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”.]

3.2
incident response team
IRT
team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle

Note 1 to entry: CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are commonly used terms for IRT.

3.3
information security event
occurrence indicating a possible breach of information security or failure of controls

3.4
information security incident
one or multiple related and identified *information security events* (3.3) that can harm an organization's assets or compromise its operations

3.5
information security incident management
exercise of a consistent and effective approach to the handling of *information security incidents* (3.4)

3.6
incident handling
actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.4)

3.7
incident response
actions taken to mitigate or resolve an *information security incident* (3.4), including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

3.8
point of contact
PoC
defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities

4 Overview

4.1 Basic concepts and principles

An information security event is an occurrence indicating a possible breach of information security or failure of controls. An information security incident is one or multiple related and identified information security events that meet established criteria and can harm an organization's assets or compromise its operations.

The occurrence of an information security event does not necessarily mean that an attack has been successful or that there are any implications on confidentiality, integrity or availability, i.e., not all information security events are classified as information security incidents.

Information security incidents can be deliberate (e.g. caused by malware or intentional breach of discipline) or accidental (e.g. caused by inadvertent human error or unavoidable acts of nature) and can be caused by technical (e.g. computer viruses) or non-technical (e.g. loss or theft of computers) means. Consequences can include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information.

Annex B provides descriptions of selected example information security incidents and their causes for informative purposes only. It is important to note that these examples are by no means exhaustive.

A threat exploits vulnerabilities (weaknesses) in information systems, services, or networks, causing the occurrence of information security events and thus potentially causing incidents to information assets exposed by the vulnerabilities. Figure 1 shows the relationship of objects in an information security incident.

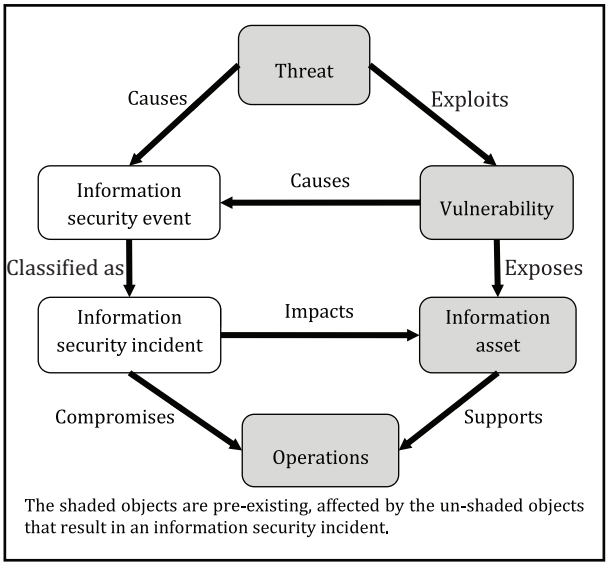

Figure 1 — Relationship of objects in an information security incident

Information sharing and coordination with external IRTs is an important consideration. Many incidents cross organizational boundaries and cannot be easily resolved by a single IRT. Information sharing and coordination relationships or partnerships with external IRTs can greatly enhance the ability to respond to and resolve incidents. For further detail about information sharing, see ISO/IEC 27010.

4.2 Objectives of incident management

As a key part of an organization's overall information security strategy, the organization should put controls and procedures in place to enable a structured well-planned approach to the management of information security incidents. From an organization's perspective, the prime objective is to avoid or contain the impact of information security incidents in order to minimize the direct and indirect damage to its operations caused by the incidents. Since damage to information assets can have a negative impact on operations, business and operational perspectives should have a major influence in determining more specific objectives for information security management.

More specific objectives of a structured well-planned approach to incident management should include the following:

a) information security events are detected and dealt with efficiently, in particular deciding when they should be classified as information security incidents;

b) identified information security incidents are assessed and responded to in the most appropriate and efficient manner;

c) the adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response;

d) a link with relevant elements from crisis management and business continuity management through an escalation process is established;

e) information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the IRT or other teams within the organization, depending on duty distribution;

f) lessons are learnt quickly from information security incidents, vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

To help achieve these objectives, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards for incident categorization, classification, and sharing, so that metrics can be derived from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls. The information security incident management system should be able to share information with relevant external parties and IRTs.

Another objective associated with this part of ISO/IEC 27035 is to provide guidance to organizations that aim to meet the Information Security Management System (ISMS) requirements specified in ISO/IEC 27001 which are supported by guidance from ISO/IEC 27002. ISO/IEC 27001 includes requirements related to information security incident management. A table that cross-references information security incident management clauses in ISO/IEC 27001 and clauses in this part of ISO/IEC 27035 is provided in Annex C. ISMS relationships are also explained in Figure 2. This part of ISO/IEC 27035 can also support the requirements of information security management systems other than ISMS.

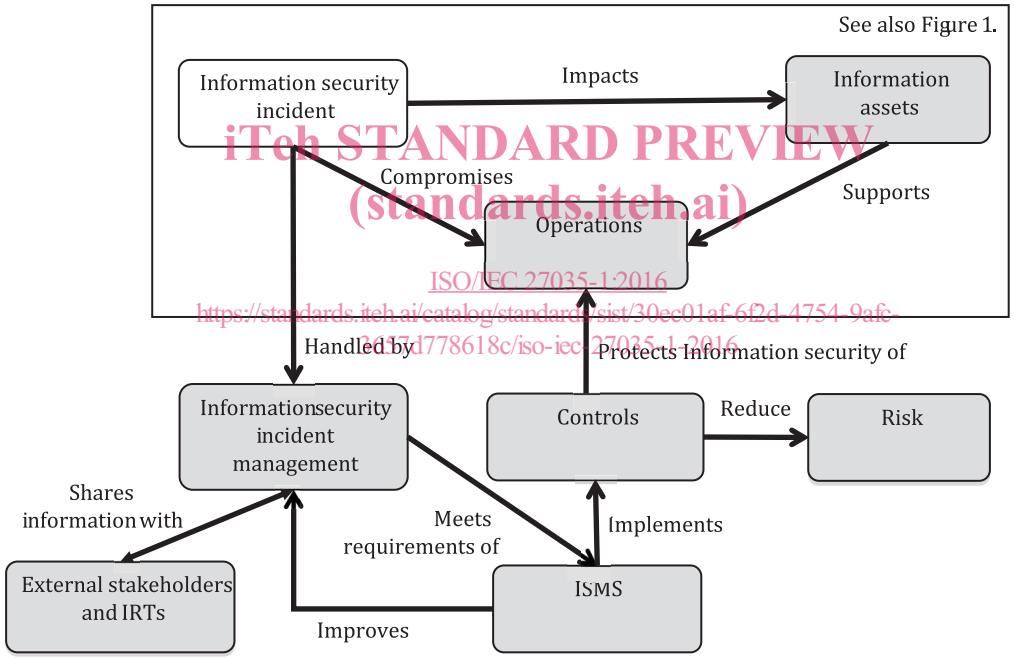

Figure 2 — Information security incident management in relation to ISMS and applied controls

4.3 Benefits of a structured approach

Using a structured approach to information security incident management can yield significant benefits, which can be grouped under the following topics.

a) Improving overall information security

A structured process for detection, reporting and assessment of and decision-making related to information security events and incidents will enable rapid identification and response. This will improve overall security by helping to quickly identify and implement a consistent solution, and thus provide a means of preventing future similar information security incidents. Furthermore, there will be benefits gained by metrics, sharing and aggregation. The credibility of the organization will be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business impacts

A structured approach to information security incident management can assist in reducing the level of potential adverse business impacts associated with information security incidents. These impacts can include immediate financial loss and longer-term loss arising from damaged reputation and credibility. For guidance on business impact analysis, see ISO/IEC 27005. For guidance on information and communication technology readiness for business continuity, see ISO/IEC 27031.

c) Strengthening the focus on information security incident prevention

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including the development of methods to identify new threats and vulnerabilities. Analysis of incident-related data enables the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and identification of appropriate actions to prevent further occurrence.

d) Improving prioritization

A structured approach to information security incident management will provide a solid basis for prioritization when conducting information security incident investigations, including the use of effective categorization and classification scales. If there are no clear procedures, there is a risk that investigation activities could be conducted in an overly reactive mode, responding to incidents as they occur and overlooking what activities should be handled with a higher priority.

e) Supporting evidence collection and investigation

If and when needed, clear incident investigation procedures will help to ensure that data collection and handling are evidentially sound and legally admissible. These are important considerations if legal prosecution or disciplinary action might follow. For more information on digital evidence and investigation, see the investigative standards in Annex A.

f) Contributing to budget and resource justifications

A well-defined and structured approach to information security incident management will help justify and simplify the allocation of budgets and resources for involved organizational units. Furthermore, benefit will accrue for the information security incident management plan itself, with the ability to better plan for the allocation of staff and resources.

One example of a way to control and optimize budget and resources is to add time tracking to information security incident management tasks to facilitate quantitative assessment of the organization's handling of information security incidents. It should be possible to provide information on how long it takes to resolve information security incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.