INTERNATIONAL STANDARD

ISO/IEC 27035-1

First edition
2016-11-01

Information technology — Security techniques — Information security incident management —

Part 1: Principles of incident management

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

Partie 1: Principes de la gestion des incidents

Reference number
ISO/IEC 27035-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035-1, together with ISO/IEC 27035-2, cancels and replaces ISO/IEC 27035:2011, which has been technically revised.

ISO/IEC 27035 consists of the following parts, under the general title *Information technology — Security techniques — Information security incident management*:

— *Part 1: Principles of incident management*

— *Part 2: Guidelines to plan and prepare for incident response*

Further parts may follow.

Introduction

Information security policies or controls alone will 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 impacts on an organization's business operations. Furthermore, it is inevitable that new instances of previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any response less effective, and increase the degree of potential adverse business impact. Therefore, it is essential for any organization desiring a strong information security program to have a structured and planned approach to:

— detect, report and assess information security incidents;

— respond to information security incidents, including the activation of appropriate controls to prevent, reduce, and recover from impacts;

— report information security vulnerabilities, so they can be assessed and dealt with appropriately;

— learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

For the purpose of achieving this planned approach, ISO/IEC 27035 provides guidance on aspects of information security incident management in the following corresponding parts.

— ISO/IEC 27035-1, *Principles of incident management* (this document), presents basic concepts and phases of information security incident management, and how to improve incident management. This part combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.

— ISO/IEC 27035-2, *Guidelines to plan and prepare for incident response*, describes how to plan and prepare for incident response. This part covers the "Plan and Prepare" and "Lessons Learnt" phases of the model presented in ISO/IEC 27035-1.

ISO/IEC 27035 is intended to complement other standards and documents that give guidance on the investigation of, and preparation to investigate, information security incidents. ISO/IEC 27035 is not a comprehensive guide, but a reference for certain fundamental principles 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 ISO/IEC 27035 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 provided in ISO/IEC 29147 and ISO/IEC 30111, respectively.

ISO/IEC 27035 also intends to inform decision-makers that need to determine 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.

Information technology — Security techniques — Information security incident management —

Part 1: Principles of incident management

1 Scope

This part of ISO/IEC 27035 is the foundation of this multipart International Standard. It presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.

The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 27035-2, *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

3 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 terminological databases for use in standardization at the following addresses:

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

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

3.1
information security investigation
application of examinations, analysis and interpretation to aid understanding of an *information security incident* (3.4)

[SOURCE: ISO/IEC 27042, 3.10, modified — The phrase “an incident” was replaced by “an information security incident”.]