

ISBN 978-0-626-32751-4

SANS 27003:2010
Edition 1
ISO/IEC 27003:2010
Edition 1

SOUTH AFRICAN NATIONAL STANDARD

Information technology — Security techniques — Information security management system implementation guidance

This national standard is the identical implementation of ISO/IEC 27003:2010, and is adopted with the permission of the International Organization for Standardization and the International Electrotechnical Commission.

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 27003:2010
Edition 1
ISO/IEC 27003:2010
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 SANS document was published in November 2010.

Compliance with a South African National Standard cannot confer immunity from legal obligations.

**Reaffirmed and reprinted in June 2016.
This document will be reviewed every five years
and be reaffirmed, amended, revised or withdrawn.**

INTERNATIONAL STANDARD

ISO/IEC 27003

First edition
2010-02-01

Information technology — Security techniques — Information security management system implementation guidance

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour la mise en œuvre du système de management de la
sécurité de l'information*

Reference number
ISO/IEC 27003:2010(E)



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

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 and definitions	1
4 Structure of this International Standard	2
4.1 General structure of clauses	2
4.2 General structure of a clause	3
4.3 Diagrams	3
5 Obtaining management approval for initiating an ISMS project	5
5.1 Overview of obtaining management approval for initiating an ISMS project	5
5.2 Clarify the organization's priorities to develop an ISMS.....	7
5.3 Define the preliminary ISMS scope	9
5.4 Create the business case and the project plan for management approval.....	11
6 Defining ISMS scope, boundaries and ISMS policy.....	12
6.1 Overview of defining ISMS scope, boundaries and ISMS policy	12
6.2 Define organizational scope and boundaries.....	15
6.3 Define information communication technology (ICT) scope and boundaries	16
6.4 Define physical scope and boundaries.....	17
6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries.....	18
6.6 Develop the ISMS policy and obtain approval from management	19
7 Conducting information security requirements analysis.....	20
7.1 Overview of conducting information security requirements analysis.....	20
7.2 Define information security requirements for the ISMS process	22
7.3 Identify assets within the ISMS scope	23
7.4 Conduct an information security assessment	24
8 Conducting risk assessment and planning risk treatment.....	25
8.1 Overview of conducting risk assessment and planning risk treatment	25
8.2 Conduct risk assessment.....	27
8.3 Select the control objectives and controls	28
8.4 Obtain management authorization for implementing and operating an ISMS.....	29
9 Designing the ISMS	30
9.1 Overview of designing the ISMS.....	30
9.2 Design organizational information security	33
9.3 Design ICT and physical information security	38
9.4 Design ISMS specific information security.....	40
9.5 Produce the final ISMS project plan	44
Annex A (informative) Checklist description	45
Annex B (informative) Roles and responsibilities for Information Security	51
Annex C (informative) Information about Internal Auditing	55
Annex D (informative) Structure of policies	57
Annex E (informative) Monitoring and measuring.....	62
Bibliography.....	68