AS ISO/IEC 27013:2017
ISO/IEC 27013:2015

AS ISO/IEC 27013:2017

Australian STANDARD

Information technology—Security techniques—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

STANDARDS Australia

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 6 April 2017.
This Standard was published on 12 May 2017.

The following are represented on Committee IT-012:

- Australian Association of Permanent Building Societies
- Australian Information Industry Association
- Australian Payments 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 27013:2017.

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Standards may also be withdrawn.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—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

First published as AS ISO/IEC 27013:2017.

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

ISBN 978 1 76035 765 8

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 guidance to organizations on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. This Standard is focused on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

This Standard is identical with, and has been reproduced from ISO/IEC 27013:2015, *Information technology—Security techniques—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*.

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

(a) In the source text 'this International Standard' 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

The relationship between information security management and service management is so close that many organizations already recognise the benefits of adopting the two International Standards for these domains: ISO/IEC 27001 for information security management and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to achieve conformity with the requirements specified in one of these International Standards and then make further improvements to achieve conformity with the requirements of the other.

There are a number of advantages in implementing an integrated management system that takes into account not only the services provided but also the protection of information. These benefits can be experienced whether one International Standard is implemented before the other, or both International Standards are implemented simultaneously. Management and organizational processes, in particular, can derive benefit from the mutually reinforcing concepts and similarities between these International Standards and their common objectives.

Key benefits of an integrated implementation of information security management and service management include the following:

a) the credibility, to internal or external customers of the organization, of an effective and secure service;

b) the lower cost of an integrated programme of two projects, where effective and efficient management of both services and information security are part of an organization's strategy;

c) a reduction in implementation time due to the integrated development of processes common to both standards;

d) better communication, reduced cost and improved operational efficiency through elimination of unnecessary duplication;

e) a greater understanding by service management and security personnel of each others' viewpoints;

f) an organization certified for ISO/IEC 27001 can more easily fulfil the requirements for information security specified in ISO/IEC 20000-1:2011, 4.6, as both International Standards are complementary in requirements.

The guidance in this International Standard is based upon the published versions of both ISO/IEC 27001 and ISO/IEC 20000-1.

This International Standard is intended for use by persons with knowledge of both, either or neither of the International Standards ISO/IEC 27001 and ISO/IEC 20000-1.

It is expected that all readers have access to copies of both ISO/IEC 27001 and ISO/IEC 20000-1. Consequently, this International Standard does not reproduce parts of either of those International Standards. Equally, it does not describe all parts of each International Standard comprehensively. Only those parts where subject matter overlaps are described in detail.

This International Standard does not provide guidance associated with the various legislation and regulations outside the control of the organization. These can vary by country and impact the planning of an organization's management system.

AUSTRALIAN STANDARD

Information technology—Security techniques—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

1 Scope

This International Standard provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organizations that are intending to either

a) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa,

b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together, or

c) integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1.

This International Standard focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

In practice, ISO/IEC 27001 and ISO/IEC 20000-1 can also be integrated with other management system standards, such as ISO 9001 and ISO 14001.

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 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC/TR 20000-10, *Information technology — Service management — Part 10: Concepts and terminology*

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 20000-1 and ISO/IEC/TR 20000-10 apply.

The following abbreviations apply.

ISMS information security management system (from ISO/IEC 27001)

SMS service management system (from ISO/IEC 20000-1)

Annex A provides a comparison of content at a clause level between ISO/IEC 27001 and ISO/IEC 20000-1.

Annex B provides a comparison of terms defined in the following:

— ISO/IEC 27000, the glossary for ISO/IEC 27001;