INTERNATIONAL STANDARD

ISO/IEC 27035-3

First edition
2020-09

Information technology — Information security incident management —

Part 3: Guidelines for ICT incident response operations

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

Partie 3: Lignes directrices relatives aux opérations de réponse aux incidents TIC

Reference number
ISO/IEC 27035-3:2020(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).

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 http://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.

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

A list of all parts in the ISO 27035 series can be found on the ISO website.

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.

Introduction

An information security incident can involve ICT or not. For example, information that spreads unintentionally through the loss of paper documents can very well be a serious information security incident, which requires incident reporting, investigation, containment, corrective actions and management involvement. This type of incident management is often carried out, for example, by the Chief Information Security Officer (CISO) within the organization. Guidance on the management of such information security incidents can be found in ISO/IEC 27035-1. This document, however, only considers incident response operations for ICT-related incidents, and not for information security incidents related to paper documents or any other non-ICT incidents. Whenever the term "information security" is used in this document, it is done so in the context of ICT-related information security.

The organizational structures for information security vary depending on the size and business field of organizations. As various and numerous incidents occur and are increasing (such as network incidents, e.g. intrusions, data breaches and hacking), higher concerns about information security have been raised by organizations. A secure ICT environment set up to withstand various types of attacks (such as DoS, worms and viruses) with network security equipment such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) should be complemented with clear operating procedures for incident handling, along with well-defined reporting structures within the organization.

To ensure confidentiality, integrity and availability of information and to handle incidents efficiently, capabilities to conduct incident response operations is required. For this purpose, a computer security incident response team (CSIRT) should be established to perform tasks such as monitoring, detection, analysis and response activities for collected data or security events. These tasks may be assisted by artificial intelligence tools and techniques.

This document supports the controls of ISO/IEC 27001:2013, Annex A, related to incident management.

Not all steps in this document are applicable since it depends on the particular incident. For example, a smaller organization may not use all guidance in this document but can find it useful for organization of their ICT-related incident operations especially if operating their own ICT environment. It can also be useful for smaller organizations that have outsourced their IT operations to better understand the requirements and execution of incident operations that they should expect from their ICT supplier(s).

This document is particularly useful to organizations providing ICT services that involve interactions between organizations of incident operations in order to follow the same processes and terms.

This document also provides a better understanding on how incident operations relates to the users/customers in order to define when and how such interaction needs to take place, even if this is not specified.

Information technology — Information security incident management —

Part 3: Guidelines for ICT incident response operations

1 Scope

This document gives guidelines for information security incident response in ICT security operations. This document does this by firstly covering the operational aspects in ICT security operations from a people, processes and technology perspective. It then further focuses on information security incident response in ICT security operations including information security incident detection, reporting, triage, analysis, response, containment, eradication, recovery and conclusion.

This document is not concerned with non-ICT incident response operations such as loss of paper-based documents.

This document is based on the "Detection and reporting" phase, the "Assessment and decision" phase and the "Responses" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1:2016.

The principles given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the provisions given in this document according to their type, size and nature of business in relation to the information security risk situation.

This document is also applicable to external organizations providing information security incident management services.

2 Normative references

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

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

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

ISO/IEC 27035-2, *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 27043, *Information technology — Security techniques — Incident investigation principles and processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27037, ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27043 and the following apply.

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

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

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

3.1
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27032:2012, 4.6]

3.2
computer security incident response team
CSIRT
team of security experts to support the handling of information security incidents

[SOURCE: ISO/IEC 27019:2017, 3.2]

3.3
investigation
systematic or formal process of inquiring into or researching, and examining facts or materials associated with a matter

Note 1 to entry: A similar definition can be found in ISO/IEC 27042:2015, 3.10.

[SOURCE: ISO/IEC 27050:2017, 3.17, modified — Note 1 to entry has been added.]

3.1.4
response
incident response
action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs

[SOURCE: ISO/IEC 27039:2015, 2.24]

4 Abbreviated terms

ASCII	American standard code for information interchange
CPU	central processing unit
DNS	domain name system or domain name service
DDoS	distributed denial of service
DoS	denial of service
ENISA	European Union agency for network and information security
FAT	file allocation table file system
FAT32	32-bit file allocation table file system
FIRST	forum of incident response and security teams
HPFS	high performance file system
HR	human resources
ICT	information and communication technology

IDS	intrusion detection system
IoC	indicators of compromise
IP	internet protocol
IPS	intrusion prevention system
ISP	internet service provider
IT	information technology
MD5	message digest 5 algorithm
NIST	national institute for standards and technology
NTFS	windows networking technology file system
OS	operating system
PoC	point of contact
SHA	secure hashing algorithm
SIEM	security information and event management system
URL	universal resource locator
WAF	web application firewall
XML	extended mark-up language

5 Overview

5.1 General

ISO/IEC 27035-1 covers the following five main phases for information security incident management:

— Plan and prepare;

— Detection and reporting;

— Assessment and decision;

— Responses;

— Lessons learnt.

ISO/IEC 27035-2 covers two of these five phases in detail, i.e. "Plan and prepare" and "Lessons learnt".

This document covers the remaining three phases in detail. These three remaining phases are collectively referred to as incident response operations, which are the focus in this document.

5.2 Structure of this document

The provisions in this document are based on the "Detection and reporting", "Assessment and decision" and "Responses" phases of the “Information security incident management phases” model presented in ISO/IEC 27035-1. Collectively, these phases are known as the incident response operation process.

The phases within the incident response operation process (which are "Detection and reporting", "Assessment and decision" and "Responses" as stipulated in ISO/IEC 27035-1) include the following:

— operations for incident identification;

— operations for incident assessment and qualification;

— operations for threat intelligence gathering;

— operations for incident containment, eradication and recovery;

— operations for incident analysis;

— operations for incident reporting.

The scope for incident response is defined in ISO/IEC 27035-1. Incident response operations should be seen as a business process that enables an organization to remain in business. Specifically, an incident response operation process is a collection of procedures aimed at identifying, responding to and investigating potential security incidents in a way that minimizes their impact and support rapid recovery.

ISO/IEC 27035-1 shows the five phases of information security incident management as Plan and prepare, Detection and reporting, Assessment and decision, Responses and Lessons learnt. As mentioned before, this document focuses on an incident response operation process. This process can be characterized by a lifecycle of incident response operations which is represented by the inner phases (detection, notification, triage, analysis, response, and reporting). These are represented in more detail in Figure 1.

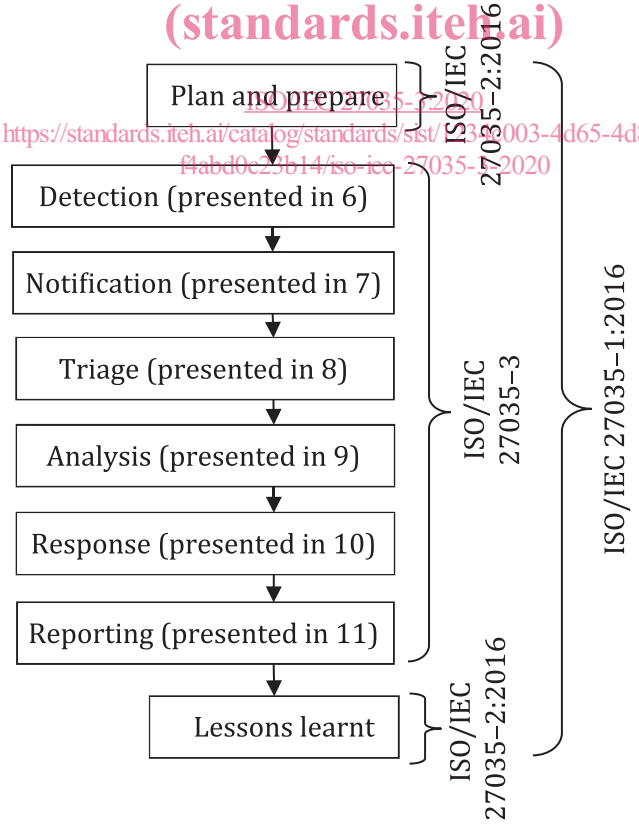

Figure 1 — Lifecycle of incident response operations

The lifecycle of incident response operations (detection, notification, triage, analysis, response, and reporting) can be mapped to the five phases of information security incident management of

ISO/IEC 27035-1 (Plan and prepare, Detection and reporting, Assessment and decision, Responses and Lessons learnt) as shown in Table 1.

Table 1 — Mapping of the five phases of information security incident management in ISO/IEC 27035-1 to the lifecycle of incident response operations in this document

Five phases of information security incident management in ISO/IEC 27035-1	Lifecycle of ICT incident response operations in this document
Plan and prepare	(None – covered in detail by ISO/IEC 27035–2)
Detection and reporting	— Detection (presented in Clause 7, which links to ISO/IEC 27035-1:2016, 5.3) — Notification (presented in Clause 8, which links to ISO/IEC 27035-1:2016, 5.3)
Assessment and decision	— Triage (presented in Clause 9, which links to ISO/IEC 27035-1:2016, 5.4) — Analysis (presented in Clause 10, which links to ISO/IEC 27035-1:2016, 5.4)
Responses	— Response (presented in Clause 11, which links to ISO/IEC 27035-1:2016, 5.5) — Reporting (presented in Clause 12, which links to ISO/IEC 27035-1:2016, 5.3)
Lessons learnt	(None – covered in detail by ISO/IEC 27035-2)

NOTE The notion of reporting appears only once in ISO/IEC 27035-1:2016, 5.3. However, during the entire lifecycle of incident response operations (as portrayed in this document), the notion of reporting appears twice: once in Clause 7 and once in Clause 11. However, both instances of reporting map to ISO/IEC 27035-1:2016, 5.3. To clarify, there are two distinct instances (occurrences) of reporting that take place during the entire lifecycle of incident response operations as portrayed in this document. The first occurrence of reporting involves the recording or registration of the fact that an incident has indeed occurred (as presented in Clause 7). The second occurrence of reporting involves the recording of the outcome of the entire lifecycle of incident response operations (as presented in Clause 11). In summary, the first occurrence reports to (notifies) a PoC that an incident has indeed occurred, while the second occurrence reports on the outcome of the entire lifecycle of incident response operations.

6 Common types of attacks

Incidents can happen in various ways and it is not practical to define all the incidents and prepare the response manual for each type of incident. However, there are common attack types/sources that an organization often encounter and should therefore be prepared to handle, such attacks efficiently. Criteria should be set for security incidents according to the importance (priority) of information and information systems, impact of each incident, damage scale, alarm ranking and its severity. See Annex A for examples of such criteria.

The following is a non-exhaustive list of common attack types/sources that can be used as the basis for defining incident handling procedures:

— external/removable media: an attack executed from removable media (e.g. flash drive, CD) or a peripheral device;

— attrition: an attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures);

— web: an attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware);

— e-mail: an attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email message);

— supply chain interdiction: an antagonistic attack on hardware or software assets utilizing physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer;

— impersonation: an attack involving replacement of something benign with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation);

— improper usage: any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system);

— loss or theft of equipment: the loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token;

— other: an attack that does not fit into any of these categories.

NOTE See the NIST Computer Security Incident Handling Guide[1)] for more incident classification guidelines and attack vectors.

An incident comprises one or multiple related information security events that can harm an organization's assets or compromise its operations, where an information security event comprise one or multiple occurrences indicating a possible breach or failure of information security controls.

7 Incident detection operations

7.1 Point of contact

Incident detection operations require that there be a point of contact (PoC) to receive information, an established methodology for the team to detect information security events. Detection is important because it starts the incident response operations.

The PoC is the organizational function or role serving as the coordinator or focal point of incident operation activities. An information security event is reported by the "User/Source" in some way, as shown in ISO/IEC 27035-1:2016, Figure 4. The main purpose of the PoC is to ensure that an event is reported as soon as possible to the organization so that the event can be handled efficiently. A critical success factor is that the PoC possesses the skills to determine whether an event indeed is an ICT-related event and that the PoC is able to describe the event.

An event should then be further handled by a PoC and then transferred into incident response operations. The organization of a PoC can be different depending on the size and structure of the organization as well as the nature of the business. This can affect how incident operations are informed of the event.

There are three different main scenarios for the PoC:

a) no formal PoC exists;

b) single PoC for all types of events irrespective of the number of geographic locations;

c) multiple PoCs depending on the nature of the event and geographic locations.

1) This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products can be used if they are applicable.

