INTERNATIONAL STANDARD

ISO/IEC 27035-2

Second edition
2023-02

Information technology — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

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

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

Reference number
ISO/IEC 27035-2:2023(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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **2**
3.1 Terms and definitions 2
3.2 Abbreviated terms 2
4 Information security incident management policy **2**
4.1 General 2
4.2 Interested parties 3
4.3 Information security incident management policy content 3
5 Updating of information security policies **5**
5.1 General 5
5.2 Linking of policy documents 6
6 Creating information security incident management plan **6**
6.1 General 6
6.2 Information security incident management plan built on consensus 7
6.3 Interested parties 7
6.4 Information security incident management plan content 8
6.5 Incident classification scale 11
6.6 Incident forms 11
6.7 Documented processes and procedures 12
6.8 Trust and confidence 13
6.9 Handling confidential or sensitive information 14
7 Establishing an incident management capability **14**
7.1 General 14
7.2 Incident management team establishment 14
7.2.1 IMT structure 14
7.2.2 IMT roles and responsibilities 16
7.3 Incident response team establishment 17
7.3.1 IRT structure 17
7.3.2 IRT types and roles 18
7.3.3 IRT staff competencies 19
8 Establishing internal and external relationships **20**
8.1 General 20
8.2 Relationship with other parts of the organization 20
8.3 Relationship with external interested parties 21
9 Defining technical and other support **22**
9.1 General 22
9.2 Technical support 24
9.3 Other support 24
10 Creating information security incident awareness and training **24**
11 Testing the information security incident management plan **25**
11.1 General 25
11.2 Exercise 26
11.2.1 Defining the goal of the exercise 26
11.2.2 Defining the scope of an exercise 27
11.2.3 Conducting an exercise 27
11.3 Incident response capability monitoring 27
11.3.1 Implementing an incident response capability monitoring programme 27

© ISO/IEC 2023 – All rights reserved

11.3.2 Metrics and governance of incident response capability monitoring 28
12 Learn lessons **28**
12.1 General 28
12.2 Identifying areas for improvement 29
12.3 Identifying and making improvements to the information security incident management plan 29
12.4 IMT evaluation 30
12.5 Identifying and making improvements to information security control implementation 30
12.6 Identifying and making improvements to information security risk assessment and management review results 31
12.7 Other improvements 31
Annex A (informative) **Considerations related to legal or regulatory requirements** **32**
Annex B (informative) **Example forms for information security events, incidents and vulnerability reports** **35**
Annex C (informative) **Example approaches to the categorization, evaluation and prioritization of information security events and incidents** **47**
Bibliography **52**

© 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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27035-2:2016), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— new roles including incident management team and incident coordinator and their responsibilities have been added;

— content related to vulnerability management has been modified;

— content on a recommended process for organizations has been added in 6.7;

— Clause 7 structure has been reorganized;

— C.3 has been replaced by a single paragraph;

— bibliography has been updated.

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

This document focuses on information security incident management which is identified in ISO/IEC 27000 as one of the critical success factors for the information security management system.

There can be a large gap between an organization’s plan for an incident and an organization's preparedness for an incident. Therefore, this document addresses the development of procedures to increase the confidence of an organization’s actual readiness to respond to an information security incident. This is achieved by addressing the policies and plans associated with incident management, as well as the process for establishing the incident response team and improving its performance over time by adopting lessons learned and by evaluation.

© ISO/IEC 2023 – All rights reserved

Information technology — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

1 Scope

This document provides guidelines to plan and prepare for incident response and to learn lessons from incident response. The guidelines are based on the "plan and prepare" and "learn lessons" phases of the information security incident management phases model presented in ISO/IEC 27035-1:2023, 5.2 and 5.6.

The major points within the "plan and prepare" phase include:

— information security incident management policy and commitment of top management;

— information security policies, including those relating to risk management, updated at both organizational level and system, service and network levels;

— information security incident management plan;

— Incident Management Team (IMT) establishment;

— establishing relationships and connections with internal and external organizations;

— technical and other support (including organizational and operational support);

— information security incident management awareness briefings and training.

The "learn lessons" phase includes:

— identifying areas for improvement;

— identifying and making necessary improvements;

— Incident Response Team (IRT) evaluation.

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

2 Normative references

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

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

ISO/IEC 27035-1:2023, *Information technology — Information security incident management — Part 1: Principles and process*

© ISO/IEC 2023 – All rights reserved

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.2 Abbreviated terms

CERT	computer emergency response team
CSIRT	computer security incident response team
IMT	Incident Management Team
IRT	Incident Response Team
PoC	Point of Contact

4 Information security incident management policy

4.1 General

NOTE Clause 4, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 a).

An organization's information security incident management policy should provide the formally documented principles and intentions used to direct decision-making. Supporting processes and procedures ensures consistent application of the policy.

Any information security incident management policy should be part of the information security strategy for an organization. It should also support the existing mission of its parent organization and be in line with already existing policies and procedures.

An organization should implement an information security incident management policy that outlines the processes, responsible persons, authority and reporting lines when an information security event/incident occurs. The policy should be reviewed regularly to ensure it reflects the latest organizational structure, processes, and technology that can affect incident management. The policy should also outline any awareness and training initiatives within the organization that are related to incident management (see Clause 10).

An organization should document its policy for managing information security events, incidents and vulnerabilities as a free-standing document, as part of its overall information security management system policy (see ISO/IEC 27001:2022, 5.2), or as part of its information security policies (see ISO/IEC 27002:2022, 5.1). The size, structure and business nature of an organization and the extent of its information security incident management programme are deciding factors in determining which of these options to adopt. An organization should direct its information security incident management policy at every person having legitimate access to its information systems and related locations.

Before the information security incident management policy is formulated, the organization should identify the following regarding its information security incident management:

a) principles, objectives and purpose;

© ISO/IEC 2023 – All rights reserved