INTERNATIONAL STANDARD

ISO/IEC 27035-1

Second edition
2023-02

Information technology — Information security incident management —

Part 1: Principles and process

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

Partie 1: Principes et processus

Reference number
ISO/IEC 27035-1:2023(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 Joint 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 27035-1:2016), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— new terms “incident management team” and “incident coordinator” are defined in Clause 3;

— new subclauses 4.5, 4.6 and 4.7 are added in Clause 4;

— the title of Clause 5 has been changed to “Process”;

— Annex C has been updated;

— a new Annex D has been added;

— the text has been editorially revised.

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

The ISO/IEC 27035 series provides additional guidance to the controls on incident management in ISO/IEC 27002. These controls should be implemented based upon the information security risks that the organization is facing.

Information security policies or controls alone do not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can reduce the effectiveness of information security and facilitate the occurrence of information security incidents. This can potentially have direct and indirect adverse consequences on an organization's business operations. Furthermore, it is inevitable that new instances of previously unidentified threats cause incidents to occur. Insufficient preparation by an organization to deal with such incidents makes any response less effective, and increases the degree of potential adverse business consequence. Therefore, it is essential for any organization desiring a strong information security programme to have a structured and planned approach to:

— plan and prepare information security incident management, including policy, organization, plan, technical support, awareness and skills training, etc.;

— detect, report and assess information security incidents and vulnerabilities involved with the incident;

— respond to information security incidents, including the activation of appropriate controls to prevent, reduce, and recover from impact;

— deal with reported information security vulnerabilities involved with the incident appropriately;

— learn from information security incidents and vulnerabilities involved with the incident, implement and verify preventive controls, and make improvements to the overall approach to information security incident management.

The ISO/IEC 27035 series is intended to complement other standards and documents that give guidance on the investigation of, and preparation to investigate, information security incidents. The ISO/IEC 27035 series is not a comprehensive guide, but a reference for certain fundamental principles and a defined process that are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise.

While the ISO/IEC 27035 series encompasses the management of information security incidents, it also covers some aspects of information security vulnerabilities. Guidance on vulnerability disclosure and vulnerability handling by vendors is also provided in ISO/IEC 29147 and ISO/IEC 30111, respectively.

The ISO/IEC 27035 series also intends to inform decision-makers when determining the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyse and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

Further information about investigative standards is available in Annex A.

Information technology — Information security incident management —

Part 1: Principles and process

1 Scope

This document is the foundation of the ISO/IEC 27035 series. It presents basic concepts, principles and process with key activities of information security incident management, which provide a structured approach to preparing for, detecting, reporting, assessing, and responding to incidents, and applying lessons learned.

The guidance on the information security incident management process and its key activities given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance 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*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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/

3.1.1
incident management team
IMT
team consisting of appropriately skilled and trusted members of an organization responsible for leading all information security incident management activities, in coordination with other parties both internal and external, throughout the incident lifecycle

Note 1 to entry: The head of this team can be called the incident manager who has been appointed by top management to adequately respond to all types of incidents.

3.1.2
incident response team
IRT
team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way

Note 1 to entry: There can be several IRTs, one for each aspect of the incident.

Note 2 to entry: Computer Emergency Response Team (CERT[1)]) and Computer Security Incident Response Team (CSIRT) are specific examples of IRTs in organizations and sectorial, regional, and national entities wanting to coordinate their response to large scale ICT and cybersecurity incidents.

3.1.3
incident coordinator
person responsible for leading all *incident response* (3.1.9) activities and coordinating the *incident response team* (3.1.2)

Note 1 to entry: An organization can decide to use another term for the incident coordinator.

3.1.4
information security event
occurrence indicating a possible breach of information security or failure of controls

3.1.5
information security incident
related and identified *information security event(s)* (3.1.4) that can harm an organization's assets or compromise its operations

3.1.6
information security incident management
collaborative activities to handle *information security incidents* (3.1.5) in a consistent and effective way

3.1.7
information security investigation
application of examinations, analysis and interpretation to aid understanding of an *information security incident* (3.1.5)

[SOURCE: ISO/IEC 27042:2015, 3.10, modified —"information security" was added to the term and the phrase "an incident" was replaced by "an information security incident" in the definition.]

3.1.8
incident handling
actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.1.5)

3.1.9
incident response
actions taken to mitigate or resolve an *information security incident* (3.1.5), including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

3.1.10
point of contact
PoC
defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities

Note 1 to entry: The most obvious PoC is the role to whom the information security event is raised.

1) CERT is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of this product.

3.2 Abbreviated terms

BCP	business continuity planning
CERT	computer emergency response team
CSIRT	computer security incident response team
DRP	disaster recovery planning
ICT	information and communications technology
IMT	incident management team
IRT	incident response team
ISMS	information security management system
PoC	point of contact
RPO	recovery point objective
RTO	recovery time objective

4 Overview

4.1 Basic concepts

Information security events and incidents may happen due to several reasons:

— technical/technological, organizational or physical vulnerabilities, partly due to incomplete implementations of the decided controls, are likely to be exploited, as complete elimination of exposure or risk is unlikely;

— humans can make errors;

— technology can fail;

— risk assessment is incomplete and risks have been omitted;

— risk treatment does not sufficiently cover the risks;

— changes in the context (internal and/or external) so that new risks exist or treated risks are no longer sufficiently covered.

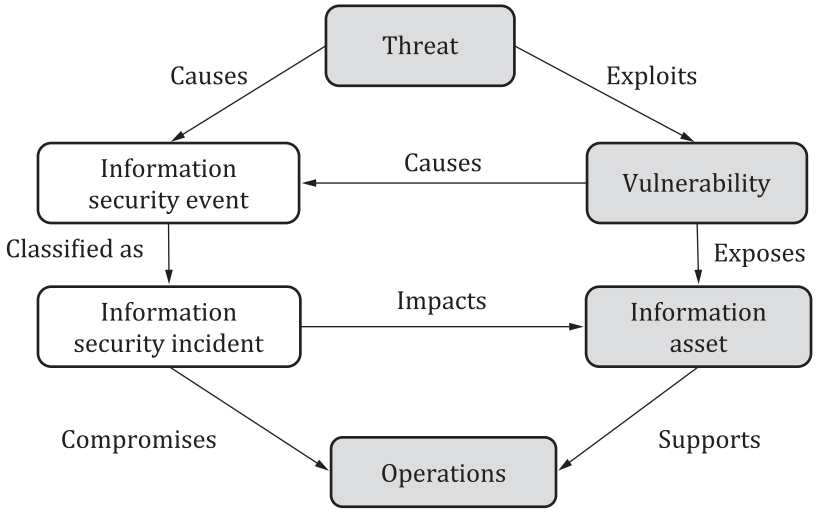
The occurrence of an information security event does not necessarily mean that an attack has been successful or that there are any implications on confidentiality, integrity or availability, i.e. not all information security events are classified as information security incidents.

Information security incidents can be deliberate (e.g. caused by malware or breach of discipline), accidental (e.g. caused by inadvertent human error) or environmental (e.g. caused by fire or flood) and can be caused by technical (e.g. computer viruses) or non-technical (e.g. loss or theft of hardcopy documents) means. Incidents can include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information.

Annex B provides descriptions of selected examples of information security incidents and their causes for informative purposes only. It is important to note that these examples are by no means exhaustive.

A threat exploits vulnerabilities (weaknesses) in information systems, services, or networks, causing the occurrence of information security events and thus potentially causing incidents to information

assets exposed by the vulnerabilities. Figure 1 shows the relationship of objects in an information security incident.



NOTE The shaded objects are pre-existing, affected by the unshaded objects that result in an information security incident.

Figure 1 — Relationship of objects in an information security incident

Coordination is an important aspect in information security incident management. Many incidents cross organizational boundaries and cannot be easily resolved by a single organization or, a part of an organization where the incident has been detected. Organizations should commit to the overall incident management objectives. Incident management coordination is required across the incident management process for multiple organizations to work together to handle information security incidents. This is for example the role of CERTs and CSIRTs. Information sharing is necessary for incident management coordination, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Organizations should protect sensitive information during information sharing and communication. See ISO/IEC 27010 for further details.

It is important to indicate that resolving an information security incident should be done within a defined time frame to avoid unacceptable damage or a resulting catastrophe. This resolution delay is not as important in case of an event, vulnerability or a non-conformity.

4.2 Objectives of incident management

As a key part of an organization's overall information security strategy, the organization should put controls including procedures in place to enable a structured well-planned approach to the management of information security incidents. From an organization's perspective, the prime objective is to avoid or contain the impacts of information security incidents in order to minimize the direct and indirect damage to its operations caused by the incidents. Since damage to information assets can have a negative consequence on operations, business and operational perspectives should have a major influence in determining more specific objectives for information security incident management.

More specific objectives of a structured well-planned approach to incident management should include the following:

a) information security events are detected and efficiently dealt with, in particular deciding whether they should be classified as information security incidents;

b) identified information security incidents are assessed and responded to in the most appropriate and efficient manner and within the predetermined time frame;

c) the adverse impact(s) of information security incidents on the organization and involved parties and their operations are minimized by appropriate controls as part of incident response;

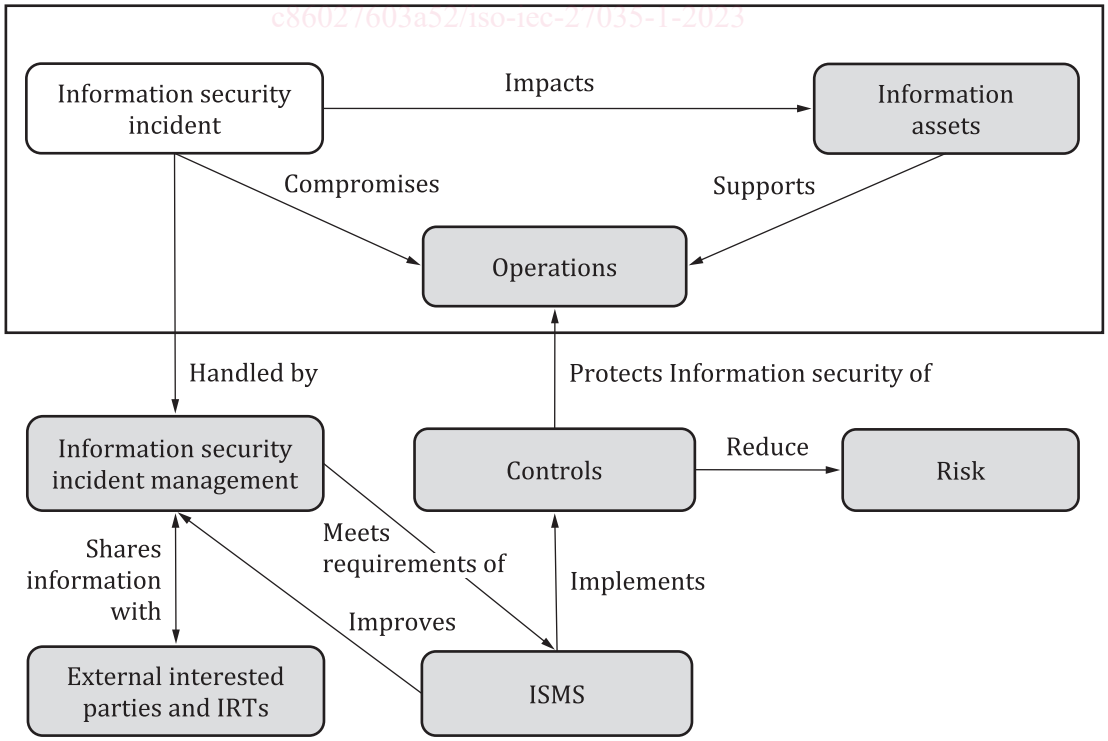
d) a link with relevant elements from crisis management and business continuity management through an escalation process is established. There is a need for a swift transfer of responsibility and action from incident management to crisis management when the situation requires it, with this order reversed once the crisis is resolved to allow for a complete resolution of the incident;

e) information security vulnerabilities involved with or discovered during the incident are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the incident response team (IRT) or other teams within the organization and involved parties, depending on duty distribution;

f) lessons are learnt quickly from information security incidents, related vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

To help achieve these objectives, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards or procedures for incident categorization, classification, prioritization and sharing, so that metrics can be derived from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls. The information security incident management system should be able to share information with relevant internal and external parties.

Another objective associated with this document is to provide guidance to organizations that aim to meet the information security management system (ISMS) requirements specified in ISO/IEC 27001 which are supported by guidance from ISO/IEC 27002. ISO/IEC 27001 includes requirements related to information security incident management. Table C.1 provides cross-references on information security incident management clauses from ISO/IEC 27001 and clauses in this document. ISMS relationships are also explained in Figure 2. This document can also support the requirements of information security management systems that do not follow ISO/IEC 27001.



NOTE See also Figure 1.

Figure 2 — Information security incident management in relation to ISMS and applied controls

4.3 Benefits of a structured approach

Using a structured approach to information security incident management can yield significant benefits, which can be grouped under the following topics.

a) Improving overall information security

To ensure adequate identification of and response to information security events and incidents, it is a prerequisite that there be a structured process for planning and preparation, detection, reporting and assessment, and relevant decision-making. This improves overall security by helping to quickly identify and implement a consistent solution, and thus provides a means of preventing similar information security incidents in the future. Furthermore, benefits are gained by metrics, sharing and aggregation. The credibility of the organization can be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business consequences

A structured approach to information security incident management can assist in reducing the level of potential adverse business consequences associated with information security incidents. These consequences can include immediate financial loss and longer-term loss arising from damaged reputation and credibility. For further guidance on consequence assessment, see ISO/IEC 27005. For guidance on information and communication technology readiness for business continuity, see ISO/IEC 27031.

c) Strengthening the focus on information security incident prevention

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including the development of methods to identify new threats and vulnerabilities. Analysis of incident-related data enables the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and identification of appropriate actions and controls to prevent further occurrence.

d) Improving prioritization

A structured approach to information security incident management provides a solid basis for prioritization when conducting information security incident investigations, including the use of effective categorization and classification scales. If there are no clear procedures, there is a risk that investigation activities may be conducted in an overly reactive mode, responding to incidents as they occur and overlooking what activities should be handled with a higher priority.

e) Supporting evidence collection and investigation

If and when needed, clear incident investigation procedures help to ensure that data collection and handling are evidentially sound and legally admissible. These are important considerations if legal prosecution or disciplinary action follows. For more information on digital evidence and investigation, see the investigative standards in Annex A.

f) Contributing to budget and resource justifications

A well-defined and structured approach to information security incident management helps to justify and simplify the allocation of budgets and resources for involved organizational units. Furthermore, benefit accrues for the information security incident management plan itself, with the ability to better plan for the allocation of staff and resources.

One example of a way to control and optimize budget and resources is to add time tracking to information security incident management tasks to facilitate quantitative assessment of the organization's handling of information security incidents. It can provide information on how long it takes to resolve information security incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

g) Improving updates to information security risk assessment and treatment results

The use of a structured approach to information security incident management facilitates:

— better collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities, and

— provision of data about frequencies of occurrence of the identified threat types, to assist with analysis of control efficacy (i.e. identify controls that failed and resulted in a breach, with uplift of such controls to reduce reoccurrence).

The data collected about adverse impacts on business operations from information security incidents is useful in business impact analysis. The data collected to identify the frequency of various threat types can improve the quality of a threat assessment. Similarly, the data collected on vulnerabilities can improve the quality of future vulnerability assessments. For guidance on information security risk assessment and treatment, see ISO/IEC 27005.

h) Providing enhanced information security awareness and training programme material

A structured approach to information security incident management enables an organization to collect experience and knowledge of how the organization and involved parties handle incidents, which is valuable material for an information security awareness programme. An awareness programme that includes lessons learned from real experience helps to reduce mistakes or confusion in future information security incident handling and improve potential response times and general awareness of reporting obligations.

i) Providing input to the information security policy and related documentation reviews

Data provided by the practice of a structured approach to information security incident management can offer valuable input to reviews of the effectiveness and subsequent improvement of incident management policies (and other related information security documents). This applies to topic-specific policies and other documents applicable both for organization-wide and for individual systems, services and networks.

4.4 Adaptability

The guidance provided by the ISO/IEC 27035 series is extensive and, if adopted in full, can require significant resources to operate and manage. It is therefore important that an organization applying this guidance should retain a sense of perspective and ensure that the resources applied to information security incident management and the complexity of the mechanisms implemented are proportional to the following:

a) size, structure and business nature of an organization including key critical assets, processes, and data that should be protected;

b) scope of any information security management system for incident handling;

c) potential risk due to incidents;

d) the goals of the business.

An organization using this document should therefore adopt its guidance in a manner that is relevant to the scale and characteristics of its business.

4.5 Capability

4.5.1 General

Information security incidents can jeopardize achievement of business objectives and generate crises. Following the risk assessment, it is possible to delineate between situations whose likelihood is medium to high, and consequence low to medium, and those whose likelihood is (very) rare and consequences very high. The second situation represents crises that are not always possible to completely prevent