

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

Replaces: N 11971

Document type: Working Draft Text

Title: WG4N0232_3rdWD_27035-2_20130708

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 N0232 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

No. of pages: 1 + 1 + 48

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 77

Document type: Request for comments

Title: Text 3rdWD 27035-2 - Text for ISO/IEC 3rd WD 27035-2, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

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 N12760.

Date of document: 2013-07-08

Source: Editors

Expected action: COMM

Action due date: 2013-09-13

No. of pages: 1 + 48

Email of secretary:

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

ISO/IEC JTC 1/SC 27 N **12679**

Date: 2013-07-7

ISO/IEC WD 27035-2.3

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology – Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

Élément introductif — Élément central — Partie 2: 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_629\15629391_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-10772 Berlin

Tel. + 49 30 2601 2652
Fax + 49 30 2601 4 2652
E-mail krystyna.passia@din.de

Web <http://www.jtc1sc27.din.de/en> (public web site)
<http://isotc.iso.org/isotcportal/index.html> (SC27 documents)

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

Violators may be prosecuted.

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions	2
3.2 Abbreviated terms	2
4 Overview.....	2
4.1 Structure of this International Standard	2
4.2 Relations with the other guidelines	3
5 Establishing information security incident management policy.....	5
5.1 Principles.....	5
5.2 Policy	5
5.3 Ownership	5
5.4 Point of contact	5
5.5 Capability.....	5
5.6 Planning.....	5
5.7 Incident management.....	6
5.7.1 Introduction.....	6
5.7.2 Preparation for detection and reporting phase.....	6
5.7.3 Preparation for assessment and decision phase	6
5.7.4 Preparation for responses phase	6
5.8 Competence	7
5.9 Records management	7
5.10 Disclosures	7
5.11 Consensus	7
5.12 Review	8
6 Updating of information security and risk management policies	8
6.1 Organizational commitment	8
6.1.1 Introduction.....	8
6.1.2 Involved parties	9
6.1.3 Content	9
6.2 Existing policy integration and review	10
6.2.1 Introduction.....	10
6.2.2 Content	10
7 Creating information security incident management scheme.....	11
7.1 Introduction.....	11
7.2 Involved parties	11
7.3 Content	11
7.4 Incident classification scale	14
7.5 Incident forms.....	14
7.6 Processes and procedures.....	15
7.7 Trust and confidence	16
7.8 Confidentiality.....	16
8 Establishing an Incident Response Team (IRT)	17
8.1 Establishment	17
8.1.1 Introduction.....	17
8.1.2 Members and structure.....	17

8.1.3	Relationship with other parts of the organization	17
8.1.4	Relationship with external interested parties	18
9	Defining technical and other support	18
9.1	Introduction	18
9.2	Examples of technical support.....	20
9.3	Examples of other support	20
10	Creating information security incident awareness and training	20
11	Testing the information security incident management scheme	21
11.1	Introduction	21
11.2	Exercise	22
11.2.1	Defining the goal of the exercise	22
11.2.2	Defining the scope of an exercise.....	23
11.2.3	Conducting an exercise	23
11.3	Incident Response Capability Monitoring	23
11.3.1	Implementing an incident response capability monitoring program	23
11.3.2	Metrics and governance of incident response capability monitoring.....	24
12	Lesson Learnt	24
12.1	Identifying the lessons learnt.....	24
12.2	Identifying and making improvements to information security control implementation.....	25
12.3	Identifying and making improvements to information security risk assessment and management review results.....	26
12.4	Identifying and making improvements to the information security incident management scheme.....	26
12.5	Other improvements.....	26
Annex A	(informative) Example approaches to the categorization and classification of information security events and incidents	27
A.1	Introduction	27
A.2	Categorization of information security incidents.....	27
A.3	Classification of information security incidents	31
A.3.1	Example approach 1	31
A.3.2	Example approach 2.....	34
Annex B	(informative) Legal and regulatory aspects	39
Bibliography	41

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 27035-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information security*, 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

The introduction to ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management, the predecessor to this International Standard, talks directly to Part 2: Guidelines to Plan and Prepare for Incident Response. The authors identify the importance of an organization having a plan to handle information security incident response by saying:

“Therefore it is essential for any organization that is serious about information security to have a structured and planned approach...”

There can be a large gap between an organization’s plan for an incident and an organization knowing it is prepared for an incident. Therefore, this International Standard addresses the development of guidelines to increase the verifiable confidence of an organization’s actual readiness to respond to an information security incident.

Information technology – Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

1 Scope

ISO/IEC 27035-2 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 "Information security incident management phases." The major points within this phase include

- information security incident management policy, and commitment of senior management,
- information security and risk management policies updated at both corporate level and system, service and network level,
- information security incident management scheme,
- IRT establishment,
- technical and other support (including organizational and operational support),
- information security incident management awareness briefings and training, and
- information security incident management scheme testing.

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.

[Editor's Note: In a general sense, it addresses a method to answer the question "are we ready for an incident?"]

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 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27035-1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

3.1.1

incident response readiness policy

is a formal commitment given by an organization to adopt and implement the principles of incident response readiness, adapted to be relevant within the business environment of that organization.

3.1.2

incident response readiness planning

is the contingency planning and capability building activities associated with implementation of incident response readiness planning

3.1.3

users

people or organizations that utilise services provided by the IRT, users can be internal (within the organization) or external (entities outside of the organization),

3.2 Abbreviated terms

CD	Compact Disk
DVD	Digital Versatile Disk
ISP	Internet Service Provider
PoC	Point-of-Contact
ROM	Read-Only Memory

4 Overview

4.1 Structure of this International Standard

The remainder of this part of this International Standard is as follows:

- Clause 5 – Covers recommendations for establishing security incident management policy
- Clause 6 – Covers the recommended requirements for updating information security and risk management policies.
- Clause 7 – Describes the information security incident management scheme, including parties, classification scale as well as forms and procedures
- Clause 8 – Covers establishing an incident response team
- Clause 9 – Covers the defining of technical and other support
- Clause 10 – Describes creating information security incident awareness and training
- Clause 11 – Describes testing the information security incident management scheme
- Clause 12 – Describes dealing with lessons learnt

— Annex A – Provides a list of categorization and classification of incidents against which the level of readiness can be broken down consistently across an organization's ISMS and information systems.

— Annex B – Provides an indication of the legal and regulatory aspects of information security incident management.

4.2 Relations with the other guidelines

This International Standard is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, Information Security Incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise.

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

This International Standard describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following standards.

— ISO/IEC 27037: Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence.

This describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

— ISO/IEC 27038: Specification for digital redaction.

In some circumstances material which is found during various phases of the investigation must not be disclosed. In these cases, redaction may be required.

— ISO/IEC 27040: Storage security.

Security mechanisms can affect ability to investigate by introducing obfuscation mechanisms. They should be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

— ISO/IEC 27041: Guidance on Assuring the Suitability and Adequacy of Investigative Methods.

It is important that methods and processes deployed during an investigation can be shown to be appropriate. This document provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

— ISO/IEC 27042: Guidelines for the Analysis and Interpretation of Digital Evidence.

This describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence and effective reporting of findings.

— ISO/IEC 27043: Guidance on Investigation Principles and Processes.

This defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

— ISO/IEC 27044: Guidelines for Security Information and Event Management (SIEM).

1 — ISO/IEC 27050: eDiscovery

2 — ISO/IEC 30121: Governance of digital forensic risk framework

3 Figure 1 shows a typical sequence of events surrounding an incident and its investigation. The standards

4 listed above are mapped onto this sequence, showing where each is most likely to be directly applicable. It is

5 recommended, however, that all should be consulted prior to, and during, the planning and preparation

6 phases.

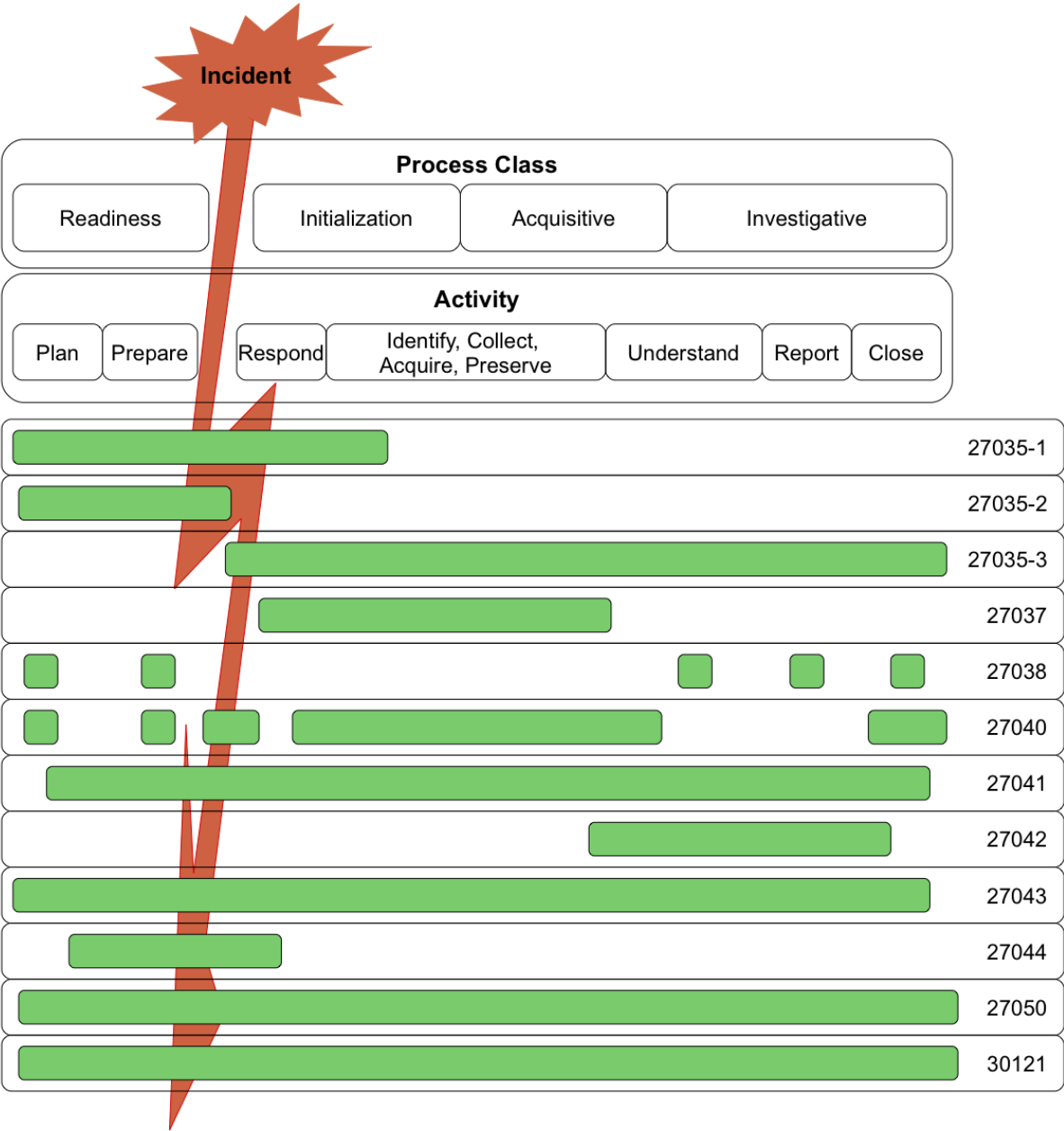


Figure 1 — Applicability of standards to Investigation process classes and activities

5 Establishing information security incident management policy

5.1 Principles

The basic principles of incident response planning and preparation would include

- information security incident management policy and commitment of senior management,
- information security and risk management policies updated at both corporate level and system, service and network level,
- information security incident management scheme,
- IRT establishment,
- technical and other support (including organizational and operational support),
- information security incident management awareness briefings and training, and
- information security incident management scheme testing.

5.2 Policy

An organization should implement a policy that outlines the steps to be taken, the responsible persons, and the reporting lines (specifically the primary point of contact for reporting potential incidents) should an information security incident occur. The policy should be reviewed regularly to ensure it reflects the latest organisation structure, processes, and technology that may affect incident response. The policy should also outline any awareness training initiatives within the organisation that is related to incident response. (See Clause 10.)

5.3 Ownership

Depending on the principles and policy adopted by the organization, clear set roles and responsibilities and even activities should be defined so that the actual organizational incident readiness is set as a process with involved actors. The process should define the roles so that ownership throughout the process is established.

5.4 Point of contact

A point of contact needs to be established for the purposes of reporting suspected incidents. This point of contact should be clearly communicated through information security and incident response policies.

5.5 Capability

An IRT should have team members with a number of speciality areas (see Clause 8.9). The IRT should be able to respond to and investigate incidents effectively, and have the necessary tools to conduct digital forensics analysis and store incident information and reports.

5.6 Planning

Planning and preparation for incident response should be undertaken by the process owner, with a clear goal or set of goals for incident response within a defined scope. Preparation for the planning process should include the following.

- Governance and policy directives that define assets and protection requirements (see 5.2) in support of stated incident response objectives.

- 1 — Participants with knowledge of assets in the environment within scope (see 5.9).
- 2 — Historical event and incident records relating to assets and processes within scope.
- 3 — Participants that have authority over normative security controls, in addition to capability (see 5.5).
- 4 — Management or other participants that have authority over additional controls and resources available for
5 response.

6 **5.7 Incident management**

7 **5.7.1 Introduction**

8 Key decision-making criteria and processes to support expected management phases should be defined and
9 reviewed before the planning and preparation process considers specific incident types and the corresponding
10 response processes. This requires available policy, formal or informal understanding of assets and controls,
11 and contribution from participants and management support (see 5.6).

12 **5.7.2 Preparation for detection and reporting phase**

13 Planning and preparation requirements for detection and reporting should enable and support the
14 development and operation of processes to find or accept information about information security incidents.

15 Criteria for intake or acceptance of an incident report should be defined, based on the condition and
16 completeness of the report and verification of one or more information security events. To support later
17 decision-making, minimum criteria for intake or acceptance of any event detection alert or manual report
18 should be defined prior to the planning process, and should include at least identification of an affected
19 environment or asset, a statement of one or more suspected or confirmed events or qualified event type, and
20 the time received. In order to support decision making, the planning process should include a method for
21 returning detection or reports that have insufficient information.

22 Reporting output or notification should be defined in the context of the organization, the incident response
23 policy, and assignment of technical and management roles. The formality of reports and notification should
24 match the incident classification scale (see 8.4) or a consistent related metric.

25 **5.7.3 Preparation for assessment and decision phase**

26 Planning and preparation requirements for assessment and decision should enable and support the
27 development and operation of processes to evaluate and direct actions in response to information security
28 incidents.

29 Prior to development of assessment and decision processes, the process owner should ensure that the
30 minimum information for identification and classification of a security incident is defined, consisting of specific
31 items of required and supporting information. This definition will allow response planners to develop consistent
32 processes for completeness and classification of detected and reported events. The information sufficiency
33 required to differentiate between true positive and false positive reports should be defined, and allow for
34 accumulation of information to support estimation of and response to false negative detection and reports.

35 If the incident planning process is to depend on automated information management and decision support
36 systems, the functions, implementation, and on-going operation of these systems should be defined. The IR
37 process owner should ensure an information security event/incident/vulnerability database sufficiently defined
38 prior to developing IR processes that depend on it.

39 **5.7.4 Preparation for responses phase**

40 Planning and preparation requirements for response should enable and support the development and
41 operation of processes to respond to information security incidents. Prior to response planning, the IR process
42 owner should gather definitions or create working thresholds or categories for priority of information and

information system, impact of each intrusion types, damage scale, intrusion alarm level, and severity. These may be qualitative or quantitative as long as they are consistent with assessment and decision preparations, and enable the IRT manager to assign the incident actions or tasks to responders.

Classes of response should also be defined prior to the planning process, organized by cost, time, technical resource minimums, and other metrics to enable assignment of response class relative to the known information about the reported and assessed incident. Immediate or deferred response should be included, as well as a definition of how single or cyclic incident tasks will be managed in the response process.

5.8 Competence

Team members in the IRT should be competent in one or more of the following fields: digital investigation, digital data collection, information security training, good communication skills, and networking.

5.9 Records management

Records, data, and information related to investigations should be stored securely. A numbering scheme should be devised to relate different files to a single investigation. An index or register of all files should be kept, indicating the current version and listing previous versions.

Should any document require changes after being submitted, a change note should be conducted to detail what is to be changed, and the reasons for the changes. The change notes are also to be index/registered along with other documents.

Files may be stored according to investigation, or file type (e.g. all reports are stored together, and all ISO images are stored together etc.). Documents may be kept in both electronic and physical form. Backups of all documents should be made.

An example of a document numbering system is as follows:

[investigation number]_[document number]_[document type]_ver[document version].[file extension]

5.10 Disclosures

Information should be kept confidential and only disclosed according to the relevant legislation. In many instances, legislation requires affected parties to be notified should any personal identifiable information be compromised.

De-sensitised information can be disclosed to national CSIRTs or CERTS or related organisations for statistical purposes.

5.11 Consensus

Where there is no guiding policy or standard, prevailing law, or other authoritative source, the incident management planning process should be based on consensus to ensure effective operation, communication, and relationships with external organizations.

Terms and definitions should be normalized between IRT members and partner organizations. This includes names and identifiers for organizations and teams, information assets, business processes. Where terminology is difficult or prone to misinterpretation, the incident management plan should include standard terms and definitions in a glossary.

Roles and relationships with external IRTs and other response organizations, as well as response activity structures and boundaries should be defined by the incident management process owner. Responsibilities of involved parties (see 6.1.2) may overlap, and should be adjusted by consensus in the incident management planning process. Where there is overlap on IR decision boundaries, the plan should identify a responsible party.

Involved parties and external IRTs often have disparate metrics. Planning participants should evaluate the available metrics contributed by their respective parties or external organizations, and either agree by consensus on particular set(s) of existing metrics, or agree to link the disparate metrics using a reversible mapping. Regardless of approach, the plan should select or connect quantitative metrics so that their scopes are identical, and select or connect qualitative metrics with definitive equivalence.

5.12 Review

The incident management review or audit processes should have a defined scope, authorization to operate and report, and assigned sufficient resources in the appropriate roles. The planning framework for review should include at least the following.

- A charter authorizing review with a scope of incident management governance, policy, and planning; and a review cycle coordinated to support both governance requirements and functional efficacy.
- A review template or framework based on past or parallel incident management planning. The framework should address phase completeness; ensuring the process flow includes major phases of detection/reporting, assessment and decision, response, closure (logging and change control), and review.
- Metrics for the constitution of a functional IRT, the team type(s), acceptable role overlaps and duty assignments, stability of the response organization, and competent staffing.
- Response operations records evaluation, including incidents and outcomes. Sufficient information should be present to evaluate correct operation where positive incidents were detected and reported and false positives were correctly identified and handled.
- Response management records evaluation, covering incident management process. Sufficient information should be present to evaluate whether decision-making criteria are stable and consistently applied, documentation and implementation of processes, how deviations are documented, managed, and reconciled with previous criteria and metrics, and whether post-operation activities and reports are verified and under access control.
- Evaluation of exception management, including whether the process is documented and followed, defined categories of incidents (see Part 3 - 8.1-5) match those covered in handling processes, whether proposed additional or alternate incident types are traceable to documented risk, threshold for recurrence or impact past which exceptions should be integrated into standard IR processes.

6 Updating of information security and risk management policies

6.1 Organizational commitment

6.1.1 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.

6.1.2 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 to every employee and contractor, and should also be addressed in information security awareness briefings and training (see Clause 7.2).

6.1.3 Content

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

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

- 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.

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

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

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

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

- Details of where the policy documentation, including procedures, is held.

- An overview of the IRT, encompassing the following topics.

- 1) The IRT organizational structure, and the identity of the IRT manager and other key roles, including who is responsible for

- i) briefing senior management on incidents,

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

- iii) liaising with the external organizations (when necessary).

- 2) The information security management charter that specifies what the IRT 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 IRT's scope, and details of the IRT's board level sponsor and authority.

- i) The IRT mission statement that focuses on the team's core activities. In order to be considered an IRT, 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.

ii) A definition of the scope of the IRT activities. Normally, the scope of an organization's IRT covers all of the organization's information systems, services and networks. In some cases, an organization may require the scope to be different (either larger or narrower), in which case it should be clearly documented what is in, and what is out of, scope.

iii) Identification of a senior executive officer, board member or senior manager who has the authority to make decisions on IRT and also establish the levels of authority for IRT. Knowing this helps all personnel in the organization to understand the background and set-up of the IRT, and it is vital information for building trust in the IRT. 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.

3) Links to organizations providing specific external support, such as forensics teams (see 5.5).

— An overview of the technical and other support mechanisms.

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

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

6.2 Existing policy integration and review

6.2.1 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.

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

— 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.

— To ensure consistency across the various policies.

— 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.

6.2.2 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.

— The relevant sections should refer to the senior management commitment.

— The relevant sections should outline the policy.

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

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

— 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 review 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 the process designed to maintain continuing effectiveness of the policies.

7 Creating information security incident management scheme

7.1 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, incidents and vulnerabilities, and communication of them. The information security incident management scheme comes into effect whenever an information security event is detected, or information security vulnerability is reported. Each organization should use the scheme as a guide for

- responding to information security events,
- determining whether information security events become information security incidents,
- managing information security incidents to conclusion,
- responding to information security vulnerabilities,
- identifying lessons learnt, and any improvements to the scheme and/or security in general that are required, and
- making those identified improvements.

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

7.2 Involved parties

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

- detecting and reporting information security events (this is the responsibility of any permanent or contracted personnel in an organization and its companies);
- 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 IRT, management, public relations personnel and legal representatives); and
- 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.

7.3 Content

Each organization should ensure that the content of the information security incident management scheme documentation includes an overview of the information security incident management policy and an overview of the whole information security incident management scheme.

- 1 The detailed activities, procedures and information, associated with the following.
- 2 — Plan and prepare.
 - 3 1) A standardized approach to information security event/incident categorization and classification, to
4 enable the provision of consistent results. In any event, the decision should be based on the actual or
5 projected adverse impacts on the organization's business operations, and associated guidance.

6 NOTE Annex A shows example approaches to the categorization and classification of information security
7 events and incidents.

8 2) An information security event/incident/vulnerability database structured in standardized formats for
9 the exchange of information, which is likely to provide the capability to share reports/alerts, compare
10 results, improve alert information and enable a more accurate view of the threats to, and
11 vulnerabilities of information systems

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

21 4) Procedures to be followed to ensure that all information security incident management activities are
22 properly logged, and that log analysis is conducted by designated personnel.

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

26 6) Procedures for information security forensics analysis.

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

31 8) Guidance and procedures associated with the technical and organizational mechanisms that are
32 established, implemented and operated in order to prevent information security incident occurrences
33 and to reduce their likelihood, and to deal with information security incidents as they occur.

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

36 10) Procedures and specifications for the testing of the information security incident management
37 scheme.

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

39 12) The terms of reference and responsibilities of the IRT as a whole, and of individual members.

40 13) Important contact information.
- 41 — Detection and reporting.

- 1) Detecting and reporting the occurrence of information security events (by human or automatic means).
- 2) Collecting the information on information security events.
- 3) Detecting and reporting on information security vulnerabilities.
- 4) Fully recording all information gathered in the information security event/incident/vulnerability database.
- Assessment and decision.
 - 1) 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.
 - 2) The IRT assessing information security events should confirm whether an event is an information security incident or not, therefore 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.
 - 3) 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.
 - 4) Fully recording all assessment results and related decisions in the information security event/incident/vulnerability database.
- Responses.
 - 1) Review by the IRT 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.
 - 2) Defining a map of all internal and external functions and organizations that should be involved during the management of an incident.
 - 3) Containing and eradicating the information security incident as appropriate to mitigate or prevent the scope and impact of the incident from increasing.
 - 4) Conducting information security forensics analysis, as required.
 - 5) Escalation, as required.
 - 6) Ensuring that all involved activities are properly logged for later analysis.
 - 7) Ensuring that electronic evidence is identified, collected/acquired and preserved.
 - 8) Ensuring that the change control regime is maintained, and thus that the information security event/incident/vulnerability database is kept up-to-date.

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

10) Dealing with information security vulnerabilities.

11) Once the incident has been successfully dealt with, formally closing it and recording this in the information security event/incident/vulnerability 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 sometime 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.

— Lessons learnt.

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

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

3) 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.

4) 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.

5) 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.

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

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

7.4 Incident classification scale

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 A shows example approaches to the categorization and classification of information security events and incidents.

7.5 Incident forms

Incident forms, if used, should be created before they are needed. The number, type and format of the forms should be determined by the IRT and revised periodically to ensure that they are still relevant. A special 'free-form' form shall exist. Its purpose is to provide mechanism to capture information in instances where existing forms are not sufficient or an appropriate form has not yet been created.

The information security event/incident/vulnerability forms are

- 1 — completed by the person reporting an information security event (i.e. not an information security incident
2 management team member), with the information recorded in an information security
3 event/incident/vulnerability database,
- 4 — used by the information security incident management personnel to build on the initially reported
5 information security event information and enable a running record of the incident assessments, etc. over
6 time until the incident is fully resolved. At each stage, the update is recorded in the information security
7 event/incident/vulnerability database. The completed information security event/incident/vulnerability
8 database record is then used in post-incident resolution activities, and
- 9 — completed by the person reporting an information security vulnerability (that has not yet been exploited to
10 cause an information security event, and possibly an information security incident), with the information
11 recorded in the information security event/incident/vulnerability database.

12 It is recommended that internationally standardized formats for the electronic exchange and input of incident
13 information (e.g. IETF RFC 5070, The Incident Object Description Exchange Format (IODEF) or the Mitre
14 Corporation's Structured Threat Information eXpression language (STIX)) are used, linking directly to the
15 electronic information security event/incident/vulnerability database. A paper-based scheme may be needed
16 for a case where an electronic scheme cannot be used.

17 NOTE Example forms are shown in Annex B of ISO/IEC 27035-3.

18 7.6 Processes and procedures

19 NOTE For brevity purposes we will use term "document" to refer to both processes and procedures in this text unless
20 the distinction between a process and procedure is significant.

21 Before being able to commence operation of the information security incident management scheme, it is
22 important that an organization has documented and checked that necessary processes and procedures are
23 available. Each document should indicate those groups or individuals responsible for its use and management.

24 It is important to understand that not all documents need be readily available either within the organization or
25 to the general public. For example, it is not necessary for all organizational personnel to understand the
26 internal operation of an IRT in order to interact with it. The IRT should ensure that available guidance,
27 including information resulting from information security incident analysis, is in readily available form, e.g. on
28 the organization's intranet and/or public web site as and if appropriate. It may also be important to keep some
29 details of the information security incident management scheme closely held to prevent an insider from
30 tampering with the investigation process. For example, if a bank employee who is embezzling funds is aware
31 of some details how the investigation is being done, he or she may be able to better hide their activities from
32 investigators or otherwise hamper the detection, investigation of and recovery from an information security
33 incident.

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

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

- 45 — the reporting process for the handling of such exceptions;
- 46 — guidance on the timing for getting approval from management in order to avoid any delay of response;
47 and

- 1 — pre-authorized delegation of decision making without normal approval process.
- 2 Operating procedures for the IRT, with documented processes and associated responsibilities, and the
- 3 allocation of roles to designated persons to conduct various activities (an individual may be allocated more
- 4 than one role, depending on the size, structure and business nature of an organization), for example including
- 5 — shutting down an affected system, service and/or network, in certain circumstances agreed by prior
- 6 arrangement with the relevant IT and/or business management,
- 7 — leaving an affected system, service and/or network, connected and running,
- 8 — monitoring data flowing from, to and within an affected system, service and/or network,
- 9 — activating normal back-up and crisis management procedures and actions in line with the system, service
- 10 and/or network security policy,
- 11 — monitoring and maintain the secure preservation of electronic evidence, in case it is required for legal
- 12 prosecution or internal disciplinary action, and
- 13 — communicating information security incident details to internal and external people or organizations.

14 **7.7 Trust and confidence**

15 The IRT plays a crucial role for the overall information security of an organization. The IRT requires the
 16 collaboration of all organizational personnel to detect, resolve and investigate information security incidents. It
 17 is fundamental that the IRT is trusted by the whole organization and that external entities have confidence in it.
 18 The trust within the organization is created by fiat and stems from the support given by the higher
 19 management – i.e. the trust is given. External entities that have to deal with the IRT (e.g., IRTs from other
 20 organizations) need to be confident that the IRT will perform its job professionally – i.e. the trust must be
 21 earned.

22 The IRT can earn trust through transparency and mature processes. The IRT should work to educate users
 23 (internal and external), explain how the IRT works, how it protects confidentiality of information collected and
 24 how it manages users' event, incident and vulnerability reports. The IRT should document and publicise
 25 provisions that clearly illustrate the expectation of anonymity, or lack thereof, for persons or parties reporting a
 26 potential information security incident or vulnerability.

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

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

35 **7.8 Confidentiality**

36 An information security incident management scheme may contain sensitive information, and people involved
 37 in addressing incidents and vulnerabilities may be required to handle sensitive information. An organization
 38 should ensure that the necessary processes and capabilities are established to anonymize sensitive
 39 information when required (e.g., when leaving the protective domain of the IRT) and require personnel with
 40 access to sensitive information to sign confidentiality agreements. If information security
 41 events/incidents/vulnerabilities are logged via a generalized problem management system where it is not
 42 possible to restrict who has access to it, sensitive details may have to be omitted. Give that the IRT would still
 43 have to have access to the omitted information this can lead to a situation where the IRT will maintain its own
 44 incident management database. 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.

8 Establishing an Incident Response Team (IRT)

8.1 Establishment

8.1.1 Introduction

The aim of establishing the IRT 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 IRT 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.

8.1.2 Members and structure

The size, structure and composition of an IRT should be appropriate for the size, structure, and the business nature of the organization. Although the IRT 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 IRT should guide the organization in this choice.

The IRT goes through different maturity stages and often adjustments to the organizational model are adopted based on the specific scenarios faced by the organization. Whenever justified, it is recommended to have a permanent team. The IRT (permanent or virtual) should be led by a senior manager who should be supported by individuals who are specialized in particular topics (e.g., 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 team member may also fulfil more than one role within the IRT. The IRT, both permanent and virtual, will always require support of individuals from different parts of the organization (e.g. business operations, ICT, audit, legal, press relations, human resources and marketing). Which parts of the organization will be engaged depends on the nature of the incidents that are being handled.

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 documentation, including any procedural documents, and the reporting forms, but not in the policy document.

The IRT manager should have a direct line of reporting to senior management which may be separate from normal business operations. The manager should have delegated authority (by the senior management) to make immediate decisions on how to deal with an incident. The IRT manager should assign investigation of each incident to the most appropriate member of his/her team, with each incident assigned a named manager.

8.1.3 Relationship with other parts of the organization

The IRT should have the responsibility for ensuring that incidents are resolved, and in this context the IRT manager and members of the 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 IRT manager reports serious information security incidents. The authority, on its part, should make commitment to make itself available to IRT members and deliver its guidance in a timely fashion.

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 IRT.

8.1.4 Relationship with external interested parties

Organizations should establish relationships between the IRT and appropriate external interested parties. External interested parties may include (but are not limited to) the following:

- contracted external support personnel;
- external organizations' IRTs;
- managed service providers, including telecommunication service providers, ISPs, vendors and suppliers;
- law enforcement organizations;
- emergency authorities;
- appropriate government organizations;
- legal personnel;
- public relations officials and/or members of the media;
- business partners;
- customers; and
- the general public.

9 Defining technical and other support

9.1 Introduction

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 linkage 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 demonstrably secure;
- e) the use of a standard format and exchange protocol to receive and process alerts or information on events/incidents/vulnerabilities to inform situational awareness of the information security operating environment, allowing for risk-based and proactive remediation;
- f) facilities for information security/digital forensics evidence collection and analysis; and

g) adequate crisis management arrangements for the information security event/incident/vulnerability database (for guidance on business continuity management see ISO/IEC 27031 and ISO/PAS 22399).

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:

- h) quick acquisition of information security event/incident/vulnerability reports;
- i) 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;
- j) 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);
- k) ensuring the collection of all data about the information system, service and/or network, and all data both stored and processed appropriately;
- l) 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;
- m) 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);
- n) 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;
- o) 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:
 - backup testing;
 - malicious code control;
 - original media with system and application software;
 - bootable media; and
 - 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 subclause 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.

9.2 Examples of technical support

Such mechanisms could include the following.

- Internal information security audit mechanisms to assess the security level and track vulnerable systems.
- Vulnerability management (including security updates and security patching of vulnerable systems).
- Technology watch to detect new kinds of threats and attacks.
- Intrusion Detection Systems (for more details, see ISO/IEC 18043).
- Network security devices, protections means and monitoring tools (for more details, see ISO/IEC 27033).
- Anti-malicious code software.
- Audit log records, and log monitoring software.

9.3 Examples of other support

Such mechanisms could include the following.

- Documented responsibilities and operating procedures for the operations support team.

10 Creating information security incident 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, IRT 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 IRT 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.

11 Testing the information security incident management scheme

11.1 Introduction

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, incidents and vulnerabilities. Periodic tests should be organized to check processes/procedures and to verify the IRT responses. These simulated scenarios can range from severe, complex incidents based on realistic attacks, failures or faults to table top exercises. The format of the simulation will depend on the pre-defined goals of the exercise. Tests can involve not only the IRT, but also some or all 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.

When conducting an exercise it is very important that all involved are aware that they are not dealing with the real attack. It is important to establish and maintain this difference to prevent people from triggering actions that might have much larger implications to the organization (e.g., initiate building evacuation). This rule can be ignored only under special circumstances when the exercise is performed within strictly controlled environment that prevents the effects of the exercise to 'spill over' into the operational environment.

Generally speaking we can distinguish the following main types of exercises:

- discussion-based;

1 — tabletop;

2 — live;

3 — combination of the above.

4 Which type of the exercise will be used depends on the goal that wants to be achieved but also available time
5 and resources.

6 Every exercise is going through the following phases:

7 — planning and preparation;

8 — execution;

9 — debrief and post-mortem analysis.

10 Planning and preparation of an exercise is based on the current incident response plans and envisaged future
11 threats and trends. The results of the post-mortem analysis are used as input to improvement of the incident
12 response plans.

13 11.2 Exercise

14 11.2.1 Defining the goal of the exercise

15 Generally speaking an exercise can have three main goals:

16 a) validation - to validate incident response plans and identify potential omissions;

17 b) training - to allow people to practice their roles and make them comfortable executing them;

18 c) testing - to test the currently existing processes and procedures.

19 It is common that an exercise have more than goal. The goal of an exercise is in good part determined by the
20 overall state of preparedness of the organization. When an organization is preparing new incident response
21 plans or updating the existing ones it can use exercises to validate them. After the plans were made and put in
22 place, the organization will use exercises to train the people. After the existing processes and procedures are
23 well established they need to be periodically tested to ensure that they are still valid.

24 Table 1 is given as guidance on what types of the exercises can be used to achieve which goal(s).

25 **Table 1 – Mapping exercise goals to the exercise types**

Goal	Type of an exercise
Validating new plans	discussion-based; tabletop
Training people	discussion-based; tabletop; live
Verifying if the existing plans are still valid	tabletop; live

26

11.2.2 Defining the scope of an exercise

The scope of an exercise is mainly defined by its goals. When defining the scope of an exercise the following items need to be considered:

The goals have direct influence on which organizations will be represented at the exercise and profile of the participants.

11.2.3 Conducting an exercise

When conducting an exercise it is very important that all involved are aware that the scenario being handled is an exercise and not a real event. If participants are unable to distinguish simulated from the real events there is potential that they will trigger actions with wider consequences or involve people outside of the exercise. In the worst case scenario this may lead to panic in general public.

There are number of tasks that need to be accomplished in order to conduct a successful exercise. The following list provides only a general overview of the main tasks:

- at the beginning brief participants on the exercise goals;
- ensure safety and security of all participants (this is especially important with live exercises where volunteers are used);
- make sure that all participants know their roles;
- ensure that sufficient number of people are available to lead participants through the exercise;
- sufficient time must be allocated to discussion during the exercise but not excessive amount to derail the exercise;
- allow sufficient time and resources to debrief all participants after the exercise and collect their feedback (note that the feedback will be twofold: what was the object of the exercise and how the exercise itself was conducted);
- create and distribute exercise reports to the stakeholders.

11.3 Incident Response Capability Monitoring

11.3.1 Implementing an incident response capability monitoring program

Incident response capabilities encompasses not only capabilities of the incident response team but also capabilities of individuals and groups that IRT may ask for help during the incident handling. While most of the incident response capabilities will be concentrate within the IRT it is possible that it may lack specialist knowledge in certain narrow areas. For that reason the IRT may engage individuals or other teams who can fill this void.

By monitoring characteristics of incidents and frequency by which these characteristics occurs in incidents it is possible to develop a picture of what capabilities the IRT need to possess. These capabilities will change over time. Some changes will happen because technology within the organization will change by either abandoning it or introducing new one. An example of the abandoning a technology might be moving all data from SQL databases to non-SQL databases. Allowing employees to use mobile telephones to perform their tasks is an example of introducing a new technology that previously did not existed within the organization. Another reason that may require change in the IRT capabilities is development of new attack techniques.

Not all capabilities are technical in nature. Some threats, especially ones that do not rely on technology, are best addressed with non-technical means (e.g., social engineering).

11.3.2 Metrics and governance of incident response capability monitoring

The IRT capabilities must be adequate to address the current threats facing the organization. As the threats change so the team capabilities has to change so that the organization can effectively respond to the new threats. At the same time some capabilities may no longer be needed as the threats are either permanently reduced to negligible levels or the underlying reason for the risk has been removed. Additionally, while the IRT must be the focal centre of the expertise and the main bearer of incident handling capabilities, it is not required that it possess all of them. Rarely used expertise and capabilities may be distributed among different individuals or groups either within or outside of the organization. The main reason for this is cost effectiveness.

With such distribution of capabilities and changing needs the organization should establish a register that would reflect organization current capabilities. The following non-exhaustive list illustrates what information may be contained in this register:

- what capabilities are available to the organization;
- who possesses them;
- are they internal or external to the organization;
- how to engage the bearer of the capability;
- how current is the capability (or its proxy measure when it was last used);
- how often the capability was required in the past time interval.

This information is then used in the planning of development of IRT capabilities. Rarely used capabilities may be left to lapse and often used capabilities not currently present within the IRT may be gained and so on.

12 Lesson Learnt

12.1 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 after handling 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 learnt can result in one or more of the following outcomes.

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

- identify trends/patterns;
- identify areas of concern; and
- 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, other IRTs 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.

12.2 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 IRT, in conjunction with the organization's information security manager, to ensure that these information security policy and procedural updates are propagated throughout the organization.

12.3 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).

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

Post-incident resolution, the IRT 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.

- Did the procedures outlined in the information security incident management scheme work as intended?
- Are there any procedures or methods that would have aided in the detection of the incident?
- Were any procedures or tools identified that would have been of assistance in the response process?
- Were there any procedures that would have aided in recovering information systems following an incident identified?
- 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.

12.5 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 acted upon.

Annex A (informative)

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

A.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.

Related work can be found in:

- RFC5070 Incident Object Description Exchange Format (IODEF);
- RFC6545 Real-time Intern-network Defence (RID);
- RFC6546 Transport of Real-time Intern-network Defence;
- Mitre's Structured Threat Information eXpression (STIX);
- Mitre's Trusted Automated eXchange of Indicator Information (TAXII).

A.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 A.1.

Table A.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.

Category	Description	Examples
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.
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.

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.	<p>Network scanning, exploitation of vulnerability, exploitation of backdoor, login attempts, interference, DoS, etc.</p> <p>Network scanning makes use of network scanning software to acquire information about network configurations, ports, services and existing vulnerabilities.</p> <p>Exploitation of vulnerability exploits and makes use of information system defects such as configurations, protocols or programs.</p> <p>Exploitation of backdoor makes use of the backdoors or harmful programs left in software and hardware system design processes.</p> <p>Login attempts try to guess, crack or brute force passwords.</p> <p>Interference obstructs computer networks, wired or wireless radio and television transmission networks, or satellite radio and television signals, through technical means.</p> <p>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.</p>
Breach of rule incident	The loss of information security is caused by breaching rules deliberately or accidentally.	<p>Unauthorized use of resources, breach of copyright, etc.</p> <p>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.</p> <p>Breach of copyright is caused by selling or installing copies of unlicensed commercial software or other copyright protected materials, for example, warez.</p>
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.	<p>Abuse of rights, forging of rights, denial of actions, mis-operations, breach of personnel availability, etc.</p> <p>Abuse of rights uses rights beyond the terms of reference.</p> <p>Forging of rights makes false rights in order to deceive.</p> <p>Denial of actions is when someone's denies what he/she has done.</p> <p>Mis-operations carry out operations incorrectly or unintentionally.</p> <p>Breach of personnel availability is caused by the lack or absence of human resources.</p>

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.	<p>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.</p> <p>Interception captures data before it is able to reach the intended recipients.</p> <p>Spying is to secretly collect and report information about the activities of another organization.</p> <p>Eavesdropping is to listen in on an external party's conversation without their knowledge.</p> <p>Disclosure is to make sensitive information known publicly.</p> <p>Masquerade is when one entity pretends to be another.</p> <p>Social engineering is to gather information from a human being in a non-technical way, for example, lies, tricks, bribes, or threats.</p> <p>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.</p> <p>Theft of data is to steal data.</p> <p>Tampering with data is to touch or make changes to data without authorization.</p> <p>Data error is to make mistakes when inputting or processing data.</p> <p>Position detection is to detect the position of sensitive information or systems.</p>
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.	<p>Illegal content, panic content, malicious content, abusive content, etc.</p> <p>Illegal content is published content that violate national or international constitutions, laws and regulations, for example, child pornography, violence glorification, counterfeit, fraud.</p> <p>Panic content is the maliciously sensationalized discussion or comment on sensitive issues on the Internet, resulting in events such as social turbulence or panic.</p> <p>Malicious content is the spreading of content that maliciously attacks society or persons, for example, hoax, harassment.</p> <p>Abusive content are the broadcasting of content that have not been granted by recipients, for example, spam.</p>
<i>Other Incidents</i>	Not categorized in any of the above incident category.	

A.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 and they can be modified to suit the needs of the business. There are others, such as the FIRST Common Vulnerability Scoring System (CVSS) and the UK government Structured Warning Information Format (SWIF).

A.3.1 Example approach 1

A.3.1.1 Classification factors

A.3.1.1.1 Introduction

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

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

A.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.

A.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.

- 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.
- 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.
- 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.

— 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.

A.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.

— 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.

— 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.

— 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.

— 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.

A.3.1.2 Classes

A.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.

1 **A.3.1.2.2 Very serious (Class IV)**

2 Very serious incidents are those that

- 3 — act on especially important information systems, and
- 4 — result in especially serious business loss, or
- 5 — lead to especially important social impact.

6 **A.3.1.2.3 Serious (Class III)**

7 Serious incidents are those that

- 8 — act on especially important information systems or important information systems, and
- 9 — result in serious business loss, or
- 10 — lead to important social impact.

11 **A.3.1.2.4 Less Serious (Class II)**

12 Less serious incidents are those that

- 13 — act on important information systems or ordinary information systems, and
- 14 — result in considerable business loss, or
- 15 — lead to considerable social impact.

16 **A.3.1.2.5 Small (Class I)**

17 Small incidents are those that

- 18 — act on ordinary important information systems and
- 19 — result in minor business loss or no business loss, and c) lead to minor social impact or no social impact
- 20 — no action required and no consequences.

21 **A.3.1.3 Incident category and severity class**

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

- 25 — intentional,
- 26 — targeted,
- 27 — timing, and
- 28 — volume.

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

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

Incident Category	Severity class	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

A.3.2 Example approach 2

A.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.

A.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.

- a) Result in financial losses/costs of x_1 or less.
- b) Result in financial losses/costs of between x_1+1 and x_2 .
- c) Result in financial losses/costs of between x_2+1 and x_3 .
- d) Result in financial losses/costs of between x_3+1 and x_4 .
- e) Result in financial losses/costs of between x_4+1 and x_5 .
- f) Result in financial losses/costs of between x_5+1 and x_6 .
- g) Result in financial losses/costs of between x_6+1 and x_7 .
- h) Result in financial losses/costs of between x_7+1 and x_8 .
- i) Result in financial losses/costs of more than x_8 .
- j) The organization will go out of business.

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

A.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.

- a) Be of interest to a competitor but of no commercial value.
- b) Be of interest to a competitor to a value that is y_1 or less (turnover).
- c) 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.
- d) Be of value to a competitor to a value that is between y_2+1 and y_3 (turnover).
- e) Be of value to a competitor to a value that is between y_3+1 and y_4 (turnover).
- f) Be of value to a competitor to a value that is more than y_4+1 (turnover).

1 g) No entry¹.

2 h) No entry.

3 i) Could substantially undermine commercial interests, or substantially undermine the financial viability of
4 the organization.

5 j) No entry.

6 Where, y_i ($i = 1, 2, \dots, 4$) represent the values to a competitor in terms of turnovers in four grades/levels which
7 are determined by the organization in its context.

8 **A.3.2.4 Personal information**

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

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

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

21 c) A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of
22 information, leading to minor embarrassment to an individual.

23 d) A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of
24 information, leading to significant embarrassment to an individual or minor embarrassment to a group of
25 individuals.

26 e) A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of
27 information, leading to serious embarrassment to an individual.

28 f) A breach in a legal, regulatory or ethical requirement or publicized intention on the protection of
29 information, leading to serious embarrassment to a group of individuals.

30 g) No entry.

31 h) No entry.

32 i) No entry.

33 j) No entry.

34 **A.3.2.5 Legal and regulatory obligations**

35 Data held and processed by an organization may be subject to, or held and processed in order to allow an
36 organization to comply with legal and regulatory obligations. Failure to comply with such obligations, either
37 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.

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

3 a) No entry.

4 b) No entry.

5 c) Enforcement notice, civil suit or criminal offence resulting in financial damages/penalty of z_1 or less.

6 d) Enforcement notice, civil suit or criminal offence resulting in financial damages/penalty of between z_1+1
7 and z_2 .

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

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

12 g) Enforcement notice, civil suit or criminal offence resulting in unlimited financial damages/penalty, or a
13 prison term in excess of ten years.

14 h) No entry.

15 i) No entry.

16 j) No entry.

17 **A.3.2.6 Management and business operations**

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

24 a) Inefficient operation of one part of an organization.

25 b) No entry.

26 c) Undermine the proper management of the organization and its operation.

27 d) No entry.

28 e) Impede the effective development or operation of the organization's policies.

29 f) Disadvantage the organization in commercial or policy negotiations with others.

30 g) Seriously impede the development or operation of major organizational policies, or shut down or
31 otherwise substantially disrupt significant operations.

32 h) No entry.

33 i) No entry.

34 j) No entry.

1 **A.3.2.7 Loss of goodwill**

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

5 a) No entry.

6 b) Cause local embarrassment within the organization.

7 c) Adversely affect relations with shareholders, customers, suppliers, employees, third party users,
8 regulatory bodies, the government, other organizations or the public, resulting in local/regional adverse
9 publicity.

10 d) No entry.

11 e) Adversely affect relations with shareholders, customers, suppliers, employees, third party users,
12 regulatory bodies, the government, other organizations or the public, resulting in some national adverse
13 publicity.

14 f) No entry

15 g) Materially affect relations with shareholders, customers, suppliers, employees, third party users,
16 regulatory bodies, the government, other organizations or the public, resulting in widespread adverse
17 publicity.

18 h) No entry.

19 i) No entry.

20 j) No entry.

Annex B (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 Fulfilment 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 IRT, 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 IRT, 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.

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

1

Bibliography

- 2 [1] ISO/IEC 27001, *Information technology — Security techniques — Information security management*
3 *systems — Requirements*
- 4 [2] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information*
5 *security management*
- 6 [3] ISO/IEC 27005, *Information technology — Security techniques — Information security risk*
7 *management*
- 8 [4] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and*
9 *communication technology readiness for business continuity*
- 10 [5] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1:*
11 *Overview and concepts*
- 12 [6] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2:*
13 *Guidelines for the design and implementation of network security*
- 14 [7] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3:*
15 *Reference networking scenarios — Threats, design techniques and control issues*
- 16 [8] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4:*
17 *Securing communications between networks using security gateways — Threats, design techniques*
18 *and control issues*
- 19 [9] Internet Engineering Task Force (IETF) Site Security Handbook,
20 <http://www.ietf.org/rfc/rfc2196.txt?number=2196>
- 21 [10] Internet Engineering Task Force (IETF) RFC 5070, The Incident Object Description Exchange Format,
22 <http://www.ietf.org/rfc/rfc5070.txt?number=5070>
- 23 [11] Mitre Corporation. STIX, Structured Threat Information eXpression, <https://stix.mitre.org/>
- 24 [12] Mitre Corporation. Trusted Automated eXchange of Indicator Information. <http://taxii.mitre.org/>
- 25 [13] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Incident Management
26 Capability Metrics Version 0.1 (2007), <http://www.cert.org/archive/pdf/07tr008.pdf>
- 27 [14] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Incident Management
28 Mission Diagnostic Method Version 1.0, <http://www.cert.org/archive/pdf/08tr007.pdf>
- 29 [15] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Defining Incident
30 Management Processes for CSIRTs: A Work in Progress, <http://www.cert.org/archive/pdf/04tr015.pdf>
- 31 [16] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Handbook for
32 Computer Security Incident Response Teams (CSIRTs), [http://www.cert.org/archive/pdf/csirt-](http://www.cert.org/archive/pdf/csirt-handbook.pdf)
33 [handbook.pdf](http://www.cert.org/archive/pdf/csirt-handbook.pdf)
- 34 [17] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, State of the Practice
35 of Computer Security Incident Response Teams, <http://www.cert.org/archive/pdf/03tr001.pdf>
- 36 [18] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, CSIRT Services,
37 <http://www.cert.org/csirts/services.html>

- 1 [19] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Action List for
2 Developing a Computer Security Incident Response Team (CSIRT),
3 http://www.cert.org/csirts/action_list.html
- 4 [20] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Staffing Your
5 Computer Security Incident Response Team – What Basic Skills Are Needed?
6 <http://www.cert.org/csirts/csirt-staffing.html>
- 7 [21] Software Engineering Institute at Carnegie Mellon “CERT Coordination Centre”, Steps for Creating
8 National CSIRTs, <http://www.cert.org/archive/pdf/NationalCSIRTs.pdf>