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/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Overview ... **2**
4.1 General ... 2
4.2 Coordination team ... 3
4.3 Principles of coordination ... 4
4.3.1 Timeliness principle ... 4
4.3.2 Roles and responsibilities principle ... 4
4.3.3 Common understanding principle ... 4
4.3.4 Confidentiality principle ... 4
5 Coordinated incident management process ... **4**
5.1 Overview ... 4
5.2 Coordinated plan and prepare ... 5
5.3 Coordinated detect and report ... 6
5.4 Coordinated assessment and decision ... 7
5.5 Coordinated respond ... 8
5.6 Coordinated learn lessons ... 9
6 Guidelines for key activities of coordinated incident management ... **10**
6.1 Developing coordination policies ... 10
6.2 Establishing communications ... 11
6.3 Threat and event Information sharing ... 11
6.3.1 Overview ... 11
6.3.2 Information types ... 12
6.3.3 Establishing information sharing relationships ... 13
6.3.4 Participating information sharing relationships ... 14
6.4 Conducting coordinated exercises ... 16
6.5 Building trust ... 17
Annex A (informative) **Examples of information security incident management coordination** ... **19**
Bibliography ... **22**

© ISO/IEC 2024 – 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).

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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/

© ISO/IEC 2024 – All rights reserved