International Standard

ISO/IEC 27035-4

First edition
2024-12

Information technology — Information security incident management —

Part 4: Coordination

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

Partie 4: Coordination

Reference number
ISO/IEC 27035-4:2024(en)

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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*.

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

Coordination is an important aspect in information security incident management. Incidents crossing organizational boundaries can occur and cannot be easily resolved by a single organization. Emerging threats are becoming increasingly sophisticated and can have a much larger impact than previously. The characteristics of emerging threats and attacks make it more urgent than ever to coordinate incidents across organizations.

Coordination can include relevant parties both within and outside the organization. For example, relevant parties within the organization include business managers and representatives from IT; external interested parties include incident response teams of external organizations and law enforcement organizations. See ISO/IEC 27035-2:2023, Clause 8 for a complete list. This document, however, only considers coordination between multiple organizations. This document provides guidelines for multiple organizations to work together to handle information security incidents. The coordination activities occur throughout the information security incident management process as defined in ISO/IEC 27035-1.

This document addresses the coordination of information security incident management between multiple organizations. Incidents sometimes involve technical vulnerabilities. Guidance on the coordination, disclosure, and handling of technical vulnerabilities is provided by ISO/IEC 29147 and ISO/IEC 30111. Additional information on the coordination of technical vulnerabilities between multiple organizations is provided by ISO/IEC TR 5895.

Information technology — Information security incident management —

Part 4: Coordination

1 Scope

This document provides guidelines for multiple organizations handling information security incidents in a coordinated manner. It also addresses the impacts of external cooperation on the internal incident management of an individual organization and provides guidelines for an individual organization to adapt to the coordination process. Furthermore, it provides guidelines for the coordination team, if it exists, to perform coordination activities supporting the cross-organization incident response.

The principles given in this document are generic and are intended to be applicable to multiple organizations to work together to handle information security incidents, regardless of their types, sizes or nature. Organizations can adjust the guidance given in this document according to their type, sizes and nature of business in relation to the information security risk situation. This document is also applicable to an individual organization that participates in partner relationships.

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 — Information security incident management — Part 1: Principles and process*

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

ISO/IEC 27035-3, *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3 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
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.

[SOURCE: ISO/IEC 27035-1:2023, 3.1.2]

3.2
coordinated incident management
CIM
process for IRTs from multiple organizations to work together to handle information security incidents

3.3
community
group of associated organizations, individuals and groups sharing common interests

Note 1 to entry: Impacted communities are the groups of people and associated organizations affected by the provision of security services, projects or operations.

[SOURCE: ISO 22300:2021, 3.1.39]

4 Overview

4.1 General

Coordination is an important aspect in information security incident management. As stated in ISO/IEC 27035-1, coordination can occur throughout the information security incident management process, and the responsible roles for coordination should be taken by the incident management team (IMT) and the incident coordinator. Coordination can include both internal and external parties (see a full list of these parties in ISO/IEC 27035-2:2023, Clause 8). Among different parties, there are different degrees of coordination relationships. Some coordination relationships are loose, only involving information disclosure, such as the contacts with internal representatives from the legal department, public relations, or external parties like law enforcement and media. Other coordination relationships are dense, targeting incident response, which involves working with multiple internal incident response teams, or the incident response teams from external organizations and internet service providers (ISPs). See Annex A for examples of information security incident management coordination. ISO/IEC 27035-1, ISO/IEC 27035-2 and ISO/IEC 27035-3 focus on guidelines for information security incident management within a single organization, and internal and external coordination activities are only briefly covered. This document gives further detail on coordination between multiple organizations, and can benefit different organizations to achieve a structured and effective cross-organization incident response. Figure 1 illustrates the scope of this document.

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.

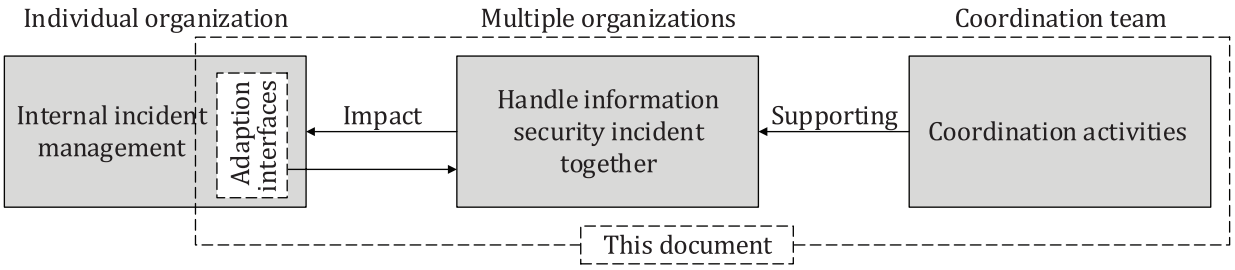

Figure 1 — Illustration of the scope of this document

It is more possible to achieve good coordination between multiple organizations, when organizations use incident management process (see ISO 22320). Based on the incident management process defined in ISO/IEC 27035-1, the coordinated incident management process can be illustrated as in Figure 2. The guidelines on the coordinated incident management process and its key activities are generic, which allows flexibility so that coordination can be applied to incident management partially or entirely as needed (e.g. the loose coordination case which only involves information disclosure is also applicable).

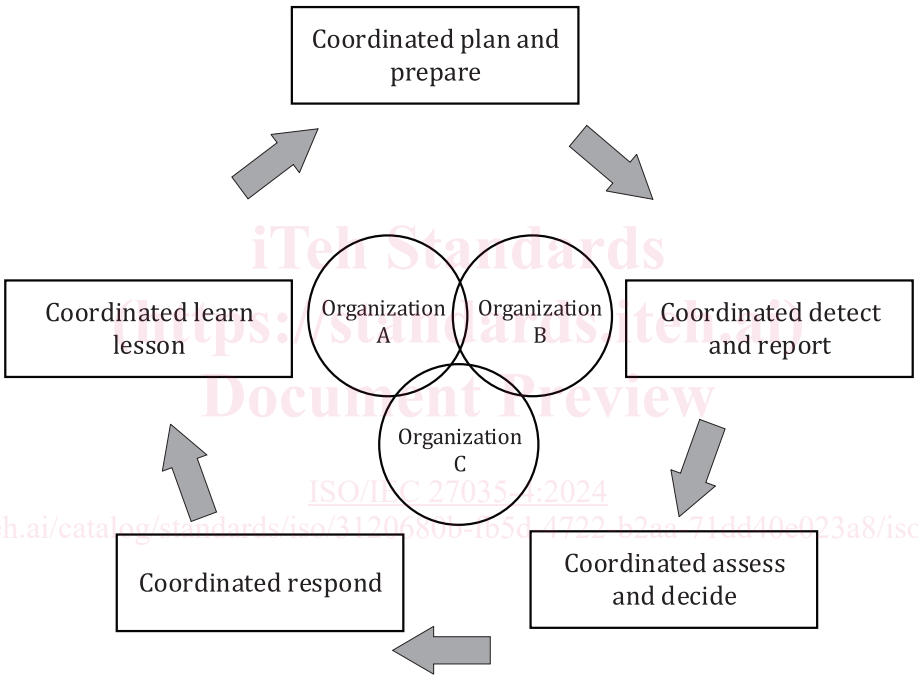

Figure 2 — Illustration of coordinated incident management process for multiple organizations

4.2 Coordination team

The coordination team is a special type of incident response team. They usually work as independent entities which focus on the incident management coordination. The coordination team has the following features.

a) The coordination teams focus on activities including information exchanging, information sharing and response coordination. It is possible that the coordination team does not implement incident response activities directly. They facilitate efficient incident management coordination and cooperation among multiple members. By fully dispatching the resources of each member, they help to realize information sharing between members and throughout the entire community.

b) The coordination team should have a defined service constituency. The constituency is usually based on a geographic location or a business domain. Typical examples of coordination teams based on geographical regions are national incident response teams and regional incident response teams in international regions or within a country. The main reason for setting up a coordination team based on

industry sectors is that organizations in the same industry face similar cybersecurity risks. Thus, the appeal and value of information sharing and response coordination is greater.

c) The coordination team acts as a central point in the incident management coordination. Multiple coordination teams can be arranged in a peer mode or a hierarchical mode. The coordination team and the members can be regarded as forming a community, whereby the coordination team acts as a central point when coordination is needed between multiple members. If the impact of the incident exceeds the coordination team's constituency or capability, the coordination team should contact another relevant coordination team or relevant community member for assistance.

4.3 Principles of coordination

4.3.1 Timeliness principle

Information security incidents are highly time-sensitive. Any threat information and incident status has a certain validity period. Therefore, all parties should agree on the time requirements of each item before performing incident management coordination and observe the agreed time in the coordinated incident management process.

4.3.2 Roles and responsibilities principle

Clear roles and responsibilities should be defined for incident management coordination activities. When working under a coordination model with multiple organizations involved, it is important for all parties to know the role that they play and what their respective responsibilities are under the model. In this manner, all parties know what is expected of them to enable cohesion and minimise confusion. In addition, where the lead coordinator role changes (e.g. depending on the content and context of the specific incident), criteria should also be established to determine who leads coordination for that incident.

4.3.3 Common understanding principle

Communicating and coordinating incident response information can be difficult unless the organizations involved utilize shared vocabulary. Organizations should use a common language and terminology to support the exchange of information and facilitate understanding. Also, by adopting a common taxonomy to classify information and standardizing data exchange format, organizations can have common understanding of the security information shared by others. A common understanding can help organizations to reach consensus and ensure their goals are consistent in the incident management coordination.

4.3.4 Confidentiality principle

During the incident management coordination, it is possible for organizations involved to carry out information communication or exchange. Organizations should be careful to protect secret business information and personal sensitive information when transmitting information to external parties. They should consult their legal department to formulate confidentiality rules for information exchange.

5 Coordinated incident management process

5.1 Overview

As illustrated in Figure 2, the coordinated incident management process has the same phases as the incident management process as defined in ISO/IEC 27035-1, namely:

— coordinated plan and prepare (see 5.2);

— coordinated detect and report (see 5.3);

— coordinated assess and decide (see 5.4);

— coordinated respond (see 5.5);

— coordinated learn lessons (see 5.6).

Figure 3 shows an overview of the activities in the coordinated incident management process, covering:

— coordinated activities for multiple organizations to complete together;

— the impacts on the internal activities of an individual organization and the adaption to make;

— if a coordination team exists, the coordination activities it performs.

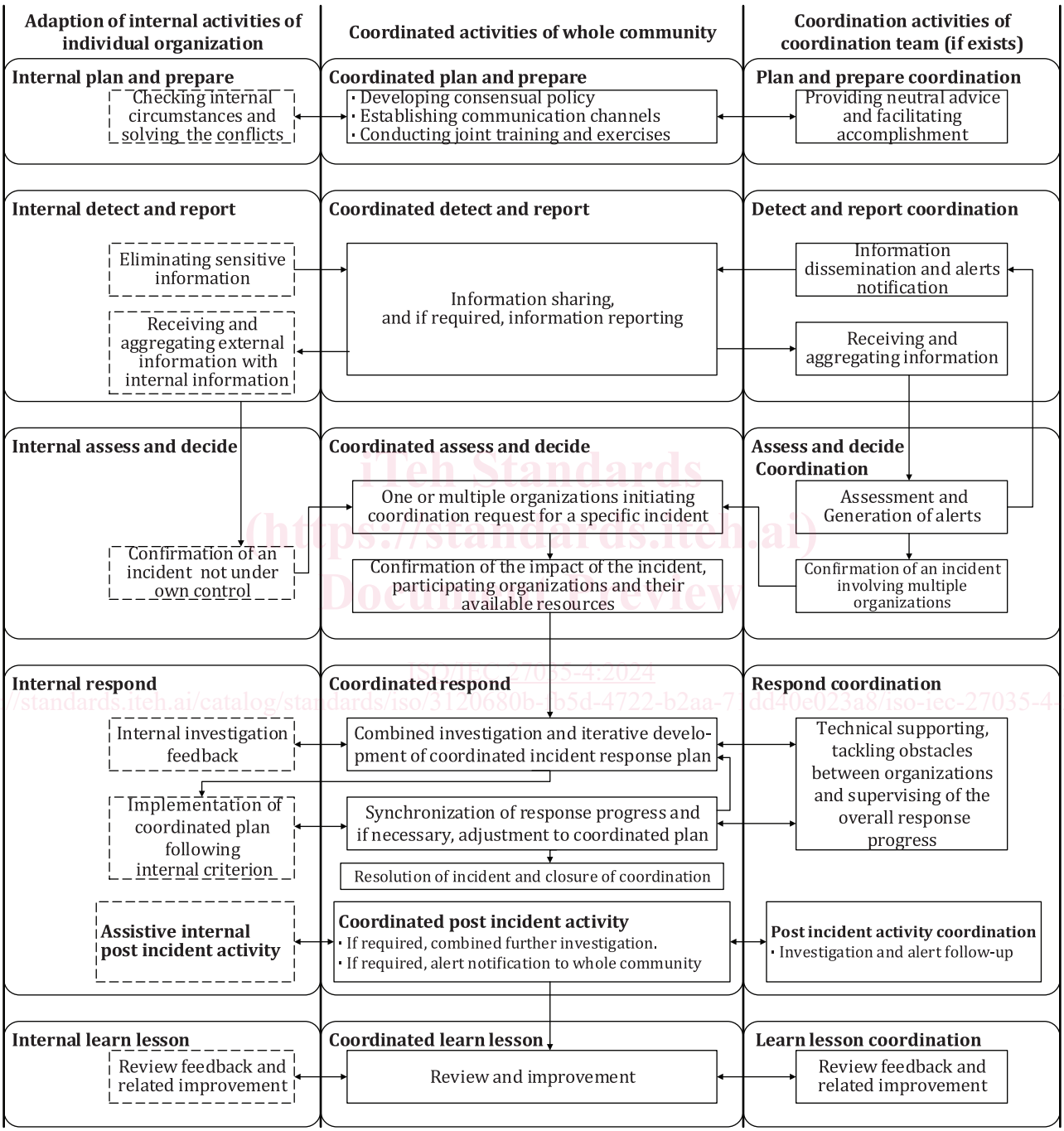

Figure 3 — Overview of coordinated incident management process

5.2 Coordinated plan and prepare

In the coordinated plan and prepare phase, organizations in the community reach an agreement on coordination policies and public framework, establish communication channels, and conduct training and