



DPC: 22 / 30389144 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 27 July 2022
Origin: International**Latest date for receipt of comments: 3 September 2022**

Project No. 2018/03872

Responsible committee: IST/33/4 Security Controls and Services

Interested committees:

Title: BS ISO/IEC 27032 Cybersecurity — Guidelines for Internet security

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 3 September 2022**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Ms Lindsey Ferrari (BSI)**
Direct tel:
E-mail: lindsey.ferrari@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27032

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2022-07-11

Voting terminates on:
2022-10-03

Cybersecurity — Guidelines for Internet security

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 27032:2022(E)
Documents
AVA Document Sharing Hub
© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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 Symbols and abbreviated terms	5
5 Relationship between Internet security, web security, network security and cybersecurity	6
6 Overview of Internet security	7
7 Interested parties	9
7.1 General	9
7.2 Users	9
7.3 Coordinator and standardization organisations	10
7.4 Government authorities	10
7.5 Law enforcement agencies	11
7.6 Internet service providers (ISP)	11
8 Internet security risk assessment and treatment	11
8.1 General	11
8.2 Threats	11
8.3 Vulnerabilities	12
8.4 Attack vectors	12
9 Security guidelines for the Internet	13
9.1 General	13
9.2 Controls for Internet security	14
9.2.1 General	14
9.2.2 Policies for Internet security	14
9.2.3 Access control	15
9.2.4 Education, awareness & training	15
9.2.5 Security incident management	16
9.2.6 Asset management	17
9.2.7 Supplier management	17
9.2.8 Business continuity over the Internet	18
9.2.9 Privacy protection over the Internet	19
9.2.10 Vulnerability management	19
9.2.11 Network management	20
9.2.12 Protection against malware	21
9.2.13 Change management	22
9.2.14 Identification of applicable legislation and compliance requirements	22
9.2.15 Use of cryptography	22
9.2.16 Application security for Internet-facing applications	23
9.2.17 Endpoint device management	24
9.2.18 Monitoring	24
Annex A (Informative) Cross-references between ISO/IEC 27032 and ISO/IEC 27002	25
Bibliography	27

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The focus of this document is to address Internet security issues and provide technical guidance for addressing common Internet security threats, such as:

- social engineering attacks;
- zero-day attacks;
- privacy attacks;
- hacking; and
- the proliferation of malicious software (malware), spyware and other potentially unwanted software.

The guidance within this document provides technical controls for addressing the Internet security risks, including controls for:

- preparing for attacks;
- preventing attacks;
- detecting and monitoring attacks; and
- responding to attacks.

The guidance focuses on providing industry best practices, broad consumer and employee education to assist interested parties in playing an active role to address the Internet security challenges. This guideline also focuses on preservation of confidentiality, integrity and availability of information over the Internet and other properties, such as authenticity, accountability, non-repudiation and reliability that can also be involved.

This includes Internet security guidance for:

- roles;
- policies;
- methods;
- processes; and
- applicable technical controls.

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

This document does not specifically address controls that organizations can require for systems supporting critical infrastructure or national security. However, most of the controls mentioned in this document can be applied for such systems.

ISO/IEC 27001 provides requirements for information security management systems. ISO/IEC 27002 provides a list of information security controls and implementation guidance that allows managing information security. ISO/IEC 27033 series provides security controls and guidance on network security and ISO/IEC 27701 provides requirements and guidance for privacy information management systems. ISO/IEC TS 27100 provides technical explanations and specifications to various cybersecurity terms and concepts. ISO/IEC 27032, is a document in the cybersecurity series that provides detailed security guidance for Internet security and uses existing concepts from ISO/IEC 27002, ISO/IEC 27033, ISO/IEC TS 27100 and ISO/IEC 27701. As mentioned in ISO/IEC TS 27100, the Internet is part of global

network of networks and organizations are using these networks for all communications, both digital and voice. Given that some users target these networks, the relevant security risks need to be addressed.

Cybersecurity — Guidelines for Internet security

1 Scope

This document provides:

- an explanation of the relationship between Internet security, web security, network security and cybersecurity,
- an overview of Internet security,
- identification of interested parties and a description of their roles in Internet security,
- high level guidance for addressing common Internet security issues.

This document is intended for organizations that use the Internet.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

attack

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.2

attack vector

path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

Note 1 to entry: attack vector can include IoT devices, smart phones etc.

3.3

attacker

person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

[SOURCE: ISO/IEC 27033-1:2015, 3.3]

3.4

blended attack

attack (3.1) that seeks to maximize the severity of damage and speed of contagion by combining multiple *attack vectors* (3.2)

3.5

bot

automated software program used to carry out specific tasks

Note 1 to entry: The word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail.

Note 2 to entry: A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access websites and gather their content for search engine indexes.

3.6

botnet

collection of remotely controlled malicious bots that run autonomously or automatically on compromised computers

EXAMPLE DDoS nodes, where the botnet controller can direct the user's computer to generate traffic to a third-party site as part of a coordinated DDoS (distributed denial of service) attack.

3.7

cybersecurity

safeguarding of society, people, organizations and nations from cyber risks

Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level.

[SOURCE: ISO/IEC TS 27100:2020, 3.2]

3.8

dark net

network of secret websites within the Internet that can only be accessed with specific software

Note 1 to entry: dark net is also known as dark web.

3.9

deceptive software

software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions.

EXAMPLE 1 A program that hijacks user configurations.

EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user.

EXAMPLE 3 Adware and spyware

3.10

hacking

intentionally accessing a computer system without the authorization of the user or the owner

3.11**hacktivism**

hacking (3.10) for a politically or socially motivated purpose

3.12**interested party**

person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.

[SOURCE: ISO/IEC 27000:2018, 2.41]

3.13**the Internet**

global system of inter-connected networks in the public domain

[SOURCE: ISO/IEC 27033-1:2015, 3.14]

3.14**Internet security**

preservation of confidentiality, integrity and availability of information over *the Internet* (3.13)

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Note 2 to entry: Please refer to definition on confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability in ISO/IEC 27000:2018.

3.15**Internet service provider****ISP**

organization that provides Internet services to a user and enables its customers access to *the Internet* (3.13)

Note 1 to entry: Also, sometimes referred to as an Internet access provider (IAP).

3.16**malicious contents**

applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

3.17**malware****malicious software**

software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system

EXAMPLE Viruses, worms and trojans.

3.18**organization**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

[SOURCE: ISO 9000:2015, 3.2.1, modified the Note 1 to entry and Note 2 to entry]

Note 1 to entry: In the context of this document, an individual is distinct from an organization.

Note 2 to entry: In general, a government is also an organization. In the context of this document, governments can be considered separately from other organizations for clarity.