Information Security
Information is one of the most valuable assets of an organization and exists in many forms: printed, electronic.

Information security refers to the protection of information from a wide range of threats so as to preserve its Confidentiality, Integrity and Availability.

Information Security Management System (ISMS)
An ISMS is a management framework, based on a risk management approach, to implement and improve information security.

It allows an organisation to:
• identify potential threats and their impacts to business processes;
• evaluate the degree of risks in several areas, and;
• apply adequate measures for eliminating or minimising those risks.

The international standard ISO/IEC 27001 offers a comprehensive set of measures comprising best practices in information security, risk management and security controls.

Benefits of an ISMS
✓ Provision of user awareness on security threats and measures
✓ Planning of effective business security objectives
✓ Promotion of effective risk management
✓ Better management of information security incidents
✓ Increase in confidence of stakeholders

Steps to implement an ISMS based on ISO 27001

For assistance in implementing an ISMS in the Civil Service, contact the IT Security Unit:
Tel. 210-2760 Fax: 212-3660
Email: itsecurity@govmu.org
ISO 27001 Security Domains

(Application of Security Controls in different areas of an organization)

Compliance
Application of legal, regulatory and contractual obligations for information security

Information Security Policies
Drafting and reviewing of Security Policies

Organisation of information security
Assignment of security responsibilities in the organisation

Business Continuity
Ensuring information security continuity in the business continuity process

Human resource Security
Application of security prior to employment, during, and at termination of employment

Information Security Incident Management
Management of Information security incidents and improvements

Asset Management
Inventory of assets, information classification and media handling

Supplier Relationship
Security of information assets accessible by suppliers and third parties

Access control
Management of user access controls on systems and information

System Acquisition, Development and Maintenance
Secure acquisition, development and support of Information Systems

Cryptography
Protection of information using data codification

Communications Security
Protection of information during transfer

Physical and Environmental Security
Security of equipment, data and premises

Operations Security
Operational procedures and responsibilities

ISO 27001 covers 14 Security Domains