FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27035-2

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

Secretariat: **DIN**

Voting begins on:
2022-10-25

Voting terminates on:
2022-12-20

Information technology — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

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.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 27035-2:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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 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 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) 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. 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;
- Clause 7 structure has been reorganized;
- 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 and www.iec.ch/national-committees.

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.

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" 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" phase includes:

— identifying areas for improvement;

— identifying and making necessary improvements;

— Incident Response Team (IRT) evaluation.

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*

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

ISO/IEC 27035-1:—[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:— [1], 5.2 a).

An 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 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:—[2], 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 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.

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

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 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. 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, 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) 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 reference to the document describing the event and incident classification, severity ratings (if used) and related terms;

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

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

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

q) 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 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 also follows any organizational requirements for disclosure, according to the classification policy and 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 ISO/IEC 27010);
- Information storage and handling policies which require records, data, and other information related to investigations to be stored securely and handled in a manner commensurate with their sensitivity. If the organization has a document labelling or classification schema, this policy is also important to information security incident management activities and personnel;
- An IRT charter that specifies in more detail what the IRT does and the authority under which it operates;
  - At a minimum, the charter should include a mission statement, a definition of the IRT's scope, and details of the IRT's top management sponsor, the IRT authority, contact information for the IRT, its list of services and core activities, its scope of authority and operation, its purpose and goals; along with a discussion of any governance structure;
  - The goals and purposes of the team are especially important and require clear, unambiguous definition;
  - The scope of an IRT normally covers all of the organization's information systems, ICT services and networks. In some cases, an organization can 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;
  - Examples of IRT authority include searching and confiscating personal belongings, detaining people and monitoring communications, where possible.
- An overview of the information security incident management awareness and training programme. This should include any training mandates, policies, or requirements for staff related employee awareness training and incident management training for the IMT members.

5 Updating of information security policies

5.1 General

NOTE Clause 5, in its entirety, links to ISO/IEC 27035-1:—[1], 5.2 b).

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

a) describe why information security incident management, particularly an information security incident reporting and handling plan, is important;

b) indicate top management's commitment to the need for proper preparation and response to information security incidents, i.e. to the information security incident management plan;

c) ensure consistency across the various policies;

d) ensure planned, systematic and composed responses to information security incidents, thus minimizing the adverse consequences of incidents;

e) align with the organization’s risk management policies and practices.

For guidance on information security risk assessment and management, see ISO/IEC 27005. Policy documents should be reviewed regularly and updated when necessary. This should be a consequence of the “learn lessons” phase. See also ISO/IEC 27002:2022, 5.1.

5.2 Linking of policy documents

An organization should update and maintain its organizational information security and risk management policies, and specific system, service or network information security policies in tandem to ensure they remain consistent and current. These organizational-level policies should refer explicitly to the information security incident management policy and associated plans.

The organizational-level policies should include the requirement that appropriate review mechanisms are established. These review mechanisms should ensure that information from the detection, monitoring, resolution of and learning from 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.

6 Creating information security incident management plan

6.1 General

NOTE 1 Clause 6, in its entirety, links to ISO/IEC 27035-1:— [1], 5.2 c).

The aim of an information security incident management plan is to document the activities and procedures for dealing with information security events, incidents and related vulnerabilities discovered during an incident analysis and response, and to communicate them. The plan stems from and is based on the information security incident management policy.

Overall, the documentation of the plan should encompass multiple documents including the forms, procedures and organizational elements. It should also include support tools for the detection and reporting of, assessment and decision making related to, responses to and learning lessons from information security incidents.

The plan may include a high-level outline of the basic flow of incident management activities to provide structure and pointers to the various detailed components of the plan. These components provide the step-by-step instructions for incident handlers to follow using specific tools, following specific workflows or handling specific types of incidents based on the situation.

The information security incident management plan comes into effect whenever an information security event is detected or information security vulnerability is reported.

An organization should use the plan as a guide for:

a) detecting events and abnormal situations and reporting them;

b) responding to information security events;

c) determining whether information security events become information security incidents;

d) managing information security incidents to conclusion;

e) handling information security vulnerabilities discovered while responding to an incident;

NOTE 2 Security vulnerabilities are reported to the incident coordinator who redirects them to the team responsible for vulnerability management.

f) requirements for reporting;

g) requirements for recording information (including its format) during the whole incident management process;

h) rules and circumstances under which information sharing with internal and external groups or organizations can take place;

i) identifying lessons that can be learned, and any improvements to the plan and/or security in general that are required.

Planning and preparation of an incident management plan should be undertaken by the process owner, with a clear goal or set of goals for incident response within a defined scope based on the information security incident management policy.

6.2 Information security incident management plan built on consensus

This document recommends the development of an information security incident management policy. However, 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 the organization and partner organizations where relevant. This includes names and identifiers for organizations and teams, information assets and 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 interested parties can overlap and should be adjusted by consensus in the incident management planning process. Where there is overlap on incident response decision boundaries, the plan should identify a responsible party.

Interested 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.

6.3 Interested parties

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

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

b) assessing and responding to information security events and incidents, being involved in the post-incident resolution activities of learning, and improving information security and the information security incident management plan itself (this is the responsibility of interested parties including the PoC (point of contact), the incident coordinator, the IRT, management, public relations personnel and legal representatives);

c) dealing with information security vulnerabilities (this is the responsibility of skilled members from vulnerability management).

The plan should also take into account any third-party users. Consideration should be given to information security incidents and associated vulnerabilities reported from third party organizations, government and commercial information security incident and vulnerability information provision organizations.

If interested parties are expected to be actively involved in handling information security incidents, then a clear division of roles and responsibilities should be made and everyone made aware of them. Division of roles should be accompanied with the agreed incident handoff protocol so that information is exchanged in an expedient manner. If appropriate and possible, the incident handoff and information exchange should be automated to speed up the process. This kind of scenario can arise if some of the organization or IRT capabilities are outsourced to a third party. Examples include when the organization uses cloud systems run by the third party, or when the third party performs digital forensics for the organization, or when the organization works with a service provider in handling incidents.

6.4 Information security incident management plan content

Key decision-making criteria and processes to support expected management phases should be defined and reviewed before the planning and preparation process. This requires available policy, formal or informal understanding of assets and controls, and contribution from participants and management support.

The content of the information security incident management plan should give an overview, as well as specifying detailed activities. As noted above, the plan documentation should encompass multiple documents including the forms, procedures, organizational elements and support tools.

The detailed activities, procedures and information should consider the following.

a) Plan and prepare.

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

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

2) An information security incident register structured for the exchange of information is likely to provide the capability to share reports/alerts, compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of information systems. The actual format and use of the incident register depend on the organization’s requirements. For example, a very small organization may use documents, while a complex organization may use more sophisticated technology such as relational databases and application tools;

3) Guidance for deciding whether escalation is required during each relevant process, and to whom, and associated procedures. Based on the guidance provided in the information security incident management plan, the incident coordinator should know under which circumstances it is necessary to escalate matters and to whom it should be escalated. In addition, there are unforeseen circumstances when this may be necessary. For example, a minor information security incident can evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up timely can become a major information security incident;

4) Procedures to be followed to ensure that all information security incident response activities are properly logged and that log analysis is conducted by designated personnel;

5) Procedures and mechanisms to ensure that the change control regime is maintained covering information security event, incident and related vulnerability tracking and information security report updates, and updates to the plan itself;

6) Procedures for information security evidence recording, safeguarding and analysis;

7) Procedures for handover to law enforcement when a crime occurs;

8) On ICT systems, procedures and guidance on using intrusion detection systems (IDS) and intrusion prevention systems (IPS), ensuring that associated legal and regulatory aspects have been addressed. Guidance should include discussion of the advantages and disadvantages of undertaking attacker surveillance activities. Further information on IDS is contained in ISO/IEC 27039;

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

10) Material for the information security event, incident and vulnerability management awareness and training programme;

11) Procedures and specifications for the testing of the information security incident management plan;

12) Organizational structure for information security incident management;

13) The terms of reference and responsibilities of the IMT, IRT and incident coordinator;

14) Important contact information;

16) Procedures and guidance regarding information sharing as agreed with the organization’s public affairs office, legal department and top management or relevant departments;

17) Establishing and maintaining the list of information security events and incidents the organization wants to be able to detect, respond to and learn from as the result of the information security risk treatment phase.

b) Detect and report.

1) Planning and preparation requirements for detection and reporting should enable and support the development and operation of processes to find or accept information about information security incidents;

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

3) Reporting output or notification should be defined in the context of the organization, the incident response procedures, and assignment of technical and management roles. The format of reports and notification should match the incident classification scale or a consistent related metric;

4) The event report should be generic, but contain as much information as possible based on a clear template everyone understands and can complete;

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

6) Collecting the information on information security events;

7) Detecting and reporting on information security vulnerabilities;