CHAPTER 2
SECURITY MANAGEMENT

2.1 Introduction to Information Security

2.1.1 Information security refers to all aspects of protection covering information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. The aim is to provide Confidentiality, Integrity, and Availability (CIA) of information systems and the information within them.

(a) **Confidentiality** – only authorised persons are allowed to know or gain access to the information stored or processed by Information Systems in any aspects.

(b) **Integrity** – only authorised persons are allowed to make changes to the information stored or processed by information systems in any aspects.

(c) **Availability** – information systems should be available to users at any given or specified period of time.

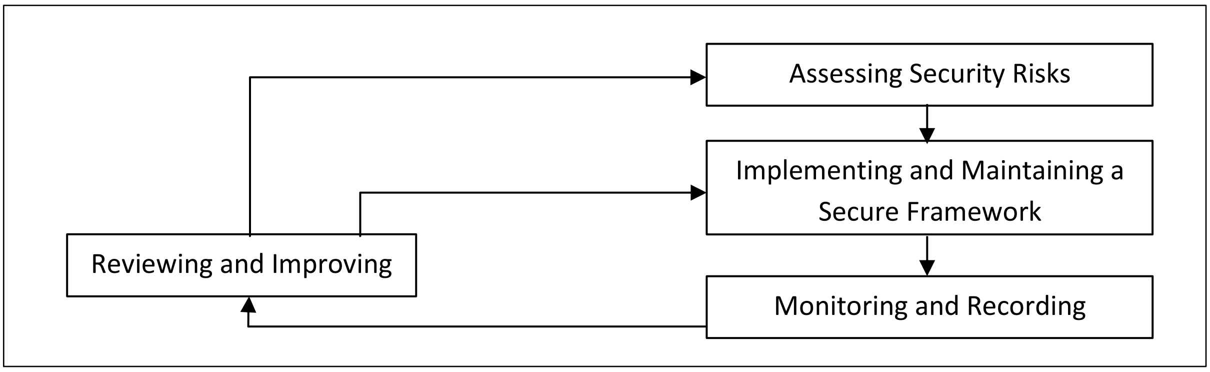
2.2 Security Management Cycle

2.2.1 The use of proper preventive measures and safeguards can reduce the risk of potentially devastating security attacks.

2.2.2 Information security management involves a combination of prevention, detection and reaction processes. It is a cycle of iterative activities and processes that require ongoing monitoring and control.

2.2.3 In order to make security management work, involvement, understanding and support from all members in the school is crucial.

2.2.4 The diagram below highlights the major activities involved in any security management cycle.



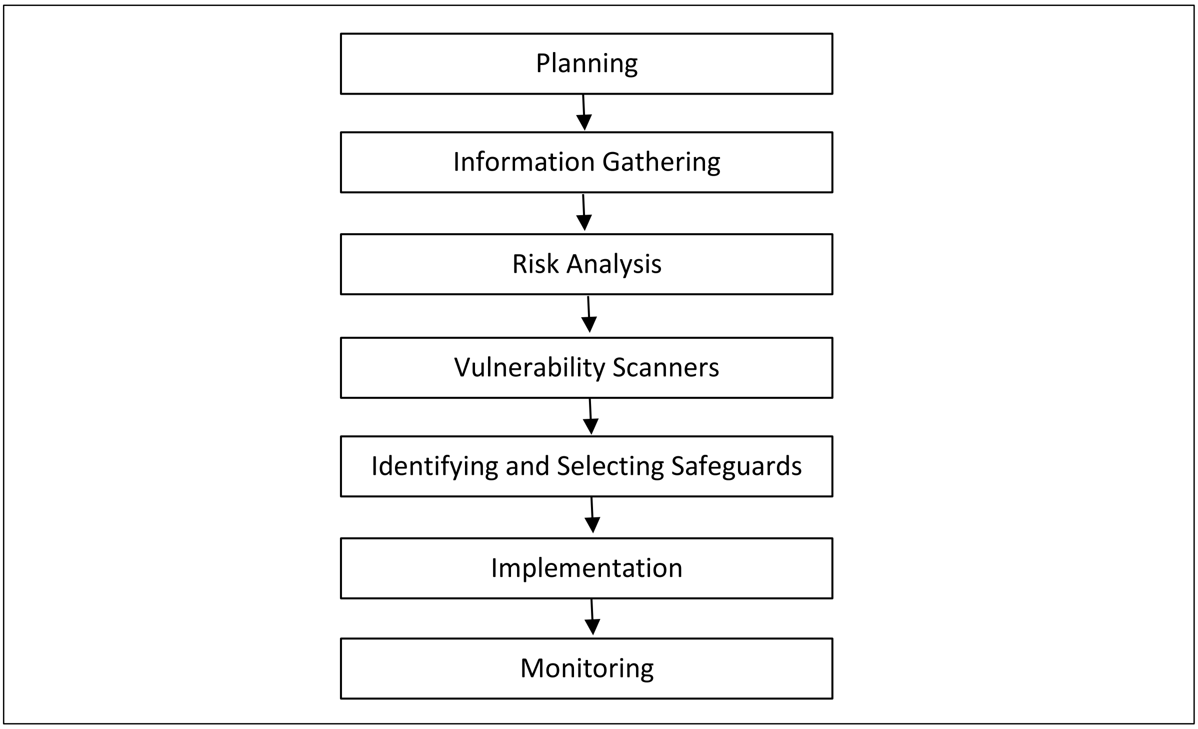
2.3 Assessing Security Risks

2.3.1 The security management cycle starts with an assessment of the security risks. Security Risk Assessment aims to identify what security measures are required. It is the initial step in evaluating and identifying the risks and consequences associated with vulnerabilities, and provides a basis for management to establish a cost-effective security programme.

2.3.2 Based on the assessment results, appropriate security protection and safeguards should be implemented to maintain a secure protection framework. This includes developing security policies and guidelines, assigning security responsibilities and implementing technical security precautions and systems.

2.3.3 This step is followed by a cyclic compliance review and re-assessment, designed to provide assurance that security controls are put into place properly in order to meet users' security requirements, and to cope with rapid technological and environmental changes. This relies on continuous feedback and monitoring. The review can be undertaken through periodic security audits to identify what enhancements may be necessary.

2.3.4 By evaluating a list of considerations, the school can identify what assets to protect, their relative importance, and each asset's priority ranking for urgency and required level of protection. The flow chart below shows the major steps in Security Risk Assessment.



2.4 Implementing and Maintaining a Secure Framework

2.4.1 Following the results obtained from the security risk assessment, the security management cycle enters a phase of implementation and maintenance, where appropriate security protection measures and safeguards are implemented in a way that builds a secure protection framework. This includes developing security policies and guidelines, assigning security responsibilities and implementing technical and administrative security measures. All these steps are crucial in contributing to the safeguards of the school's assets.

2.4.2 Set up and Implement a Security Policy:

(a) A good security policy sets out the basic rules for information security within the school. These rules are mandatory and must be observed throughout the school. Since security requirements vary from one school to another, so should the security policy. Therefore, it is of the utmost importance that the security policy be in accordance with requirements and the school's operational goals and policies such that it is supported by all employees, and is enforceable.

(b) In fact, a security policy can be very high-level and technology-neutral or detailed and technology-specific. A security policy can be categorised into three basic types:

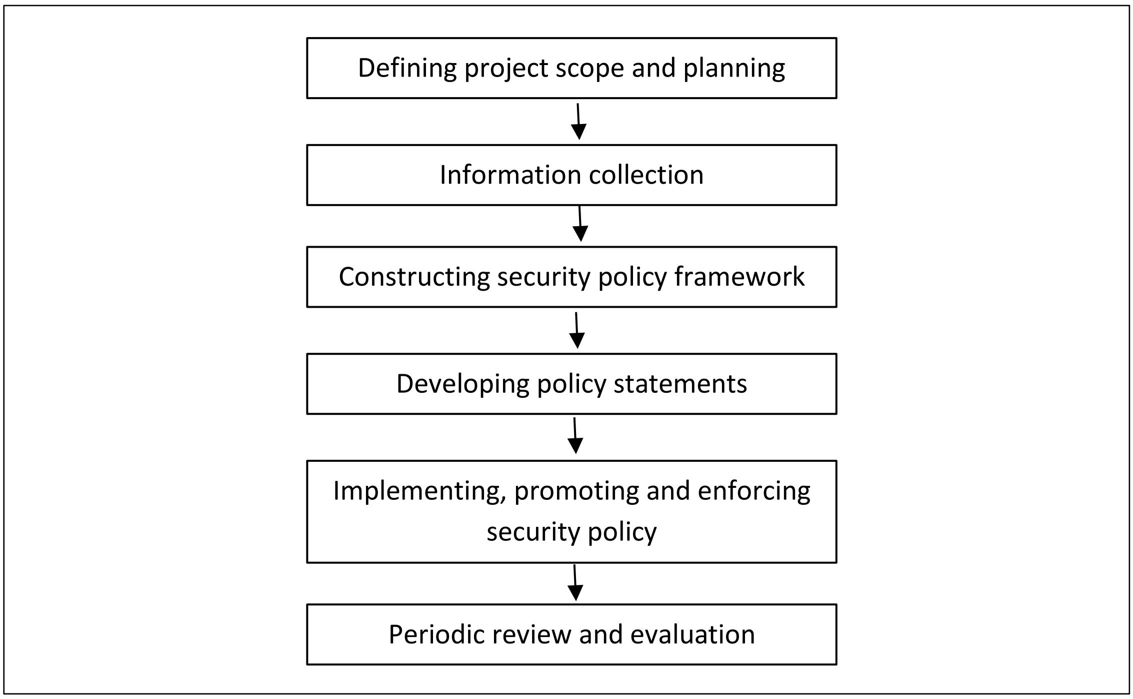
- Program-level policy

- Issue-specific policy

- System-specific policy

(c) The System-specific policy focuses on policy issues concerning the management of a specific system. It addresses only one system. The program-level policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organisation.

(d) The choice to develop a particular type of policy depends on your school's requirements. However, the most important thing is that policy sets the direction, and that it can be used. The flowchart below is a bird-eye view of the development cycle of a security policy.


Defining project scope and planning
Information collection
Constructing security policy framework
Developing policy statements
Implementing, promoting and enforcing security policy
Periodic review and evaluation

(e) An information security policy should cover the school's expectations of the proper use of its computer and network resources as well as the procedures to prevent and respond to security incidents. During the drafting of the policy, the school-based requirements on security should be considered. The drafting of the policy should consider the following aspects:

- Goals and direction of the school

- Existing policies, rules, regulations and laws of the Government of HKSAR

- Schools’ requirements and needs

- Implementation, distribution and enforcement issues

2.4.3 Set up and Implement Management and Administrative Processes

(a) Depending on the direction and parameters set out in the security policy, management and administration processes will need to be set up to support policy implementation. These are the major management and administrative activities:

- Assign roles and responsibilities
- Guidelines and standards
- Security awareness and training
- Enforcement
- On-going involvement of all parties

(i) **Assign roles and responsibilities**: Development of an IT security policy requires active support and ongoing participation of individuals from multiple ranks and functional units. Thus, clear definitions and proper assignment of accountability and responsibility for securing the school's information and system assets is necessary and may involve the following roles depending on the school’s operational needs and environment:

✧ **School Management (School Sponsor Body (SSB) / Incorporated Management Committee (IMC) / School Management Committee (SMC) / Principal / Vice Principal)**

- Direct and enforce the development of security measures.
- Provide the necessary resources required for the measures to be implemented.
- Ensure participation at all levels of management, administrative, technical and operational staff, and provide full support to them.
- Ensure the alignment of security strategy with the school’s security requirements.
- Provide management endorsement in respect of the line-to-take for publicity on the incident.

- **IT Head**
  - Establish proper security governance process to evaluate, direct, monitor and communicate the IT security related tasks within the school.
  - Lead in the establishment, maintenance and implementation of IT security policies, standards, guidelines and procedures.
  - Disseminate security alerts on impending and actual threats from the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to responsible parties within the school.
  - Ensure information security risk assessments and audits are performed as necessary.
  - Initiate investigations and rectification in case of breach of security.
  - Provide overall supervision and co-ordination of information security incident handling for all information systems within the school.
  - Make decisions on critical matters such as damage containment, system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery etc.
  - Trigger the school's disaster recovery procedure where appropriate, depending on the impact of the incident on the operation of the school.
  - Provide management endorsement on the provision of resources for the incident handling process.
  - Report information security incidents for school's recording and necessary follow-up actions.
  - Determine the data classifications, the authorised data usage, and the corresponding security requirements for protection of the information.

- **IT Committee Members**
  - Monitor, review and improve the effectiveness and efficiency of IT security management.
  - Advise on the set up and review of the security policy.
  - Discharge responsibilities for all aspects of security in the school.
  - Facilitate experience and information sharing within the school on information security incident handling and related matters.
  - Promote security awareness in the school.

✧ **Technical Support Staff (TSS)**

- Responsible for the day-to-day administration, operation and configuration of the computer systems and network in the school.
- Implement the security mechanisms in accordance with procedures / guidelines established by the school.
- Assist in leading, monitoring and coordinating of IT security matters within the school.
- Assist in identifying system vulnerabilities.
- Perform security administrative work of the system.
- Maintain control and access rule of the data and system.
- Check and manage audit logs.

✧ **User (Teacher / Supporting Staff / Student / Visitor)**

- Users shall be accountable for all their activities.
- Responsibilities of a user include:

  - Know, understand, follow and apply all the possible and available security mechanisms to the maximum extent possible.
  - Prevent leakage and unauthorised access to information under his/her custody.
  - Safekeep computing and storage devices, and protect them from unauthorised access or malicious attack with his/her best effort.
  - Report any abnormal incident or fault case.

(ii) **Guidelines and standards**: Guidelines and standards are tools used to implement the security policy. As a policy may be written at a broad level, it is essential to develop standards, guidelines and procedures to offer users, administrators, computer personnel and top management a clearer approach with regards to implementing the security policy and meeting the school's security requirements.

(iii) **Security awareness and training**: Security awareness is crucial to ensuring that all related parties understand the risks, and accept and adopt the good security practices. Training and education can provide principal, IT head, TSS, users and other related parties with the necessary skills and knowledge for implementation of security measures.

No policy is considered to have been implemented unless users or related parties have commitment and communication. This means users and related parties:

- are informed about the policy through briefings or orientations;
- are invited to participate in developing policy proposals;
- are trained in the skills needed to follow the policy;
- feel that security measures are created for their own benefit;
- are periodically reminded about new security issues;
- have signed an acknowledgement; and
- are provided with policy guidance.

(iv) **Enforcement**: This refers to the task of enforcement of rights arising from implementation of the policy and redress for violations of those rights. Schools should set up procedures to provide prompt assistance in investigative matters relating to breaches of security. Establishing a school incident management team and setting up a security incident handling procedure can improve the effectiveness of any enforcement policy.

(v) **On going involvement of all parties**: An effective security policy also relies on continuous exchange of information, consultation, co-ordination and co-operation among all parties in a school. Injection of knowledge on standards, methods, codes of practice and other expertise on IT security from all parties involved will also help to keep the security policy up-to-date and relevant.

2.4.4 Select and Implement Technological Measures

(a) Besides management and administrative processes, the implementation of a security policy might involve technological measures through selection and application of appropriate technologies and products. These technological measures should undergo proper testing before operation.

(b) Some suggestions to schools are as follows:

- Selection and implementation of measures involving technologies and products, such as:

  - ✧ Anti-malware software
  - ✧ Access Control Systems

  - ✧ Firewalls
  - ✧ Intrusion Detection Systems
  - ✧ Encryption
  - ✧ Key Management and Key Distribution Systems
  - ✧ Network Management Systems and Security Management Systems

- Adoption of proper procedures in operations, such as:

  - ✧ Adopt proper procedures to manage accounts and personal data
  - ✧ Adopt proper procedures to manage incidents
  - ✧ Adopt proper procedures to keep track of system activities and alerts
  - ✧ Adopt proper procedures to monitor the health of the security infrastructure
  - ✧ Adopt proper procedures to manage and control changes

2.5 Monitoring and Recording

2.5.1 With implementation and maintenance being carried out to provide a secure framework, there is also the need for constant monitoring and recording so that proper arrangements can be made when tackling a security incident.

2.5.2 Day-to-day operations such as users' access attempts and activities while using a resource or information, need to be properly monitored, audited, and logged as well, e.g. individual user ID needs to be included in audit logs to enforce individual responsibility. Each user should understand his responsibility when using school resources and be accountable for their actions.

2.5.3 Major activities for constant recording should include:

(a) Maintaining a security incident handling and reporting procedure

(b) Maintaining an audit trail for major systems and critical applications

(c) Maintaining a proper record of how privileged accounts are distributed and updated

(d) Maintaining an event history and error log for operating systems

(e) Maintaining access records of visitors or guests enter the school network

(f) Maintaining records to keep track of authorisation to access and undertake critical activities

2.6 Reviewing and Improving

2.6.1 Reviewing and improving are ongoing review that identifies what enhancements are necessary. This is a series of a cyclic compliance reviews and re-assessments designed to make sure that security controls are properly put into place to meet security requirements, and to cope with any rapid technological and environmental changes. It also requires continuous feedback and monitoring. The review can be done through periodic security audits to monitor and review security practices and strategies on an on-going basis.

2.6.2 Security audit is a repetitive checking process to ensure that security measures are properly implemented from time to time. A security audit is performed more frequently than a security risk assessment. It aims to find out if the current environment is securely protected in accordance with the defined security policy.

2.6.3 Objectives of a Security Audit

(a) to provide evidence of compliance with the security policy

(b) to examine and analyse safeguards to the system and the operational environment

(c) to assess the technical and non-technical implementation of the security design

(d) to validate proper or improper integration and operation of all security features

2.6.4 Auditing Steps

(a) Defining the audit scope and activities

(b) Planning

(c) Collecting audit data

(d) Performing audit tests

(e) Reporting audit results

(f) Protecting audit data and tools

(g) Making enhancements and follow-up

2.6.5 The security control compliance of auditors should be monitored and reviewed actively and periodically. The school must reserve the right to audit the responsibilities of auditors defined in the service level agreement, and have those audits carried out by an independent third party.

2.6.6 To ensure an effective and comprehensive review, detailed inventories should be maintained accurately and kept up-to-date, including:

(a) a list of servers and systems within the scope of the project, and which servers / systems are storing sensitive or personal information;

(b) a list of support staff from third party service providers as well as the user IDs and access privileges granted to individual support staff; and

(c) a list of data, especially sensitive or personal data, transferred to any third party service providers.