

BS ISO/IEC 27032:2012



BSI Standards Publication

Information technology — Security techniques — Guidelines for cybersecurity

bsi.

...making excellence a habit.™

This is a preview. [Click here to purchase the full publication.](#)

National foreword

This British Standard is the UK implementation of ISO/IEC 27032:2012.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

ISBN 978 0 580 59489 2

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2012.

Amendments issued since publication

| Date | Text affected |
|------|---------------|
|------|---------------|

**Information technology — Security
techniques — Guidelines for
cybersecurity**

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



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 |

13.4 People and organizations 36

13.5 Technical..... 37

13.6 Implementation guidance..... 38

Annex A (informative) Cybersecurity readiness..... 40

Annex B (informative) Additional resources 44

Annex C (informative) Examples of related documents..... 47

Bibliography 50

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27032 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks. However there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices as there are gaps between these domains, as well as a lack of communication between organizations and providers in the Cyberspace. This is because the devices and connected networks that have supported the Cyberspace have multiple owners, each with their own business, operational and regulatory concerns. The different focus placed by each organization and provider in the Cyberspace on relevant security domains where little or no input is taken from another organization or provider has resulted in a fragmented state of security for the Cyberspace.

As such, the first area of focus of this International Standard is to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace. In particular this International Standard provides technical guidance for addressing common Cybersecurity risks, including:

- social engineering attacks;
- hacking;
- the proliferation of malicious software (“malware”);
- spyware; and
- other potentially unwanted software.

The technical guidance provides controls for addressing these risks, including controls for:

- preparing for attacks by, for example, malware, individual miscreants, or criminal organizations on the Internet;
- detecting and monitoring attacks; and
- responding to attacks.

The second area of focus of this International Standard is collaboration, as there is a need for efficient and effective information sharing, coordination and incident handling amongst stakeholders in the Cyberspace. This collaboration must be in a secure and reliable manner that also protects the privacy of the individuals concerned. Many of these stakeholders can reside in different geographical locations and time zones, and are likely to be governed by different regulatory requirements. Stakeholders include:

- consumers, which can be various types of organizations or individuals; and
- providers, which include service providers.

Thus, this International Standard also provides a framework for

- information sharing,
- coordination, and
- incident handling.

The framework includes

- key elements of considerations for establishing trust,
- necessary processes for collaboration and information exchange and sharing, as well as
- technical requirements for systems integration and interoperability between different stakeholders.

Given the scope of this International Standard, the controls provided are necessarily at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within this International Standard for further guidance.