

ISO/IEC JTC 1/SC 27
IT Security techniques
Secretariat: DIN (Germany)

Replaces: N 12376

Document type: Working Draft Text

Title: WG4N0230_3rdWD_27035-1_20130707

Status: As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

PLEASE submit your comments on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27> **by the due date 2013-09-13.**

Secretariat's note:

This request for comments is also concurrently being circulated as WG 4 document N34 for test purposes ONLY as part of the WG 4 Livelink trial via the Working Group Consultation application accessible at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

For the test purposes the National Bodies and liaison organizations of SC 27/WG 4 are kindly invited to send their responses to the hereby attached document via the above-mentioned WG 4 Working Group Consultation application.

Any responses received are greatly appreciated and will be taken into account when assessing the trial results and preparing a report for consideration at the next SC 27 Heads of Delegation meeting in Incheon, Republic of Korea, 24th October 2013.

Date of document: 2013-07-12

Source: Project editors

Expected action: COMM

Action due date: 2013-09-13

Email of secretary: krystyna.passia@din.de

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

ISO/IEC JTC 1/SC 27/WG 4
Security controls and services
Secretariat: SABS (South Africa)

Replaces: N 76

Document type: Request for comments

Title: Text 3rd WD 27035-1 - Text for ISO/IEC 3rd WD 27035-1, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management

Status: As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

A Working group consultation will be created for submissions to this request. Submissions should be sent directly via the SC 27/WG 4 commenting website at <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4> before the action due date.

A request for review and comment will be issued in parallel by SC 27 as SC 27 N12668.

Date of document: 2013-07-07

Source: Editors

Expected action: COMM

Action due date: 2013-09-13

No. of pages: 1 + 30

Email of secretary:

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

ISO/IEC JTC 1/SC 27 N **12668**

Date: 2013-07-06

ISO/IEC WD 27035-1.3

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology – Security techniques — Information security incident management — Part 1: Principles of incident management

Élément introductif — Élément central — Partie 1: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

D:\ISO\isomacroserver-prod\temp\DOCX2PDFISOTC\DOCX2PDFISOTC.Iliadmin@srvweb23_552\15628499_1.doc STD Version 2.1c2

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
DE-10787 Berlin

Tel. + 49 30 2601 2652
Fax + 49 30 2601 1723

E-mail krystyna.passia@din.de
Web <http://www.jtc1sc27.din.de/en> (public web site)
<http://isotc.iso.org/isotcportal/index.html> (SC 27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview.....	3
4.1 Basic concepts and principles.....	3
4.2 Objectives of incident management	4
4.3 Benefits of a structured approach	5
4.4 Adaptability	6
5 Phases	7
5.1 Overview.....	7
5.2 Plan and Prepare	10
5.3 Detection and Reporting.....	11
5.4 Assessment and Decision	12
5.5 Responses	13
5.6 Lessons Learnt	15
Annex A (informative) Examples of information security incidents and their causes	16
A.1 Attacks.....	16
A.1.1 Denial of Service.....	16
A.1.2 Unauthorized access.....	17
A.1.3 Malware.....	17
A.1.4 Abuse.....	17
A.2 Information gathering	17
Annex B (informative) Cross reference table of ISO/IEC 27001 vs ISO/IEC 27035.....	19
Bibliography	22

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

ISO/IEC 27035 consists of the following parts, under the general title *Information technology – Security techniques — Information security incident management*:

- *Part 1: Principles of incident management*
- *Part 2: Guidelines to plan and prepare for incident response*
- *Part 3: Guidelines for incident response operations*

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;
- 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.

For the purpose of achieving the approach, ISO/IEC 27035 provides guidance on information security incident management from the following aspects in the corresponding parts of this International Standard:

- ISO/IEC 27035-1, *Principles of incident management*, (this document) presents basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach to detecting, reporting, assessing, responding and applying lessons learned.
- ISO/IEC 27035-2, *Guidelines to plan and prepare for incident response*, presents the concepts to plan and prepare for incident response. The concepts are based on the plan and prepare phase of the model presented in ISO/IEC 27035-1. This Part also covers the “Lessons Learned” phase of the model.
- ISO/IEC 27035-3, *Guidelines for incident response operations*, including staff responsibilities and practical incident response activities.

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

Information technology – Security techniques — Information security incident management — Part 1: Principles of incident management

1 Scope

ISO/IEC 27035-1 is the foundation of this multipart standard. It presents basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach to detecting, reporting, assessing, responding and applying lessons learned.

The principles given in this International Standard are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this International Standard according to their type, size and nature of business in relation to the information security risk situation. This International Standard is also applicable to 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*

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

ISO/IEC 27035-2, *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC 27035-3, *Information technology — Security techniques — Information security incident management — Part 3: Guidelines for incident response operations*

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

honeypot

generic term for a decoy system used to deceive, distract, divert and 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

Note 1 to entry: Additionally honeypots are covertly monitored so that defenders can gather data on attack methods and approaches

[SOURCE: ISO/IEC 27039—¹, 2.19]

3.2

information security investigation

application of investigative and analysis techniques to capture, record and analyse information security incidents

3.3

Incident Response Team

IRT

team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle

Note 1 to entry: The IRT 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 are commonly used abbreviations, 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.

3.4

information security event

occurrence indicating a possible breach of information security, policy or failure of controls

3.5

information security incident

one or multiple related and identified information security events that may compromise operations

3.6

information security incident management

exercise of a consistent and effective approach to the handling of information security incidents

3.7

incident handling

actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents

3.8

incident response

actions taken to protect and restore the normal operational conditions of an information system and the information stored in it when an information security incident occurs

[SOURCE: ISO/IEC 27039—², 2.23]

¹ To be published.

² To be published.

3.9**Point of Contact****PoC**

previously identified person and/or department serving as the coordinator or focal point of information concerning a specific resource, through whom communication regarding the specific resource should take place

[Editor's Note: NBs are kindly asked to contribute a definition text for this term.]

3.10**tarpit**

systems that are intentionally exposed and designed to delay attacks

4 Overview**4.1 Basic concepts and principles**

An information security event is an occurrence indicating a possible breach of information security, policy or failure of controls. An information security incident is one or multiple related and identified information security events that may compromise operations.

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.

Information security incidents may be deliberate (e.g. caused by malware or intentional breach of discipline) or accidental (e.g. caused by inadvertent errors of human or unavoidable acts of nature), and may be caused by technical or physical means. Their consequences may include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information. If unreported information security events are later determined to be incidents, it becomes difficult to investigate the incidents and to take control in order to prevent recurrence.

Annex A 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.

A threat acts in unwanted ways to exploit the vulnerabilities (weaknesses) of information systems, services or networks, causing the occurrence of information security events and thus potentially causing 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.

[Editor's Note: NBs are kindly asked to contribute a brief explanation of what information security incident chain refers to.]

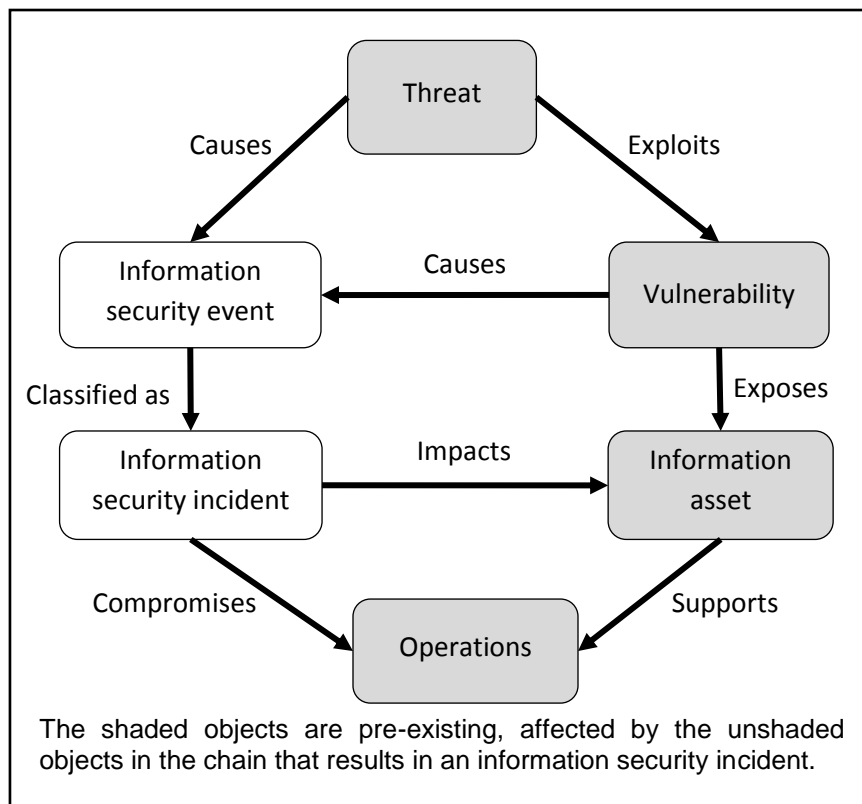


Figure 1 — The relationship of objects in an information security incident chain

4.2 Objectives of incident management

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 an organization's perspective, the prime objective is to avoid or contain the impact of information security incidents to minimize the direct and indirect damage caused by the incidents.

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

- 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.
- Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
- The adverse effects of information security incidents on the organization and its organization operations are minimized by appropriate controls as part of the incident response.
- A link with relevant elements from crisis management and business continuity management through an escalation process is established.
- Information security vulnerabilities are assessed and dealt with appropriately.
- Lessons are learnt quickly from information security incidents, vulnerabilities and their 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 derived 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 B.

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 following.

a) Improving overall information security

A structured process for 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 for new threats and vulnerabilities. Analysis of incident related data enables the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and thus identification of appropriate actions to prevent their occurrence.

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 higher priority areas where they are really needed.

e) Strengthening evidence

Clear incident investigation procedures will 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. For more information on digital evidence and investigation, see ISO/IEC 27037, 27041, 27042 and 27043.

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 ability to better plan for the allocation of staff and resources.

One example 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 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 improve the quality of the threat assessment. Similarly, the data collected on vulnerabilities will improve 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 solutions. Furthermore, such awareness helps to reduce mistakes or panic/confusion in the event of an information security incident.

[Editor's Note: NBs are kindly asked to contribute for defining "focused information".]

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.

[Editor's Note: NBs are kindly asked to reconsider and contribute the description of the above paragraph.]

4.4 Adaptability

The guidance provided by this International Standard (all parts) 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 for incident handling,
- c) potential for loss through unprevented incidents, 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.

5 Phases

5.1 Overview

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

- Plan and Prepare (see Clause 5.2),
- Detection and Reporting (see Clause 5.3),
- Assessment and Decision (see Clause 5.4),
- Responses (see Clause 5.5), and
- Lessons Learnt (see Clause 5.6).

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.

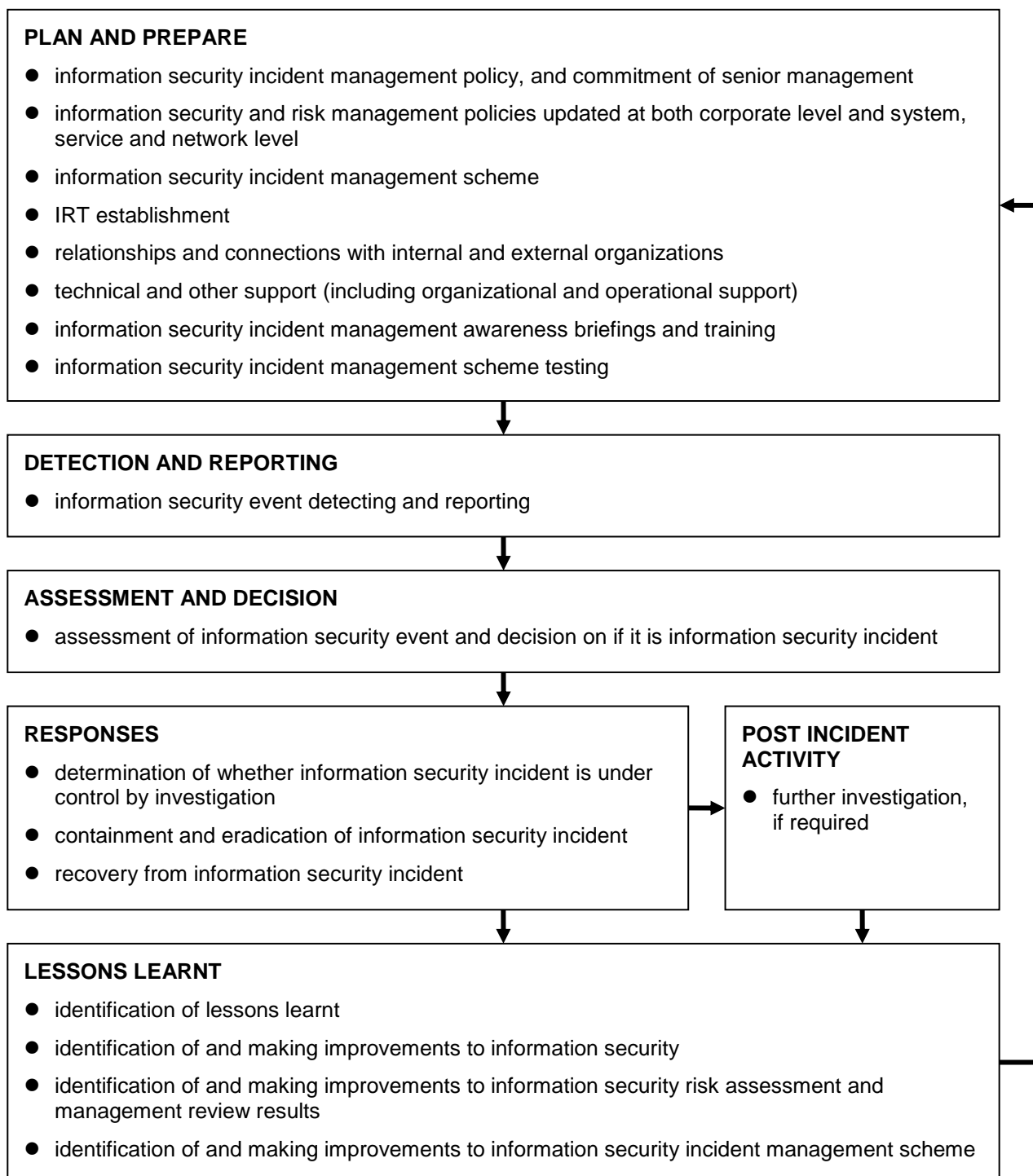


Figure 2 — Information security incident management phases

Figure 3 shows information security event and incident flow through information security incident management phases and related activities.

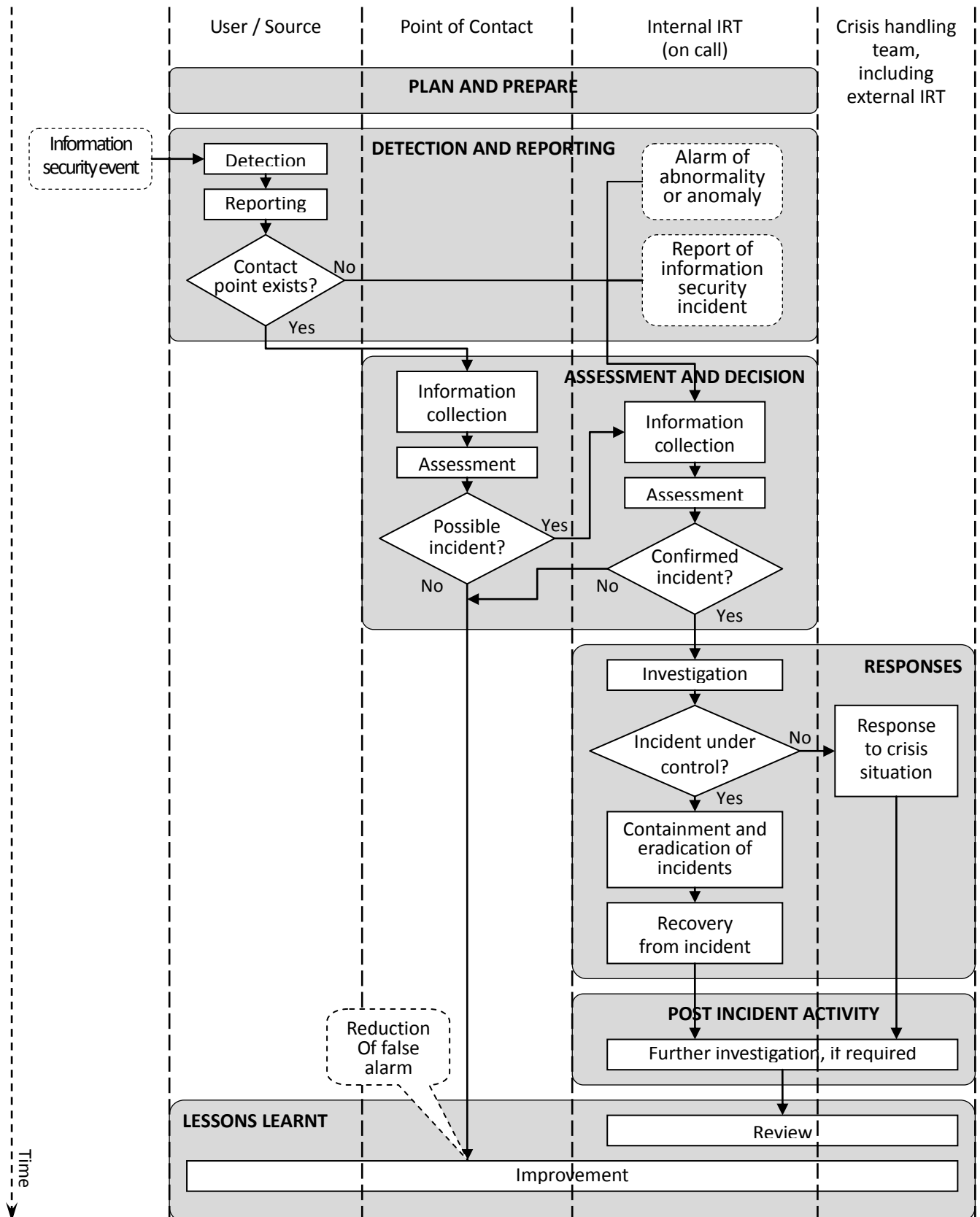


Figure 3 — Information security event and incident flow diagram

NOTE False alarm is an indication of a reported event that is found not to be real or of any consequence.

5.2 Plan and Prepare

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 incident 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. 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.

- c) Activity to define and document a detailed **information security incident management scheme**.

[Editor's Note: NBs are kindly asked to consider and contribute the definition and use of term "scheme" (versus "plan") throughout this document.]

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.

In some organizations, the scheme may be referred to as an information security incident response plan.

- d) Activity to establish the IRT, 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 IRT 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 (ICT, legal, public relations, outsourcing companies, etc.) that should cooperate closely with the IRT during the resolution of an information security incident. 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 malware attacks, who will be called upon depending on the type of incident concerned.

- 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 and operational support) mechanisms for supporting the information security incident management scheme (and thus the work of the IRT), and in order to prevent information security incident occurrences or reduce the likelihood of occurrences of information security incidents.
- 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 incident management scheme, its benefits and how to report information security events, incidents and vulnerabilities. In parallel, appropriate training should be provided to those personnel responsible for managing the information security incident 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.

- 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 IRT 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. 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. Part 2 of this International Standard describes each of the activities listed above, including the contents of each document required.

The following subclauses 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 IRT). Information on vulnerabilities and their resolutions should be entered into the information security event/incident/vulnerability database managed by the IRT.

5.3 Detection and Reporting

The second phase (Detection and Reporting) of information security incident management involves the detection of, collecting information associated with, and reporting on occurrences of information security events and the existence of information security vulnerabilities that may have not yet been exploited to cause information security events and possibly information security incidents, by human or automatic means.

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 Intrusion Detection System (IDS)/ Intrusion Detection and Prevention System (IDPS), antivirus program, honeypots/tarpits, 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) alerts shared from partners, vendors, or those in information sharing groups on known and emerging attack vectors (for more details, see ISO/IEC 27010:2012 and IETF RFC 5070.),
 - 4) analysis of log information from devices, services, hosts, and various systems,
 - 5) escalation of event reporting anomalous events detected by ICT,
 - 6) escalation of event reporting anomalous events detected by help desks,

- 7) user reports, and
 - 8) external notifications coming from third parties such as other IRTs, information security services, Internet Service Providers (ISPs), telecommunication service providers, outsourcing companies or national IRTs.
- 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 digital 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 (for more detailed information on the identification, collection, acquisition and preservation of digital evidence, see ISO/IEC 27037).
 - 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 IRT. 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.

5.4 Assessment and Decision

The third phase of information security incident management involves the assessment of information associated with occurrences of information security events and decision on if it is information security incident.

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

- a) 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.
- b) 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).
- c) Activity to use guidelines for thorough documentation of an information security event and the subsequent actions for an information security incident if the information security event becomes classified as an information security incident.
- d) Activity to update the information security event/incident/vulnerability database.

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

- e) Activity for information collection that can include testing, measurement activities and data gathering on the detection of an information security event. The actual information collected will depend on the information security event that has occurred. For details, refer to 27035-2.

- f) 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.

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. 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.
- g) Activity for the IRT 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). 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 investigation and communications activities are required, in the next phase (Responses – see also 5.5).

- h) Activity to ensure that all involved, particularly the IRT, properly log all activities, results and related decisions for later analysis.
- i) 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 IRT. 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.

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.

5.5 Responses

The fourth phase of information security incident management 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 investigation.

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

- a) Activity to conduct investigation of incidents, as required and relative to the information security incident classification scale rating, and changing that scale rating as necessary.
- b) Activity to review by the IRT 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.

Crisis handling function then is responsible for the incident, with full support of the IRT (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).

- c) Activity to assign internal resources and identify external resources in order to respond to an incident.
- 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 IRT, properly log all activities for later analysis.
- f) Activity to ensure that digital 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 IRT, 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:

- i) 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.
- j) 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).
- k) Activity to use guidelines for thorough documentation of an information security incident and the subsequent actions for the information security incident.
- l) Activity to update the information security event/incident/vulnerability database.
- m) Activity to conduct further information security investigation after recovery from an information security incident, as required.

Once any information security incident has been dealt with successfully, it should be formally closed and this recorded in the information security event/incident/vulnerability 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 event/incident/vulnerability database.

5.6 Lessons Learnt

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 identify the lessons learnt from information security incidents and vulnerabilities.
- b) 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 or many information security incidents 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.
- c) 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.
- d) 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.
- e) Activity to update the information security event/incident/vulnerability database.
- f) Activity to communicate and share the results of review within a trusted community (if the organization so wishes).
- g) Activity to determine if the incident information, associated attack vectors and vulnerabilities may be shared with partner organizations to assist in preventing the same incidents from occurring in their environments through notification of identified threats (for more details, see ISO/IEC 27010:2012 on information sharing).

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.

Annex A

(informative)

Examples of information security incidents and their causes

A.1 Attacks

A.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 Bots, a computer system running malware that is controlled via a botnet. A botnet is a central bot command and control network managed by humans. 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.

A.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.

A.1.3 Malware

Malware 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. Malware attacks could be divided into five categories: viruses, worms, Trojan horses, mobile code and blended. Whilst viruses are created to target any vulnerable infected system, other malware are also used to perform targeted attacks. This is sometimes performed by modifying an existing malware and creating a variant that often is not recognized by malware detection technologies.

A.1.4 Abuse

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 IRT. 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).

A.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, File Transfer Protocol (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 B (informative)

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

[Editor's Note: This Annex will be updated to follow the new contents and structures of the revision of 27001 and Part2 & Part3 of 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.	Part 1: 4 (Overview) for the overview of the implementation of information security incident management. Part 1: 5 (Plan and Prepare) – the content could help to implement information security incident management. Part 1: 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.	Part 1: 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.	Part 1: 5.1 (Overview of key activities) and 6 (Detection and Reporting) – the content could help to define the scope of the records.
13 Information security incident management	Part 1: 4 (Overview) for the overview of the implementation of information security incident management. Part 1: 5 (Plan and Prepare) – the content could help to implement information security incident management.

ISO/IEC 27001:2005 Clause	ISO/IEC 27035 Clause
<p>A.13.1 Reporting information security events and vulnerabilities</p> <p>Objective: To ensure information security events and vulnerabilities associated with information systems are communicated in a manner allowing timely corrective action to be taken.</p> <p>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.</p>	<p>Part 1: 5 (Plan and Prepare) (in particular, see 5.4 Information security incident management scheme, 5.5 Establishment of the IRT, 5.6 Technical and other support, 5.7 Awareness and training and 5.8 Scheme testing.) and 6 (Detection and Reporting) – the content could help to report information security events and vulnerabilities</p>
<p>A.13.1.1 Reporting information security events</p> <p>Control: Information security events should be reported through appropriate management channels as quickly as possible.</p>	
<p>A.13.1.2 Reporting security vulnerabilities</p> <p>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.</p>	
<p>A.13.2 Management of information security incidents and improvements</p> <p>Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.</p> <p>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.</p> <p>Where evidence is required, it should be collected to ensure compliance with legal requirements.</p> <p>A.13.2.1 Responsibilities and procedures</p> <p>Control: Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.</p>	<p>Part 1: 7 (Assessment and Decision), 8 (Responses) and 9 (Lessons Learnt) and Annex A (Example of Information Security Incidents and Their Causes).</p> <p>Part 1: 7 (Assessment and Decision) and 8 (Responses) – the content could help to define the responsibilities and procedures.</p>

ISO/IEC 27001:2005 Clause	ISO/IEC 27035 Clause
<p>A.13.2.2 Learning from information security incidents</p> <p>Control: There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.</p> <p>A.13.2.3 Collection of evidence</p> <p>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).</p>	<p>Part 1: 9 (Lessons Learnt) and Annex A (Example of Information Security Incidents and Their Causes) – the content could help to learn from information security incidents.</p> <p>Part 1: 7 (Assessment and Decision) and 8 (Responses) – the content could help to define the procedures to collect evidence.</p>

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 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*
- [10] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [11] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*
- [12] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*
- [13] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*
- [14] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
- [15] ISO/IEC 27041—³, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of investigation methods*
- [16] ISO/IEC 27042—⁴, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*
- [17] ISO/IEC 27043—⁵, *Information technology — Security techniques — Investigation principles and processes*

³ To be published.

⁴ To be published.

- [18] ISO/IEC 27044—⁶, *Information technology — Security techniques — Security Information and Event Management (SIEM)*
- [19] Internet Engineering Task Force (IETF) Site Security Handbook, <http://www.ietf.org/rfc/rfc2196.txt?number=2196>
- [20] Internet Engineering Task Force (IETF) RFC 2350, *Expectations for Computer Security Incident Response*, <http://www.ietf.org/rfc/rfc2350.txt?number=2350>
- [21] NIST Special Publication 800-61, *Computer Security Incident Handling Guide (2004)*, <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>
- [22] Internet Engineering Task Force (IETF) RFC 5070, *The Incident Object Description Exchange Format (IODEF)*
- [23] Internet Engineering Task Force (IETF) RFC 3227, *Guidelines for evidence collection and archiving*
- [24] CESA GOVCERTUK, Incident Response Guidelines (2008), http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf
- [25] 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>
- [26] 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>
- [27] 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>
- [28] 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>
- [29] 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>
- [30] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, *CSIRT Services*, <http://www.cert.org/csirts/services.html>
- [31] 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
- [32] 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>
- [33] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, *Steps for Creating National CSIRTs*, <http://www.cert.org/archive/pdf/NationalCSIRTs.pdf>
- [34] SANS Institute, *An approach to the ultimate in-depth security event management framework (2008)*
- [35] SANS Institute, *Mining gold, A primer on incident handling and response (2008)*
- [36] SANS Institute, *Incident Handling for SMEs (Small to Medium Enterprises) (2008)*

⁵ To be published.

⁶ To be published.

- [37] SANS Institute, *Breach Notification in Incident Handling* (2008)
- [38] SANS Institute, *Baselines and Incident Handling* (2008)
- [39] SANS Institute, *Documentation is to Incident Response as an Air Tank is to Scuba Diving* (2007)
- [40] SANS Institute, *Creating and Managing an Incident Response Team for a Large Company* (2007)
- [41] SANS Institute, *An Incident Handling Process for Small and Medium Businesses* (2007)
- [42] SANS Institute, *Incident Management 101 Preparation & Initial Response (aka Identification)* (2005)
- [43] SANS Institute, *Building an Incident Response Program To Suit Your Business* (2003)
- [44] ISACA, *COBIT 4.1 (Section DS5.11)*, www.isaca.org/cobit
- [45] ENISA, *A step-by-step approach on how to set up a CSIRT*, <http://www.enisa.europa.eu/act/cert/support/guide>
- [46] ENISA, *CERT cooperation and its further facilitation by relevant stakeholders*, <http://www.enisa.europa.eu/act/cert/background/coop>
- [47] ENISA, *A basic collection of good practices for running a CSIRT*, <http://www.enisa.europa.eu/act/cert/support/guide2>
- [48] TERENA's *Incident Object Description and Exchange Format Requirements (IODEF)* (produced by IETF), RFC 3067
- [49] 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>
- [50] SWIF — *Structured Warning Information Format (Version 2.3)*, ITsafe, 9 May 2008
- [51] ITIL, *ITIL framework document*, <http://www.itil-officialsite.com/home/home.asp>