

ISBN 978-0-626-32958-7

SANS 27032:2016
Edition 1
ISO/IEC 27032:2012
Edition 1

SOUTH AFRICAN NATIONAL STANDARD

Information technology — Security techniques — Guidelines for cybersecurity

This national standard is the identical implementation of ISO/IEC 27032:2012, 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 27032:2016
Edition 1
ISO/IEC 27032:2012
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 approved for publication in January 2016.

INTERNATIONAL STANDARD

ISO/IEC 27032

First edition
2012-07-15

Information technology — Security techniques — Guidelines for cybersecurity

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour la cybersécurité*

Reference number
ISO/IEC 27032:2012(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	v
Introduction	vi
1 Scope	1
2 Applicability	1
2.1 Audience	1
2.2 Limitations	1
3 Normative references	2
4 Terms and definitions	2
5 Abbreviated terms	8
6 Overview	9
6.1 Introduction	9
6.2 The nature of the Cyberspace	10
6.3 The nature of Cybersecurity	10
6.4 General model	11
6.5 Approach	13
7 Stakeholders in the Cyberspace	14
7.1 Overview	14
7.2 Consumers	14
7.3 Providers	14
8 Assets in the Cyberspace	15
8.1 Overview	15
8.2 Personal assets	15
8.3 Organizational assets	15
9 Threats against the security of the Cyberspace	16
9.1 Threats	16
9.2 Threat agents	17
9.3 Vulnerabilities	17
9.4 Attack mechanisms	18
10 Roles of stakeholders in Cybersecurity	20
10.1 Overview	20
10.2 Roles of consumers	20
10.3 Roles of providers	21
11 Guidelines for stakeholders	22
11.1 Overview	22
11.2 Risk assessment and treatment	22
11.3 Guidelines for consumers	23
11.4 Guidelines for organizations and service providers	25
12 Cybersecurity controls	28
12.1 Overview	28
12.2 Application level controls	28
12.3 Server protection	29
12.4 End-user controls	29
12.5 Controls against social engineering attacks	30
12.6 Cybersecurity readiness	33
12.7 Other controls	33
13 Framework of information sharing and coordination	33
13.1 General	33
13.2 Policies	34
13.3 Methods and processes	35