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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27032:2012](https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012)

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 27032:2012](https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012)

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>



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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27032:2012](https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012)

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>

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*.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 27032:2012](https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012)

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>

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.

ITeH STANDARD PREVIEW
(standards.iteh.ai)
<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>

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.

Information technology — Security techniques — Guidelines for cybersecurity

1 Scope

This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>

2 Applicability

2.1 Audience

This International Standard is applicable to providers of services in the Cyberspace. The audience, however, includes the consumers that use these services. Where organizations provide services in the Cyberspace to people for use at home or other organizations, they may need to prepare guidance based on this International Standard that contains additional explanations or examples sufficient to allow the reader to understand and act on it.

2.2 Limitations

This International Standard does not address:

- Cybersafety,
- Cybercrime,
- CIIP,
- Internet safety, and
- Internet related crime.

It is recognized that relationships exist between the domains mentioned and Cybersecurity. It is, however, beyond the scope of this International Standard to address these relationships, and the sharing of controls between these domains.

It is important to note that the concept of Cybercrime, although mentioned, is not addressed. This International Standard does not provide guidance on law-related aspects of the Cyberspace, or the regulation of Cybersecurity.

The guidance in this International Standard is limited to the realization of the Cyberspace on the Internet, including the endpoints. However, the extension of the Cyberspace to other spatial representations through communication media and platforms are not addressed, nor the physical security aspects of them.

EXAMPLE 1 Protection of the infrastructure elements, such as communications bearers, which underpin the Cyberspace are not addressed.

EXAMPLE 2 The physical security of mobile telephones that connect to the Cyberspace for content download and/or manipulation is not addressed.

EXAMPLE 3 Text messaging and voice chat functions provided for mobile telephones are not addressed.

3 Normative references

The following referenced documents are indispensable for the application 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*

4 Terms and definitions

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

4.1 adware

application which pushes advertising to users and/or gathers user online behaviour

NOTE The application may or may not be installed with the user's knowledge or consent or forced onto the user via licensing terms for other software.

4.2 application

IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

[ISO/IEC 27034-1:2011]

4.3 application service provider

operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models

EXAMPLE Online game operators, office application providers and online storage providers.

4.4 application services

software with functionality delivered on-demand to subscribers through an online model which includes web based or client-server applications

4.5 application software

software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself

[ISO/IEC 18019]

4.6**asset**

anything that has value to an individual, an organization or a government

NOTE Adapted from ISO/IEC 27000 to make provision for individuals and the separation of governments from organizations (4.37).

4.7**avatar**

representation of a person participating in the Cyberspace

NOTE 1 An avatar can also be referred to as the person's alter ego.

NOTE 2 An avatar can also be seen as an "object" representing the embodiment of the user.

4.8**attack**

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

[ISO/IEC 27000:2009]

4.9**attack potential**

perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation

[ISO/IEC 15408-1:2005]

ITeh STANDARD PREVIEW
(standards.iteh.ai)

4.10**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

[ISO/IEC 27032:2012](https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012)

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012>

4.11**blended attack**

attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attacking methods

4.12**bot****robot**

automated software program used to carry out specific tasks

NOTE 1 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 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.

4.13**botnet**

remote control software, specifically a collection of malicious bots, that run autonomously or automatically on compromised computers

4.14**cookie**

<access control> capability or ticket in an access control system

4.15**cookie**

<IPSec> data exchanged by ISAKMP to prevent certain Denial-of-Service attacks during the establishment of a security association

4.16

cookie

<HTTP> data exchanged between an HTTP server and a browser to store state information on the client side and retrieve it later for server use

NOTE A web browser can be a client or a server.

4.17

control

countermeasure

means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature

[ISO/IEC 27000:2009]

NOTE ISO Guide 73:2009 defines control as simply a measure that is modifying risk.

4.18

Cybercrime

criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime

4.19

Cybersafety

condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable

NOTE 1 This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protection of people or of assets.

NOTE 2 Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions.

4.20

Cybersecurity

Cyberspace security

preservation of confidentiality, integrity and availability of information in the Cyberspace

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

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.

4.21

the Cyberspace

complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

4.22

Cyberspace application services

application services (4.4) provided over the Cyberspace

4.23

cyber-squatter

individuals or organizations that register and hold on to URLs that resemble references or names of other organizations in the real world or in the Cyberspace

4.24

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.

4.25

hacking

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

4.26

hactivism

hacking for a politically or socially motivated purpose

4.27

information asset

knowledge or data that has value to the individual or organization

NOTE Adapted from ISO/IEC 27000:2009.

4.28

internet

internetwork

collection of interconnected networks

NOTE 1 Adapted from ISO/IEC 27033-1:2009

NOTE 2 In this context, reference would be made to “an internet”. There is a difference between the definition of “an internet” and “the Internet”.

4.29

the Internet

global system of inter-connected networks in the public domain

[ISO/IEC 27033-1:2009]

NOTE There is a difference between the definition of “an internet” and “the Internet”.

4.30

Internet crime

criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime

4.31

Internet safety

condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Internet which could be considered non-desirable

4.32

Internet security

preservation of confidentiality, integrity and availability of information in the Internet

4.33

Internet services

services delivered to a user to enable access to the Internet via an assigned IP address, which typically include authentication, authorization and domain name services

4.34

Internet service provider

organization that provides Internet services to a user and enables its customers access to the Internet

NOTE Also sometimes referred to as an Internet access provider.

4.35

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

EXAMPLES Viruses, worms, trojans.

4.36

malicious contents

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

4.37

organization

group of people and facilities with an arrangement of responsibilities, authorities and relationships

[ISO 9000:2005]

NOTE 1 In the context of this International Standard, an individual is distinct from an organization.

NOTE 2 In general, a government is also an organization. In the context of this International Standard, governments can be considered separately from other organizations for clarity.

4.38

phishing

fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication

NOTE Phishing can be accomplished by using social engineering or technical deception.

4.39

physical asset

asset that has a tangible or material existence

[ISO/IEC 27032:2012](https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-c8e3a27b5bd/iso-iec-27032-2012)

<https://standards.iteh.ai/catalog/standards/sist/941c888d-2440-469f-862c-c8e3a27b5bd/iso-iec-27032-2012>

NOTE Physical assets usually refer to cash, equipment, inventory and properties owned by the individual or organization. Software is considered an intangible asset, or a non-physical asset.

4.40

potentially unwanted software

deceptive software, including malicious and non-malicious software, that exhibits the characteristics of deceptive software

4.41

scam

fraud or confidence trick

4.42

spam

abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages

NOTE While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

4.43

spyware

deceptive software that collects private or confidential information from a computer user

NOTE Information can include matters such as websites most frequently visited or more sensitive information such as passwords.

4.44**stakeholder**

<risk management> person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[ISO Guide 73:2009]

4.45**stakeholder**

<system> individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations

[ISO/IEC 12207:2008]

4.46**threat**

potential cause of an unwanted incident, which may result in harm to a system, individual or organization

NOTE Adapted from ISO/IEC 27000:2009.

4.47**trojan****trojan horse**

malware that appears to perform a desirable function

4.48**unsolicited email**

email that is not welcome, or was not requested, or invited

4.49**virtual asset**

representation of an asset in the Cyberspace

NOTE In this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise.

4.50**virtual currency**

monetary virtual assets

4.51**virtual world**

simulated environment accessed by multiple users through an online interface

NOTE 1 The simulated environments are often interactive.

NOTE 2 The physical world in which people live, and the related characteristics, will be referred to as the “real world” to differentiate it from a virtual world.

4.52**vulnerability**

weakness of an asset or control that can be exploited by a threat

[ISO/IEC 27000:2009]

4.53
zombie
zombie computer
drone

computer containing hidden software that enables the machine to be controlled remotely, usually to perform an attack on another computer

NOTE Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious activities under remote direction.

5 Abbreviated terms

The following abbreviated terms are used in this International Standard.

AS	Autonomous System
AP	Access Point
CBT	Computer Based Training
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
CIIP	Critical Information Infrastructure Protection
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
HIDS	Host-based Intrusion Detection System
IAP	Independent Application Provider
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPO	Information Providing Organization
IPS	Intrusion Prevention System
IRO	Information Receiving Organization
ISP	Internet Service Provider
ISV	Independent Software Vendor
IT	Information Technology
MMORPG	Massively Multiplayer Online Role-Playing Game
NDA	Non-Disclosure Agreement
SDLC	Software Development Life-cycle
SSID	Service Set Identifier

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

6 Overview

6.1 Introduction

Security on the Internet and in the Cyberspace has been a subject of growing concern. Stakeholders have been establishing their presence in the Cyberspace through websites and are now attempting to further leverage the virtual world provided by the Cyberspace.

EXAMPLE Increasing numbers of individuals spend increasing amounts of time with their virtual avatars on MMORPGs.

While some individuals are careful in managing their online identity, most people are uploading details of their personal profiles to share with others. Profiles on many sites, in particular social networking sites and chat rooms, can be downloaded and stored by other parties. This can lead to the creation of a digital dossier of personal data that can be misused, disclosed to other parties, or used for secondary data collection. While the accuracy and integrity of this data are questionable, they create links to individuals and organizations that often cannot be completely erased. These developments in the communication, entertainment, transportation, shopping, financial, insurance, and healthcare domains create new risks to stakeholders in the Cyberspace. Thus, risks can be associated with loss of privacy.

The convergence of information and communication technologies, the ease of getting into the Cyberspace, and the narrowing of personal space between individuals are gaining the attention of individual miscreants and criminal organizations. These entities are using existing mechanisms, such as phishing, spam and spyware, as well as developing newer attack techniques, to exploit any weaknesses they can discover in the Cyberspace. In recent years, security attacks in the Cyberspace have evolved from hacking for personal fame to organized crime, or Cybercrime. A plethora of tools and processes previously observed in isolated Cybersecurity incidents are now being used together in multi-blended attacks, often with far reaching malicious objectives. These objectives range from personal attacks, identity theft, financial frauds or thefts, to political hactivism. Specialist forums to highlight potential security issues have also served to showcase attack techniques and criminal opportunities.

The multiple modes of business transactions that are carried out in the Cyberspace are becoming the target of Cybercrime syndicates. Ranging from business-to-business, business-to-consumer to consumer-to-consumer services, the risks posed are inherently complex. Concepts such as what constitute a transaction or an agreement are dependent on the interpretation of the law and how each party in the relationship manages their liability. Often, the issue of usage of data collected during the transaction or relationship is not addressed adequately. This can eventually lead to security concerns such as the leakage of information.

The legal and technical challenges posed by these Cybersecurity issues are far-reaching and global in nature. The challenges can only be addressed by having the information security technical community, legal community, nations and community of nations coming together through a coherent strategy. This strategy should take into account the role of each stakeholder and existing initiatives, within a framework of international cooperation.

EXAMPLE An example of a challenge sprouts from the fact that the Cyberspace affords virtual anonymity and stealth of attack, making detection difficult. This makes it increasingly difficult for individuals and organizations to establish trust and transact, as well as for law enforcement agencies to enforce related policies. Even if the source of attack can be determined, cross-border legal issues often prevent further progress for any investigation or legal repatriation.

Current progress to address these challenges has been hampered by many issues, and Cybersecurity issues are increasing and continuing to evolve.