INTERNATIONAL STANDARD

ISO/IEC 27035

First edition
2011-09-01

Information technology — Security techniques — Information security incident management

Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information

Reference number
ISO/IEC 27035:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27035 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035 cancels and replaces ISO/IEC TR 18044:2004, which has been technically revised.

Introduction

In general, information security policies or controls alone will not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can make information security ineffective and thus information security incidents possible. This can potentially have both direct and indirect adverse impacts on an organization's business operations. Further, it is inevitable that new instances of previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any response less effective, and increase the degree of potential adverse business impact. Therefore, it is essential for any organization serious about information security to have a structured and planned approach to:

- detect, report and assess information security incidents;
- respond to information security incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas);
- report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

This International Standard provides guidance on information security incident management in Clause 4 to Clause 9. These clauses consist of several subclauses, which include a detailed description of each phase.

The term ‘information security incident management’ is used in this International Standard to encompass the management of not just information security incidents but also information security vulnerabilities.

Information technology — Security techniques — Information security incident management

1 Scope

This International Standard provides a structured and planned approach to:

a) detect, report and assess information security incidents;

b) respond to and manage information security incidents;

c) detect, assess and manage information security vulnerabilities; and

d) continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

This International Standard provides guidance on information security incident management for large and medium-sized organizations. Smaller organizations can use a basic set of documents, processes and routines described in this International Standard, depending on their size and type of business in relation to the information security risk situation. It also provides guidance for external organizations providing information security incident management services.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
information security forensics
application of investigation and analysis techniques to capture, record and analyse information security incidents

3.2
information security incident response team
ISIRT
team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle

NOTE The ISIRT as described in this International Standard is an organizational function that covers the process for information security incidents and is focused mainly on IT related incidents. Other common functions (with similar abbreviations) within the incident handling may have a slightly different scope and purpose. The following commonly used abbreviations have a meaning similar to that of ISIRT, though not exactly the same:

- CERT: A Computer Emergency Response Team mainly focuses on Information and Communications Technology (ICT) incidents. There may be other specific national definitions for CERT.
- CSIRT: A Computer Security Incident Response Team is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. These services are usually performed for a defined constituency, which could be a parent entity such as a corporation, governmental organization, or educational organization; a region or country; a research network; or a paid client.

3.3
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant

[ISO/IEC 27000:2009]

3.4
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[ISO/IEC 27000:2009]

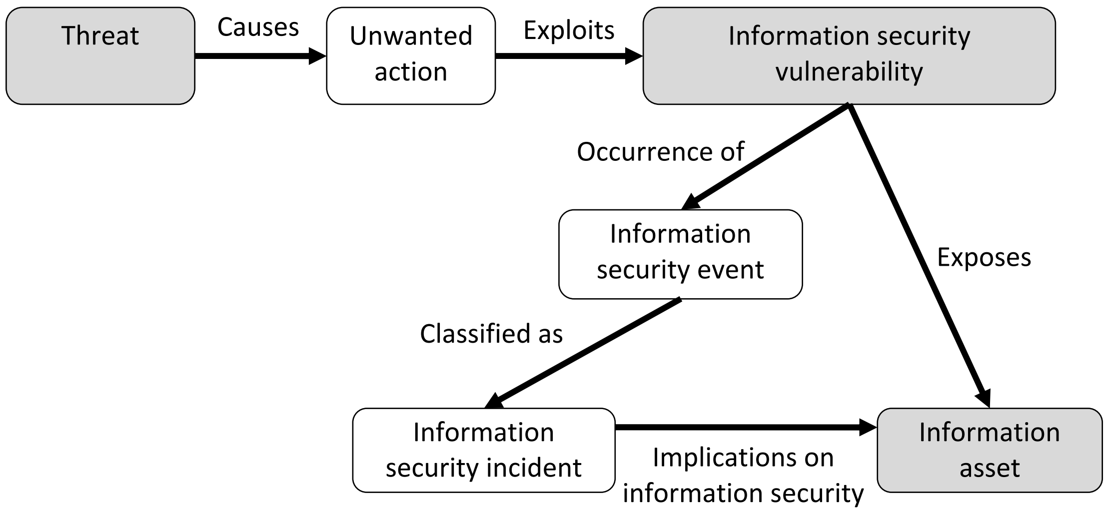
4 Overview

4.1 Basic concepts

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

The occurrence of an information security event does not necessarily mean that an attempt has been successful or that there are any implications on confidentiality, integrity and/or availability, i.e. not all information security events are classified as information security incidents.

A threat acts in unwanted ways to exploit the vulnerabilities (weaknesses) of information systems, services or networks, which is the occurrence of information security events and potentially causes unwanted incidents to information assets exposed by the vulnerabilities. Figure 1 shows this relationship of objects in an information security incident chain. The shaded objects are pre-existing, affected by the unshaded objects in the chain that results in an information security incident.



The shaded objects are pre-existing, affected by the unshaded objects in the chain that results in an information security incident.

Figure 1 — The relationship of objects in an information security incident chain

4.2 Objectives

As a key part of an organization's overall information security strategy, the organization should put controls and procedures in place to enable a structured well-planned approach to the management of information security incidents. From a business perspective, the prime objective is to avoid or contain the impact of information security incidents to reduce the direct and indirect costs caused by the incidents.

The primary steps to minimize the direct negative impact of information security incidents are the following:

- stop and contain,
- eradicate,
- analyse and report, and
- follow up.

The objectives of a structured well-planned approach are more refined and should ensure the following:

a) Information security events are detected and dealt with efficiently, in particular in identifying whether they need to be categorized and classified as information security incidents or not.

b) Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.

c) The adverse effects of information security incidents on the organization and its business operations are minimized by appropriate controls as part of the incident response, possibly in conjunction with relevant elements from a crisis management plan or plans.

d) Reported information security vulnerabilities are assessed and dealt with appropriately.

e) Lessons are learnt quickly from information security incidents, vulnerabilities and associated management. This is to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management scheme.

To help achieve this, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards for incident categorization and classification, and sharing, so that metrics are created from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls.

It is re-iterated that another objective associated with this International Standard is to provide guidance to organizations that aim to meet the requirements specified in ISO/IEC 27001 (and thus supported by guidance from ISO/IEC 27002). This includes information security incident management related requirements. A table that cross-references information security incident management related clauses in ISO/IEC 27001 and ISO/IEC 27002, and clauses in this International Standard is shown in Annex A.

4.3 Benefits of a structured approach

An organization using a structured approach to information security incident management will accrue significant benefits, which can be grouped under the followings.

a) Improving overall information security

A structured process for the detection, reporting and assessment of and decision-making related to information security events and incidents will enable rapid identification and response. This will improve overall security by helping to quickly identify and implement a consistent solution, and thus providing a means of preventing future similar information security incidents. Further, there will be benefits facilitated by metrics, sharing and aggregation. The credibility of the organization will be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business impacts

A structured approach to information security incident management can assist in reducing the level of potential adverse business impacts associated with information security incidents. These impacts can include immediate financial loss and longer-term loss arising from damaged reputation and credibility (for guidance on business impact analysis, see ISO/IEC 27005:2008).

c) Strengthening the information security incident prevention focus

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including identification methods of new threats and vulnerabilities. Analysis of incident related data would enable the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and thus identification of appropriate actions to prevent incidents occurring.

d) Strengthening prioritization

A structured approach to information security incident management will provide a solid basis for prioritization when conducting information security incident investigations, including the use of effective categorization and classification scales. If there are no clear procedures, there is a risk that investigation activities could be conducted in a reactive mode, by responding to incidents as they occur and overlooking what activities are needed. This could prevent investigation activities from being directed to areas where they may be a higher priority where they are really needed and in the ideal priority.

e) Strengthening evidence

Clear incident investigation procedures can help to ensure that data collection and handling are evidentially sound and legally admissible. These are important considerations if legal prosecution or disciplinary action might follow. It should be recognized, however, that there is a chance that the actions necessary to recover from an information security incident might jeopardize the integrity of any such collected evidence.

f) Contributing to budget and resource justifications

A well-defined and structured approach to information security incident management will help justify and simplify the allocation of budgets and resources within involved organizational units. Further, benefit will accrue for the information security incident management scheme itself, with the

- use of less skilled staff to identify and filter out the alarms of abnormality or anomaly,
- provision of better direction for the activities of skilled personnel, and
- engagement of skilled personnel only for those processes where their skills are needed and only at the stage of the process where their contribution is needed.

Another useful approach to control and optimize budget and resources, is to add time tracking to information security incident management to facilitate quantitative assessments of the organization's handling of information security incidents. It should, for example, be possible to provide information on how long it takes to resolve information security incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

g) Improving updates to information security risk assessment and management results

The use of a structured approach to information security incident management will facilitate the

- better collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities, and
- provision of data on frequencies of occurrence of the identified threat types.

The data collected on the adverse impacts on business operations from information security incidents will be useful in the business impact analysis. The data collected to identify the occurrence frequency of the various threat types will greatly aid the quality of the threat assessment. Similarly, the data collected on vulnerabilities will greatly aid the quality of future vulnerability assessments (for guidance on information security risk assessment and management, see ISO/IEC 27005:2008).

h) Providing enhanced information security awareness and training program material

A structured approach to information security incident management will provide focused information for information security awareness programs. This focused information will provide real examples demonstrating that information security incidents happen to real organizations. It will also be possible to demonstrate the benefits associated with the rapid availability of solution information. Furthermore, such awareness helps to reduce a mistake or panic/confusion by an individual in the event of an information security incident.

i) Providing input to information security policy and related documentation reviews

Data provided by an information security incident management scheme could provide valuable input to reviews of the effectiveness and subsequent improvement of information security policies (and other related information security documents). This applies to policies and other documents applicable both for organization-wide and for individual systems, services and networks.

4.4 Adaptability

The guidance provided by this International Standard is extensive and if adopted in full, could require significant resources to operate and manage. It is therefore important that an organization applying this guidance should retain a sense of perspective and ensure that the resources applied to information security incident management and the complexity of the mechanisms implemented, are kept in proportion to the following:

a) size, structure and business nature of an organization,

b) scope of any information security management system within which incidents are handled,

c) potential for loss through unprevented incidents arising, and

d) the goals of the business.

An organization using this International Standard should therefore adopt its guidance in due proportion to the scale and characteristics of their business.

4.5 Phases

To achieve the objectives outlined in Clause 4.2, information security incident management consists of the following five distinct phases:

- Plan and prepare,
- Detection and reporting,
- Assessment and decision,
- Responses, and
- Lessons learnt.

The first phase involves getting all that is required in place to operate successful information security incident management. The other four phases involve the operational use of information security incident management.

A high-level view of these phases is shown in Figure 2.

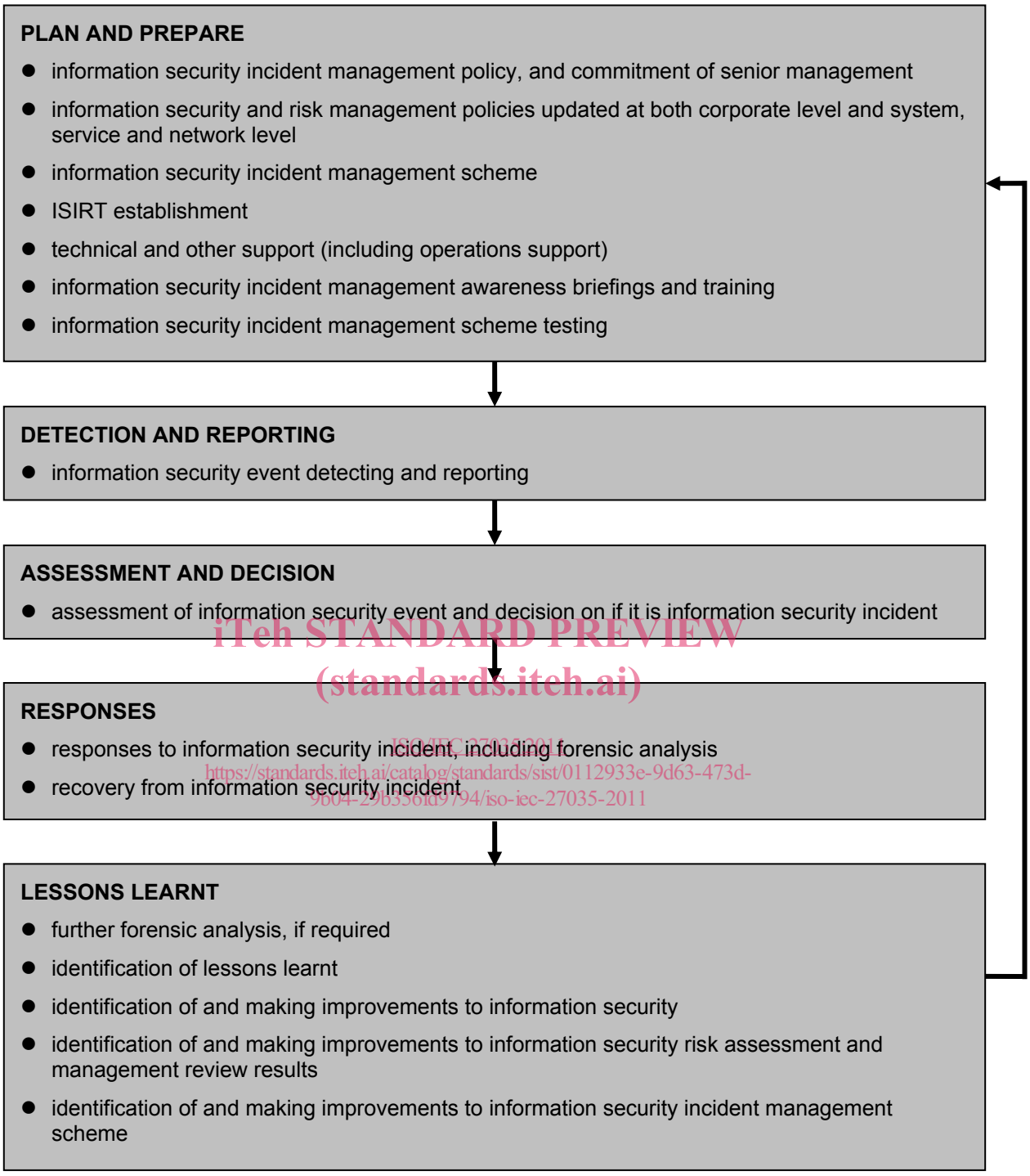


Figure 2 — Information security incident management phases

4.6 Examples of information security incidents

Information security incidents may be deliberate or accidental (e.g. caused by error or acts of nature), and may be caused by technical or physical means. Their consequences may include the disclosure, modification, destruction, or unavailability of information in an unauthorized manner, or the damage or theft of organizational assets. If unreported information security events are determined to be incidents, it becomes difficult to investigate the incidents and to take control in order to prevent recurrence.

Annex B provides descriptions of selected example information security incidents and their causes for informative purposes only. It is important to note that these examples are by no means exhaustive.

5 Plan and prepare phase

5.1 Overview of key activities

Effective information security incident management requires appropriate planning and preparation.For an efficient and effective information security event, incident and vulnerability management scheme to be put into operational use, an organization should complete a number of preparatory activities after the necessary planning. The organization should ensure that the activities of the plan and prepare phase include the following:

a) Activity to formulate and produce an information security event/incident/vulnerability management policy, and gaining senior management commitment to that policy. This should be preceded by an information security review of the organization's vulnerabilities, confirmation of the need for an information security incident management scheme, and identification of the benefits to the organization as a whole and to its departments (see Clause 5.2). Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident, know what to do and understand the benefits of the approach to the organization. Management needs to be supportive of the management scheme to ensure that the organization commits to resourcing and maintaining an incident response capability.

b) Activity to update information security and risk management policies at a corporate level and specific system, service and network levels. This should include reference to information security event, incident and vulnerability management. Policies need to be reviewed regularly in the context of output from the information security incident management scheme (see Clause 5.3).

c) Activity to define and document a detailed information security incident management scheme. Overall, the scheme documentation should encompass the forms, procedures, organizational elements and support tools for the detection and reporting of, assessment and decision making related to, making responses to, and learning lessons from, information security incidents. The topics for inclusion include:

   1) An information security event/incident classification scale to be used to grade events/incidents. In any event, the decision should be based on the actual or projected adverse impacts on the organization's business operations.

   NOTE Annex C shows an example approach to the categorization and classification of information security events and incidents.

   2) The information security event/incident/vulnerability forms:

      i) completed by the person reporting an information security event (i.e. not an information security incident management team member), with the information recorded in an information security event/incident/vulnerability database,

      ii) used by the information security incident management personnel to build on the initially reported information security event information and enable a running record of the incident assessments, etc. over time until the incident is fully resolved. At each stage, the update is recorded in the information security event/incident/vulnerability database. The completed information security event/incident/vulnerability database record is then used in post-incident resolution activities, and

      iii) completed by the person reporting an information security vulnerability (that has not yet been exploited to cause an information security event, and possibly an information security incident), with the information recorded in the information security event/incident/vulnerability database.

It is recommended that these forms are electronic (e.g. in secure web page), linking directly to the electronic information security event/incident/vulnerability database. In today's world, the operation of a paper-based scheme would be time consuming. However, a paper-based scheme may be needed for a case where an electronic scheme can not be used.

NOTE Example forms are shown in Annex D.

3) The documented procedures and actions related to the use of the forms, i.e. associated with information security event, incident and vulnerability detection, with links to the normal procedures for the use of data and system, service and/or network backups and crisis management plans.

4) Operating procedures for the ISIRT, with documented processes and associated responsibilities, and the allocation of roles to designated persons to conduct various activities (an individual may be allocated more than one role, depending on the size, structure and business nature of an organization), for example including:

   i) shut down an affected system, service and/or network, in certain circumstances agreed by prior arrangement with the relevant IT and/or business management,

   ii) leave an affected system, service and/or network, connected and running,

   iii) monitor data flowing from, to and within an affected system, service and/or network,

   iv) activate normal back-up and crisis management procedures and actions in line with the system, service and/or network security policy,

   v) monitor and maintain the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action, and

   vi) communicate information security incident details to internal and external people or organizations.

In some organizations, the scheme may be referred to as an information security incident response plan (see Clause 5.4).

d) Activity to establish the ISIRT, with an appropriate training program designed, developed and provided to its personnel. According to the size, structure and the nature of the business, an organization may have an ISIRT of a dedicated team, a virtual team, or a mix of the two options. A dedicated team may have virtual members identified in specific units/functions that should cooperate closely with the ISIRT during the resolution of an information security incident (ICT, legal, public relations, outsourcing companies, etc.). A virtual team may have a senior manager leading the team supported by groups of individuals specialized in particular topics, e.g. in the handling of malicious code attacks, who will be called upon depending on the type of incident concerned (see Clause 5.5).

e) Activity to establish and preserve appropriate relationships and connections with internal and external organizations that are directly involved in information security event, incident and vulnerability management.

f) Activity to establish, implement and operate technical and other support (including organizational) mechanisms for supporting the information security incident management scheme (and thus the work of the ISIRT), and in order to prevent information security incident occurrences or reduce the likelihood of occurrences of information security incidents (see Clause 5.6). Such mechanisms could include the following:

   1) Internal information security audit mechanisms to assess the security level and track vulnerable systems,

   2) Vulnerability management (including security updates and security patching of vulnerable systems).

   3) Technology watch to detect new kinds of threats and attacks.