INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

What is ISMS?

Information Security Management Systems (**ISMS**) is a systematic and structured approach to managing information so that it remains secure. ISMS implementation includes policies, processes, procedures, organizational structures and software and hardware functions. The ISMS implementation should be directly influenced by the organization's objectives, security requirements, processes employed, size and structure.

Why do we need ISMS?

Organizations and their information systems and networks are exposed with security **THREATS** such as fraud, espionage, fire, flood and sabotage from a wide range of sources. The increasing number of security breaches has led to increasing information security concerns among organizations worldwide.

ACHIEVING INFORMATION SECURITY is a huge challenge for organization as it **CANNOT BE ACHIEVED THROUGH TECHNOLOGICAL MEANS ALONE**, and should never be implemented in a way that is either out of line with the organization's approach to risk or which undermines or creates difficulties for its business operations.

Thus there is a need to look at information security from a **HOLISTIC PERSPECTIVE**, and to have an information security management methodology to protect information systematically. This is where the need for ISMS comes in.

What standards should be referred to for ISMS implementation?

ISMS is based on two international standards:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

ISO/IEC 27001:2005

ISO/IEC 27001:2005 is the Requirements for Information Security Management Systems. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. The ISMS processes are based on the following Plan-Do-Check-Act model:

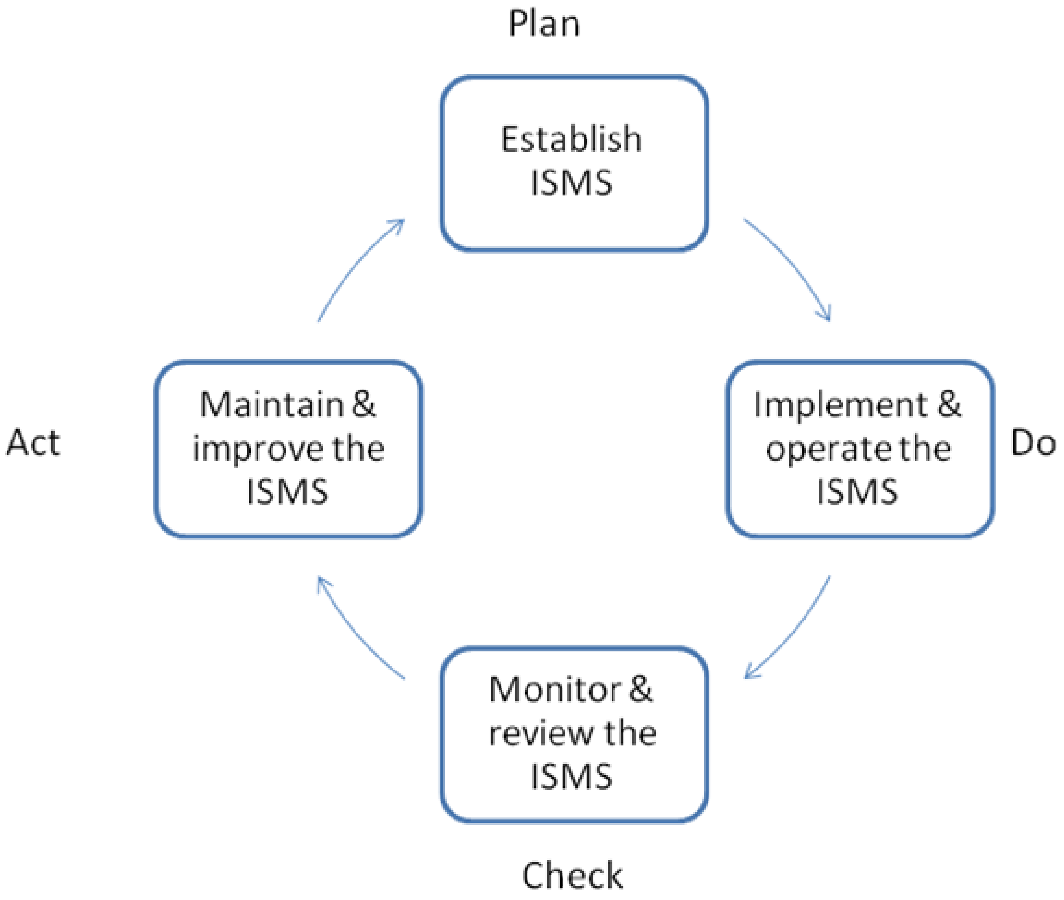
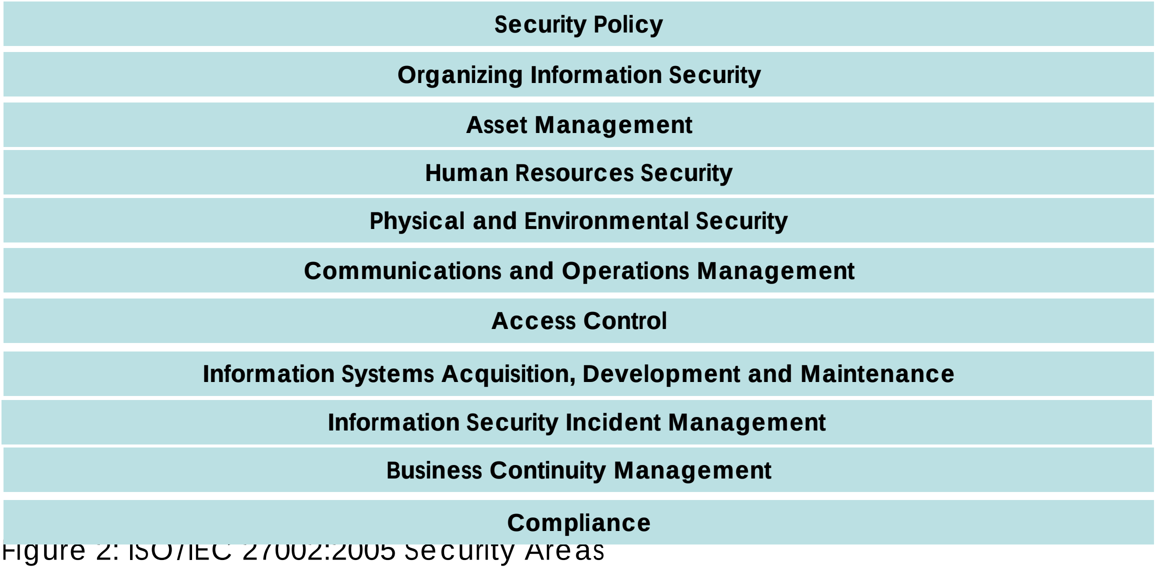

Plan
Establish ISMS
Act
Maintain & improve the ISMS
Implement & operate the ISMS
Do
Monitor & review the ISMS
Check

Figure 1: PDCA Model

ISO/IEC 27002:2005

ISO/IEC 27002:2005 is the Code of Practice for Information Security Management. It provides a catalogue of controls that can be implemented for ISMS. The standard comprises of 11 security areas, 39 controls objectives and 133 controls. The 11 security areas of ISO/IEC 27002 are listed in Figure 2:



Security Policy

Organizing Information Security

Asset Management

Human Resources Security

Physical and Environmental Security

Communications and Operations Management

Access Control

Information Systems Acquisition, Development and Maintenance

Information Security Incident Management

Business Continuity Management

Compliance

Figure 2: ISO/IEC 27002:2005 Security Areas

<u>What are the advantages if my organization is ISMS certified?</u>

Certification of ISMS brings several advantages;

- Provide a structured way of managing information security within an organisation
- Provide an independent assessment of an organization's conformity to the best practices agreed by a community of experts for ISMS.
- Provide evidence and assurance that an organization has complied with the standards requirement.
- Enhance information security governance within the organization.
- Enhance the organization's global positioning and reputation.
- Increase the level of information security in the organization.

<u>Recommended references for ISMS</u>

- ISO/IEC 27001:2005 Information security management systems - Requirements
- ISO/IEC 27002:2005 Code of practice for information security management

- ISO/IEC 27004: 2009 Information security management - Measurement
- ISO/IEC 27005:2008 Information security risk management

  For further information, please contact: info@cybersecurity.my