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/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms, definitions and abbreviated terms ... **1**
3.1 Terms and definitions ... 1
3.2 Abbreviated terms ... 3
4 Overview ... **3**
4.1 Basic concepts ... 3
4.2 Objectives of incident management ... 4
4.3 Benefits of a structured approach ... 6
4.4 Adaptability ... 7
4.5 Capability ... 7
4.5.1 General ... 7
4.5.2 Policies, plan and process ... 8
4.5.3 Incident management structure ... 8
4.6 Communication ... 10
4.7 Documentation ... 10
4.7.1 General ... 10
4.7.2 Event report ... 10
4.7.3 Incident management log ... 10
4.7.4 Incident report ... 11
4.7.5 Incident register ... 11
5 Process ... **11**
5.1 Overview ... 11
5.2 Plan and prepare ... 15
5.3 Detect and report ... 16
5.4 Assess and decide ... 17
5.5 Respond ... 18
5.6 Learn lessons ... 20
Annex A (informative) **Relationship to investigative standards** ... **22**
Annex B (informative) **Examples of information security incidents and their causes** ... **25**
Annex C (informative) **Cross-reference table of ISO/IEC 27001 to the ISO/IEC 27035 series** ... **29**
Annex D (informative) **Considerations of situations discovered during the investigation of an incident** ... **31**
Bibliography ... **32**

© ISO/IEC 2023 – All rights reserved

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.

© ISO/IEC 2023 – All rights reserved

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.

© ISO/IEC 2023 – All rights reserved

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.

© ISO/IEC 2023 – All rights reserved

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.

© ISO/IEC 2023 – All rights reserved