
**Information technology — Security
techniques — Information security
incident management —**

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

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

*Partie 2: Lignes directrices pour planifier et préparer une réponse aux
incidents*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions.....	2
3.2 Abbreviated terms.....	2
4 Information security incident management policy	3
4.1 General.....	3
4.2 Involved parties.....	3
4.3 Information security incident management policy content.....	4
5 Updating of information security policies	6
5.1 General.....	6
5.2 Linking of policy documents.....	6
6 Creating information security incident management plan	6
6.1 General.....	6
6.2 Information security incident management plan built on consensus.....	7
6.3 Involved parties.....	8
6.4 Information security incident management plan content.....	8
6.5 Incident classification scale.....	12
6.6 Incident forms.....	12
6.7 Processes and procedures.....	12
6.8 Trust and confidence.....	13
6.9 Handling confidential or sensitive information.....	14
7 Establishing an incident response team (IRT)	14
7.1 General.....	14
7.2 IRT types and roles.....	14
7.3 IRT staff.....	16
8 Establishing relationships with other organizations	19
8.1 General.....	19
8.2 Relationship with other parts of the organization.....	19
8.3 Relationship with external interested parties.....	20
9 Defining technical and other support	20
9.1 General.....	20
9.2 Examples of technical support.....	22
9.3 Examples of other support.....	22
10 Creating information security incident awareness and training	22
11 Testing the information security incident management plan	24
11.1 General.....	24
11.2 Exercise.....	24
11.2.1 Defining the goal of the exercise.....	24
11.2.2 Defining the scope of an exercise.....	25
11.2.3 Conducting an exercise.....	25
11.3 Incident response capability monitoring.....	26
11.3.1 Implementing an incident response capability monitoring program.....	26
11.3.2 Metrics and governance of incident response capability monitoring.....	26
12 Lessons learned	27
12.1 General.....	27
12.2 Identifying the lessons learned.....	27

12.3	Identifying and making improvements to information security control implementation	28
12.4	Identifying and making improvements to information security risk assessment and management review results	28
12.5	Identifying and making improvements to the information security incident management plan	28
12.6	IRT evaluation	29
12.7	Other improvements	30
Annex A (informative) Legal and regulatory aspects		31
Annex B (informative) Example information security event, incident and vulnerability reports and forms		34
Annex C (informative) Example approaches to the categorization and classification of information security events and incidents		46
Bibliography		57

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 27035-2, together with ISO/IEC 27035-1, 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

ISO/IEC 27035 is an extension of ISO/IEC 27000 series of standards and it focuses on information security incident management which is identified in ISO/IEC 27000 as one of the critical success factor for the information security management system.

There can be a large gap between an organization's plan for an incident and an organization knowing it is prepared for an incident. Therefore, this part of ISO/IEC 27035 addresses the development of guidelines to increase the confidence of an organization's actual readiness to respond to an information security incident. This is achieved by addressing the policies and plans associated with incident management, as well as how to establish the incident response team and improve its performance over time by adopting lessons learned and by evaluation.

Information technology — Security techniques — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

1 Scope

This part of ISO/IEC 27035 provides the guidelines to plan and prepare for incident response. The guidelines are based on the “Plan and Prepare” phase and the “Lessons Learned” phase of the “Information security incident management phases” model presented in ISO/IEC 27035-1.

The major points within the “Plan and Prepare” phase include the following:

- information security incident management policy and commitment of top management;
- information security policies, including those relating to risk management, updated at both corporate level and system, service and network levels;
- information security incident management plan;
- incident response team (IRT) establishment;
- establish relationships and connections with internal and external organizations;
- technical and other support (including organizational and operational support);
- information security incident management awareness briefings and training;
- information security incident management plan testing.

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 27035-1:2016, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*