

ISBN 978-0-626-30175-0

SANS 27013:2014
Edition 1
ISO/IEC 27013:2012
Edition 1

SOUTH AFRICAN NATIONAL STANDARD

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

This national standard is the identical implementation of ISO/IEC 27013:2012, and is adopted with the permission of the International Organization for Standardization and the International Electrotechnical Commission.

WARNING
This document references other documents normatively.

Published by SABS Standards Division
1 Dr Lategan Road Groenkloof ☒ Private Bag X191 Pretoria 0001
Tel: +27 12 428 7911 Fax: +27 12 344 1568
www.sabs.co.za
© SABS

SABS

SANS 27013:2014
Edition 1
ISO/IEC 27013:2012
Edition 1

Table of changes

Change No.	Date	Scope

National foreword

This South African standard was approved by National Committee SABS/TC 001/SC 27, *Information technology – Information security*, in accordance with procedures of the SABS Standards Division, in compliance with annex 3 of the WTO/TBT agreement.

This document was published in July 2014.

INTERNATIONAL STANDARD

ISO/IEC 27013

First edition
2012-10-15

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

*Technologies de l'information — Techniques de sécurité — Guide sur la
mise en oeuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1*

Reference number
ISO/IEC 27013:2012(E)





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

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	iv
Introduction.....	v
1 Scope	1
2 Normative references.....	1
3 Terms, abbreviated terms and definitions	1
4 Overviews of ISO/IEC 27001 and ISO/IEC 20000-1	2
4.1 Understanding the International Standards	2
4.2 ISO/IEC 27001 concepts	2
4.3 ISO/IEC 20000-1 concepts	2
4.4 Similarities and differences.....	2
5 Approaches for integrated implementation.....	3
5.1 General	3
5.2 Considerations of scope	4
5.3 Pre-implementation scenarios	5
5.3.1 General	5
5.3.2 Neither standard is currently used as the basis for a management system.....	5
5.3.3 A management system exists which fulfils the requirement of one of the standards.....	6
5.3.4 Separate management systems exist which fulfil the requirements of each standard	6
6 Integrated implementation considerations.....	7
6.1 General	7
6.2 Potential challenges.....	7
6.2.1 The usage and meaning of asset.....	7
6.2.2 Design and transition of services.....	8
6.2.3 Risk assessment and management.....	8
6.2.4 Differences in risk acceptance levels.....	9
6.2.5 Incident and problem management.....	9
6.2.6 Change management	11
6.3 Potential gains	12
6.3.1 Use of the Plan-Do-Check-Act cycle	12
6.3.2 Service level management and reporting	12
6.3.3 Management commitment	12
6.3.4 Capacity management	13
6.3.5 Management of third party risk.....	13
6.3.6 Continuity and availability management.....	14
6.3.7 Supplier management.....	14
6.3.8 Configuration management.....	14
6.3.9 Release and deployment management.....	15
6.3.10 Budgeting and accounting	15
Annex A (informative) Correspondence between ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011.....	16
Annex B (informative) Comparison of ISO/IEC 27000:2009 and ISO/IEC 20000-1:2011 terms.....	18
Bibliography.....	38
Figures	
Figure 1: Comparison between concepts in ISO/IEC 27001 and ISO/IEC 20000-1	3
Figure 2: Relationship between information assets in ISO/IEC 27001 and CIs in ISO/IEC 20000-1.....	8
Figure 3: Illustration of relationship between standards for incident management	10