~~ISO/IEC JTC 1/SC 27/WG 4 N~~

Date: 2022-~~06-11~~09-22

ISO/IEC ~~DIS~~ FDIS 27035-~~1~~-2:2022(E)

~~ISO/IEC JTC 1/SC 27/WG 4~~

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: ILNAS

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

Style Definition: Base_Text: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Style Definition: List Continue 1

Style Definition: List Continue 5: Font: Indent: Hanging: 20.15 pt, Don't add space between paragraphs of the same style, Line spacing: At least 12 pt

Style Definition: List Number: Indent: Left: 0 pt, Hanging: 20 pt, No bullets or numbering

Style Definition: List Number 1: Tab stops: Not at 20.15 pt

Style Definition: RefNorm

Style Definition: MTEquationSection: Not Hidden

Style Definition: TOC Heading

Style Definition: Body Text_Center

Style Definition: Code: Tab stops: 16.15 pt, Left + 32.6 pt, Left + 48.75 pt, Left + 65.2 pt, Left + 81.35 pt, Left + 97.8 pt, Left + 113.95 pt, Left + 130.4 pt, Left + 146.55 pt, Left + 162.75 pt, Left

Style Definition: Dimension_100

Style Definition: Figure Graphic

Style Definition: Figure subtitle

Style Definition: List Continue 2 (-): Indent: Left: 19.5 pt, Hanging: 40.5 pt, Space After: 12 pt

Style Definition: 未处理的提及

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Font: Not Bold

Formatted: Font color: Black

Formatted: Font: 12 pt, Font color: Black

Formatted

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: Font: 11 pt, Not Bold, English (United Kingdom)

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Contents

Page

Formatted: Font: Not Bold
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted Table
Formatted: English (United Kingdom)
Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: Font: 11 pt, Not Bold, English (United Kingdom)

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: English (United Kingdom)

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: Font: 11 pt, Not Bold, English (United Kingdom)

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Foreword

ISO (the International Organization for Standardization) ~~is a~~and IEC (the International Electrotechnical Commission) form the specialized system for worldwide ~~federation of national standards~~standardization. National bodies ~~(~~that are members of ISO ~~member bodies). The work of preparing~~or IEC participate in the development of International Standards ~~is normally carried out~~ through ~~ISO~~ technical committees. ~~Each member body interested in a subject for which a technical committee has been~~ established ~~has the right to be represented on that committee. International~~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. ~~ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.~~

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ~~ISO documents~~document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see ~~www.iso.org/directives~~www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see ~~www.iso.org/patents~~www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT~~), see www.iso.org/iso/foreword.html~~) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27035-2:2016), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— new roles including incident management team and incident coordinator and their responsibilities have been added;

— content related to vulnerability management has been modified;

— content on a recommended process for organizations has been added in 6.7;

Formatted: Line spacing: At least 15.5 pt
Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_publisher
Formatted: std_docNumber
Formatted: English (United Kingdom)
Formatted: Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Cambria, English (United Kingdom)
Formatted: List Continue 1, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: cite_sec
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted Table
Formatted: English (United Kingdom)
Formatted: Font: 11 pt, English (United Kingdom)

— Clause 7 structure has been reorganized;

— ~~Annex~~ C.3 has been replaced by a single paragraph;

— bibliography has been updated;

— document has been aligned with the ISO/IEC Directives Part 2, 2021.

A list of all parts in the ISO/IEC 27035 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at ~~www.iso.org/members.html~~www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: cite_sec
Formatted: cite_sec
Formatted: cite_sec
Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted Table
Formatted: Font: 11 pt, Not Bold, English (United Kingdom)
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Introduction

This document focuses on information security incident management which is identified in ISO/IEC 27000 as one of the critical success factors for the information security management system.

There can be a large gap between an organization's plan for an incident and an organization's preparedness for an incident. Therefore, this document addresses the development of procedures to increase the confidence of an organization's actual readiness to respond to an information security incident. This is achieved by addressing the policies and plans associated with incident management, as well as the process for establishing the incident response team and improving its performance over time by adopting lessons learned and by evaluation.

Formatted: Default Paragraph Font

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: English (United Kingdom)

Formatted: Font: 11 pt, English (United Kingdom)

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

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

1 Scope

This document provides guidelines to plan and prepare for incident response and to learn lessons from incident response. The guidelines are based on the "plan and prepare" and "learn lessons ~~learned~~" phases of the information security incident management phases model presented in ISO/IEC 27035-1:—[1], 5.2 and 5.6.

The major points within the "plan and prepare" phase include:

— information security incident management policy and commitment of top management;

— information security policies, including those relating to risk management, updated at both organizational level and system, service and network levels;

— information security incident management plan;

— Incident Management Team (IMT) establishment;

— establishing relationships and connections with internal and external organizations;

— technical and other support (including organizational and operational support);

— information security incident management awareness briefings and training.

The "learn lessons ~~learned~~" phase includes:

— identifying areas for improvement;

— identifying and making necessary improvements;

— Incident Response Team (IRT) evaluation.

[1] Under preparation. Stage at the time of publication: ISO/IEC/~~DIS~~FDIS 27035-1:2022.

Formatted: Line spacing: Exactly 11 pt
Formatted Table
Formatted: Default Paragraph Font
Formatted: std_year
Formatted: Default Paragraph Font
Formatted: cite_section
Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: Body Text
Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt, English (United Kingdom)
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted Table
Formatted: Font: 11 pt, English (United Kingdom)
Formatted: Font: 11 pt, Not Bold, English (United Kingdom)

The guidance given in this document is generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this document according to their type, size and nature of business in relation to the information security risk situation. This document is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 27035-1:[2,1)] *Information technology — Information security incident management — Part 1: Principles and process*

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 ISO/IEC 27035-1 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.2 Abbreviated terms

CERT	computer emergency response team
CSIRT	computer security incident response team
IMT	Incident Management Team
IRT	Incident Response Team
PoC	Point of Contact

4 Information security incident management policy

4.1 General

NOTE Clause 4, in its entirety, links to ISO/IEC 27035-1:[3,1)] 5.2 a).

[2] Under preparation. Stage at the time of publication: ISO/IEC/DIS 27035-1:2022.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Default Paragraph Font

Formatted: std_year

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: English (United Kingdom)

Formatted: Font: Cambria, 11 pt, English (United Kingdom)

Formatted: No underline, Font color: Auto, English (United Kingdom)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: English (United Kingdom)

Formatted: Default Paragraph Font, English (United Kingdom)

Formatted: No underline, Font color: Auto, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Default Paragraph Font, English (United Kingdom)

Formatted: Body Text

Formatted: Body Text

Formatted: Body Text

Formatted: Body Text

Formatted: Body Text

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Default Paragraph Font

Formatted: std_year

Formatted: cite_section

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: English (United Kingdom)

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Font: 11 pt, English (United Kingdom)

An ~~organization~~organization's information security incident management policy should provide the formally documented principles and intentions used to direct decision-making. Supporting processes and procedures- ensures consistent application of the policy.

Any information security incident management policy should be part of the information security strategy for an organization. It should also support the existing mission of its parent organization and be in line with already existing policies and procedures.

An organization should implement an information security incident management policy that outlines the processes, responsible persons, authority and reporting lines when an information security event/incident occurs. The policy should be reviewed regularly to ensure it reflects the latest organizational structure, processes, and technology that can affect incident management. The policy should also outline any awareness and training initiatives within the organization that ~~is~~are related to incident management (see Clause 10).

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 ISO/IEC 27001~~:2013~~:—[4], 5.2), or as part of its information security policies (see ISO/IEC 27002:2022, 5.1). The size, structure and business nature of an organization and the extent of its information security incident management ~~program~~programme are deciding factors in determining which of these options to adopt. An organization should direct its information security incident management policy at every person having legitimate access to its information systems and related locations.

Before the information security incident management policy is formulated, the organization should identify the following regarding its information security incident management:

a) principles, objectives and purpose;

b) the scope, including not only which parts of the organization it applies to, but also what information it applies to e.g. hardcopy, electronic, verbal;

c) internal and external interested parties;

d) specific incident types and vulnerabilities that are controlled, responded to and resolved;

e) any specific roles that are involved;

f) benefits to the whole organization and to its departments;

g) understanding of its legal and regulatory environment;

h) dependencies including alignment to risk management;

i) skills and competency requirements.

4.2 Interested parties

A successful information security incident management policy should be created and implemented as an enterprise-wide process. To that end, all interested parties or their representatives should be involved in the development of the policy from the initial planning stages through to the implementation of any process or response team. This may include legal advisors, public relations and

~~[3] Under preparation. Stage at the time of publication: ISO/IEC/DIS 27035-1:2022.~~

[4] Under preparation. Stage at the time of publication ISO/IEC FDIS 27001:2022.

Formatted: Right
Formatted: Footnote re, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Body Text Char
Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: Font: 11 pt, English (United Kingdom)
Formatted Table
Formatted: Font: 11 pt, English (United Kingdom)
Formatted: Font: 11 pt, English (United Kingdom)
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Font: 11 pt, Not Bold, English (United Kingdom)
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

marketing staff, departmental managers, security staff, ICT responsible persons, upper-level management, and, in some cases, even facilities and human resources staff.

An organization should ensure that its information security incident management policy is approved by top management.

Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. It is important that personnel recognize an event, know what to do and understand the benefits of the approach by the organization. It is also important that management is supportive of the information security incident management policy to ensure that the organization commits to resourcing and maintaining an incident management capability.

The information security incident management policy should be made available to every employee and contractor ~~and.~~ It should also be addressed in information security awareness briefings and training.

4.3 Information security incident management policy content

The information security incident management policy should be high-level. Detailed information and step-by-step instructions should be included in the series of documents that make up the information security incident management plan, which is outlined in Clause 6.

An organization should ensure that its information security incident management policy content addresses, but is not limited to, the following topics:

a) the purpose, objectives and the scope (to whom it applies and under what circumstances) of the policy;

b) policy owner and review cycle;

c) the importance of information security incident management to the organization ~~and,~~ top management's commitment to it and the related plan documentation;

d) a definition of security incident;

e) a description of the type of security incidents or categories (or a reference to another document which describes this in more depth);

f) a description of how incidents should be reported, including what to report, the mechanisms used for reporting, where and to whom to report;

g) a high-level overview or visualization of the incident management process flow (showing the basic steps for handling a security incident) encompassing detection and reporting, assessment and decision, response and lessons learned;

h) a requirement for post information security incident resolution activities, including learning from and improving the process, following the resolution of information security incidents;

i) if appropriate, also a summary of reporting and handling vulnerabilities that are related to incident (although this can be a separate document);

j) ~~Defined~~a defined set of roles, responsibilities, and decision-making authority for each phase of the information security incident management process and related activities (including reporting and handling vulnerabilities that are related to incident if appropriate);

k) ~~A~~a reference to the document describing the event and incident classification, severity ratings (if used) and related terms;

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted Table

Formatted: English (United Kingdom)

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Font: 11 pt, English (United Kingdom)

l) ~~An~~an overview of the IMT, encompassing the IMT organizational structure, key roles, responsibilities, and authority, along with summary of duties including, but not limited to:

   1) reporting and notification requirements related to incidents that have been confirmed~~;~~.

   2) dealing with enquiries, instigating follow-up, and resolving incidents~~;~~.

   3) liaising with the external organizations (when necessary~~);~~).

   4) requirement and rationale for ensuring all information security incident management activities performed by the IRT are properly logged for later analysis~~;~~.

m) ~~Requirements~~requirements for establishing/terminating IRTs to respond to specific incidents which have different scopes and expertise depending on the incident. Several IRTs may exist, depending on the aspect of business that is affected by the incident;

n) ~~A~~a requirement that components across the organization work in collaboration to detect, analyse, and respond to information security incidents;

o) ~~A~~a description of any oversight or governance structure and its authority and duties, if applicable;

p) ~~Links~~links to organizations providing specific external support such as forensics teams, legal counsel, other IT operations, etc;

q) ~~A~~a summary of the legal and regulatory compliance requirements or mandates associated with information security incident management activities (for more details, see Annex A).

There are other related policies or procedures that support the information security incident management policy and can also be established as part of the preparation phase, if they are not already existent~~,~~ and are appropriate for the organization. These include, but are not limited to, the following:

— An information security incident management plan, described in Clause 6;

— A continuous monitoring policy for specific ICT systems stating that such activity is conducted by the organization and describing the basic monitoring tasks. Continuous monitoring ensures preservation of electronic evidence in case it is required for legal prosecution or internal disciplinary action;

— Authority granting the IRT access to the outputs of this monitoring or the ability to request logs as needed from other parts of the ~~organisation~~organization (this can also be put in the information security incident management policy);

— Information sharing, disclosure and communication policies which outline how and when information related to incident management activities can be shared by whom and with whom. 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. Apart from the legal requirements, it is expected that information ~~should~~ also ~~follow~~follows any organizational requirements for disclosure, according to the classification policy and ~~in accordance~~according to ISO/IEC 27002:2022, 5.14. It may be important to share information in the course of incident handling when a third party is involved or modified. The scope, circumstances and purpose of this information sharing are described, or referenced, in the appropriate policies and procedures. An example of information disclosure guidance and markings is the use of traffic light protocol (TLP) (~~See~~see ISO/IEC 27010);

Formatted: Right
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_year
Formatted: std_section
Formatted: std_publisher
Formatted: std_docNumber
Formatted: Font: 11 pt, English (United Kingdom)
Formatted Table
Formatted: Font: 11 pt, English (United Kingdom)
Formatted: Font: 11 pt, English (United Kingdom)
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Font: 11 pt, Not Bold, English (United Kingdom)
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt