BS ISO/IEC 27035:2011

BSI Standards Publication

Information technology — Security techniques — Information security incident management

raising standards worldwide™

National foreword

This British Standard is the UK implementation of ISO/IEC 27035:2011. It supersedes PD ISO/IEC TR18044:2004 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 63587 8

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2011.

Amendments issued since publication

Date	Text affected

BS ISO/IEC 27035:2011

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)

COPYRIGHT PROTECTED DOCUMENT

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.

INTERNATIONAL STANDARD **ISO/IEC 27035:2011(E)**

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.

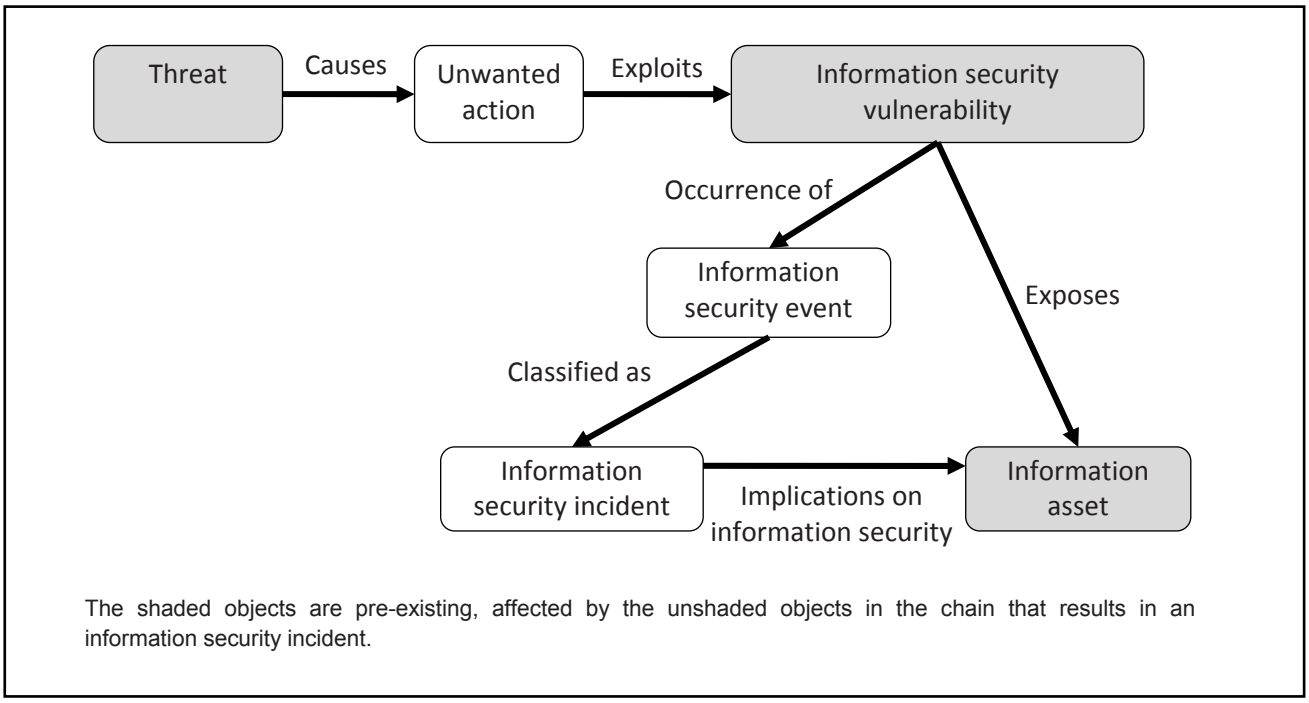

Figure 1 — The relationship of objects in an information security incident chain

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.

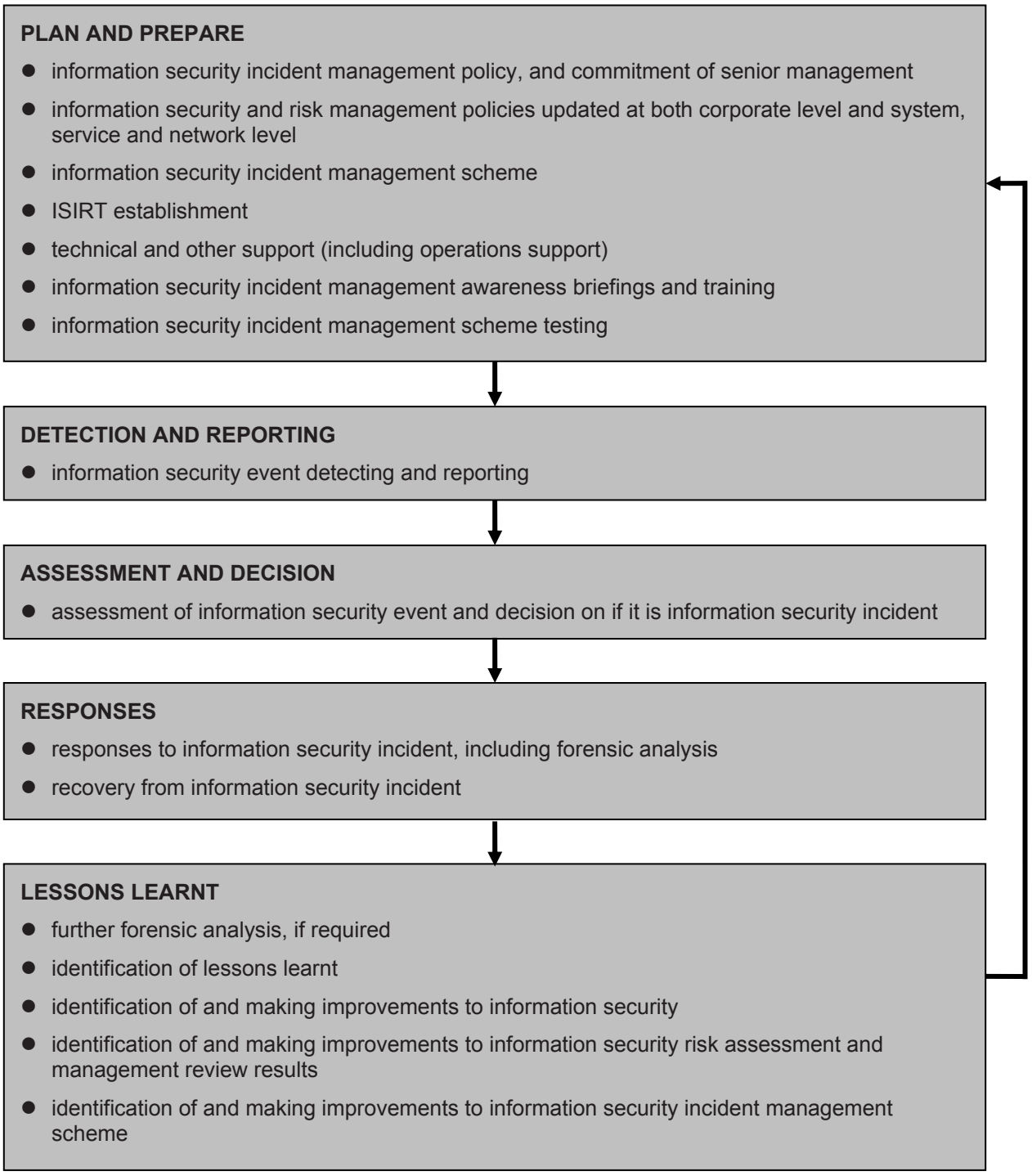

Figure 2 — Information security incident management phases

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.

4) Intrusion Detection Systems (for more details, see ISO/IEC 18043).

5) Network security devices, protections means and monitoring tools (for more details, see ISO/IEC 27033).

6) Anti-malicious code software.

7) Audit log records, and log monitoring software.

8) Documented responsibilities and operating procedures for the operations support team.

g) Activity to design and develop an information security event, incident and vulnerability management awareness and training program. All organizational personnel should be made aware through briefings and/or other mechanisms, of the existence of the information security event, incident and vulnerability management scheme, its benefits and how to report information security events and incidents (and vulnerabilities). In parallel, appropriate training should be provided to those personnel responsible for managing the information security event, incident and vulnerability management scheme, decision makers involved in determining whether information security events are incidents, and those individuals involved in the investigation of incidents. Awareness briefings and training sessions should be repeated later to accommodate changes in personnel (see Clause 5.7).

h) Activity to test the use of the information security incident management scheme, its processes and procedures. Tests should be organized periodically not only to test the scheme in a real situation, but also to verify how the ISIRT behaves under the pressure of a severe complex incident. Particular attention should be given to the creation of tests that focus on the evolving vulnerability, threat and risk scenarios (see Clause 5.8). The scheme should include standards that support information sharing, both within the organization and outside (if required by the organization). One of the benefits of sharing is the aggregation of data into useful metrics to aid strategic business decisions. Membership of a trusted information sharing community also provides early warning of attacks and should be encouraged in any information security incident management scheme and associated policy.

With this phase completed, organizations should be fully prepared to properly manage information security incidents. The following clauses describe each of the activities listed above, including the contents of each document required.

5.2 Information security incident management policy

5.2.1 Introduction

An organization should document its policy for managing information security events, incidents and vulnerabilities as a free-standing document, as part of its overall information security management system policy (see Clause 4.2.1 b) of ISO/IEC 27001:2005), or as part of its Information Security Policy (see Clause 5.1.1 of ISO/IEC 27002:2005). The size, structure and business nature of an organization and the extent of its information security incident management program are deciding factors in determining which of these options to adopt. Each organization should direct its information security incident management policy at every person having legitimate access to its information systems and related locations.

Before the policy is formulated, the organization should conduct an information security review highlighting its vulnerabilities, confirmation of the need for information security incident management, and identification of the benefits to the organization as a whole and to its departments.

5.2.2 Involved parties

An organization should ensure that its information security incident management policy is approved by a senior organization executive officer, with confirmed documented commitment from all of senior management. It should be made available for every employee and contractor, and should also be addressed in information security awareness briefings and training (see Clause 5.7).

5.2.3 Content

An organization should ensure that its information security incident management policy content addresses the following topics:

a) The importance of information security incident management to the organization, and senior management's commitment to it and the related scheme.

b) An overview of information security event detection, reporting and collection of relevant information, and how this information should be used to determine information security incidents.

   This overview should include a summary of possible types of information security events, how to report them, what to report, where and to whom, and how to handle entirely new types of information security events. It should also include a summary of information security vulnerability reporting and handling.

c) An overview of information security incident assessment, including a summary of who is responsible, what has to be done, notification, and escalation.

d) A summary of the activities that follow the confirmation that an information security event is an information security incident.

e) A reference to the need for ensuring that all information security incident management activities are properly logged for later analysis, and that continuous monitoring is conducted to ensure the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action.

f) Post information security incident resolution activities, including learning from and improving the process, following information security incidents.

g) An overview of information security vulnerability reporting and handling.

h) Details of where the scheme documentation, including procedures, is held.

i) An overview of the ISIRT, encompassing the following topics.

   1) The ISIRT organizational structure, and the identity of the ISIRT manager and other key personnel, including who is responsible for:

      i) briefing senior management on incidents,

      ii) dealing with enquiries, instigating follow up, etc., and

      iii) the link with the external organizations (when necessary).

   2) The information security management charter that specifies what the ISIRT is to do and the authority under which it does it. At a minimum, the charter should include a mission statement, a definition of the ISIRT's scope, and details of the ISIRT's board level sponsor and authority.

   3) The ISIRT mission statement that focuses on the team's core activities. In order to be considered an ISIRT, the team should support the assessing of, responding to, and managing of, information security incidents, to a successful conclusion. The goals and purposes of the team are especially important, and require clear, unambiguous definition.

   4) A definition of the scope of the ISIRT activities. Normally, the scope of an organization's ISIRT covers all of the organization's information systems, services and networks. In other cases, an organization may, for whatever reason, require the scope to be less than that, in which case it should be clearly documented what is in, and what is out of, scope.

5) Identification of a senior executive officer, board member or senior manager who has the authority to make decision on ISIRT and also establish the levels of authority for ISIRT. Knowing this helps all personnel in the organization to understand the background and set-up of the ISIRT, and it is vital information for building trust in the ISIRT. It should be noted that before this detail is promulgated, it should be checked from a legal perspective. In some circumstances, disclosure of a team's authority may expose it to claims of liability.

6) Links to organizations providing specific external support, such as forensics teams (see Clause 5.5.4).

j) An overview of the technical and other support mechanisms.

k) An overview of the information security incident management awareness and training program.

l) A summary of the legal and regulatory aspects that have to be addressed (for more details, see Annex E).

5.3 Information security incident management integration in other policies

5.3.1 Introduction

An organization should include information security incident management content in its information security and risk management policies at corporate level as well as on specific system, service and network levels and relate this content to the incident management policy. The integration should aim for the following:

a) To describe why information security incident management, particularly an information security incident reporting and handling scheme, is important.

b) To indicate senior management commitment to the need for proper preparation and response to information security incidents, i.e. to the information security incident management scheme.

c) To ensure consistency across the various policies.

d) To ensure planned, systematic and calm responses to information security incidents, thus minimizing the adverse impacts of incidents.

For guidance on information security risk assessment and management, see ISO/IEC 27005:2008.

5.3.2 Content

Each organization should update and maintain its corporate information security and risk management policies, and specific system, service or network information security policies. These policies need to refer to a corporate information security incident management policy and associated scheme explicitly.

a) The relevant sections should refer to the senior management commitment.

b) The relevant sections should outline the policy.

c) The relevant sections should outline scheme processes, and related infrastructure.

d) The relevant sections should outline requirements for detecting, reporting, assessing and managing information security events, incidents and vulnerabilities.

e) The relevant sections should clearly indicate those personnel responsible for authorizing and/or undertaking certain critical actions (e.g. taking an information system off-line or even shutting it down).

The policies should include the requirement that appropriate review mechanisms need to be established. These mechanisms need to ensure that information from the detection, monitoring and resolution of information security incidents and from dealing with reported information security vulnerabilities is used as input to ensure the continuing effectiveness of the corporate information security and risk management policies, and specific system, service or network information security policies.

5.4 Information security incident management scheme

5.4.1 Introduction

The aim of an information security incident management scheme is to provide detailed documentation describing the activities and procedures for dealing with information security events and incidents, and the communication of such events, incidents and vulnerabilities. The information security incident management scheme comes into effect whenever an information security event is detected, or an information security vulnerability is reported. Each organization should use the scheme as a guide for:

a) responding to information security events,

b) determining whether information security events become information security incidents,

c) managing information security incidents to a conclusion,

d) responding to information security vulnerabilities,

e) identifying lessons learnt, and any improvements to the scheme and/or security in general that are required, and

f) making identified improvements.

5.4.2 Involved parties

An organization should ensure that the information security incident management scheme is addressed to all personnel and associated contractors, ICT service providers, telecommunication providers and outsourcing companies, thus covering the following responsibilities:

a) detecting and reporting information security events (this is the responsibility of any permanent or contracted personnel in an organization and its companies),

b) assessing and responding to information security events and incidents, being involved in the post-incident resolution activities of learning, and improving information security and the information security incident management scheme itself (this is the responsibility of members of the PoC (Point of Contact), the ISIRT, management, public relations personnel and legal representatives), and

c) reporting information security vulnerabilities (this is the responsibility of any permanent or contracted personnel in an organization and its companies), and dealing with them.

The scheme should also take into account any third party users, and information security incidents and associated vulnerabilities reported from third party organizations and government and commercial information security incident and vulnerability information provision organizations.

5.4.3 Content

Each organization should ensure that the content of the information security incident management scheme documentation includes the following:

a) An overview of the information security incident management policy.

b) An overview of the whole information security incident management scheme.

c) The detailed activities, procedures and information, associated with the following:

1) Plan and prepare

i) A standardized approach to information security event/incident categorization and classification, to enable the provision of consistent results. In any event, the decision should be based on the actual or projected adverse impacts on the organization's business operations, and associated guidance.

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

ii) A standard information security event/incident/vulnerability database structure, which is likely to provide the capability to compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of information systems

iii) Guidance for deciding whether escalation is required during each relevant process, and to whom, and associated procedures. Based on the guidance provided in the information security incident management scheme documentation, anyone assessing an information security event, incident or vulnerability should know in which circumstances it is necessary to escalate matters, and to whom it should be escalated to. In addition, there are unforeseen circumstances when this may be necessary. For example, a minor information security incident could evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up in a week could become a major information security incident. The guidance should define information security event and incident types, escalation types and who may institute escalation.

iv) Procedures to be followed to ensure that all information security incident management activities are properly logged in the appropriate form, and that log analysis is conducted by designated personnel.

v) Procedures and mechanisms to ensure that the change control regime is maintained covering information security event, incident and vulnerability tracking and information security event/incident/vulnerability report updates, and updates to the scheme itself,

vi) Procedures for information security forensics analysis.

vii) Procedures and guidance on using Intrusion Detection Systems (IDS), ensuring that associated legal and regulatory aspects have been addressed. Guidance should include discussion of the advantages and disadvantages of undertaking attacker surveillance activities. Further information on IDS is contained in ISO/IEC 18043:2006.

viii) Guidance and procedures associated with the technical and organizational mechanisms that are established, implemented and operated in order to prevent information security incident occurrences and to reduce the likelihood of occurrences of information security incidents, and to deal with occurred information security incidents.

ix) Material for the information security event, incident and vulnerability management awareness and training program.

x) Procedures and specifications for the testing of the information security incident management scheme.

xi) The scheme of organizational structure for information security incident management.

xii) The terms of reference and responsibilities of the ISIRT as a whole, and of individual members.

xiii) Important contact information.

2) Detection and reporting

   i) Detecting and reporting the occurrence of information security events (by human or automatic means).

   ii) Collecting the information on information security events.

   iii) Detecting and reporting on information security vulnerabilities.

   iv) Fully recording all information gathered in the information security incident management database.

3) Assessment and decision

   i) The PoC conducting assessments of information security events (including escalation as required), using the agreed information security event/incident classification scale (including determining the impacts of events based on the affected assets/services) and deciding whether events should be classified as information security incidents.

   ii) The ISIRT assessing information security events should confirm whether an event is an information security incident or not, and then another assessment should be conducted using the agreed information security event/incident classification scale to confirm the details of the event (potential incident) type and affected resource (categorization). This should be followed by decisions being made on how the confirmed information security incident should be dealt with, by whom and in what priority, as well as escalation levels.

   iii) Assessing information security vulnerabilities (that have not yet been exploited to cause information security events and potential information security incidents), with decisions made on which need to be dealt with, by whom, how and in what priority.

   iv) Fully recording all assessment results and related decisions in the information security incident management database.

4) Responses

   i) Review by the ISIRT to determine if the information security incident is under control, and

      - if the incident is under control, instigate the required response, either immediately (in real-time or in near real-time) or at a later time,

      - if the incident is not under control or it is going to have a severe impact on the organization's core services, instigate crisis activities through escalation to crisis handling function.

   ii) Defining a map of all internal and external functions and organizations that should be involved during the management of an incident.

   iii) Conducting information security forensics analysis, as required.

   iv) Escalation, on an as required basis.

   v) Ensuring that all involved activities are properly logged for later analysis.

   vi) Ensuring that electronic evidence is gathered and stored provably securely.

   vii) Ensuring that the change control regime is maintained, and thus that the information security event/incident/vulnerability database is kept up-to-date.

   viii) Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations.

   ix) Dealing with information security vulnerabilities.

x) Once the incident has been successfully dealt with, formally closing it and recorded this in the information security incident management database.

Each organization should ensure that the information security incident management scheme documentation allows for information security incident responses, both immediately and longer-term. All information security incidents should undergo an early assessment of the potential adverse impacts on business operations, both short and longer-term (for example, a major disaster could occur some time after an initial information security incident). Further, it should allow for some responses necessary for information security incidents that are completely unforeseen, where ad hoc controls are required. Even for this situation, organizations should encompass general guidelines in the scheme documentation on the steps that may be necessary.

5) Lessons learnt

i) Conducting further information security forensic analysis, as required.

ii) Identifying the lessons learnt from information security incidents and vulnerabilities.

iii) Reviewing, identifying and making improvements to information security control implementation (new and/or updated controls), as well as information security incident management policy, as result of the lessons learnt.

iv) Reviewing, identifying and if possible, making improvements to the organization's existing information security risk assessment and management review results, as a result of the lessons learnt.

v) Reviewing how effective the processes, procedures, the reporting formats and/or the organizational structure were in responding to assessing and recovering from each information security incident and dealing with information security vulnerabilities, and on the basis of the lessons learnt identifying and making improvements to the information security incident management scheme and its documentation.

vi) Updating the information security event/incident/vulnerability database.

vii) Communicating and sharing the results of review within a trusted community (if the organization so wishes.

5.4.4 Procedures

Before being able to commence operation of the information security incident management scheme, it is important that an organization has documented and checked that the procedures are available. Each procedure should indicate those groups or individuals responsible for its use and management, as appropriate from the PoC and/or the ISIRT. Such procedures should ensure that electronic evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case it is required for legal prosecution or internal disciplinary action. Further, there should be documented procedures covering not just PoC and ISIRT activities, but those involved in information security forensic analysis and crisis activities – if not covered elsewhere, e.g. in a business continuity plan or a crisis management plan. The documented procedures should be entirely in line with the documented information security incident management policy and other information security incident management scheme documentation.

It is important to understand that not all procedures need be publicly available. For example, it is not necessary for all organizational personnel to understand the internal operation of an ISIRT in order to interact with it. The ISIRT should ensure that publicly available guidance, including information resulting from information security incident analysis, is in readily available form, e.g. on the organization's intranet. It may also be important to keep some details of the information security incident management scheme closely held to prevent an insider from tampering with the investigation process. For example, if a bank employee who is embezzling funds is aware of some details of the scheme, he or she may be able to better hide their activities from investigators or otherwise hamper the detection, investigation of and recovery from an information security incident.

The content of operating procedures depends on a number of criteria, especially related to the nature of known potential information security events, incidents and vulnerabilities and the types on information system assets that might be involved and their environment. Thus, an operating procedure could be related to a particular type of incident or product (for example firewalls, databases, operating systems, applications) or to a specific product. Each operating procedure should clearly identify the steps to be undertaken and by whom. It should reflect experience from external (for example government and commercial ISIRTs or similar, and suppliers) as well as from internal sources.

There should be operating procedures for dealing with types of information security events and incidents that are already known, as well as vulnerabilities. There should also be operating procedures to be followed when an identified information security event, incident or vulnerability is not of any known type. In this case the following should be addressed:

a) the reporting process for the handling of such exceptions,

b) guidance on the timing for getting approval from management in order to avoid any delay of response, and

c) pre-authorized delegation of decision making without normal approval process.

5.4.5 Trust

The ISIRT plays a crucial role for the overall information security of an organization. The ISIRT requires the collaboration of all organizational personnel to detect, resolve and investigate information security incidents. It is fundamental that the ISIRT is trusted by everybody, both internally and externally. Adoption of anonymity with regard to reporting information security vulnerabilities, events and incidents may be helpful to build trust.

An organization should ensure that its information security incident management scheme addresses situations where it is important to ensure the anonymity of the person or party that reports potential information security incidents or vulnerabilities under specific circumstances. Each organization should have provisions that clearly illustrate the expectation of anonymity, or lack thereof, for persons or parties reporting a potential information security incident or vulnerability. The ISIRT may need to obtain additional information not initially relayed by the person or party who reported the incident. Furthermore, important information about the information security incident or vulnerability itself may be derived from who detects it first.

Another approach that may be adopted by the ISIRT is to win users' trust through transparency and mature processes. The ISIRT should work to educate users, explain how the ISIRT works, how it protects confidentiality of information collected and how it manages users' event, incident and vulnerability reports.

The ISIRT should be capable of efficiently satisfying the functional, financial, legal and political needs of the organization and be able to exercise organizational discretion when managing information security incidents and vulnerabilities. The function of the ISIRT should also be independently audited to confirm that all business requirements are being satisfied effectively.

Further, a good way of achieving another aspect of independence is to separate the incident and vulnerability reporting chain from operational line management and to make a senior manager directly responsible for managing incident and vulnerability responses. Finance of the capability should also be segregated to avoid undue influence.

5.4.6 Confidentiality

An information security incident management scheme may contain sensitive information, and people involved in addressing incidents and vulnerabilities may be required to handle sensitive information. An organization should ensure that the necessary processes are established to anonymize sensitive information and require personnel with access to sensitive information to sign confidentiality agreements.. If information security events/incidents/vulnerabilities are logged via a generalized problem management system, sensitive details may have to be omitted. Additionally, an organization should ensure that the information security incident management scheme makes provision for controlling the communication of incidents and vulnerabilities to external parties, including the media, business partners, customers, law enforcement organizations, and the general public.

5.5 Establishment of the ISIRT

5.5.1 Introduction

The aim of establishing the ISIRT is to provide the organization with appropriate capability for assessing, responding to and learning from information security incidents, and providing the necessary co-ordination, management, feedback and communication. An ISIRT contributes to the reduction in physical and monetary damage, as well as the reduction of the damage to the organization's reputation that is sometimes associated with information security incidents.

5.5.2 Members and structure

The size, structure and composition of an ISIRT should be appropriate for the size, structure, and the business nature of the organization. Although the ISIRT may constitute an isolated team or department, members may share other duties, which encourage the input of members from a range of areas within the organization. An organization should evaluate if it requires a dedicated team, a virtual team, or a mix of the two. The number of incidents and the activities performed by the ISIRT should guide the organization in this choice.

The ISIRT goes through different maturity stages and often adjustments to the organizational model are adopted based on the specific scenario faced by the organization. Whenever justified, it is recommended to have a permanent team led by a senior manager. Virtual ISIRTs teams may be led by a senior manager. The senior manager should be supported by individuals who are specialized in particular topics, for example in handling malicious code attacks, which are called upon depending on the type of information security incident concerned. Depending on the size, structure and business nature of an organization, a member may also fulfil more than one role within the ISIRT. The ISIRT may comprise individuals from different parts of the organization (e.g. business operations, ICT, audit, human resources and marketing). This also applies to permanent ISIRTs; even in case of dedicated personnel, the ISIRT always requires support from other departments.

Team members should be accessible for contact, so the names and contact details of each member and their backup members should be available within the organization. The necessary details should be clearly indicated in the information security incident management scheme documentation, including any procedural documents, and the reporting forms, but not in policy statements.

The ISIRT manager should usually have a separate line of reporting to senior management, separate from normal business operations. He/she should have delegated authority to make immediate decisions on how to deal with an incident, and should ensure that all ISIRT members have the required knowledge and skills levels, and that these continue to be maintained. The ISIRT manager should assign investigation of each incident to the most appropriate member of his/her team, with each incident assigned a named manager.

5.5.3 Relationship with other parts of the organization

The ISIRT should have the responsibility for ensuring that incidents are resolved, and in this context the ISIRT manager and members of his/her team should have a degree of authority to take the necessary actions deemed appropriate in response to information security incidents. However, actions that may have adverse effects on the overall organization, either financially or in terms of reputation, should be agreed with senior management. For this reason, it is essential that the information security incident management policy and scheme details the appropriate authority to which the ISIRT manager reports serious information security incidents.

Procedures and responsibilities for dealing with the media should also be agreed with senior management and documented. These procedures should specify who in the organization deals with media inquiries, and how that part of the organization interacts with the ISIRT.

5.5.4 Relationship with external interested parties

Organizations should establish relationships between the ISIRT and appropriate external interested parties. External interested parties may include the following:

a) contracted external support personnel,

b) external organizations' ISIRTs ,

c) managed service providers, including tellecommunication service providers, ISPs and suppliers,

d) law enforcement organizations,

e) emergency authorities,

f) appropriate government organizations,

g) legal personnel,

h) public relations officials and/or members of the media,

i) business partners,

j) customers, and

k) the general public.

5.6 Technical and other support (including operational support)

To ensure that quick and effective responses to information security incidents can be achieved, an organization should acquire, prepare and test all necessary technical and other support means. This includes the following:

a) access to details of the organization's assets with an up-to-date asset register and information on their links to business functions,

b) access to the documented procedures related to crisis management,

c) documented and promulgated communications processes,

d) the use of an information security event/incident/vulnerability database and the technical means to populate and update the database quickly, analyze its information and facilitate responses (in some instances manual records may be required by an organization), with the database kept provably secure,

e) facilities for information security forensics evidence collection and analysis, and

f) adequate crisis management arrangements for the information security event/incident/vulnerability database (for guidance on business continuity management see ISO/IEC 27031).

An organization should ensure that the technical means used to populate and update the database quickly, analyze its information and facilitate responses to information security incidents support the following:

g) quick acquisition of information security event/incident/vulnerability reports,

h) notification of previously selected external personnel by appropriate means (for example electronic mail, fax or telephone), thus requiring the maintenance of a reliable, readily accessible contact database (including paper and other backups), and the facility to transmit information to individuals in a secure fashion where appropriate,

i) taking precautions commensurate with assessed risks for ensuring that electronic communication, whether internet or non-internet, cannot be eavesdropped and stays available while the system, service and/or network is under attack (this may require pre-planned alternative communications mechanisms being in place),

j) ensuring the collection of all data about the information system, service and/or network, and all data processed,

k) using cryptographic integrity control to help in determining whether and what parts of the system, service and/or network, and what data, were changed, if commensurate with assessed risks,

l) facilitating the archiving and securing of collected information (for example, by applying digital signatures to logs and other evidence before off-line storage in read-only media such as CD or DVD ROM),

m) enabling the preparation of printouts (e.g. of logs), including those showing the progress of an incident, and the resolution process and chain of custody,

n) recovery of the information system, service and/or network to normal operation, with the following procedures that are in line with the relevant crisis management:

   1) backup testing,

   2) malicious code control,

   3) original media with system and application software,

   4) bootable media, and

   5) clean, reliable and up-to-date system and application patches.

   It is increasingly common for organizations to create a standard baseline image from the installation media and use that image as the clean basis for creating systems. Using such an image instead of the original media is often preferable because the image has already been patched, hardened, tested, etc.

An attacked information system, service or network may not function correctly. Thus as far as possible, no technical means (software and hardware) necessary for responding to an information security incident should rely in their operations on the organization's 'mainstream' systems, services and/or networks, proportionate to the assessed risks. All technical means should be carefully selected, correctly implemented and regularly tested (including testing of the backups made). If it is possible, the technical means should be fully independent.

NOTE Technical means described in this clause do not include technical means used to detect information security incidents and intrusions directly and to automatically notify appropriate persons. Such technical means are described in ISO/IEC 18043.

Whilst the organization's PoC has a much wider ongoing role in the organization to provide support for all aspects of IT and related information handling, it has a key role to play in information security incident management. When information security events are first reported, the PoC deals with them in the detection and reporting phase. The PoC should review the information gathered and make the initial assessment as to whether events should be classified as incidents or not. If the event is not classified as an incident, the PoC should deal with it accordingly. If an event is classified as an incident, it may be that the PoC deals with it, albeit it is expected that in most cases the responsibility for dealing with the incident needs to be handed over to the ISIRT. It is not expected that personnel at the PoC are security experts.

5.7 Awareness and training

Information security incident management is a process that involves not only technical means but also people. Thus, it should be supported by appropriately information security-aware and trained individuals within the organization.

The awareness and participation of all organization personnel is crucial for the success of a structured information security incident management approach. Whilst users should be required to participate, they are less likely to participate effectively in its operation if they are unaware of how they and their department may benefit from participating in a structured approach to information security incident management, Further, the operational efficiency and quality of a structured approach to information security incident management relies on a number of factors, including obligation to notify incidents, quality of notification, ease of use, speed and training. Some of these factors relate to making sure that users are aware of the value of information security incident management and being motivated to report incidents.

The organization should ensure that the role of information security incident management is actively promoted as part of the corporate information security awareness and training program. The awareness program and related material should be available to all personnel, including new employees, third party users and contractors, as relevant. There should be a specific training program for the PoC, ISIRT members, information security personnel and specific administrators, as necessary. Each group of people involved directly with the management of incidents may require different levels of training, depending on the type, frequency and criticality of their interaction with the information security incident management scheme.

The organization's awareness briefings should encompass the following:

a) benefits to be derived from the structured approach to information security incident management, both to the organization and to its personnel,

b) how the information security incident management scheme works, including its scope and the security event, incident and vulnerability management workflow,

c) how to report on information security events, incidents and vulnerabilities,

d) incident information held in, and the outputs from the information security event/incident/vulnerability database,

e) controls on confidentiality of sources as relevant,

f) scheme service level agreements,

g) notification of outcomes – under what circumstances sources are advised,

h) any constraints imposed by non-disclosure agreements,

i) the authority of the information security incident management organization and its reporting line, and

j) who receives reports from the information security incident management scheme, and how the reports are distributed.

In some cases, it may be desirable for the organization to include awareness detail specifically about information security incident management in other training programs (for example, personnel orientation programs or general corporate security awareness programs). This awareness approach may provide valuable context relevant to particular groups of people, and improves training program effectiveness and efficiency.

Before the information security incident management scheme becomes operational, the organization should ensure that all relevant personnel are familiar with the procedures involved in the detection and reporting of information security events, and selected personnel are very knowledgeable about the subsequent activities. This should be followed up by regular awareness briefings and training courses. The training should be supported by specific exercises and testing for PoC and ISIRT members, and information security personnel and specific administrators.

In addition, the awareness and training programs should be complemented by the establishment and operations of ‘hot line’ support from information security incident management personnel, in order to minimize delays in reporting and handling information security events, incidents and vulnerabilities.

5.8 Scheme testing

The organization should schedule regular checking and testing of the information security incident management processes and procedures to highlight potential flaws and problems that may arise during the management of information security events and incidents and vulnerabilities. Periodic tests should be organized to check processes/procedures and to verify how the ISIRT responds to severe complex incidents, through the simulation of realistic attacks, failures or faults. Particular attention should be paid to the creation of the simulated scenarios, which should be based on real new information security threats. Tests should involve not only the ISIRT, but all the internal and external organizations that are involved in the management of information security incidents. Organizations should ensure that any changes made as a result of post testing reviews are subject to thorough checking, including further testing, before the changed scheme goes live.

6 Detection and reporting phase

6.1 Overview of key activities

The first phase of the operational use of an information security incident management scheme involves the detecting of, collecting information associated with, and reporting on occurrences of information security events and existence of information security vulnerabilities by human or automatic means. Information security incident management in operation comprises three main phases: Detection and reporting, Assessment and decision (see Clause 7) and Responses (see Clause 8) phases. These are followed by the Lessons learnt (see Clause 9) phase where improvements are identified and made. These phases and their associated activities were introduced in Clause 4.5.

The following clauses predominantly address the handling of information security events and incidents. The organization should ensure that the appropriate personnel deal with reported information security vulnerabilities in a similar manner to how non-information security faults are handled, possibly with assessment and resolution using technical personnel (who may or may not be members of the ISIRT). Information on vulnerabilities and their resolutions should be entered into the information security event/incident/vulnerability database managed by the ISIRT. Annex D shows an example template for the information security vulnerability reporting form .

Figure 3 shows all of the operational phases and related activities.

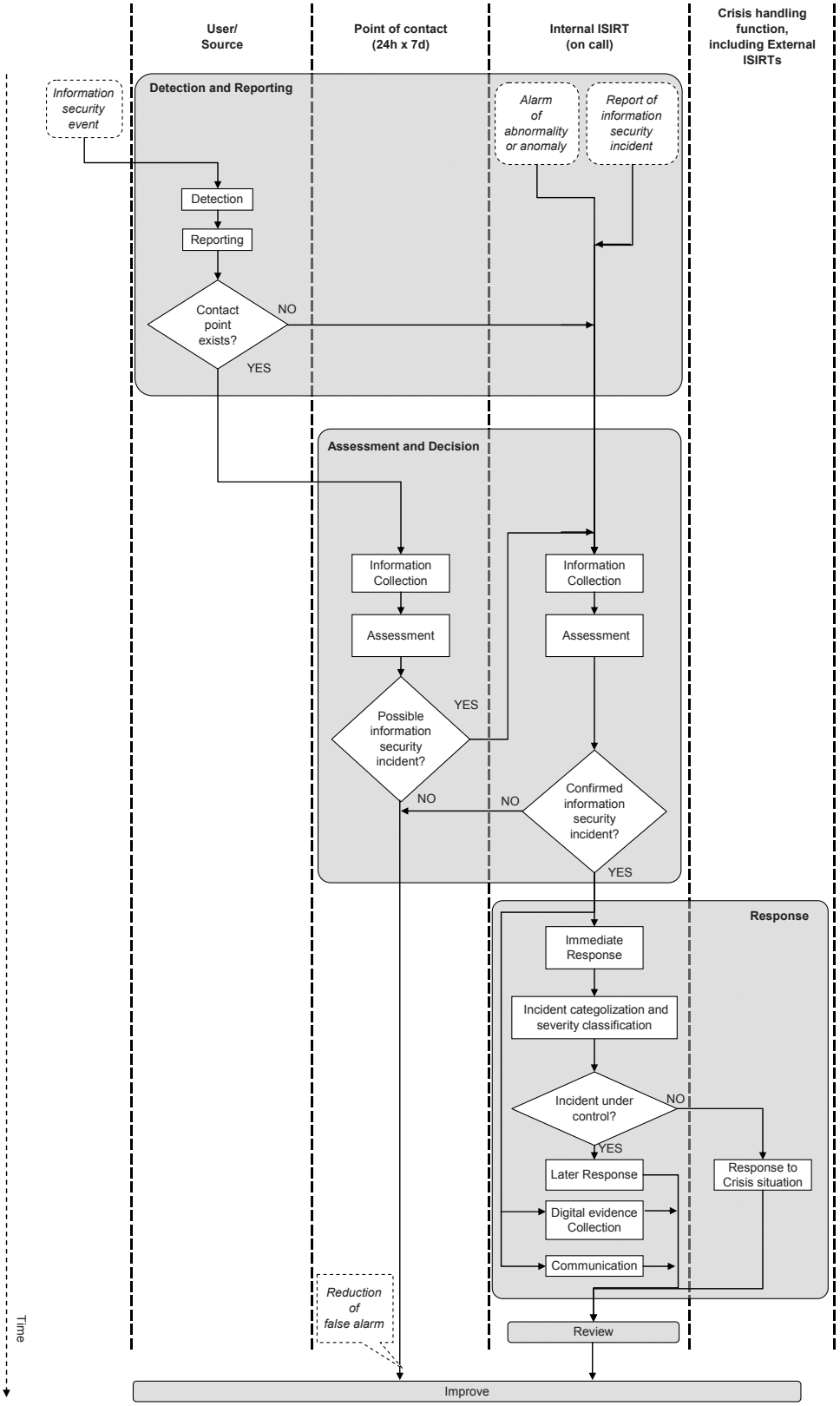

Figure 3 — Information security event and incident flow diagram

NOTE False alarm is an indication of an unwanted event, but is found not to be real or of any consequence.

The first phase of operational use of an information security incident management scheme involves the detecting of, collecting information associated with, and reporting on, occurrences of information security events, by human or automatic means. The organization should ensure that this phase involves detection of information security vulnerabilities that have not yet been exploited to cause information security events, and possibly information security incidents, and reporting on them.

For the Detection and reporting phase, an organization should ensure that the key activities are the following:

a) Activity to detect and report the occurrence of an information security event or the existence of an information security vulnerability, whether by one of the organization's personnel/customers or automatically, aided by the following:

   1) alerts from security monitoring systems such as IDS/IDP, antivirus program, honeypots (generic term for a decoy system used to deceive, distract, divert and to encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user [ISO/IEC 18043:2006]) / tarpits (systems that are intentionally exposed and designed to delay attacks), log monitoring systems, security information management systems, correlation engines and others,

   2) alerts from network monitoring systems such as firewalls, network flow analysis, web filtering and others,

   3) analysis of log information from devices, services, hosts, and various systems,

   4) escalations of anomalous events detected by ICT,

   5) escalations of anomalous events detected by help desks,

   6) user reports, and

   7) external notifications coming from third parties such as other ISIRTs, information security services, ISPs, telecommunication service providers, outsourcing companies or national ISIRTs.

b) Activity to collect information on an information security event or vulnerability.

c) Activity to ensure that all involved in the PoC properly log all activities, results and related decisions for later analysis.

d) Activity to ensure that electronic evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case it is required for legal prosecution or internal disciplinary action.

   NOTE A future International Standard (ISO/IEC 27037) will provide more detailed information on the identification, collection, acquisition and preservation of digital evidence.

e) Activity to ensure that the change control regime is maintained covering information security event and vulnerability tracking and event and vulnerability report updates, and thus that the information security event/incident/vulnerability database is kept up-to-date.

f) Activity to escalate, on an as required basis throughout the phase, for further review and/or decisions.

g) Activity to register in an Incident Tracking System.

All information collected pertaining to an information security event or vulnerability should be stored in the information security event/incident/vulnerability database managed by the ISIRT. The information reported during each activity should be as complete as possible at the time, to ensure that there is a good base available for the assessments and decisions to be made, and of course the actions taken.

6.2 Event detection

Information security events could be detected directly by a person or persons noticing something that gives cause for concern, whether technical, physical or procedural related. Detection could be, for example, from fire/smoke detectors or intruder (burglar) alarms, with the alerts notifying at pre-designated locations for human action. Technical information security events could be detected by automatic means, for example, alerts made by audit trail analysis facilities, firewalls, intrusion detection systems, and anti-malicious code (including viruses) tools, in each case stimulated by pre-set parameters.

Possible information security event detection sources include the following:

a) users,

b) line managers and security managers,

c) customers,

d) IT department, including Network Operations Center and Security Operations Center (through 2nd level support),

e) IT help desk (through 1st level support),

f) managed service providers (including ISPs, telecommunication service providers, and suppliers),

g) ISIRTs,

h) other units and staff that may detect anomalies during their daily work,

i) mass media (news paper, television, etc.), and

j) websites (public security information websites, websites by security researchers, defacement archive websites, etc.);

6.3 Event reporting

Whatever the source of the detection of an information security event, the person notified by automatic means, or directly noticing something unusual, is responsible for initiating the detection and reporting process. This could be any member of an organization's personnel, whether permanent or contracted personnel.

The person should follow the procedures and use the information security event reporting form specified by the information security incident management scheme, to bring the information security event to the attention of the PoC and management. Accordingly, it is essential that all personnel are well aware of, and have access to, the guidelines for reporting the different types of possible information security events. This includes the format of the information security event reporting form and details of the personnel who should be notified on each occasion (all personnel should at least be aware of the format of the information security incident reporting form, to aid their understanding of the scheme.) It should be noted that fixed telephone, cordless phone and mobile telephone without safeguard for tapping are considered not safe. When dealing with highly confidential or secret information, the additional safeguards should be taken.

The following information can be used as the basis for an incident tracking system form:

- time/date for detection,
- observations, and
- contact information (optional).

The completed form (either paper-based or in an e-mail or web form submission) should be used by ISIRT personnel only when registering information security incidents in the Incident Tracking System. It is more crucial to obtain knowledge/reports of a suspected/experienced/detected information security event than being complete with all information.

Information security event (possibly incident) tracking should be supported, whenever possible, by an automated application. The use of an information system is essential to force personnel to follow established procedures and checklists. It is also extremely helpful to keep track of "who did what and when", details that could be missed by mistake during an information security event (possibly incident).

How an information security event is handled is dependent upon what it is, and the implications and repercussions that may flow from it. For many people, this will be a decision beyond their competence. Thus, the person reporting an information security event should complete the information security event reporting form with as much narrative and other information as is readily available at the time, liaising with his/her local manager if necessary. That form should be securely communicated to the designated PoC, with a copy to the responsible ISIRT. The PoC should preferably provide a 24-hour service for 7 days per week. Annex D shows an example template for the information security event reporting form.

The ISIRT should appoint one team member or delegate per shift to be responsible for all incoming reports via e-mail, phone, fax, forms and direct conversation. This responsibility may rotate between team members on a weekly basis. The appointed team member makes the assessment and takes proper actions to inform responsible and involved parties as well as resolve the information security incident.

It is emphasized that not only accuracy but also timeliness is important in the content filled in the information security event reporting form. It is not good practice to delay the submission of a reporting form in order to improve the accuracy of its content. If the reporting person is not confident of the data in any field on the reporting form, it should be submitted with appropriate notation, and revisions communicated later. It should also be recognized that some reporting mechanisms (e.g. e-mail) are themselves visible targets for attack.

When problems exist, or are considered to exist, with the electronic reporting mechanisms (e.g. e-mail), alternative means of communication should be used. This includes when it is thought possible that the system is under attack and unauthorized people could read reporting electronic forms. Alternative means could include in person, by telephone or text messaging. Such alternative means should be used particularly when it becomes evident early in an investigation that an information security event appears likely to be classified as an information security incident, particularly one that may be significant.

Whilst in many cases an information security event has to be reported onwards for action by the PoC, there may be occasions where an information security event is handled locally, possibly with the help of local management. It is advisable that local management be trained to make the same assessment as the ISIRT and take similar/same countermeasures as well as use the same incident tracking system, in order to successfully use locally resources. This will prevent the ISIRT from doing duplicate work .

An information security event may be quickly determined as a false alarm, or it may be resolved to a satisfactory conclusion. In such cases a reporting form should be completed and forwarded to local management, to the PoC and to the ISIRT for recording purposes, i.e. into the information security event/incident/vulnerability database. In such circumstance, the person reporting closure of an information security event may be able to complete some of the information required for the information security incident reporting form – if this is the case then the information security incident reporting form should also be completed and forwarded. The use of automatic tools can assist with completion of some fields for example time stamps. It can also assist with the sharing\transfer of necessary information.

7 Assessment and decision phase

7.1 Overview of key activities

The second phase of operational use of an information security incident management scheme involves the assessment of information associated with occurrences of information security events and decision on if it is information security incident.

For the Assessment and decision phase, an organization should ensure that the key activities are the following:

a) Activity for the PoC to conduct the assessment to determine whether the event is a possible or concluded information security incident or a false alarm, and if it is not a false alarm, whether escalation is required. Assessments should include the use of the agreed information security event/incident classification scale (including determining the impacts of events based on the affected assets/services) and should decide whether events should be classified as information security incidents (see Annex C for example guidelines). Whilst determining the impacts of information security events (and thus possible incidents) in terms of the effects of breaches of confidentiality, integrity and availability, organizations should ensure that the following are identified:

   1) impact domain (physical or logical),

   2) assets, infrastructures, information, processes, services and applications that are affected, or are going to be affected, and

   3) possible effects on organization core services.

b) Activity for the ISIRT to conduct the assessment to confirm the results of the PoC's assessment whether the event is an information security incident or not, if applicable. As necessary, another assessment should be conducted using the agreed information security event/incident classification scale, with details of the event (possibly incident) type and affected resource (categorization) (see Annex C for example guidelines). This should be followed by decisions on how the confirmed information security incident should be dealt with, by whom and in what priority. It should involve the predetermined prioritizing process to enable a clear focus on assigning each information security incident to suitable persons and determining the urgency of the handling and the responses to information security incident, including whether an immediate response, information security forensics analysis and communications activities are required, in the next phase (Responses – see also Clause 8).

c) Activity to escalate, on an as required basis throughout the phase, for further assessments and/or decisions.

d) Activity to ensure that all involved, particularly the ISIRT, properly log all activities for later analysis.

e) Activity to ensure that electronic evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case it is required for legal prosecution or internal disciplinary action.

f) Activity to ensure that the change control regime is maintained covering information security incident tracking and incident report updates, and thus that the information security event/incident/vulnerability database is kept up-to-date.

All information collected pertaining to an information security event, incident or vulnerability should be stored in the information security event/incident/vulnerability database managed by the ISIRT. The information reported during each activity should be as complete as possible at the time, to ensure that there is a good base available for the assessments and decisions to be made, and of course the actions taken.

Once an information security event has been detected and reported, the subsequent activities are the following.

g) Activity to distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel, with assessment, decision making and actions involving both security and non-security personnel.

h) Activity to provide formal procedures for each notified person to follow, including reviewing and amending the report made, assessing the damage, and notifying the relevant personnel (with the individual actions depending on the type and severity of the incident).

i) Activity to use guidelines for thorough documentation of an information security event.

j) Activity to use guidelines for thorough documentation of the subsequent actions for an information security incident if the information security event becomes classified as an information security incident.

k) Activity to update the information security event/incident/vulnerability database.

The organization should ensure that this phase involves the assessment of the information gathered on reported information security vulnerabilities (that have not yet been exploited to cause information security events, and possibly information security incidents), with decisions made on which need to be dealt with, by whom, how and in what priority.

7.2 Assessment and initial decision by the PoC

The receiving person in the PoC should acknowledge receipt of the completed information security event reporting form, enter it into the information security event/incident/vulnerability database, and review it. He/she should seek any clarification from the person reporting the information security event, and collect any further information required and known to be available, whether from the reporting person or elsewhere. Then, the PoC should conduct an assessment to determine whether the information security event should be classified as an information security incident or is in fact a false alarm (including through use of the organization's agreed incident classification scale). If the information security event is determined to be a false alarm, the information security event reporting form should be completed and communicated to the ISIRT for addition to the information security event/incident/vulnerability database and review, and copied to the reporting person and his/her local manager.

Information and other evidence collected at this stage may need to be used at a future time for disciplinary or legal proceedings. The person or people undertaking the information collection and assessment tasks should be trained in the requirements for collection and preservation of evidence.

In addition to recording the date(s) and time(s) of actions, it is necessary to fully document the following:

a) what was seen and done (including tools used) and why,

b) the location of the potential evidence,

c) how evidence is archived (if applicable),

d) how evidence verification was performed (if applicable), and

e) details of storage/safe custody of material and subsequent access to it.

If the information security event is determined as a likely information security incident, and if the person at PoC has the appropriate level of competence, further assessment may be conducted. This may require remedial actions, for example identifying additional emergency controls being and referral for action to the appropriate person. It may be evident that an information security event is determined to be a significant information security incident (using the organization's pre-determined severity scale), in which case the ISIRT manager should be informed directly. It may be evident that a crisis situation should be declared, and for example, the crisis management manager be notified for possible activation of a crisis management plan, and the ISIRT manager and senior management be informed. However, the most likely situation is that the information security incident needs to be referred directly to the ISIRT for further assessment and action.

Whatever the next step is determined to be, the PoC should complete as much as possible of the information security incident reporting form. The information security incident reporting form should contain narrative, and as far as possible should confirm and describe the following:

a) what the information security incident is,

b) how it was caused and by what or whom,

c) what it affects or could affect,

d) the impact or potential impact of the information security incident on the business of the organization,

e) an indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined classification scale), and

f) how it has been dealt with so far.

When considering the potential or actual adverse effects of an information security incident on the business of an organization, the following are some examples:

a) unauthorized disclosure of information,

b) unauthorized modification of information,

c) repudiation of information,

d) unavailability of information and/or service,

e) destruction of information and/or service, and

f) reduced performance of service.

The first step is to consider which of a number of consequences is relevant. For those considered relevant, the related category guideline should be used to establish the potential or actual impacts for entry into the information security incident report. Example guidelines are given in Annex C. Example categories are the following:

a) financial loss/disruption to business operations,

b) commercial and economic interests,

c) personal information,

d) legal and regulatory obligations,

e) management and business operations,

f) loss of goodwill,

g) injury or loss of life, and

h) societal disruption.

If an information security incident has been resolved, the report should include details of the controls that have been taken and any lessons learned (e.g. controls to be adopted to prevent re-occurrence or similar occurrences). Once completed as far as possible, the reporting form should then be referred to the ISIRT for entry into the information security event/incident/vulnerability database and review.

If an investigation is likely to be longer than a time period defined in the information security incident management policy, an interim report should be produced within a time period specified by the policy.

It is emphasized that the PoC assessing an information security incident should be aware, based on the guidance provided in the information security incident management scheme documentation. It includes the following for example:

a) when it is necessary to escalate matters and to whom, and

b) change control procedures should be followed in all activities conducted by the PoC.

In a similar manner to that mentioned in Clause 6.2 and Clause 6.3 above regarding event detection and reporting, alternative means of communication of updated reporting forms should be used when problems exist, or are considered to exist, with electronic reporting mechanisms (e.g. e-mail).

7.3 Assessment and incident confirmation by the ISIRT

The assessment, and confirmation of the decision as to whether an information security event is to be classified as an information security incident, should be the responsibility of the ISIRT. The receiving person in the ISIRT should do the following:

a) Acknowledge receipt of the information security incident reporting form, completed as far as possible by the PoC.

b) Enter the form into the information security event/incident/vulnerability database if it was not done by the PoC and update the database if necessary.

c) Seek clarification from the PoC, if necessary.

d) Review the reporting form content.

e) Collect any further information required and known to be available, whether from the PoC, the person who completed the information security event reporting form or elsewhere.

If there is still a degree of uncertainty as to the authenticity of the information security incident or the completeness of the reported information, the ISIRT member should conduct an assessment to determine whether the information security incident is real or in fact a false alarm (through use of the organization's agreed incident classification scale). If the information security incident is determined to be a false alarm, the information security event report should be completed, added to the information security event/incident/vulnerability database and communicated to the ISIRT manager. Copies of the report should be sent to the PoC, and the reporting person and his/her local manager.

An information security incident should be correlated to any other event/incident reported to the ISIRT. This important activity is to verify if the incident is connected to any other event/incident or it is simply the effect of another incident, i.e. in Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The correlation of incidents is also important in prioritizing the efforts of the ISIRT.

If the information security incident is determined to be real, the ISIRT member and colleagues as required, should conduct further assessment. The aim is to confirm the following as soon as possible:

a) What the information security incident is, how it was caused and by what or whom, what it affects or could affect, the impact or potential impact of the information security incident on the business of the organization, an indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale). If the incident causes severe negative impact on the business, crisis activities should be initiated. (see Clause 8.2.4).

b) The following aspects for deliberate human technical attack on an information system, service and/or network, for example:

    1) how deeply the system, service and/or network has been infiltrated, and what level of control the attacker has,

    2) what data has been accessed by the attacker, possibly copied, altered or destroyed,

    3) what software has been copied, altered or destroyed by the attacker,

c) the direct and indirect effects (for example, is physical access open because of a fire, is an information system vulnerable because of some software or communications line malfunction, or because of human error), and

d) how the information security incident has been dealt with so far and by whom.

When reviewing the potential or actual adverse effects of an information security incident on the business of an organization, from some information and/or services shown in Clause 7.2, it is necessary to confirm which of a number of consequences is relevant. Example categories are shown in Clause 7.2 and Annex C.

A prioritizing process should be used to assign an information security incident to the most suitable person or group of persons in the ISIRT to facilitate an adequate response to the information security incident. In particular, when several information security incidents are being dealt with the same time, priorities have to be set to order the responses to be given to information security incidents.

Priorities should be set in accordance with the determined adverse business impacts associated with the information security incident and the estimated effort needed to respond to the information security incident. For incidents with the same priority, the required effort is one metric to determine the order in which they need to be responded. For example, an incident that is easily resolved may be dealt with before an incident requiring a greater effort.

For those considered relevant, the related category guideline should be used to establish the potential or actual impacts for entry into the information security incident report. Example guidelines are given in Annexes C and D.

8 Responses phase

8.1 Overview of key activities

The third phase of operational use of an information security incident management scheme involves the making of responses to information security incidents in accordance with the actions agreed in the assessment and decision phase. Dependent on the decisions the responses could be made immediately, in real-time or in near real-time, and some could well involve information security forensics analysis.

For the Responses phase, an organization should ensure that the key activities are the following:

a) Activity to review by the ISIRT to determine if the information security incident is under control, and activity below:

   1) Activity to instigate the required response, if it is under control. This could be an immediate response , which could include the activation of recovery procedures, and/or issuing communications to relevant involved personnel, or a later slower time response (for example, in facilitating full recovery from a disaster), whilst ensuring all information is ready for post-incident review activities.

   2) Activity to instigate crisis activities through escalation to crisis handling function, if it is not under control or it is going to have a severe impact on the organization's core services (See also Clause 8.2.4). Crisis handling function then is responsible of the incident, with full support of the ISIRT (including such as activating a crisis management plan), and involving the related personnel, for example the organization's crisis management manager and team (for guidance on business continuity management see ISO/IEC 27031 and ISO/PAS 22399:2007).

b) Activity to assign internal resources and identify external resources in order to respond to an incident.

c) Activity to conduct information security forensics analysis, as required and relative to the information security incident classification scale rating, and changing that scale rating as necessary.

d) Activity to escalate, on an as required basis throughout the phase, for further assessments and/or decisions.

e) Activity to ensure that all involved, particularly the ISIRT, properly log all activities for later analysis.

f) Activity to ensure that electronic evidence is gathered and stored provably securely, and that its secure preservation is continually monitored, in case it is required for legal prosecution or internal disciplinary action.

g) Activity to ensure that the change control regime is maintained covering information security incident tracking and incident report updates, and thus that the information security event/incident/vulnerability database is kept up-to-date.

h) Activity to communicate the existence of the information security incident or any relevant details thereof to other internal and external people or organizations, in particular asset/information/service owners (determined during the impact analysis) and internal/external organizations that should be involved in the management and resolution of the incident.

All information collected pertaining to an information security event, incident or vulnerability should be stored in the information security event/incident/vulnerability database managed by the ISIRT, including for the purposes of further analysis. The information reported during each activity should be as complete as possible at the time, to ensure that there is a good base available for the assessments and decisions to be made, and of course the actions taken.

Once an information security incident has been determined and the responses agreed, the subsequent activities are the following:

a) Activity to distribute the responsibility for incident management activities through an appropriate hierarchy of personnel, with decision making and actions involving both security and non-security personnel as necessary.

b) Activity to provide formal procedures for each involved person to follow, including reviewing and amending reports made, re-assess the damage, and notify the relevant personnel (with the individual actions depending on the type and severity of the incident).

c) Activity to use guidelines for thorough documentation of an information security incident, of the subsequent actions, and updating of the information security event/incident/vulnerability database.

d) Activity to use guidelines for thorough documentation of the subsequent actions.

e) Activity to update the information security event/incident/vulnerability database.

Once any information security incident has been dealt with successfully, it should be formally closed and this recorded in the information security incident management database. The organization should ensure that this phase also involves the making of responses to reported information security vulnerabilities in accordance with the actions agreed in the assessment and decision phase. Once any vulnerability has been dealt with details should be recorded in the information security incident management database.

Guidance on responses to information security incidents is provided in Clause 8.2.

8.2 Responses

8.2.1 Immediate responses

8.2.1.1 Overview

In the majority of cases, the next activities for the ISIRT member are to identify the immediate response actions to deal with the information security incident, record details on the information security incident form and within the information security event/incident/vulnerability database, and notify the required actions to the appropriate persons or groups. This may result in emergency controls (for example, cutting off/shutting down an affected information system, service and/or network, with the prior agreement of the relevant IT and/or business management), and/or additional permanent controls being identified, and notified for action to the

appropriate person or group. If not already done so, the significance of the information security incident should be determined, using the organization's pre-determined classification scale, and if sufficiently significant appropriate senior management should be notified directly. If it is evident that a crisis situation should be declared, for example the crisis management manager should be notified for possible activation of a crisis management plan, with the ISIRT manager and senior management also informed.

The overall objectives in responding to information security incidents are the following:

a) to confine the potential adverse impacts (of information security incidents), and

b) to improve information security.

The primary goal of the information security incident management scheme and associated activities should be the minimization of adverse business impacts, whereas identification of the attacker should be considered a secondary goal.

8.2.1.2 Example actions

As an example of relevant immediate response actions in the case of deliberate attack on an information system, service and/or network, it could be left connected to the internet, or other network. This will allow business critical applications to function correctly, and collect as much information as possible about the attacker, provided that the attacker does not know that he/she is under surveillance.

It is vitally important to follow planned processes and record action. Beware of Trojans, rootkits and kernel modules that may cause serious damage to the system. Evidence can be protected with cryptography, locks and records of access.

a) While undertaking such a decision, it needs to be considered that the attacker may realize that he/she is being observed and may undertake actions that cause further damage to the affected information system, service and/or network, and related data, and the attacker could destroy the information that may be useful to track him/her.

b) It is essential that it is technically possible to quickly and reliably cut-off and/or shut down the attacked information system, service and/or network, once a decision had been taken. This serves to contain the incident.

A further consideration is that the prevention of re-occurrence is usually of high priority, and it might well be concluded that the attacker has exposed a vulnerability that should be rectified, and the gains from tracking him/her do not justify the effort in doing so. This is especially relevant when the attacker is non-malicious and has caused little or no damage.

With regard to information security incidents that are caused by something other than deliberate attack, the source should be identified. It may be necessary to shut the information system, service and/or network down, or isolate the relevant part and shut it down (with the prior agreement of the relevant IT and/or business management), while controls are implemented. This may take longer if the vulnerability is fundamental to the information system, service and/or network design, or if it is a critical vulnerability.

Another response activity may be to activate surveillance techniques (for example, honeypots – see ISO/IEC 18043). This should be on the basis of procedures documented for the information security incident management scheme.

Information that may be corrupted by the information security incident should be checked by the ISIRT member against backup records for modifications, deletions, or insertions of information. It may be necessary to check the integrity of the logs, as a deliberate attacker may have manipulated these logs to cover his/her tracks.

8.2.1.3 Incident information update

Whatever the next step is determined to be, the ISIRT member should update the information security incident report as much as possible, add it to the information security event/incident/vulnerability database, and notify the ISIRT manager and others as necessary. The update may cover further information on the following:

a) what the information security incident is,

b) how it was caused and by what or whom,

c) what it affects or could affect,

d) the impact or potential impact of the information security incident on the business of the organization,

e) changes to the indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale), and

f) how it has been dealt with so far.

If an information security incident has been resolved, the report should include details of the controls that have been taken and any other lessons learned (e.g. further controls to be adopted to prevent re-occurrence or similar occurrences). The updated report should be added to the information security event/incident/vulnerability database, and notified to the ISIRT manager and others as required.

It is emphasized that the ISIRT is responsible for ensuring the secure retention of all information pertaining to an information security incident for further analysis, and potential legal evidential use. For example, for an IT oriented information security incident, the following actions should be taken.

After the initial discovery of the incident, all volatile data should be collected before the affected IT system, service and/or network is shut down, for a complete information security forensics investigation. Information to be collected includes contents of memory, cache and registers, and detail of any activities running, and the following.

a) A full information security forensics duplication of the affected system or a low level backup of logs and important files should be undertaken depending on the nature of the information security incident.

b) Logs from neighbouring systems, services and networks, for example including from routers and firewalls, should be collected and reviewed.

c) All information collected should be stored securely on read only media.

d) Two or more persons should be present when information security forensics duplication is performed, to assert and certify that all activities have been carried out in accordance with relevant legislation and regulation.

e) Specifications and descriptions of the tools and commands used to perform the information security forensics duplication should be documented and stored together with the original media.

An ISIRT member is also responsible for facilitating the return of the affected facility (whether IT or otherwise) to a secure operational state that is not susceptible to a compromise by the same attack, if possible at this stage.

8.2.1.4 Further activities

If an ISIRT member determines that an information security incident is real, then other important activities should be the following:

a) activity to institute information security forensics analysis, and

b) activity to inform those responsible for internal and external communications of the facts and proposals for what should be communicated, in what form and to whom.

Once an information security incident report has been completed as far as possible, it should be entered into the information security event/incident/vulnerability database and communicated to the ISIRT manager.

If an investigation is likely to be longer than a time period pre-agreed within the organization, an interim report should be produced.

The ISIRT member assessing an information security incident should be aware, based on the guidance provided in the information security incident management scheme documentation including the following:

a) when it is necessary to escalate matters and to whom, and

b) change control procedures should be followed in all activities conducted by the ISIRT.

When problems exist or are considered to exist, with electronic communications facilities (e.g. e-mail or web), including when it is thought possible that the system is under attack, the report to the relevant people should be done by telephone or text messaging.

If it is concluded that an information security incident is significant or a crisis situation has been determined, then the ISIRT manager, in liaison with the organization's information security manager and the relevant board member/senior manager, should liaise with all related parties, both internal and external to the organization.

To ensure that the liaisons are organized quickly and are effective, it is necessary to establish a secure method of communication in advance that does not wholly rely on the system, service and/or network that may be affected by the information security incident. These arrangements may include the nomination of backup advisors or representatives in the case of absence.

8.2.2 Assessment of control over information security incidents

After the ISIRT member has instigated the immediate responses and relevant information security forensics analysis and communications activities, it needs to be quickly ascertained whether the information security incident is under control. If necessary, the ISIRT member may consult with colleagues, the ISIRT manager and/or other persons or groups.

If the information security incident is confirmed as being under control, the ISIRT member should institute any required later responses, and information security forensic analysis and communications, to end the information security incident and restore the affected information system to normal operations.

If the information security incident is confirmed as not being under control, then the ISIRT member should institute crisis activities.

If the information security incident is related to loss of availability, the metric to assess whether an information security incident is under control could be the time elapsed before recovering to a normal situation further to the occurrence of an information security incident. The organization should determine for each asset, based upon the results of the information security risk assessment, its acceptable interruption window that supports the recovery time objective before resumption of the service or the access of the information. As soon as the response exceeds the acceptable interruption window of the targeted asset, the information security incident may not be under control anymore and the decision to escalate the information security incident should be taken.

Information security incidents related to loss of confidentiality, integrity etc. needs other types of judgements to determine if the situation is under control and possible related metrics according to organization crisis management plans.

8.2.3 Later responses

Having determined that an information security incident is under control, and not subject to crisis activities, the ISIRT member should identify if and what further responses are required to deal with the information security incident. This could include restoring the affected information system(s), service(s) and/or network(s) back to normal operation. He/she should then record details on the information security incident reporting form and in the information security event/incident/vulnerability database, and notify those responsible for completing the related actions. Once those actions have been successfully completed, details should be recorded on the information security incident reporting form and in the information security event/incident/vulnerability database, and then the information security incident should be closed and appropriate personnel notified.

Some responses are directed at preventing information security incident re-occurrence or similar occurrence. For example, if it is determined that the cause of an information security incident is an IT hardware or software fault without an available patch, the supplier should be contacted immediately. If a known IT vulnerability was involved in an information security incident, it should be patched with the relevant information security update. Any IT configuration related problems highlighted by the information security incident should be dealt with thereafter. Other measures to decrease the possibility of re-occurrence or similar occurrence of an IT information security incident may include changing system passwords and disabling unused services.

Another area of response activity may involve monitoring the IT system, service and/or network. Following the assessment of an information security incident, it may be appropriate to have additional monitoring controls in place to assist in detecting unusual and suspicious events that would be symptomatic of further information security incidents. Such monitoring may also reveal a greater depth to the information security incident, and identify other IT systems that were compromised.

It may well be necessary for activation of specific responses documented in the relevant crisis management plan. This could apply for both IT and non-IT related information security incidents. Such responses should include those for all business aspects, not just directly IT related but also key business function maintenance and later restoration – including, as relevant, of voice telecommunications, and personnel levels and physical facilities.

The last area of activity is the restoration of the affected information system(s), service(s) and/or network(s) to normal operation. The restoration of an affected system(s), service(s) and/or network(s) to a secure operational state may be achieved through the application of patches for known vulnerabilities or by disabling an element that was the subject of the compromise. If the entire extent of the information security incident is unknown, due to the destruction of the logs during the incident, then a complete system, service and/or network rebuild may be necessary. It may well be necessary for activation of parts of the relevant crisis management plan.

If an information security incident is non-IT related, for example caused by a fire, flood or bomb, then the recovery activities to be followed are those documented in the relevant crisis management plan.

8.2.4 Responses to crisis situations

As discussed in Clause 8.2.2, it may be that the ISIRT determines an information security incident is not under control and needs to be escalated to crisis situation, using a pre-designated plan.

The best options for dealing with all possible types of information security incidents that might affect availability and to some extent integrity of an information system, should have been identified in the organization's crisis management plan. These options should be directly related to the organization's business priorities and related timescales for recovery, and thus the maximum acceptable outage time periods for IT, voice, people and accommodation. The strategy should have identified the following:

a) the required preventive, resilience and crisis management measures,

b) the required organizational structure and responsibilities for responding to crisis, and

c) the required structure and outline content for the crisis management plan or plans.

The crisis management plan(s) and the controls put in place to support the activation of those plan(s), once tested satisfactorily, form the basis for dealing with most escalated incidents once so designated.

Depending on the type of incident and if it is not under control, the escalation may lead to serious activities to deal with the incident and activate the crisis management plan if such is in place. Such activities may include, but are not limited to, the activation of:

a) fire suppression facilities and evacuation procedures,

b) flood prevention facilities and evacuation procedures,

c) bomb handling and related evacuation procedures,

d) specialist information system fraud investigators, and

e) specialist technical attack investigators.

8.2.5 Information security forensics analysis

Where identified by prior assessment as required for evidential purposes, de facto in the context of a significant information security incident, information security forensic analysis should be conducted by the ISIRT. It should involve the use of IT based investigative techniques and tools, supported by documented procedures, to review the designated information security incident(s) in more detail than has been the case hitherto in the information security incident management process. It should be conducted in a structured manner, and, as relevant, identify what may be used as evidence, whether for internal disciplinary procedures or legal actions.

The facilities needed for information security forensic analysis is likely to be categorized into technical (e.g. audit tools, evidence recovery facilities), procedural, personnel and secure office facilities. Each information security forensic analysis activity should be fully documented, including relevant photographs, audit log analysis reports, and data recovery logs. The proficiency of the person or people performing the information security forensic analysis should be documented along with records of proficiency testing. Any other information that demonstrates the objectivity and logical nature of analysis should also be documented. All records of the information security incidents themselves, the information security forensic analysis activities, etc. and associated media, should be stored in a physically secure environment and controlled by procedures to prevent unauthorized people from accessing, altering or rendering it unavailable. Information security forensic analysis IT based tools should comply with standards such that their accuracy cannot be legally challenged, and should be kept up-to-date in line with technology changes. The ISIRT physical environment should provide demonstrable conditions that ensure the evidence is handled in such a way that it cannot be challenged. Enough personnel should be available, if necessary on an on-call basis, to be able to respond at any time.

Over time, new requirements may arise to review evidence of a variety of information security incidents, including fraud, theft, and vandalism. Thus, to assist the ISIRT there needs to be a number of IT based means and supporting procedures available for uncovering information hidden in an information system, service or network, including information that on an initial inspection appears to have been deleted, encrypted, or damaged. These means should address all known aspects associated with known types of information security incidents and be documented in the ISIRT procedures.

In today's environment, information security forensic analysis is frequently needed to encompass complex networked environments, where investigation needs to encompass an entire operating environment, including a multitude of servers (e.g. file, print, communications and e-mail), as well as remote access facilities. There are many tools available, including text search tools, drive imaging software and information security forensic suites. The main focus of information security forensic analysis procedures is to ensure that evidence is kept intact and checked to ensure that it stands up to any legal challenge.

It is emphasized that information security forensic analysis should be performed on an exact copy of the original data, to prevent the analysis work prejudicing the original media integrity. The overall information security forensic analysis process should encompass, as relevant, the following activities:

a) Activity to ensure that the target system, service and/or network is protected during the information security forensic analysis from being rendered unavailable, altered or otherwise compromised, including by malicious code (including viruses) introduction, and that there are no or minimal effects on normal operations.

b) Activity to prioritize the acquisition and collection of evidence i.e. proceeding from the most volatile to the least volatile (this depends in large measure on the nature of the information security incident).

c) Activity to identify all relevant files on the subject system, service and/or network, including normal files, password or otherwise protected files, and encrypted files.

d) Activity to recover as much as possible discovered deleted files, and other data.

e) Activity to uncover IP addresses, host names, network routes and web site information

f) Activity to extract the contents of hidden, temporary and swap files used by both application and operating system software.

g) Activity to access the contents of protected or encrypted files (unless prevented by law).

h) Activity to analyze all possibly relevant data found in special (and typically inaccessible) disc storage areas.

i) Activity to analyze file access, modification and creation times.

j) Activity to analyze system/service/network and application logs.

k) Activity to determine the activity of users and/or applications on a system/service/network.

l) Activity to analyze e-mails for source information and content.

m) Activity to perform file integrity checks to detect Trojan horse files and files not originally on the system.

n) Activity to analyze, if applicable, physical evidence, for example fingerprints, property damage, video surveillance, alarm system logs, pass card access logs, and interview witnesses.

o) Activity to ensure that extracted potential evidence is handled and stored in such a way that it cannot be damaged or rendered unusable, and that sensitive material cannot be seen by those not authorized. It is emphasized that evidence gathering should always be in accordance with the rules of the court or hearing in which the evidence may be presented.

p) Activity to conclude on the reasons for the information security incident, the actions required and in what timeframe, with evidence including lists of relevant files included in an attachment to the main report.

q) Activity to provide expert support to any disciplinary or legal action as required.

The method(s) to be followed should be documented in the ISIRT procedures.

The ISIRT should accommodate sufficient combinations of skills to provide wide coverage of technical knowledge (including of the tools and techniques likely to be used by deliberate attackers), analysis/investigative experience (including regarding the preservation of usable evidence), knowledge of relevant legislation and regulation implications, and ongoing knowledge of incident trends.

The following should be recognized:

a) some organizations may not have all these resources available and that it may need to out-source information security forensic analysis work to specialists,

b) collecting information security forensic material may only be a resort (i.e. the effort and expense justified) where serious loss has occurred and/or criminal proceedings are likely, and

c) not using specialist resources to capture information security forensic material may render the findings as being inadmissible if court action is required.

8.2.6 Communications

In many cases when an information security incident has been confirmed by the ISIRT as real, there is a need for certain people to be informed both internally (outside of normal ISIRT/management lines of communication) and externally, including the press. This may need to occur at a number of stages, for example when an information security incident is confirmed as real, when it is confirmed as under control, when it is designated for crisis activities, when it is closed and when post incident review has been completed and conclusions reached.

When communication is needed, due care should be taken to ensure who needs to know what and when. Stakeholders that are affected should be determined and preferably divided into groups such as:

a) direct internal stakeholders (crises management, management staff etc.),

b) direct external stakeholders (owners, customers, partners, suppliers etc.), and

c) other external contacts such as press and/or other media.

Each group may need special information that should come through the appropriate channels of the organization. One of the most important task for communication after an information security incident is to ensure that direct external and direct internal stakeholders will have the information prior to that it comes through other external contacts such as press.

To aid this activity when the need arises, it is sensible practice to prepare certain information in advance such that it is quickly adjusted to the circumstances of a particular information security incident and issued to each relevant group and in particular the press and/or other media. If any information pertaining to information security incidents is to be released to the press it should be done in accordance with organization's information dissemination policy. Information to be released should be reviewed by the relevant parties, which may include senior management, public relations co-ordinators and information security personnel.

NOTE The communications of information security incident may wary depending on the incident and its impact in combination with the organization relations and type of business. The type of business may also set specific rules for how communication should be done, for example if the organization is listed on a public stock market.

8.2.7 Escalation

In extreme circumstances, matters may have to be escalated to accommodate incidents that are out of control and a potential danger for unacceptable business impact. These incidents need to be escalated to activate the business continuity plan if in place by reporting to either senior management, another group within the organization or persons or groups outside of the organization. This may be for a decision to be made on recommended actions to deal with an information security incident or for further assessment to determine what actions are required. This could be following the assessment activities described above in Clauses 7.2 and 7.3, or during those activities if some major issue becomes evident early. Guidance should be available in the information security incident management scheme documentation for those who are likely at some point to need to escalate matters, i.e. PoC and ISIRT members.

8.2.8 Activity logging and change control

It is emphasized that all involved in the reporting and management of an information security incident should properly log all activities for later analysis. This should be included with the information security incident reporting form and in the information security event/incident/vulnerability database, continually kept up-to-date throughout the cycle of an information security incident from first reporting to completion of post-incident review.

This information should be retained provably secure and with an adequate back-up regime. Further, all changes made in the context of tracking an information security incident and updating the information security incident reporting form and the information security event/incident/vulnerability database should be under a formally accepted change control scheme.

9 Lessons learnt phase

9.1 Overview of key activities

The fourth phase of operational use of an information security incident management scheme follows when information security incidents have been resolved/closed, and involves learning the lessons from how incidents (and vulnerabilities) have been handled and dealt with. For the lessons learnt phase, an organization should ensure that the key activities are the following:

a) Activity to conduct further information security forensics analysis, as required.

b) Activity to identify the lessons learnt from information security incidents and vulnerabilities.

c) Activity to review, identify and make improvements to information security control implementation (new and/or updated controls), as well as information security incident management policy, as result of the lessons learnt, whether from one information security incident or many (or indeed from reported security vulnerabilities). This is aided by the metrics fed into the organization's strategy on where to invest in information security controls.

d) Activity to review, identify and make improvements to the organization's existing information security risk assessment and management review results, as a result of the lessons learnt.

e) Activity to review of how effective the processes, procedures, the reporting formats and/or the organizational structure were in responding to, assessing and recovering from each information security incident and dealing with information security vulnerabilities, and on the basis of the lessons learnt identifying and making improvements to the information security incident management scheme and its documentation.

f) Activity to update the information security event/incident/vulnerability database.

g) Activity to communicate and share the results of review within a trusted community (if the organization so wishes).

It is emphasized that the information security incident management activities are iterative, and thus an organization should make regular improvements to a number of information security elements over time. These improvements should be proposed on the basis of reviews of the data on information security incidents and the responses to them and of reported information security vulnerabilities, as well as trends over time.

9.2 Further information security forensic analysis

It may be that once an incident has been resolved there is still a need for information security forensics analysis to identify evidence. This should be conducted by the ISIRT using the same toolset and procedures as suggested in Clause 8.2.5.

9.3 Identifying the lessons learnt

Once an information security incident has been closed, it is important that the organization should quickly identify and learn from the lessons from the handing of an information security incident and ensure that the conclusions are acted upon. Further, there may be lessons to be learnt from the assessment and resolution of reported information security vulnerabilities. The lessons could be in terms of the following:

a) New or changed requirements for information security controls. These could be technical or non-technical (including physical) controls. Dependent on the lessons learned, these could include the need for rapid material updates for, and delivery of, security awareness briefings (for users as well as other personnel), and rapid revision and issue of security guidelines and/or standards.

b) New or changed threat and vulnerability information and thus changes to the organization's existing information security risk assessment and management review results.

c) Changes to the information security incident management scheme and its processes, procedures, the reporting formats and/or the organizational structure, and the information security event/incident/vulnerability database.

An organization should look beyond a single information security incident or vulnerability and check for trends/patterns which themselves may help identify the need for controls or approach changes. It is also sensible practice following an IT oriented information security incident, to conduct information security testing, particularly vulnerability assessment. Thus, an organization should analyze the data in the information security event/incident/vulnerability database on a regular basis in order to do the following:

a) identify trends/patterns,

b) identify areas of concern, and

c) analyze where preventive action could be taken to reduce the likelihood of future incidents.

Relevant information acquired throughout the course of an information security incident should be channelled into the trend/pattern analysis (similarly to the way reported information security vulnerabilities are handled). It contributes significantly to the early identification of information security incidents and provides a warning of what further information security incidents may arise, based on previous experience and documented knowledge.

Use should also be made of information security incident and related vulnerability information received from government, commercial ISIRTs and suppliers.

Vulnerability assessment/security testing of an information system, service and/or network following an information security incident, should not be confined to only the information system, service and/or network, affected by the information security incident. It should be expanded to include any related information systems, services and/or networks. A complete vulnerability assessment is used to highlight the existence of the vulnerabilities exploited during the information security incident on other information systems, services and/or networks and to ensure that no new vulnerabilities are introduced.

It is important to stress that vulnerability assessments should be conducted on a regular basis, and that the re-assessment of vulnerabilities after an information security incident has occurred should be part of this continuous assessment process, and not as a replacement.

Summary analyses of information security incidents and vulnerabilities should be produced for tabling at each meeting of the organization's management information security forum and/or other forum defined in the overall organizational information security policy.

9.4 Identifying and making improvements to information security control implementation

During review after one or more information security incidents or vulnerabilities, have been resolved, new or changed controls may be identified as being required. The recommendations and related control requirements may be such that it is not financially or operationally feasible to implement them immediately, in which case they should feature in the longer-term aims of the organization. For example, migration to a more secure robust firewall may not be financially feasible in the short term, but needed to be factored into an organization's long-term information security goals.

In accordance with the agreed recommendations, the organization should implement the updated and/or new controls. These could be technical (including physical) controls, and may include the need for rapid material updates for, and delivery of, security awareness briefings (for users as well as other personnel), and rapid revision and issue of security guidelines and/or standards. Further, an organization's information systems, services and/or networks should be subject to regular vulnerability assessments to aid in the identification of vulnerabilities and provide a process of continual system/service/network hardening.

In addition, whilst reviews of information security related procedures and documentation may be conducted in the immediate aftermath of an information security incident or a resolved vulnerability, it is more likely that this is required as a later response. Following an information security incident or a resolved vulnerability, if relevant an organization should update its information security policies and procedures to take into account information gleaned and any problem issues identified during the course of the incident management process. It should be a long-term aim of the ISIRT, in conjunction with the organization's information security manager, to ensure that these information security policy and procedural updates are propagated throughout the organization.

9.5 Identifying and making improvements to information security risk assessment and management review results

Depending on the severity and impact of an information security incident (or the severity and potential impact related to a reported information security vulnerability), an assessment of information security risk assessment and management review results may be necessary to take into account new threats and vulnerabilities. As a follow-on to the completion of an updated information security risk assessment and management review, it may be necessary to introduce changed or new controls (see Clause 9.4).

9.6 Identifying and making improvements to the information security incident management scheme

Post-incident resolution, the ISIRT manager or a nominee should review all that has happened to assess and thus quantify the effectiveness of the entire response to an information security incident. Such an analysis aims to determine which parts of the information security incident management scheme worked successfully and identify if any improvements are required.

An important aspect of post response analysis is to feed information and knowledge back into the information security incident management scheme. If of sufficient severity, an organization should ensure that a meeting of all the relevant parties is scheduled shortly after an incident resolution while information is still fresh in people's minds. Factors to consider in such a meeting include the following:

a) Did the procedures outlined in the information security incident management scheme work as intended?

b) Are there any procedures or methods that would have aided in the detection of the incident?

c) Were any procedures or tools identified that would have been of assistance in the response process?

d) Were there any procedures that would have aided in recovering information systems following an incident identified?

e) Was the communication of the incident to all relevant parties effective throughout the detection, reporting and response process?

The results of the meeting should be documented. The organization should ensure that the areas identified for improvement to the information security incident management scheme are reviewed and justified changes incorporated into an update of the scheme documentation. The changes to the information security incident management processes, procedures and the reporting forms should be subject to thorough checking and testing before going live.

9.7 Other improvements

Other improvements may have been identified during the lessons learnt phase, for example changes in information security policies, standards and procedures, and changes to IT hardware and software configurations. The organization should ensure that these are actioned.

Annex A
(informative)

Cross reference table of ISO/IEC 27001 vs ISO/IEC 27035

ISO/IEC 27001:2005 Clause	ISO/IEC 27035 Clause
4.2.2 Implement and operate the ISMS The organization shall do the following. h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents.	4 (Overview) for the overview of the implementation of information security incident management. 5 (Plan and prepare) – the content could help to implement information security incident management. 6 (Detection and reporting), 7 (Assessment and decision), 8 (Responses) and 9 (Lessons learnt) – the content could help to operate information security incident management.
4.2.3 Monitor and review the ISMS The organization shall do the following. a) Execute monitoring and reviewing procedures and other controls to: 2) promptly identify attempted and successful security breaches and **incidents**; 4) help detect security events and thereby prevent security **incidents** by the use of indicators. b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, **incidents,** effectiveness measurements, suggestions and feedback from all interested parties.	9 (Lessons learnt) – the content could help to monitor and review information security incident management.
4.3.3 Control of records Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security **incidents** related to the ISMS.	5.1 (Overview of key activities), 6 (Detection and reporting) and Annex D (Example Information Security Event, Incident and Vulnerability Reports and Forms) – the content could help to define the scope of the records..
13 Information security incident management	4 (Overview) for the overview of the implementation of information security incident management. 5 (Plan and prepare) – the content could help to implement information security incident management.

ISO/IEC 27001:2005 Clause	ISO/IEC 27035 Clause
A.13.1 Reporting information security events and vulnerabilities Objective: To ensure information security events and vulnerabilities associated with information systems are communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of events and vulnerabilities that may have an impact on the security of organizational assets. They should be required to report any information security events and vulnerabilities as quickly as possible to the designated PoC.	5 (Plan and Prepare) (in particular, see 5.4 Information security incident management scheme, 5.5 Establishment of the ISIRT, 5.6 Technical and other support, 5.7 Awareness and training and 5.8 Scheme testing.), 6 (Detection and Reporting), Annexes C (Example Approaches to the Categorization and Classification of Information Security Events and Incidents) and Annex D (Example Information Security Event, Incident and Vulnerability Reports and Forms) – the content could help to report information security events and vulnerabilities
A.13.1.1 Reporting information security events Control: Information security events should be reported through appropriate management channels as quickly as possible.	Annex D.2.1 (Example items of the record for information security event) and Annex D.4.1 (Example from for information security event report) for the example of report form.
A.13.1.2 Reporting security vulnerabilities Control: All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security vulnerabilities in systems or services.	Annex D.2.3 (Example items of the record for information security vulnerability) and Annex D.4.3 (Example form for information security vulnerability report) for the example of report form.
A.13.2 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach is applied to the management of information security incidents. Responsibilities and procedures should be in place to handle information security events and vulnerabilities effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements.	7 (Assessment and Decision), 8 (Responses),and 9 (Lessons Learnt) and Annex B (Example of Information Security Incidents and Their Causes), Annex C (Example Approaches to the Categorization and Classification of Information Security Events and Incidents) and Annex E (Legal and Regulatory Aspects).
A.13.2.1 Responsibilities and procedures Control: Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	7 (Assessment and decision), 8 (Responses), Annex D.2.2 (Example items of the record for information security incident) and Annex D.4.2 (Example form for information security incident report) – the content could help to define the responsibilities and procedures..

ISO/IEC 27001:2005 Clause	ISO/IEC 27035 Clause
A.13.2.2 Learning from information security incidents Control: There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	9 (Lessons learnt) and Annex B (Example of Information Security Incidents and Their Causes) and Annex C (Example Approaches to the Categorization and Classification of Information Security Events and Incidents) – the content could help to learn from information security incidents.
A.13.2.3 Collection of evidence Control: Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	7 (Assessment and decision), 8 (Responses) (in particular, see 8.2.5 Information security forensics analysis) and Annex E (Legal and Regulatory Aspects) – the content could help to define the procedures to collect evidence.

Annex B
(informative)

Examples of information security incidents and their causes

B.1 Attacks

B.1.1 Denial of Service

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are a broad category of incidents with a common thread. Such incidents cause a system, service or network to fail to continue operating in its intended capacity, most often with complete denial of access to legitimate users. There are two main types of DoS/DDoS incidents caused by technical means: resource elimination and resource starvation.

Some typical examples of deliberate technical DoS/DDoS incidents include:

- pinging network broadcast addresses in order to fill up network bandwidth with response traffic,
- sending data in an unexpected format to a system, service or network in an attempt to crash it, or disrupt its normal operation,
- opening up multiple authorized sessions with a particular system, service or network in an attempt to exhaust its resources (i.e., to slow it down, lock it up or crash it).

Such attacks are often performed through Botnets, a collection of software robots (malicious code) that run autonomously and automatically. Botnets can relate to some hundreds to millions of affected computers.

Some technical DoS incidents may be caused accidentally, for example caused by operator misconfiguration or through incompatibility of application software, but most of the time they are deliberate. Some technical DoS incidents are intentionally launched in order to crash a system or service, or take down a network, while others are merely the by-products of other malicious activity. For instance, some of the more common stealth scanning and identification techniques can cause older or misconfigured systems or services to crash when scanned. It should be noted that many deliberate technical DoS incidents are often executed anonymously (i.e. the source of the attack is ‘faked’), since they typically do not rely on the attacker receiving any information back from the network or system being attacked.

DoS incidents caused by non-technical means, resulting in loss of information, service and/or facilities, could be caused, for example, by:

- breaches of physical security arrangements resulting in theft or wilful damage and destruction of equipment,
- accidental damage to hardware (and/or its location) by fire or water damage/flood,
- extreme environmental conditions, for example high operating temperatures (e.g. due to air conditioning failure),
- system malfunctions or overload,
- uncontrolled system changes,
- malfunctions of software or hardware.

B.1.2 Unauthorized access

In general this category of incidents consists of actual unauthorized attempts to access or misuse a system, service or network. Some examples of technically stimulated unauthorized access incidents include:

- attempts to retrieve password files,
- buffer overflow attacks to attempt to gain privileged (e.g., system administrator) access to a target,
- exploitation of protocol vulnerabilities to hijack or misdirect legitimate network connections,
- attempts to elevate privileges to resources or information beyond what a user or administrator already legitimately possesses.

Unauthorized access incidents caused by non-technical means, resulting in direct or indirect disclosure or modification of information, breaches of accountability or misuse of information systems, could be caused, for example, by:

- breaches of physical security arrangements resulting in unauthorized access to information,
- poorly and/or mis-configured operating systems due to uncontrolled system changes, or malfunctions of software or hardware.

B.1.3 Malicious code

Malicious code identifies a program or part of a program inserted into another program with the intent to modify its original behaviour, usually to perform malicious activities as information and identify theft, information and resource destruction, Denial of Service, Spam, etc. Malicious code attacks could be divided into five categories: viruses, worms, Trojan horses, mobile code and blended. Whilst a few years ago viruses were created to target any vulnerable infected system, today malicious codes are used to perform targeted attacks. This is sometimes performed modifying an existing malicious code, creating a variant that often is not recognized by malicious code detection technologies.

B.1.4 Inappropriate usage

This kind of incident occurs when a user violates an organization's information system security policies. Such incidents are not attacks in the strict sense of the word, but are often reported as incidents and should be managed by an ISIRT. Inappropriate usage could be:

- downloading and installing hacking tools,
- using corporate e-mail for spam or promotion of personal business,
- using corporate resources to set up an unauthorized web site,
- using peer-to peer activities to acquire or distribute pirated files (music, video, software).

B.2 Information gathering

In general terms, the information gathering category of incidents includes those activities associated with identifying potential targets and understanding the services running on those targets. This type of incident involves reconnaissance, with the goal being to identify the:

- existence of a target, and understand the network topology surrounding it, and with whom the target routinely communicates, and
- potential vulnerabilities in the target or its immediate network environment that could be exploited.

Typical examples of information gathering attacks by technical means include:

- dumping Domain Name System (DNS) records for the target's Internet domain (DNS zone transfer),
- pinging network addresses to find systems that are ‘alive’,
- probing the system to identify (e.g., fingerprint) the host operating system,
- scanning the available network ports on a system to identify the related services (e.g. e-mail, FTP, web, etc.) and the software version of those services,
- scanning for one or more known vulnerable services across a network address range (horizontal scanning).

In some cases, technical information gathering extends into unauthorized access if, for example, as part of searching for vulnerabilities the attacker also attempts to gain unauthorized access. This commonly occurs with automated hacking tools that not only search for vulnerabilities but also automatically attempt to exploit the vulnerable systems, services and/or networks that are found.

Information gathering incidents caused by non-technical means, resulting in:

- direct or indirect disclosure or modification information,
- theft of intellectual property stored electronically,
- breaches of accountability, e.g. in account logging,
- misuse of information systems (e.g. contrary to law or organization policy),

could be caused, for example, by:

- breaches of physical security arrangements resulting in unauthorized access to information, and theft of data storage equipment that contains important data, for example encryption keys,
- poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, resulting in internal or external personnel gaining access to information for which they have no authority.

Annex C
(informative)

Example approaches to the categorization and classification of information security events and incidents

C.1 Introduction

This annex provides example approaches to the categorization and classification of information security incidents. These approaches enable personnel and organizations to document information security incidents in a consistent manner, so that the following benefits are achieved:

- promoting the exchange and sharing of the information on information security incidents,
- making it easier for automating information security incident reporting and responses,
- improving the efficiency and effectiveness of information security incident handling and management,
- facilitating the collection and analysis of data on information security incidents, and
- identifying the severity levels of information security incidents using a consistent criteria.

These example approaches to categorization and classification can also be applied to information security events, but they do not cover information security vulnerabilities.

C.2 Categorization of information security incidents

Information security incidents may be caused by deliberate or accidental actions of human being, and may be caused by technical or physical means. The following approach categorizes information security incidents by considering threats as categorization factors. (For threats, ISO/IEC 27005:2008, Annex C Example of typical threats is referred to.) A list of categories of information security incidents is shown in Table C.1.

Table C.1 — Categories of information security incidents according to threats

Category	Description	Examples
Natural disaster incident	The loss of information security is caused by natural disasters beyond human control.	Earthquake, volcano, flood, violent wind, lightning, tsunami, collapse, etc.
Social unrest incident	The loss of information security is caused by the instability of society.	Bedin, terrorist assault, war, etc.
Physical damage incident	The loss of information security is caused by deliberately or accidentally physical actions.	Fire, water, electrostatic, abominable environment (such as pollution, dust, corrosion, freezing), destruction of equipment, destruction of media, theft of equipment, theft of media, loss of equipment, loss of media, tampering with equipment, tampering with media, etc.
Infrastructure failure incident	The loss of information security is caused by the failures of the basic systems and services that support the running of information systems.	Power-supply failure, networking failure, air-conditioning failure, water-supply failure, etc.

Table C.1 (*continued*)

Category	Description	Examples
Radiation disturbance incident	The loss of information security is caused by the disturbance due to radiation.	Electromagnetic radiation, electromagnetic pulse, electronic jamming, voltage fluctuation, thermal radiation, etc.
Technical failure incident	The loss of information security is caused by the faults in information systems or related non-technical facilities, as well as unintentional man-made problems, resulting in information systems unavailability or destruction.	Hardware failure, software malfunction, overloading (saturating the capacity of information systems), breach of maintainability, etc.
Malware incident	The loss of information security is caused by malicious programs that are created and disseminated deliberately. A malicious program is inserted into information systems to damage the confidentiality, integrity or availability of data, applications or operating systems, and/or affect the normal operation of information systems.	Computer virus, network worm, Trojan horse, botnet, blended attacks, malicious code embedded web page, malicious code hosting site, etc. A computer virus is a set of computer instructions or code which is inserted into computer programs. Unlike normal programs, it has self-replicating capability, and normally carries a payload that may disrupt computer operations or destroy data. In contrast to a computer virus, a network worm is a kind of malicious program which spreads and replicates itself through networks automatically, by exploiting the vulnerabilities of information systems on networks. A Trojan horse is a kind of malicious program disguised as benign functions in the information systems, and capable of enabling the author to control the information systems, including stealing or intercepting information from the systems. A botnet is a group of compromised (‘zombie’) computers on networks that are centrally controlled by the author of the botnet who is known as botnet controller or herder. Botnets are deliberately formed through infecting a mass of computers on networks with bot programs. Botnets can be used for opportunistic network attacks, information theft, and the dissemination of Trojan horses, network worms and other malicious programs. Blended attacks may have combined characteristics of computer viruses, network worms, Trojan horses or botnets and so on. Blended attacks may also result from the combined operations of a series of different malicious programs. For example, a computer virus or network worm intrudes into a computer system, and then installs a Trojan horse in the system. A malicious code embedded web page defaces website by including malicious code that installs malware on a computer system accessing it. A malicious code hosting site decoys a website to host malicious code which is downloaded by targeted users.

Table C.1 (*continued*)

Category	Description	Examples
Technical attack incident	The loss of information security is caused by attacking information systems through networks or other technical means, either by exploiting information systems' vulnerabilities in configurations, protocols or programs, or by force, which results in an abnormal status of information systems, or potential harm to the current system operations.	Network scanning, exploitation of vulnerability, exploitation of backdoor, login attempts, interference, DoS, etc. Network scanning makes use of network scanning software to acquire information about network configurations, ports, services and existing vulnerabilities. Exploitation of vulnerability exploits and makes use of information system defects such as configurations, protocols or programs. Exploitation of backdoor makes use of the backdoors or harmful programs left in software and hardware system design processes. Login attempts try to guess, crack or brute force passwords. Interference obstructs computer networks, wired or wireless radio and television transmission networks, or satellite radio and television signals, through technical means. DoS is caused by greedily using information system and network resources such as CPU, memory, disk space or network bandwidth, and so affect the normal operation of information systems, for example, SYS-a, PING-flooding, Email bombing.
Breach of rule incident	The loss of information security is caused by breaching rules deliberately or accidentally.	Unauthorized use of resources, breach of copyright, etc. Unauthorized use of resources accesses resources for unauthorised purposes, including profit-making ventures, for example, the use of e-mail to participate in illegal chain letters for profit or pyramid schemes. Breach of copyright is caused by selling or installing copies of unlicensed commercial software or other copyright protected materials, for example, warez.
Compromise of functions incident	The loss of information security is caused by deliberately or accidentally compromising the functions of information systems in terms of security.	Abuse of rights, forging of rights, denial of actions, mis-operations, breach of personnel availability, etc. Abuse of rights uses rights beyond the terms of reference. Forging of rights makes false rights in order to deceive. Denial of actions is when someone's denies what he/she has done. Mis-operations carry out operations incorrectly or unintentionally. Breach of personnel availability is caused by the lack or absence of human resources.

Table C.1 (*continued*)

Category	Description	Examples
Compromise of information incident	The loss of information security is caused by deliberately or accidentally compromising the security of information such as confidentiality, integrity, availability and etc.	Interception, spying, eavesdropping, disclosure, masquerade, social engineering, network phishing, theft of data, loss of data, tampering with data, data error, data flow analysis, position detection, etc. Interception captures data before it is able to reach the intended recipients. Spying is to secretly collect and report information about the activities of another organization. Eavesdropping is to listen in on an external party's conversation without their knowledge. Disclosure is to make sensitive information known publicly. Masquerade is when one entity pretends to be another. Social engineering is to gather information from a human being in a non-technical way, for example, lies, tricks, bribes, or threats. Network phishing is to make use of fraudulent computer network technology to entice users to divulge important information, such as obtaining users' bank account details and passwords by deceptive e-mails. Theft of data is to steal data. Tampering with data is to touch or make changes to data without authorization. Data error is to make mistakes when inputting or processing data. Position detection is to detect the position of sensitive information or systems.
Harmful contents incident	The loss of information security is caused by propagating undesirable content through information networks, which endangers national security, social stability and/or public safety and benefits.	Illegal content, panic content, malicious content, abusive content, etc. Illegal content is published content that violate national or international constitutions, laws and regulations, for example, child pornography, violence glorification, counterfeit, fraud. Panic content is the maliciously sensationalized discussion or comment on sensitive issues on the Internet, resulting in events such as social turbulence or panic. Malicious content is the spreading of content that maliciously attacks society or persons, for example, hoax, harassment. Abusive content are the broadcasting of content that have not been granted by recipients, for example, spam.
Other Incidents	Not categorized in any of the above incident category.	

C.3 Classification of information security incidents

Two example approaches to classify information security incidents are introduced in the following.

It is emphasized that these are examples. There are others, such as the FIRST / Mitre Common Vulnerability Scoring System (CVSS) and the UK government Structured Warning Information Format (SWIF).

C.3.1 Example approach 1

C.3.1.1 Classification factors

C.3.1.1.1 Introduction

This approach classifies information security incidents by considering the following three factors:

- information system importance,
- business loss,
- social impact.

C.3.1.1.2 Information System Importance

The importance of the information systems affected by information security incidents is determined by considering the importance of the organization business operations supported by the information systems. Importance could be expressed in relation to national security, social order, economic development and public interest, and the dependency of the business on the information systems. This approach classifies information system importance into three broad levels: especially important information system, important information system and ordinary information system.

C.3.1.1.3 Business Loss

The loss of organization business caused by information security incidents is determined by considering the severity of the impact of business interruption due to the damage of the hardware/software, functions and data of information systems. The severity of the impact can depend on the cost of recovering business to normal operation and other negative effects of the information security incidents, including loss of profit and/or opportunity. This approach classifies business loss into four broad levels: especially serious business loss, serious business loss, considerable business loss, and minor business loss, as described below.

a) Especially serious business loss would mean large business paralysis to the extent of losing business ability, and/or very serious damage to the confidentiality, integrity and availability of key business data. It would mean enormous cost to recover business to normal operation and eliminate the negative effects. An organization could not bear this level of business loss.

b) Serious business loss would mean interruption to business operations for a long time or local business paralysis to the extent of seriously influencing business ability, and/or serious damage to the confidentiality, integrity and availability of key business data. It would mean high cost to recover business to normal operation and eliminate the negative effects. An organization could bear this level of business loss.

c) Considerable business loss would mean interruption to business operations to the extent of considerably influencing business ability, and/or considerable damage to the confidentiality, integrity and availability of important business data. It would mean considerable cost to recover business to normal operation and eliminate the negative effects. An organization could completely bear this level of business loss.

d) Minor business loss would mean interruption to business operations for a short time to the extent of some influence on business ability, and/or minor impact to the confidentiality, integrity and availability of important business data. It would mean minor cost to recover business to normal operation and eliminate the negative effects.

C.3.1.1.4 Social Impact

The impact on society caused by information security incidents is determined by considering the scale and degree of the impact on national security, social order, economic development and public interest. This approach classifies social impact into four levels: especially important social impact, important social impact, considerable social impact and minor social impact, as described below.

I. Especially important social impact would mean adverse effects spanning most areas of one or more provinces/states, greatly threatening national security, causing social turbulence, bringing extremely adverse consequences on economic development, and/or seriously damaging public interest.

II. Important social impact would mean adverse effects spanning most areas of one or more cities, threatening national security, causing social panic, bringing significant adverse consequences on economic development, and/or damaging public interest.

III. Considerable social impact would mean adverse effects spanning partial areas of one or more cities, with limited threatening of national security, with some disturbance to social order, bringing some adverse consequences on economic development, and/or influencing public interest.

IV. Minor social impact would mean adverse effects on a partial area of one city, and little chance of threatening national security, social order, economic development and public interest, but with damage to the interests of individuals, corporations and other organizations.

C.3.1.2 Classes

C.3.1.2.1 Introduction

Based upon the classification factors, information security incidents should be classified by severity using a scale. Such a scale can be simple as ‘major’ and ‘minor’ or more detailed as:

- Emergency: severe impact;
- Critical: medium impact;
- Warning: low impact;
- Information: no impact, but analysis could be used to improve information security policies, procedures or controls.

According to the above classification factors, this approach classifies information security incidents into four classes:

- Very serious (Class IV)
- Serious (Class III)
- Less serious (Class II)
- Small (Class I).

It is emphasized that the severity classes are an example. In some approaches, the most serious class is represented as the highest scale level. In other approaches, the most serious is represented as the lowest scale level.

C.3.1.2.2 Very serious (Class IV)

Very serious incidents are those that

a) act on especially important information systems, and

b) result in especially serious business loss, or

c) lead to especially important social impact.

C.3.1.2.3 Serious (Class III)

Serious incidents are those that

a) act on especially important information systems or important information systems, and

b) result in serious business loss, or

c) lead to important social impact.

C.3.1.2.4 Less Serious (Class II)

Less serious incidents are those that

a) act on important information systems or ordinary information systems, and

b) result in considerable business loss, or

c) lead to considerable social impact.

C.3.1.2.5 Small (Class I)

Small incidents are those that

a) act on ordinary important information systems and

b) result in minor business loss or no business loss, and

c) lead to minor social impact or no social impact

d) no action required and no consequences.

C.3.1.3 Incident category and severity class

Information security incident category and severity class are often linked. One information security incident category may have different severity class depending not only on the business but also on the nature of the information security incident such as

- intentional,
- targeted,
- timing,
- volume.

Some examples of information security incident categories that may have different severity classes depending on their nature are provided in Table C.2.

Table C.2 — Examples of incident category and severity class

Severity class / Incident Category	Small	Less Serious	Serious	Very Serious
Technical Attacks	Failed Attempts	Single ordinary (User compromise)	Multiple (User compromise) Single important (Application, root compromise)	Mass (Application, root compromise)
Technical Attacks		Annoyance (Scratch the surface)	Disturbance (Throughput impact)	Unavailability (Stop in services)
Malware	Single known (Detected and blocked by antivirus protection)	Single unknown	Multiple infections Server infections	Mass infections

C.3.2 Example approach 2

C.3.2.1 Introduction

This approach presents outline example guidelines for assessing the adverse consequences of information security incidents, with each guideline using a scale of 1 (low) to 10 (high) scale to classify the information security incidents. (In practice, other scales could be used, say 1 to 5, and each organization should adopt a scale best suited to its environment.)

Before reading the guidelines below, the following explanatory points should be noted:

- In some of the example guidelines set out below, some of the entries are annotated as “No entry”. This is because the guidelines are formulated such that the adverse consequences at each of the ascending levels, expressed on the 1 to 10 scale, are broadly similar across all of the six types shown in C.3.2.2 through C.3.2.7. However, at some of the levels (on the 1 to 10 scale) for some of the types, it is considered that there is not sufficient differentiation over the immediate lower consequence entries to make an entry – and this is annotated “No entry”. Similarly, at the higher end of some types it is considered that there is no greater consequence than the highest entry shown – and thus the higher end entries are annotated “No entry”. (Thus, it would be logically incorrect to take out the “No entry” lines and compact the scale.)

Thus, using the following as an example set of guidelines, when considering the adverse consequences of an information security incident on the business of an organization, from

- unauthorized disclosure of information,
- unauthorized modification of information,
- repudiation of information,
- unavailability of information and/or service,
- destruction of information and/or service,

The first step is to consider which of the following types is relevant. For those considered relevant, the type guideline should be used to establish the actual adverse impact on business operations (or value) for entry into the information security incident reporting form.

C.3.2.2 Financial loss/disruption to business operations

The consequences of unauthorized disclosure and modification, repudiation, as well as unavailability and destruction, of such information, could well be financial loss, for example from reduction in share prices, fraud or breach of contract because of no or late action. Equally the consequences particularly of unavailability or destruction of any information could be disruptions to business operations. To rectify and/or recover from such incidents will require the expenditure of time and effort. This will in some cases be significant and should be considered. In order to use a common denominator, the time to recover should be calculated for a unit of personnel time and converted to a financial cost. This cost should be calculated by reference to the normal cost for a person month at the appropriate grade/level within the organization. The following guideline should be used.

1 Result in financial losses/costs of x_1 or less

2 Result in financial losses/costs of between x_1+1 and x_2

3 Result in financial losses/costs of between x_2+1 and x_3

4 Result in financial losses/costs of between x_3+1 and x_4

5 Result in financial losses/costs of between x_4+1 and x_5

6 Result in financial losses/costs of between x_5+1 and x_6

7 Result in financial losses/costs of between x_6+1 and x_7

8 Result in financial losses/costs of between x_7+1 and x_8

9 Result in financial losses/costs of more than x_8

10 The organization will go out of business

where, x_i (i = 1, 2, …, 8) represent the financial losses/costs in eight grades/levels which are determined by the organization in its context.

C.3.2.3 Commercial and economic interests

Commercial and economic information needs to be protected, and is valued by considering its value to competitors or the effect its compromise could have on commercial interests. The following guideline should be used.

1 Be of interest to a competitor but of no commercial value

2 Be of interest to a competitor to a value that is y_1 or less (turnover)

3 Be of value to a competitor to a value that is between y_1+1 and y_2 (turnover), or cause financial loss, or loss of earning potential, or facilitate improper gain or advantage for individuals or organizations, or constitute a breach of proper undertakings to maintain the confidence of information provided by third parties

4 Be of value to a competitor to a value that is between y_2+1 and y_3 (turnover)

5 Be of value to a competitor to a value that is between y_3+1 and y_4 (turnover)

6 Be of value to a competitor to a value that is more than y_4+1 (turnover)

7 *No entry*[1]

8 *No entry*

9 Could substantially undermine commercial interests, or substantially undermine the financial viability of the organization

10 *No entry*

where, y_i (i = 1, 2, …, 4) represent the values to a competitor in terms of turnovers in four grades/levels which are determined by the organization in its context.

C.3.2.4 Personal information

Where information about individuals is held and processed, it is morally and ethically correct, and occasionally required by law, that the information is protected against unauthorized disclosure which could result in at best embarrassment and at worst adverse legal action, for example under data protection legislation. Equally, it is required that information about persons is always correct, as unauthorized modification resulting in incorrect information could have similar effects as for unauthorized disclosure. It is also important that information about persons is not made unavailable or destroyed, as this could result in incorrect decisions or no action by a required time, with similar effects as for unauthorized disclosure or modification. The following guideline should be used.

1 Minor distress (concern) to an individual (anger, frustration, disappointment) but no breach of legal or regulatory requirement occurs

2 Distress (concern) to an individual (anger, frustration, disappointment) but no breach of legal or regulatory requirement occurs

3 A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of information, leading to minor embarrassment to an individual

4 A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of information, leading to significant embarrassment to an individual or minor embarrassment to a group of individuals

5 A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of information, leading to serious embarrassment to an individual

6 A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of information, leading to serious embarrassment to a group of individuals

7 *No entry*

8 *No entry*

9 *No entry*

10 *No entry*

C.3.2.5 Legal and regulatory obligations

Data held and processed by an organization may be subject to, or held and processed in order to allow an organization to comply with legal and regulatory obligations. Failure to comply with such obligations, either intentionally or unintentionally, may result in legal or administrative actions taken against individuals within the

[1] The term ‘no entry’ means that there is no corresponding entry for this impact level.

organization concerned. These actions may result in fines and/or prison sentences. The following guideline should be used.

1 *No entry*

2 *No entry*

3 Enforcement notice, civil suit or criminal offence resulting in financial damages/penalty of z_1 or less

4 Enforcement notice, civil suit or criminal offence resulting in financial damages/penalty of between z_1+1 and z_2

5 Enforcement notice, civil suit or criminal offence resulting in financial damages/penalty of between z_2+1 and z_3 or a prison term of up to two years

6 Enforcement notice, civil suit or criminal offence resulting in financial damages/penalty of between z_3+1 and z_4, or a prison term in excess of two years and up to ten years

7 Enforcement notice, civil suit or criminal offence resulting in unlimited financial damages/penalty, or a prison term in excess of ten years

8 *No entry*

9 *No entry*

10 *No entry*

C.3.2.6 Management and business operations

Information may be such that its compromise would prejudice the effective performance of an organization. For example, information relating to a change in a policy may provoke public reaction if disclosed, to the extent that it would not be possible to implement the policy. Modification, repudiation or unavailability of information concerned with financial aspects, or computer software, could also have serious ramifications for the operation of an organization. Further, repudiation of commitments could have adverse business consequences. The following guideline should be used.

1 Inefficient operation of one part of an organization

2 *No entry*

3 Undermine the proper management of the organization and its operation

4 *No entry*

5 Impede the effective development or operation of the organization's policies

6 Disadvantage the organization in commercial or policy negotiations with others

7 Seriously impede the development or operation of major organizational policies, or shut down or otherwise substantially disrupt significant operations

8 *No entry*

9 *No entry*

10 *No entry*

C.3.2.7 Loss of goodwill

The unauthorized disclosure or modification, repudiation, or indeed unavailability, of information, could lead to a loss of goodwill towards an organization, with resultant damage to its reputation, loss of credibility and other adverse consequences. The following guideline should be used.

1 *No entry*

2 Cause local embarrassment within the organization

3 Adversely affect relations with shareholders, customers, suppliers, employees, third party users, regulatory bodies, the government, other organizations or the public, resulting in local/regional adverse publicity

4 *No entry*

5 Adversely affect relations with shareholders, customers, suppliers, employees, third party users, regulatory bodies, the government, other organizations or the public, resulting in some national adverse publicity

6 *No entry*

7 Materially affect relations with shareholders, customers, suppliers, employees, third party users, regulatory bodies, the government, other organizations or the public, resulting in widespread adverse publicity

8 *No entry*

9 *No entry*

10 *No entry*

Annex D
(informative)

Example information security event, yncident and vulnerability reports and forms

D.1 Introduction

This annex contains example items to be recorded for information security events, incidents and vulnerabilities and example forms for reporting on information security events, incidents and vulnerabilities, with related notes. It is emphasized that these are examples. There are others, such as form the Schema from Incident Object Description and Exchange Format (IODEF) standard.

D.2 Example items in records

D.2.1 Example items of the record for information security event

This includes basic information of the information security event, such as when, what, how and why the event occurred, as well as the contact information of the reporting person.

Basic information

- Date of event
- Event number
- Related event and/or incident numbers (if applicable)

Reporting person details

- Name
- Contact information such as address, organization, department, telephone and e-mail

Event description

- What occurred
- How occurred
- Why Occurred
- Initial views on components/assets affected
- Adverse business impacts
- Any vulnerability identified

Event details

- Date and time the event occurred
- Date and time the event was discovered
- Date and time the event was reported

D.2.2 Example items of the record for information security incident

This includes basic information of the information security incident, such as when, what, how and why the incident occurred, as well as the incident category, impact, and result of incident response.

Basic information

- Date of incident
- Incident number
- Related event and/or incident numbers (if applicable)

Reporting person

- Name
- Contact information such as address, organization, department, telephone and e-mail

Point of Contact (PoC) member

- Name
- Contact information such as address, organization, department, telephone and e-mail

ISIRT member details

- Name
- Contact information such as address, organization, department, telephone and e-mail

Incident description

- What occurred
- How occurred
- Why Occurred
- Initial views on components/assets affected
- Adverse business impacts
- Any vulnerability identified

Incident details

- Date and time the incident occurred
- Date and time the incident was discovered
- Date and time the incident was reported

Incident category

Components/assets affected

Adverse business impact/effect of incident

Total recovery cost from incident

Incident resolution

Person(s)/perpetrator(s) involved (if incident caused by people)

Description of perpetrator

Actual or perceived motivation

Actions taken to resolve incident

Actions planned to resolve incident

Actions outstanding

Conclusion

Internal individuals/entities notified

External individuals/entities notified

D.2.3 Example items of the record for information security vulnerability

This includes basic information of the information security vulnerability, such as when, what and how the vulnerability was identified, as well as the potential impact and the resolution

Basic information

- Date of vulnerability identified
- Vulnerability number

Reporting person details

- Name
- Contact information such as address, organization, department, telephone and e-mail

Vulnerability description

Vulnerability resolution

D.3 How to use forms

D.3.1 Format of date and time

Dates should be entered in the format CCYY-MM-DD (and if required HH-MM-SS). If relevant, UTC should be used for ready comparison when many events could be occurring across time zones (and at the least state the UTC offset applied to the time).

D.3.2 Notes for completion

The purpose of the information security event and incident report forms is to provide information about an information security event, and then, if it is determined to be an information security incident, about the incident, to the appropriate people.

If you suspect that an information security event is in progress or may have occurred – particularly one which may cause substantial loss or damage to the organization's property or reputation, you should *immediately* complete and submit an information security event report form (see the first part of this Annex) in accordance with the procedures described in the organization's information security incident management scheme.

The information you provide will be used to initiate appropriate assessment, which will determine whether the event is to be classified as an information security incident or not, and if it is any remedial measures necessary to prevent or limit any loss or damage. Given the potentially time-critical nature of this process, *it is not essential to complete all fields in the reporting form at this time*.

If you are a PoC member reviewing already completed/part-completed forms, then you will be required to take a decision as to whether the event needs to be classified as an information security incident. If an event is classified as such, you should complete the information security incident form with as much information as you are able and forward both the information security event and incident forms to the ISIRT. Whether the information security event is classified as an incident or not, the information security event/incident/vulnerability database should be updated.

If you are an ISIRT member reviewing information security event and incident forms forwarded by a PoC member, then the incident form should be then updated as the investigation progresses and related updates made to the information security event/incident/vulnerability database.

The purpose of the information security vulnerability report form is to provide information about a perceived vulnerability, and to act as the repository of information on the resolution of the reported vulnerability.

Please observe the following guidelines when completing the forms:

- The form is recommended to be completed and submitted electronically[2]. (When problems exist, or are considered to exist, with electronic reporting mechanisms (e.g. e-mail), including when it is thought possible that the system is under attack and report electronic forms could be read by unauthorized people, then alternative means of reporting should be used. Alternative means could include in person, by telephone or text messaging.)
- Only provide information you know to be factual – do not speculate in order to complete fields. Where it is necessary to provide information you cannot confirm, please clearly state that the information is unconfirmed, and what leads you to believe it may be true.
- You should provide your full contact details. It may be necessary to contact you – either urgently or at a later date – to obtain further information concerning your report.

If you later discover that any information you have provided is inaccurate, incomplete or misleading, you should amend and re-submit your form.

[2] For example in secure web page form with linkage to the electronic information security event/incident/ vulnerability database. In today's world, to operate a paper-based scheme would be time consuming. However, paper-based scheme is also needed to prepare for the case which electronic scheme can not be used.

D.4 Example forms

D.4.1 Example form for information security event report

Information Security Event Report

1. Date of Event | **Page 1 of 1**

2. Event Number[3] | **3. (If Applicable) Related Event and/or Incident Identity Numbers**

4. REPORTING PERSON DETAILS

4.1 Name ---------- **4.2 Address** ----------

4.3 Organization ---------- **4.4 Department** ----------

4.5 Telephone ---------- **4.6 E-mail** ----------

---

5. INFORMATION SECURITY EVENT DESCRIPTION

5.1 Description of the Event:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

6. INFORMATION SECURITY EVENT DETAILS

6.1 Date and Time the Event Occurred

6.2 Date and Time the Event was Discovered

6.3 Date and Time the Event was Reported

6.4 Is the Response to this Event Closed? **YES** ☐ **NO** ☐
(tick as appropriate)

6.5 If yes, Specify How Long the Event has Lasted in Days/Hours/Minutes

---

[3] Event numbers should be allocated by the organization's ISIRT Manager.

D.4.2 Example form for information security incident report

Information Security Incident Report

1. Date of Incident | **Page 1 of 6**

2. Incident Number[4] | **3. (If Applicable) Related Event and/or Incident Identity Numbers**

4. POINT OF CONTACT MEMBER DETAILS

4.1 Name		**4.2 Address**	
4.3 Organization		**4.4 Department**	
4.5 Telephone		**4.6 E-mail**	

5. ISIRT MEMBER DETAILS

5.1 Name		**5.2 Address**	
5.3 Organization		**5.4 Department**	
5.5 Telephone		**5.6 E-mail**	

6. INFORMATION SECURITY INCIDENT DESCRIPTION

6.1 Further Description of the Incident:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

7. INFORMATION SECURITY INCIDENT DETAILS

7.1 Date and Time the Incident Occurred

7.2 Date and Time the Incident was Discovered

7.3 Date and Time the Incident was Reported

7.4 Identity/Contact Details of Reporting Person

7.5 Is the Incident Over? ***(tick as appropriate)*** **YES** ☐ **NO** ☐

7.6 If yes, Specify How Long the Incident has Lasted in Days/Hours/Minutes

---

[4] Incident numbers should be allocated by the organization's ISIRT Manager, and linked to the associated event numbers.

Information Security Incident Report

8. INFORMATION SECURITY INCIDENT CATEGORY

(Tick one, then complete related section below.) **8.1 Actual** *(incident has occurred)* ☐ **8.2 Suspected** *(incident thought to have occurred but not confirmed)* ☐

(One of) **8.3 Natural disaster** ☐ *(indicate threat types involved)*

Earthquake ☐ **Volcano** ☐ **Flood** ☐ **Violent wind** ☐
Lightning ☐ **Tsunami** ☐ **Collapse** ☐ **Other** ☐

Specify:

(One of) **8.4 Social unrest** ☐ *(indicate threat types involved)*

Bedin ☐ **Terrorist assault** ☐ **War** ☐ **Other** ☐

Specify:

(One of) **8.5 Physical damage** ☐ *(indicate threat types involved)*

Fire ☐ **Water** ☐ **Electrostatic** ☐
Abominable environment (such as pollution, dust, corrosion, freezing) ☐
Destruction of equipment ☐ **Destruction of media** ☐ **Theft of equipment** ☐
Theft of media ☐ **Loss of equipment** ☐ **Loss of media** ☐
Tampering with equipment ☐ **Tampering with media** ☐ **Other** ☐

Specify:

(One of) **8.6 Infrastructure failure** ☐ *(indicate threat types involved)*

Power-supply failure ☐ **Networking failure** ☐ **Air-conditioning failure** ☐
Water-supply failure ☐ **Other** ☐

Specify:

(One of) **8.7 Radiation disturbance** ☐ *(indicate threat types involved)*

lectromagnetic radiation ☐ **lectromagnetic pulse** ☐ **Electronic jamming** ☐
Voltage fluctuation ☐ **Thermal radiation** ☐ **Other** ☐

Specify:

(One of) **8.8 Technical failure** ☐ *(indicate threat types involved)*

Hardware failure ☐ **Software malfunction** ☐
Overloading (saturating the capacity of information systems) ☐
Breach of maintainability ☐ **Other** ☐

Specify:

Information Security Incident Report

8. INFORMATION SECURITY INCIDENT CATEGORY

(One of) **8.9 Malware** ☐ *(indicate threat types involved)*

Network worm ☐ **Trojan horse** ☐ **Botnet** ☐ **Blended attacks** ☐
Malicious code embedded web page ☐ **Malicious code hosting site** ☐ **Other** ☐

Specify:

(One of) **8.10 Technical attack** ☐ *(indicate threat types involved)*

Network scanning ☐ **Exploitation of vulnerability** ☐ **Exploitation of backdoor** ☐
Login attempts, Interference ☐ **Denial of Service (DoS)** ☐ **Other** ☐

Specify:

(One of) **8.11 Breach of rule** ☐ *(indicate threat types involved)*

Unauthorized use of resources ☐ **Breach of copyright** ☐ **Other** ☐

Specify:

(One of) **8.12 Compromise of functions** ☐ *(indicate threat types involved)*

Abuse of rights ☐ **Forging of rights, Denial of actions** ☐ **Mis-operations** ☐
Breach of personnel availability ☐ **Other** ☐

Specify:

(One of) **8.13 Compromise of information** ☐ *(indicate threat types involved)*

Interception ☐ **Spying, Eavesdropping** ☐ **Disclosure** ☐
Masquerade, Social engineering ☐ **Network phishing** ☐ **Theft of data** ☐
Loss of data ☐ **Tampering with data** ☐ **Data error** ☐ **Data flow analysis** ☐
Position detection ☐ **Other** ☐

Specify:

(One of) **8.14 Harmful contents** ☐ *(indicate threat types involved)*

Illegal contents ☐ **Panic contents** ☐ **Malicious contents** ☐
Abusive contents ☐ **Other** ☐

Specify:

8.15 Others ☐ *(If not yet established whether incident belongs to the above category, tick here)*

Specify:

Information Security Incident Report

9. COMPONENTS/ASSETS AFFECTED[5]

Components/ Assets Affected *(if any)* — *(Provide descriptions of the components/assets affected by or related to the incident, including serial, license and version numbers where relevant.)*

9.1 Information/Data

9.2 Hardware

9.3 Software

9.4 Communications

9.5 Documentation

9.6 Processes

9.7 Other

10. ADVERSE BUSINESS IMPACT/EFFECT OF INCIDENT

For each of the following indicate if relevant in the tick box, then against "value" record the level(s) of adverse business impact, covering all parties affected by the incident, on a scale of 1 to 10 using the guidelines for the categories of: Financial Loss/Disruption to Business Operations, Commercial and Economic Interests, Personal Information, Legal and Regulatory Obligations, Management and Business Operations, and Loss of Goodwill. (See Annex C.3.2 for examples). Record the code letters for the applicable guidelines against "Guideline", and if actual costs are known, enter these against "cost".

		VALUE	GUIDELINE(S)	COST
10.1 Breach of Confidentiality ***(i.e. unauthorized disclosure)***	☐			
10.2 Breach of Integrity ***(i.e. unauthorized modification)***	☐			
10.3 Breach of Availability ***(i.e. unavailability)***	☐			
10.4 Breach of Non-Repudiation	☐			
10.5 Destruction	☐			

11. TOTAL RECOVERY COSTS FROM INCIDENT

(Where possible, the actual total costs of recovery for the incident as a whole should be shown, against "value" using the 1 to 10 scale and against "cost" in actuals.)	VALUE	GUIDELINES	COST

[5] This is for more details of the components/assets affected is available as investigation and analysis proceeds (in the early stages of event and incident analysis normally only 'high level' information will be collected).

Information Security Incident Report

12. INCIDENT RESOLUTION

12.1 Incident Investigation Commenced Date ----------

12.2 Incident Investigator(s) Names(s) ----------

12.3 Incident End Date ----------

12.4 Impact End Date ----------

12.5 Incident Investigation Completion Date ----------

12.6 Reference and Location of Investigation Report ----------

13. (IF INCIDENT CAUSED BY PEOPLE) PERSON(S)/PERPETRATOR(S) INVOLVED

(One of)

Person ☐ **Legally Established Organization/Institution** ☐

Organized Group ☐ **Accident** ☐

No Perpetrator ☐
e.g. natural elements, equipment failure, human error

14. DESCRIPTION OF PERPETRATOR

15. ACTUAL OR PERCEIVED MOTIVATION

(One of)

Criminal/Financial Gain ☐ **Pastime/Hacking** ☐

Political/Terrorism ☐ **Revenge** ☐

Other ☐

Specify:

16. ACTIONS TAKEN TO RESOLVE INCIDENT

(e.g. 'no action', 'in-house action', 'internal investigation', 'external' investigation by ...')

17. ACTIONS PLANNED TO RESOLVE INCIDENT

(e.g. see above examples)

18. ACTIONS OUTSTANDING

(e.g. investigation is still required by other personnel)

Information Security Incident Report

19. CONCLUSION

(tick to indicate that the incident is considered Major or Minor, and include a short narrative to justify the conclusion

Major ☐ **Minor** ☐

(indicate any other conclusions)

20. INTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)

Information Security Manager/ Responsible Official	☐	**ISIRT Manager**	☐
Site Manager *(state which site)*	☐	**Information Systems Manager**	☐
Report Originator	☐	**Report Originator's Manager/ Line User Management Affected**	☐
		Other *(e.g. Help Desk, Human Resources, Management, Internal Audit,* *Specify:*	☐

21. EXTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)

Police	☐	**Other** *(e.g. Regulatory Body, External ISIRT* *Specify:*	☐

21. SIGN-OFFS

ORIGINATOR		REVIEWER		REVIEWER	
Digital Signature		**Digital Signature**		**Digital Signature**	
Name		**Name**		**Name**	
Role		**Role**		**Role**	
Date		**Date**		**Date**	

D.4.3 Example form for information security vulnerability report

Information Security Vulnerability Report

1. Date Vulnerability identified | **Page 1 of 1**

2. Vulnerability Number[6]

3. REPORTING PERSON DETAILS

3.1 Name | **3.2 Address** .....

3.3 Organization | **3.4 Department** .....

3.5 Telephone | **3.6 E-mail** .....

4. INFORMATION SECURITY VULNERABILITY DESCRIPTION

4.1 Date and Time the Vulnerability Reported

4.2 Description in Narrative Terms of the Perceived Information Security Vulnerability:

- How Vulnerability Noticed
- Characteristics of Vulnerability – Physical, Technical, etc.
- If Technical, what IT/Networking Components/Assets Concerned
- Components/Assets that might be Affected if Vulnerability were to be Exploited
- Potential Adverse Business Impacts if Vulnerability were to be Exploited

5. INFORMATION SECURITY VULNERABILITY RESOLUTION

5.1 Has Vulnerability been Confirmed? ***(tick as appropriate)*** **YES** ☐ **NO** ☐

5.2 Date and Time of Vulnerability Confirmation

5.3 Name of Person Authorising ..... **5.4 Address** .....

5.5 Organization ....

5.6 Telephone ..... **5.7 E-mail** .....

5.8 Has Vulnerability been Resolved? ***(tick as appropriate)*** **YES** ☐ **NO** ☐

5.9 Description in Narrative Terms of how Information Security Vulnerability has been Resolved, with Date and Name of Person Authorising Resolution

---

6 Vulnerability numbers should be allocated by the organization's ISIRT Manager.

Annex E
(informative)

Legal and regulatory aspects

The following legal and regulatory aspects of information security incident management should be addressed in the information security incident management policy and associated scheme:

- **Adequate Data Protection and Privacy of Personal Information is Provided.** In those countries where specific legislation exists that covers data confidentiality and integrity, it is often restricted to the control of personal data. As information security incidents need to be typically attributed to an individual, information of a personal nature may therefore need to be recorded and managed accordingly. A structured approach to information security incident management therefore needs to take into account the appropriate privacy protection. This may include:
  - those individuals with access to the personal data should, so far as is practical, not personally know the person(s) being investigated,
  - non-disclosure agreements should be signed by those individuals with access to the personal data prior to them being allowed access to it,
  - information should only be used for the express purpose for which it has been obtained, i.e. for information security incident investigation.
- **Appropriate Record Keeping is Maintained.** Some national laws require that companies maintain appropriate records of their activities for review in the annual organization audit process. Similar requirements exist with regard to government organizations. In certain countries organizations are required to report or to generate archives for law enforcement (e.g. regarding any case that may involve a serious crime or penetration of a sensitive government system).
- **Controls are in place to Ensure Fulfillment of Commercial Contractual Obligations.** Where there are binding requirements on the provision of an information security incident management service, for example covering required response times, an organization should ensure that appropriate information security is provided to ensure that such obligations can be met in all circumstances. (Related to this, if an organization contracts with an external party for support, for example an external ISIRT, then it should be ensured that all requirements, including response times, are included in the contract with the external party.).
- **Legal Issues related to Policies and Procedures are dealt with**. The policies and procedures associated with the information security incident management scheme should be checked for potential legal and regulatory issues, for example if there are statements about disciplinary and/or legal action taken against those causing information security incidents. In some countries it not easy to terminate employment.
- **Disclaimers are Checked for Legal Validity.** All disclaimers regarding actions taken by the information incident management team, and any external support personnel, should be checked for legal validity.
- **Contracts with External Support Personnel cover all Required Aspects.** Contracts with any external support personnel, for example from an external ISIRT, should be thoroughly checked regarding waivers on liability, non-disclosure, service availability, and the implications of incorrect advice.
- **Non-Disclosure Agreements are Enforceable**. Information security incident management team members may be required to sign non-disclosure agreements both when starting and leaving employment. In some countries, having signed non-disclosure agreements may not be effective in law; this should be checked.
- **Law Enforcement Requirements are Addressed**. The issues associated with the possibility that law enforcement agencies might legally request information from an information security incident management scheme need to be clear. It may be the case that clarity is required on the minimum level required by law at which incidents should be documented, and how long that documentation should be retained.

- **Liability Aspects are Clear.** The issues of potential liability, and related required controls to be in place, need to be clarified. Examples of events which may have associated liability issues are:
  - if an incident could affect another organization (for example, disclosure of shared information), and it is not notified in time and the other organization suffers an adverse impact,
  - if a new vulnerability in a product is discovered, and the vendor is not notified and a major related incident occurs later with major impact on one or more other organizations,
  - a report is not made where, in the particular country, organizations are required to report to or generate archives for law enforcement agencies regarding any case that may involve a serious crime, or penetration of a sensitive government system or part of the critical national infrastructure,
  - information is disclosed that seems to indicate that someone, or an organization, may be involved in an attack. This could damage the reputation and business of the person or organization involved,
  - information is disclosed that there may be a problem with a particular item of software and this is found not to be true.
- **Specific Regulatory Requirements are Addressed**. Where required by specific regulatory requirements, incidents should be reported to a designated body, for example as required in the nuclear power industry, Telecommunications companies and Internet Service Providers in many countries.
- **Prosecutions, or Internal Disciplinary Procedures, can be Successful**. The appropriate information security controls should be in place, including provably tamper-proof audit trails, to be able to successfully prosecute, or bring internal disciplinary procedures against, ‘attackers’, whether the attacks are technical or physical. In support of this, evidence will typically need to be collected in a manner that is admissible in the appropriate national courts of law or other disciplinary forum. It should be possible to show that:
  - records are complete and have not been tampered with in any way,
  - copies of electronic evidence are provably identical to the originals,
  - any IT system from which evidence has been gathered was operating correctly at the time the evidence was recorded.
- **Legal Aspects Associated with Monitoring Techniques are Addressed.** The implications of using monitoring techniques need to be addressed in the context of the relevant national legislation. The legality of different techniques will vary from country to country. For example, in some countries it is necessary to make people aware that monitoring of activities, including through surveillance techniques, takes place. Factors that need to be considered include who/what is being monitored, how they/it are being monitored, and when the monitoring is occurring. It should also be noted that monitoring/surveillance in the context of IDS is specifically discussed in ISO/IEC 18043.
- **Acceptable Use Policy is Defined and Communicated.** Acceptable practice/use within the organization should be defined, documented and communicated to all intended users. (For example, users should be informed of the acceptable use policy and asked to provide written acknowledgement that they understand and accept that policy when they join an organization or are granted access to information systems.).

Bibliography

[1] ISO/IEC 18043, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems*

[2] ISO/IEC 20000 (all parts), *Information technology — Service management*

[3] ISO/PAS 22399, *Societal security — Guidelines for incident preparedness and operational continuity management*

[4] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

[6] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[8] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[11] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*[7]

[12] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[13] Internet Engineering Task Force (IETF) Site Security Handbook, http://www.ietf.org/rfc/rfc2196.txt?number=2196

[14] Internet Engineering Task Force (IETF) RFC 2350, Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt?number=2350

[15] NIST Special Publication 800-61, Computer Security Incident Handling Guide (2004), http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

[16] TERENA's Incident Object Description Exchange Format Data Model and XML Implementation (IODEF) (produced by IETF), RFC 5070

[17] Internet Engineering Task Force (IETF) RFC 3227, Guidelines for evidence collection and archiving

[18] CESG GOVCERTUK, Incident Response Guidelines (2008), http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf

[7] To be published.

[19] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Incident Management Capability Metrics Version 0.1 (2007), http://www.cert.org/archive/pdf/07tr008.pdf

[20] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Incident Management Mission Diagnostic Method Version 1.0, http://www.cert.org/archive/pdf/08tr007.pdf

[21] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Defining Incident Management Processes for CSIRTs: A Work in Progress, http://www.cert.org/archive/pdf/04tr015.pdf

[22] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Handbook for Computer Security Incident Response Teams (CSIRTs), http://www.cert.org/archive/pdf/csirt-handbook.pdf

[23] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", State of the Practice of Computer Security Incident Response Teams, http://www.cert.org/archive/pdf/03tr001.pdf

[24] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", CSIRT Services, http://www.cert.org/csirts/services.html

[25] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Action List for Developing a Computer Security Incident Response Team (CSIRT), http://www.cert.org/csirts/action_list.html

[26] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed? http://www.cert.org/csirts/csirt-staffing.html

[27] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Steps for Creating National CSIRTs, http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

[28] SANS Institute, An approach to the ultimate in-depth security event management framework (2008)

[29] SANS Institute, Mining gold, A primer on incident handling and response (2008)

[30] SANS Institute, Incident Handling for SMEs (Small to Medium Enterprises) (2008)

[31] SANS Institute, Breach Notification in Incident Handling (2008)

[32] SANS Institute, Baselines and Incident Handling (2008)

[33] SANS Institute, Documentation is to Incident Response as an Air Tank is to Scuba Diving (2007)

[34] SANS Institute, Creating and Managing an Incident Response Team for a Large Company (2007)

[35] SANS Institute, An Incident Handling Process for Small and Medium Businesses (2007)

[36] SANS Institute, Incident Management 101 Preparation & Initial Response (aka Identification) (2005)

[37] SANS Institute, Building an Incident Response Program To Suit Your Business (2003)

[38] ISACA, COBIT 4.1 (Section DS5.11), www.isaca.org/cobit

[39] ENISA, A step-by-step approach on how to set up a CSIRT, http://www.enisa.europa.eu/act/cert/support/guide

[40] ENISA, CERT cooperation and its further facilitation by relevant stakeholders, http://www.enisa.europa.eu/act/cert/background/coop

[41] ENISA, A basic collection of good practices for running a CSIRT, http://www.enisa.europa.eu/act/cert/support/guide2

[42] TERENA's Incident Object Description and Exchange Format Requirements (IODEF) (produced by IETF), RFC 3067

[43] CVSS — A complete Guide to the Common Vulnerability Scoring System (Version 2.0), FIRST, 20 June 2007, http://www.first.org/cvss/cvss-guide.html

[44] SWIF — Structured Warning Information Format (Version 2.3), ITsafe, 9 May 2008

[45] ITIL, ITIL framework document, http://www.itil-officialsite.com/home/home.asp

ICS 35.040
Price based on 78 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™