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

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



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

| | |
|--------------------------------------------------------------------------------------------------------------------------------------|----|
| Foreword | v |
| Introduction..... | vi |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 Overview..... | 2 |
| 4.1 Basic concepts | 2 |
| 4.2 Objectives | 3 |
| 4.3 Benefits of a structured approach | 4 |
| 4.4 Adaptability | 5 |
| 4.5 Phases | 6 |
| 4.6 Examples of information security incidents..... | 7 |
| 5 Plan and prepare phase | 8 |
| 5.1 Overview of key activities..... | 8 |
| 5.2 Information security incident management policy | 10 |
| 5.3 Information security incident management integration in other policies | 12 |
| 5.4 Information security incident management scheme | 13 |
| 5.5 Establishment of the ISIRT | 18 |
| 5.6 Technical and other support (including operational support)..... | 19 |
| 5.7 Awareness and training | 20 |
| 5.8 Scheme testing | 22 |
| 6 Detection and reporting phase | 22 |
| 6.1 Overview of key activities..... | 22 |
| 6.2 Event detection..... | 25 |
| 6.3 Event reporting | 25 |
| 7 Assessment and decision phase | 26 |
| 7.1 Overview of key activities..... | 26 |
| 7.2 Assessment and initial decision by the PoC | 28 |
| 7.3 Assessment and incident confirmation by the ISIRT | 30 |
| 8 Responses phase | 31 |
| 8.1 Overview of key activities..... | 31 |
| 8.2 Responses | 32 |
| 9 Lessons learnt phase | 40 |
| 9.1 Overview of key activities..... | 40 |
| 9.2 Further information security forensic analysis | 40 |
| 9.3 Identifying the lessons learnt..... | 41 |
| 9.4 Identifying and making improvements to information security control implementation | 42 |
| 9.5 Identifying and making improvements to information security risk assessment and management review results | 42 |
| 9.6 Identifying and making improvements to the information security incident management scheme | 42 |
| 9.7 Other improvements | 43 |
| Annex A (informative) Cross reference table of ISO/IEC 27001 vs ISO/IEC 27035..... | 44 |
| Annex B (informative) Examples of information security incidents and their causes | 47 |
| Annex C (informative) Example approaches to the categorization and classification of information security events and incidents | 50 |

Annex D (informative) Example information security event, incident and vulnerability reports and forms.....62

Annex E (informative) Legal and regulatory aspects74

Bibliography.....76

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27035 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035 cancels and replaces ISO/IEC TR 18044:2004, which has been technically revised.

Introduction

In general, 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 make information security ineffective and thus information security incidents possible. This can potentially have both direct and indirect adverse impacts on an organization's business operations. Further, 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 serious about information security 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 for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas);
- report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

This International Standard provides guidance on information security incident management in Clause 4 to Clause 9. These clauses consist of several subclauses, which include a detailed description of each phase.

The term 'information security incident management' is used in this International Standard to encompass the management of not just information security incidents but also information security vulnerabilities.

Information technology — Security techniques — Information security incident management

1 Scope

This International Standard provides a structured and planned approach to:

- a) detect, report and assess information security incidents;
- b) respond to and manage information security incidents;
- c) detect, assess and manage information security vulnerabilities; and
- d) continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

This International Standard provides guidance on information security incident management for large and medium-sized organizations. Smaller organizations can use a basic set of documents, processes and routines described in this International Standard, depending on their size and type of business in relation to the information security risk situation. It also provides guidance for external organizations providing information security incident management services.

2 Normative references

The following referenced documents are indispensable for the application 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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1

information security forensics

application of investigation and analysis techniques to capture, record and analyse information security incidents

3.2

information security incident response team

ISIRT

team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle