AS ISO/IEC 27035.1:2017
ISO/IEC 27035-1:2016

AS ISO/IEC 27035.1:2017

Information technology—Security techniques—Information security incident management

Part 1: Principles of incident management

This Australian Standard® was prepared by Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 5 April 2017.
This Standard was published on 11 May 2017.

The following are represented on Committee IT-012:

- Australian Association of Permanent Building Societies
- Australian Information Industry Association
- Australian Payment Network
- Department of Defence (Australian Government)
- Department of Finance (Australian Government)
- Engineers Australia
- Office of the Commissioner for Privacy and Data Protection

This Standard was issued in draft form for comment as DR AS ISO/IEC 27035.1:2017.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Information technology—Security techniques—Information security incident management

Part 1: Principles of incident management

First published as AS ISO/IEC 27035.1:2017.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 76035 762 7

PREFACE

This Standard was prepared by the Standards Australia Committee IT-012, Information Systems, Security and Identification Technology.

The objective of this Standard is to present 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. This Standard provides the foundation for the *Information technology—Security techniques—Information security incident management* series.

This Standard is identical with, and has been reproduced from ISO/IEC 27035-1:2016, *Information technology—Security techniques—Information security incident management*, Part 1: Principles of *incident management.*

As this Standard is reproduced from an International Standard, the following applies:

(a) In the source text 'this part of ISO/IEC 27035' should read 'this Australian Standard'.

(b) A full point substitutes for a comma when referring to a decimal marker.

None of the normative references in the source document have been adopted as Australian or Australian/New Zealand Standards.

The term 'informative' has been used in this Standard to define the application of the annex to which it applies. An 'informative' annex is only for information and guidance.

CONTENTS

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.

AUSTRALIAN STANDARD

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”.]