INTERNATIONAL STANDARD

ISO/IEC 27035-2

First edition
2016-11-01

Information technology — Security techniques — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information —

Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents

Reference number
ISO/IEC 27035-2:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035-2, together with ISO/IEC 27035-1, cancels and replaces ISO/IEC 27035:2011, which has been technically revised.

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*

Further parts may follow.

Introduction

ISO/IEC 27035 is an extension of ISO/IEC 27000 series of standards and it focuses on information security incident management which is identified in ISO/IEC 27000 as one of the critical success factor for the information security management system.

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 part of ISO/IEC 27035 addresses the development of guidelines 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 how to establish the incident response team and improve its performance over time by adopting lessons learned and by evaluation.

Information technology — Security techniques — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

1 Scope

This part of ISO/IEC 27035 provides the guidelines to plan and prepare for incident response. The guidelines are based on the “Plan and Prepare” phase and the “Lessons Learned” phase of the “Information security incident management phases” model presented in ISO/IEC 27035-1.

The major points within the “Plan and Prepare” phase include the following:

- information security incident management policy and commitment of top management;
- information security policies, including those relating to risk management, updated at both corporate level and system, service and network levels;
- information security incident management plan;
- incident response team (IRT) establishment;
- establish 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;
- information security incident management plan testing.

The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 27035-1:2016, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

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, ISO/IEC 27035-1 and the following apply.

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

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

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

3.1.1
users
people or organizations that utilise services provided by the incident response team (IRT)

Note 1 to entry: Users can be internal (within the organization) or external (outside the organization).

3.2 Abbreviated terms

CD	compact disk
CERT	computer emergency response team, sometimes also referred as incident response team (IRT) or computer security response team (CSIRT)
DNS	domain name system
DVD	digital versatile disk
ICMP	internet control message protocol
IDS	intrusion detection system
IPv4	internet protocol v4
IPv6	internet protocol v6
IRT	incident response team
ISP	internet service provider
PoC	point of contact
SMTP	simple mail transfer protocol
SSL	secure sockets layer protocol
TCP	transmission control protocol
TLP	traffic light protocol
TLS	transport layer security protocol
UDP	user datagram protocol
WiFi	wireless fidelity

4 Information security incident management policy

4.1 General

NOTE Clause 4, in its entirety, links to ISO/IEC 27035-1:2016, 5.2 a).

An organization information security incident management policy should provide the formally documented principles and intentions used to direct decision-making and ensure consistent and appropriate implementation of processes, procedures, etc. with regard to this 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 (specifically the primary point of contact for reporting suspected incidents) when an information security incident occurs. The policy should be reviewed regularly to ensure it reflects the latest organizational structure, processes, and technology that can affect incident response. The policy should also outline any awareness and training initiatives within the organization that is related to incident response (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, 5.2), or as part of its Information Security Policies (see ISO/IEC 27002:2013, 5.1.1). 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. 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) objectives;

b) interested parties internally and externally;

c) specific incident types and vulnerabilities that need to be highlighted;

d) any specific roles that need to be highlighted;

e) benefits to the whole organization and to its departments.

4.2 Involved parties

A successful information security incident management policy should be created and implemented as an enterprise-wide process. To that end, all stakeholders or their representatives should be involved in the development of the policy from the initial planning stages through the implementation of any process or response team. This may include legal advisors, public relations and marketing staff, departmental managers, security staff, system and network administrators, ICT staff, helpdesk staff, upper-level management, and, in some cases, even facilities staff.

An organization should ensure that its information security incident management policy is approved by a member of top management, with commitment from all of top management.

Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident, know what to do and understand the benefits of the approach by the organization. Management needs to be supportive of the information security incident policy to ensure that the organization commits to resourcing and maintaining an incident response capability.

The information security incident management policy should be made available to every employee and contractor and 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 what a security incident is.

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) from detection, through reporting, information collection, analysis, response, notification, escalation, and resolution.

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 vulnerability reporting and handling (although this could be a separate policy document).

j) Defined set of roles, responsibilities, and decision-making authority for each phase of the information security incident management process and related activities (including vulnerability reporting and handling if appropriate).

k) A reference to the document describing the event and incident classification, severity ratings (if used) and related terms. The overview should either contain a description of what constitutes an incident or a reference to the document where that is described.

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

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

   2) briefing top management on incidents;

   3) dealing with enquiries, instigating follow up, and resolving incidents;

   4) liaising with the external organizations (when necessary);

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

m) A requirement that components across the organization work in collaboration to detect, analyse, and respond to information security incidents.

n) A description of any oversight or governance structure and its authority and duties, if applicable.

o) Links to organizations providing specific external support such as forensics teams, legal counsel, other IT operations, etc.

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

q) A list and reference to other policies, procedures, and documents that support the information security incident management process and related activities. Many of the items listed in the policy may have their own more detailed procedures or guidance documents.

There are other related policies or procedures that will support the information security incident management policy and could also be established as part of the preparation phase, if they don't already exist and if they 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 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 operation (this could 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 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, information should also follow any organizational requirements for disclosure. Information may need to be shared in the course of incident handling when a third party needs to be involved or modified. The scope, circumstances and purpose of this information sharing need to be 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). An example of TLP guidance can be seen at https://www.us-cert.gov/tlp.

— 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 will also be important to information security incident management activities and personnel.

— An IRT charter that specifies in more detail what the IRT is to do 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, 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.

  — IRT governance might include the identification of an executive officer, board member or top 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 can expose it to claims of liability.

- An overview of the information security incident management awareness and training program. This should include any training mandates, policies, or requirements for staff related employee awareness training and incident management training for the IRT members.

5 Updating of information security policies

5.1 General

NOTE Clause 5, in its entirety, links to ISO/IEC 27035-1:2016, 5.2 b).

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

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

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

c) To ensure consistency across the various policies.

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

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

5.2 Linking of policy documents

An organization should update and maintain its corporate 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 corporate-level policies should refer explicitly to the information security incident management policy and associated plans.

The corporate-level 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.

6 Creating information security incident management plan

6.1 General

NOTE Clause 6, in its entirety, links to ISO/IEC 27035-1:2016, 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 vulnerabilities, and communication of them. The plan stems from and is based on the information security incident management policy.

Overall, the plan documentation should encompass multiple documents including the forms, procedures, organizational elements and 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 will 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 the following:

a) responding to information security events;

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

c) managing information security incidents to conclusion;

d) responding to information security vulnerabilities;

e) requirements for reporting;

f) requirements for storing information (including its format) during the whole incident management process;

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

h) identifying lessons learned, and any improvements to the plan and/or security in general that are required;

i) making those identified improvements.

Planning and preparation of the incident response 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 part of ISO/IEC 27035 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 IRT members and partner organizations. This includes names and identifiers for organizations and teams, information assets, business processes, etc. 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 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.

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.

6.3 Involved 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 members of the PoC (Point of Contact), the IRT, management, public relations personnel and legal representatives);

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

The plan 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.

If involved 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 be 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 of instances like this are when the organization is using cloud system run by the third party or when third party is performing digital forensics for the organization or when working 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 considers specific incident types and the corresponding response processes. 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 be associated with 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 impacts on the organization's business operations, and associated guidance.

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

   2) An information security database 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 database will 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, anyone assessing an information security event, incident or vulnerability 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 could evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up in a week could become a major information security incident.

4) Procedures to be followed to ensure that all information security incident management 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 vulnerability tracking and information security report updates, and updates to the plan itself.

6) Procedures for information security evidence analysis.

7) 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.

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

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

10) Procedures and specifications for the testing of the information security incident management plan.

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

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

13) Important contact information.

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

b) Detection and reporting.

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 incident 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, and 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 policy, and assignment of technical and management roles. The format of reports and notification should match the incident classification scale or a consistent related metric.