Information Security Management ensures confidentiality, authenticity, non-repudiation, integrity, and availability of organization data and IT services. It also ensures reasonable use of organization’s information resources and appropriate management of information security risks.

Information Security Manager is the process owner of this process.

Information security is considered to be met when:

- Information is observed or disclosed on only authorized persons
- Information is complete, accurate and protected against unauthorized access
- Information is available and usable when required, and the systems providing the information resist attack and recover from or prevent failures
- Business transaction as well information exchanges between enterprises, or with partners, can be trusted

**ISM Security Policy**

It is required for ISM security policies cover all areas of security, be appropriate, meet the needs of business and should include the policies shown in the following diagram:

![ISM Policies Diagram](http://www.tutorialspoint.com/itil/information_security_management.htm)

**ISM Framework**

**ISM Process**

The following diagram shows the entire process of Information Security Management ISM:
Key elements in ISM Framework

ISM framework involves the following key elements:

**Control**

The objective of Control element is to:
- Establish an organization structure to prepare, approve and implement the information security policy
- Allocate responsibilities
- Establish and control documentation

**Plan**

The purpose of this element is to devise and recommend the appropriate security measures, based on an understanding of the requirements of the organization.

**Implement**

This key element ensures that appropriate procedures, tools and controls are in place to underpin the security policy.

**Evaluation**

The objective of Evaluation element is to:
- Carry out regular audits of the technical security of IT systems
- Supervise and check compliance with security policy and security requirements in SLAs and OLAs

**Maintain**

The objective of Maintain element is to:
- Improve on security agreements as specified in, for example, SLAs and OLAs
- Improve the implementation of security measures and controls

**Preventive**

This key element ensures prevention from security incidents to occur. Measures such as control of access rights, authorization, identification, and authentication and access control are required for this preventive security measures to be effective.

**Reductive**

It deals with minimizing any possible damage that may occur.

**Detective**

It is important to detect any security incident as soon as possible.

**Repressive**

This measure is used to counteract any repetition of security incident.

**Corrective**

This measure ensures damage is repaired as far as possible.