.9.2.4 Management of secret authentication information of users

A.9.2.5 Review of user access rights

A.9.2.6 Removal or adjustment of access rights

## A.9 Access Control

### A.9.3 User responsibilities

Objective : To prevent unauthorized access to systems and applications.

#### A.9.3.1 Use of secret authentication information



## A.9 Access Control

### A.9.4 System and application access control

**Objective :** To prevent unauthorized access to systems and applications

A.9.4.1 Information access restriction

A.9.4.2 Secure log-on procedures

A.9.4.3 Password management system

A.9.4.4 Use of privileged utility programs

A.9.4.5 Access control to program source code

## A.10 Cryptography

### A.10.1 Cryptographic controls

**Objective :** To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 Policy on the use of cryptographic controls

A.10.1.2 Key management

## A.11 Physical and environmental security

### A.11.1 Secure Areas

**Objective :** To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.1.1 Physical security perimeter

A.11.1.2 Physical entry controls

A.11.1.3 Securing offices, rooms and facilities

A.11.1.4 Protecting against external and environmental threats

A.11.1.5 Working in secure areas

A.11.1.6 Delivery and loading areas

## A.11 Physical and environmental security

### A.11.2 Equipment security

**Objective :** To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.1 Equipment siting and protection

A.11.2.2 Supporting utilities

A.11.2.3 Cabling security

A.11.2.4 Equipment maintenance

A.11.2.5 Removal of assets

A.11.2.6 Security of equipment and assets off-premises

A.11.2.7 Secure disposal or reuse of equipment

A.11.2.8 Unattended user equipment

A.11.2.9 Clear desk and clear screen policy

## A.12 Operation security

### A.12.1 Operational procedures and responsibilities

**Objective :** To ensure correct and secure operations of information processing facilities.

A.12.1.1 Documented operating procedures

A.12.1.2 Change management

A.12.1.3 Capacity management

A.12.1.4 Separation of development, testing and operational environments

## A.12 Operation security

### A.12.2 Protection from malware

Objective : To ensure that information and information processing facilities are protected against malware.

#### A.12.2.1 Controls against malware

## A.12 Operation security

### A.12.3 Back-Up

Objective : To protect against loss of data.

#### A.12.3.1 Information backup

## A.12 Operation security

### A.12.4 Logging and monitoring

Objective : To record events and generate evidence.

A.12.4.1 Event logging

A.12.4.2 Protection of log information

A.12.4.3 Administrator and operator logs

A.12.4.4 Clock synchronization



## A.12 Operation security

### A.12.5 Control of operational software

Objective : To ensure the integrity of operational systems.

A.12.5.1 Installation of software on operational systems

## A.12 Operation security

### A.12.6 Technical vulnerability management

Objective : To prevent exploitation of technical vulnerabilities.

A.12.6.1 Management of technical vulnerabilities

A.12.6.2 Restrictions on software installation

## A.12 Operation security

### A.12.7 Information systems audit considerations

Objective : To minimise the impact of audit activities on operational systems.

#### A.12.7.1 Information systems audit controls

## A.13 Communication security

### A.13.1 Network security management

Objective : To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.1 Network controls

A.13.1.2 Security of network services

A.13.1.3 Segregation in networks

## A.13 Communication security

### A.13.2 Information transfer

Objective : To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 Information transfer policies and procedures

A.13.2.2 Agreements on information transfer

A.13.2.3 Electronic messaging

A.13.2.4 Confidentiality or nondisclosure agreements

## A.14 System acquisition, development and maintenance

### A.14.1 Security requirements of information systems

Objective : To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.1 Information security requirements analysis and specification

A.14.1.2 Securing application services on public networks

A.14.1.3 Protecting application services transactions

## A.14 System acquisition, development and maintenance

### A.14.2 Security in development and support processes

**Objective :** To ensure that information security is designed and implemented within the development lifecycle of information systems.

- A.14.2.1 Secure development policy
- A.14.2.2 System change control procedures
- A.14.2.3 Technical review of applications after operating platform changes
- A.14.2.4 Restrictions on changes to software packages
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.7 Outsourced development
- A.14.2.8 System security testing
- A.14.2.9 System acceptance testing

## A.14 System acquisition, development and maintenance

### A.14.3 Test data

Objective : To ensure the protection of data used for testing.

#### A.14.3.1 Protection of test data



## A.15 Supplier relationships

### A.15.1 Information security in supplier relationships

Objective : To ensure protection of the organization's assets that is accessible by suppliers.

A.15.1.1 Information security policy for supplier relationships

A.15.1.2 Addressing security within supplier agreements

A.15.1.3 Information and communication technology supply chain

## A.15 Supplier relationships

### A.15.2 Supplier service delivery management

Objective : To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 Monitoring and review of supplier services

A.15.2.2 Managing changes to supplier services

## A.16 Information security incident management

### A.16.1 Management of information security incidents and improvements

**Objective :** To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 Responsibilities and procedures

A.16.1.2 Reporting information security events

A.16.1.3 Reporting information security weaknesses

A.16.1.4 Assessment of and decision on information security events

A.16.1.5 Response to information security incidents

A.16.1.6 Learning from information security incidents

A.16.1.7 Collection of evidence

## A.17 Information security of Business continuity management

### A.17.1 Information security continuity

Objective : Information security continuity shall be embedded in the organization's business continuity management systems.

A.17.1.1 Planning information security continuity

A.17.1.2 Implementing information security continuity

A.17.1.3 Verify, review and evaluate information security continuity

## A.17 Information security of Business continuity management

### A.17.2 Information security continuity

Objective : Information security continuity shall be embedded in the organization's business continuity management systems..

A.17.2.1 Availability of information processing facilities

# A.18 Compliance

## A.18.1 Compliance with legal and contractual requirements

Objective : To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1 Identification of applicable legislation and contractual requirements

A.18.1.2 Intellectual property rights

A.18.1.3 Protection of records

A.18.1.4 Privacy and protection of personally identifiable information

A.18.1.5 Regulation of cryptographic controls

# A.18 Compliance

## A.18.1 Compliance with legal and contractual requirements

Objective : To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1 Identification of applicable legislation and contractual requirements

A.18.1.2 Intellectual property rights

A.18.1.3 Protection of records

A.18.1.4 Privacy and protection of personally identifiable information

A.18.1.5 Regulation of cryptographic controls

Q & A

THANK YOU