AS ISO/IEC 27035.2:2017
ISO/IEC 27035-2:2016

AS ISO/IEC 27035.2:2017

Information technology—Security techniques—Information security incident management

Part 2: Guidelines to plan and prepare for incident response

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 27035.2:2017.

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Standards may also be withdrawn.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 2: Guidelines to plan and prepare for incident response

First published as AS ISO/IEC 27035.2:2017.

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

ISBN 978 1 76035 763 4

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 provide guidelines to plan and prepare for incident response. The guidelines are based on the 'Plan and Prepare' and 'Lessons Learnt' phases of the 'Information security incident management phases' model presented in ISO/IEC 27035-1.

This Standard is identical with, and has been reproduced from ISO/IEC 27035-2:2016, *Information technology—Security techniques—Information security incident management*, Part 2: *Guidelines to plan and prepare for incident response.*

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

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.

AUSTRALIAN STANDARD

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*