INTERNATIONAL STANDARD

ISO/IEC 27035-3

First edition
2020-09

Information technology — Information security incident management —

Part 3: Guidelines for ICT incident response operations

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

Partie 3: Lignes directrices relatives aux opérations de réponse aux incidents TIC

Reference number
ISO/IEC 27035-3:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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 2020 – All rights reserved

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Overview **3**
5.1 General 3
5.2 Structure of this document 3
6 Common types of attacks **5**
7 Incident detection operations **6**
7.1 Point of contact 6
7.2 Monitoring and detection 7
7.3 Common ways detection is performed 8
7.3.1 Monitoring public sources to look for potential reports (and threats) 8
7.3.2 Validation of external source data 9
7.3.3 Proactive detection 10
7.3.4 Reactive methods 10
8 Incident notification operations **11**
8.1 Overview 11
8.2 Immediate incident notification 12
8.2.1 Incident reporting forms 12
8.2.2 Critical information that incident reports should (ideally) contain 12
8.2.3 Methods to receive reports 12
8.2.4 Considerations for escalation 13
8.3 PoC structure 13
8.3.1 Incident response operation notification if a single PoC exists 13
8.3.2 Incident response operation notification if multiple PoCs exist 14
9 Incident triage operations **14**
9.1 Overview 14
9.2 How triage is conducted 14
10 Incident analysis operations **15**
10.1 Overview 15
10.2 Purpose of analysis 17
10.3 Intra-incident analysis 18
10.4 Inter-incident analysis 19
10.5 Analysis tools 20
10.6 Storing evidence and analysis results 20
11 Incident containment, eradication and recovery operations **21**
11.1 Overview 21
11.2 Conducting the response for containment, eradication and recovery 21
11.2.1 Containment description 21
11.2.2 Containment goals 21
11.2.3 Common containment strategies 21
11.2.4 Issues associated with containment 22
11.3 Eradication 22
11.3.1 Eradication description 22
11.3.2 Eradication strategies 22
11.3.3 Issues associated with eradication 23
11.4 Recovery 23

© ISO/IEC 2020 – All rights reserved

11.4.1 Recovery description 23
11.4.2 Recovery strategies 23
11.4.3 Issues associated with recovery 23

12 Incident reporting operations 23
12.1 Overview 23
12.2 How to establish reporting 24
12.3 How to establish external reporting, if required 25
12.4 Information sharing 26
12.5 Other reporting considerations 26
12.6 Types of reports 27
12.7 Methods for storing reports and analysts' knowledge 27

Annex A (informative) **Example of the incident criteria based on information security events and incidents 28**

Bibliography 31

 © ISO/IEC 2020 – 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).

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 http://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.

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 27035 series can be found on the ISO website.

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.

© ISO/IEC 2020 – All rights reserved

Introduction

An information security incident can involve ICT or not. For example, information that spreads unintentionally through the loss of paper documents can very well be a serious information security incident, which requires incident reporting, investigation, containment, corrective actions and management involvement. This type of incident management is often carried out, for example, by the Chief Information Security Officer (CISO) within the organization. Guidance on the management of such information security incidents can be found in ISO/IEC 27035-1. This document, however, only considers incident response operations for ICT-related incidents, and not for information security incidents related to paper documents or any other non-ICT incidents. Whenever the term "information security" is used in this document, it is done so in the context of ICT-related information security.

The organizational structures for information security vary depending on the size and business field of organizations. As various and numerous incidents occur and are increasing (such as network incidents, e.g. intrusions, data breaches and hacking), higher concerns about information security have been raised by organizations. A secure ICT environment set up to withstand various types of attacks (such as DoS, worms and viruses) with network security equipment such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) should be complemented with clear operating procedures for incident handling, along with well-defined reporting structures within the organization.

To ensure confidentiality, integrity and availability of information and to handle incidents efficiently, capabilities to conduct incident response operations is required. For this purpose, a computer security incident response team (CSIRT) should be established to perform tasks such as monitoring, detection, analysis and response activities for collected data or security events. These tasks may be assisted by artificial intelligence tools and techniques.

This document supports the controls of ISO/IEC 27001:2013, Annex A, related to incident management.

Not all steps in this document are applicable since it depends on the particular incident. For example, a smaller organization may not use all guidance in this document but can find it useful for organization of their ICT-related incident operations especially if operating their own ICT environment. It can also be useful for smaller organizations that have outsourced their IT operations to better understand the requirements and execution of incident operations that they should expect from their ICT supplier(s).

This document is particularly useful to organizations providing ICT services that involve interactions between organizations of incident operations in order to follow the same processes and terms.

This document also provides a better understanding on how incident operations relates to the users/customers in order to define when and how such interaction needs to take place, even if this is not specified.

© ISO/IEC 2020 – All rights reserved

Information technology — Information security incident management —

Part 3: Guidelines for ICT incident response operations

1 Scope

This document gives guidelines for information security incident response in ICT security operations. This document does this by firstly covering the operational aspects in ICT security operations from a people, processes and technology perspective. It then further focuses on information security incident response in ICT security operations including information security incident detection, reporting, triage, analysis, response, containment, eradication, recovery and conclusion.

This document is not concerned with non-ICT incident response operations such as loss of paper-based documents.

This document is based on the "Detection and reporting" phase, the "Assessment and decision" phase and the "Responses" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1:2016.

The principles given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the provisions 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, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

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

ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 27043, *Information technology — Security techniques — Incident investigation principles and processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27037, ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27043 and the following apply.

© ISO/IEC 2020 – All rights reserved

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

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

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

3.1
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27032:2012, 4.6]

3.2
computer security incident response team
CSIRT
team of security experts to support the handling of information security incidents

[SOURCE: ISO/IEC 27019:2017, 3.2]

3.3
investigation
systematic or formal process of inquiring into or researching, and examining facts or materials associated with a matter

Note 1 to entry: A similar definition can be found in ISO/IEC 27042:2015, 3.10.

[SOURCE: ISO/IEC 27050:2017, 3.17, modified — Note 1 to entry has been added.]

3.1.4
response
incident response
action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs

[SOURCE: ISO/IEC 27039:2015, 2.24]

4 Abbreviated terms

ASCII	American standard code for information interchange
CPU	central processing unit
DNS	domain name system or domain name service
DDoS	distributed denial of service
DoS	denial of service
ENISA	European Union agency for network and information security
FAT	file allocation table file system
FAT32	32-bit file allocation table file system
FIRST	forum of incident response and security teams
HPFS	high performance file system
HR	human resources
ICT	information and communication technology

© ISO/IEC 2020 – All rights reserved