Benefits of ISO/IEC 27005:2011 to SMEs

By **Noor Aida Idris & Lt Col Asmuni Yusof (Rtd)**

The increasing number of cyber security incidents has made managing information security a top priority in many SMEs. Enterprises have to keep up-to-date with information security risks introduced by new and advanced technologies, in addition to their own reliance on such technology since organisational information now resides in a digital world as well as in physical mediums.

Information security management was introduced to ensure that SMEs were able to secure their information assets, which contain critical business information. By proactively protecting information assets and managing information security risks, SMEs can reduce the likelihood and/or the impact on their information assets from a wide range of information security threats. Today, there are various mechanisms utilised to manage information security. Among them are information security management systems based on ISO/IEC 27001: 2005 Information Security Management Systems (ISMS) - Requirements.

ISO/IEC 27001 is part of the ISO 27000 family that provides general requirements for implementing information security management systems. This standard provides SMEs with the means of protecting information (in terms of confidentiality, integrity and availability) while providing clients, partners and regulators with the assurance of compliance to internationally recognised information security requirements. It is a risk-based approach that provides a holistic and structured way to manage information security.

Information security risk management is needed to ensure that the confidentiality, integrity and availability of information assets (CIA) are preserved. Risk management is the key to information security governance by an SME and to the protection of its information assets. If the SME is unaware of the risks it faces, it will not deploy or implement security controls; thus failing to protect critical assets. Several guides are available to assist SMEs in managing information security risks. One such guide is the ISO/IEC 27005:2011 Information Security Risk Management.

Introduction to ISO/IEC 27005

ISO/IEC 27005 contains a description of information security risk management processes and activities, which provide guidelines to SMEs to manage their information security risks. This standard, which was first introduced in 2005, has been revised recently and re-published in 2011. The standard plays a significant role in the successful implementation of ISMS.

Benefits of ISO/IEC 27005

There are several key advantages when SMEs refer to ISO/IEC 27005 when implementing information security risk management. First, any SME can use this standard. Second, this standard supports the requirements of the information security risk assessment specified in ISO/IEC 27001. And third, this standard, which has been revised to align with three other risk management standards, can be used by SMEs that wish to manage their information security risks in a similar fashion to the way they manage other risks.

One of the attractions of ISO/IEC 27005 is the risk management processes described in the standard which is applicable to all SMes, no matter the size or type. As a matter of fact, the information security risk management processes defined by the standard can be applied not just to the SME as a whole, but to any discrete part of the organisation (e.g. a department, a physical location, a business service or a critical function), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

Information security risk management described in ISO/IEC 27005 consists of five processes which are: context establishment, information security risk assessment, information security risk treatment, information security risk acceptance, information security risk communication and consultation and information security risk monitoring and review. These five processes are illustrated in Figure 1.

Another key benefit offered by the ISO/IEC 27005 standard is that it supports the information security risk assessment requirements specified in ISO/IEC 27001. Thus, organisations that wish to be certified against ISO/IEC 27001 certification may refer to ISO/IEC 27005 when implementing the information security risk assessment.

The mapping of clauses in ISO/IEC 27005 with risk assessment requirements in ISO/IEC 27001 is discussed below:

Clause 7 – Context establishment

In ISO/IEC 27005, the context of risk management for an SME is established first. The external and internal contexts are looked at when setting the basic criteria necessary for information security risk management, defining the scope and boundaries, as well as establishing an appropriate organisation to operate the information security risk management. The context establishment process is in line with ISO/IEC 27001:2005 clause 4.2.1 c) Define the risk assessment approach of the organisation.

Clause 8 – Information security risk assessment

The context establishment process is followed by a risk assessment process. There are three sub processes included in a risk assessment process which are risk identification, risk analysis and risk evaluation. The risk assessment process determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritises the derived risks and ranks them against the risk evaluation criteria

> TURN TO **PAGE 36**

Managing information security risk

FROM PAGE 35

set in the context establishment. The information security risk assessment process is in line with ISO/IEC 27001:2005 clause 4.2.1 d) Identify the risks and e) Analyse and evaluate the risks.

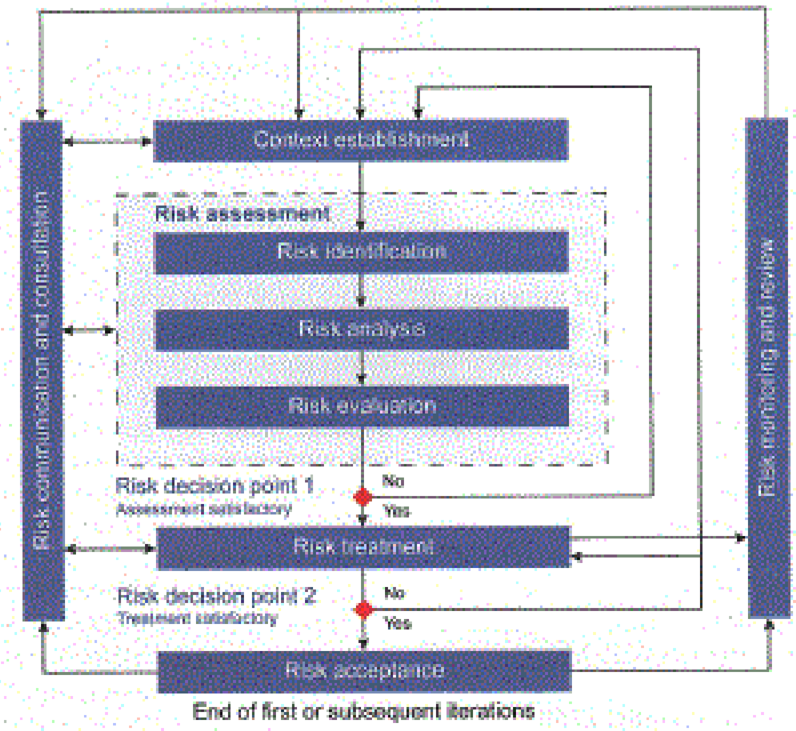
Clause 9 – Information security risk treatment

Next is the risk treatment process. The information security risk treatment process involves planning to treat the identified risks. There are four options available for risk treatment: risk modification, risk retention, risk avoidance and risk sharing. Selecting the risk treatment options should be based on the outcome of the risk assessment, the expected cost for implementing these risk treatment options and the expected benefits from these options. The information security risk treatment processes is in line with ISO/IEC 27001:2005 clause 4.2.1 f) Identify and evaluate options for the treatment of risks.

Clause 10 – Information security risk acceptance

The decision to accept the risks and responsibilities for decisions are made and formally recorded in the information security risk acceptance process. This process is important to ensure that the upper management is aware of the risks and plans to treat the risks. The information security risk acceptance process is in line with ISO/IEC 27001:2005 clause 4.2.1 g) Select control objectives and controls for the treatment of risks and h) Obtain management approval of the proposed residual risks.

Figure 1: ISO/IEC 27005 Information Security Risk Management Processes



Clause 11 – Information security risk communication and consultation

The risk communication and consultation process involves activities to achieve an agreement on how to manage risks by exchanging and/or sharing information about those risks between decision-makers and other stakeholders. The information security risk communication and consultation process is in line with ISO/IEC 27001:2005 clause 4.2.4 c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

Clause 12 – Information security risk monitoring and review

On-going monitoring and review of current information security risks are important because risks are not static. New threats and vulnerabilities may arise at any point in time; likelihood or consequences may change abruptly without any indication. Thus, constant and continuous monitoring is necessary to detect these changes. Regular monitoring and reviews will ensure that the risk management context, the outcome of the risk assessment and risk treatment plans remain relevant to the organisation. The information security risk monitoring and review process is in line with ISO/IEC 27001:2005 clause 4.2.3 d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks.

Easy alignment

Another advantage for SMEs that choose ISO/IEC 27005 is that they can align the way they manage other risks, such as enterprise-wide risks, with information security risks. This is due to ISO/IEC 27005 being revised recently to reflect changes in three risk management standards, which are:

ISO 31000:2009 - Risk management - Principles and Guidelines;

ISO 31010:2009 - Risk management - Risk Assessment Techniques; and

ISO Guide 73:2009 - Risk Management Vocabulary.

As an example, SMEs that have adopted ISO 31000 for managing their enterprise-wide risks may find that they can manage their information security risks in a similar fashion. Thus, lesser time and resources may be used when embarking on the journey of adopting ISO/IEC 27005 for information security risk management and implementing ISMS based on ISO/IEC 27001.

Noor Aida Idris & Lt Col (R) Asmuni Yusof are Ordinary Members of the Information Security Professional Association of Malaysia (ISPA). The article was reviewed by ISPA President Col (R) Prof Dato' Husin Jazri. The opinions expressed here are their own.