INTERNATIONAL STANDARD

ISO/IEC 27032

Second edition
2023-06

Cybersecurity — Guidelines for Internet security

Cybersécurité — Lignes directrices relatives à la sécurité sur l'internet

Reference number
ISO/IEC 27032:2023(E)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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 document 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This second edition cancels and replaces the first edition (ISO/IEC 27032:2012) which has been technically revised.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed;

— the risk assessment and treatment approach has been changed, with the addition of content on threats, vulnerabilities and attack vectors to identify and manage the Internet security risks;

— a mapping between the controls for Internet security cited in 9.2 and the controls contained in ISO/IEC 27002 has been added to Annex A.

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 and www.iec.ch/national-committees.

Introduction

The focus of this document is to address Internet security issues and provide 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 and non-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. The document 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. See Annex A for the correspondence between the controls cited in this document and those in ISO/IEC 27002.

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 to such systems.

This document uses existing concepts from ISO/IEC 27002, the ISO/IEC 27033 series, ISO/IEC TS 27100 and ISO/IEC 27701, to illustrate:

— the relationship between Internet security, web security, network security and cybersecurity;

— detailed guidance on Internet security controls cited in 9.2, addressing cyber-security readiness for Internet-facing systems.

As mentioned in ISO/IEC TS 27100, the Internet is a global network, used by organizations for all communications, both digital and voice. Given that some users target attacks towards these networks, it is critical to address the relevant security risks.

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

EXAMPLE 1 IoT devices.

EXAMPLE 2 Smart phones.

3.2
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]

3.3
blended attack
attack that seeks to maximize the severity of damage and speed of contagion by combining multiple *attack vectors* (3.1)

3.4
bot
automated software program used to carry out specific tasks

Note 1 to entry: This 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.

3.5
botnet
collection of remotely controlled malicious bots that run autonomously or automatically on compromised computers

EXAMPLE Distributed denial-of-service (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 attack.

3.6
cybersecurity
safeguarding of people, society, 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]

3.7
dark net
network of secret websites within the Internet that can only be accessed with specific software

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

3.8
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.

3.9
hacking
intentionally accessing a computer system without the authorization of the user or the owner

3.10
hacktivism
hacking (3.9) for a politically or socially motivated purpose

3.11
Internet
global system of inter-connected networks in the public domain

[SOURCE: ISO/IEC 27033-1:2015, 3.14, modified — "the" has been deleted from the term.]

3.12
Internet security
preservation of confidentiality, integrity and availability of information over the *Internet* (3.11)

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 definitions on confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability in ISO/IEC 27000:2018, Clause 3.

3.13
Internet service provider
ISP
organization that provides Internet services to a user and enables its customers access to the *Internet* (3.11)

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

3.14
malicious content
applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

3.15
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.

3.16
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

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.

[SOURCE: ISO 9000:2015, 3.2.1, modified — Note 1 to entry and Note 2 to entry have been replaced.]

3.17
phishing
fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication

Note 1 to entry: Phishing can be accomplished by using social engineering or technical deception.

3.18
potentially unwanted software
deceptive software (3.8), including *malicious* (3.15) and non-malicious software, that exhibit the characteristics of deceptive software

3.19
spam
unsolicited emails that can carry malicious content and/or scam messages

Note 1 to entry: 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.

[SOURCE: ISO/IEC 27033-1:2015, 3.37, modified — Note 1 to entry has been added.]

3.20
spyware
deceptive software (3.8), that collects private or confidential information from a computer user

Note 1 to entry: Information can include matters such as websites most frequently visited or more sensitive information such as passwords.

3.21
threat
potential cause of an unwanted incident, which can result in harm to a system, individual or *organization* (3.16)

3.22
trojan
malware (3.15) that appears to perform a desirable function for the user but that mislead the user of its true intent

3.23
vishing
voice phishing done to acquire private or confidential information by masquerading as a trustworthy entity

Note 1 to entry: Vishing can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

3.24
waterhole technique
technique inciting people to access a website that specifically contains (lots of) malware

Note 1 to entry: Waterhole is also known as watering hole.

3.25
World Wide Web
Web
universe of network-accessible information and services

[SOURCE: ISO 19101-1:2014, 4.1.40]

4 Abbreviated terms

The following abbreviated terms are used in this document.

AI	artificial intelligence
API	application programming interface
APT	advanced persistent threat
BYOD	bring your own device
CERT	computer emergency response team
DDoS	distributed denial-of-service
DLP	data loss prevention
DMZ	demilitarized zone
DNS	domain name system

DoS	denial-of-service
EDR	endpoint detection and response
FTP	file transfer protocol
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure socket layer
ICANN	internet corporation for assigned names and numbers
ICT	information and communications technology
IDS	intrusion detection system
IETF	Internet engineering task force
IMT	incident management team
IoT	internet of things
IP	Internet protocol
IPS	intrusion prevention system
ISP	Internet service provider
ISV	independent software vendor
IRT	incident response team
ISMS	information security management system
OWASP	open web application security project
PII	personally identifiable information
SDLC	software development life cycle
SIEM	security information and event management
SME	small and medium enterprises
URL	uniform resource locator
USB	universal serial bus
VPN	virtual private network
W3C	World Wide Web consortium
WWW	World Wide Web

5 Relationship between Internet security, web security, network security and cybersecurity

Figure 1 shows a high-level view of the relationship between Internet security, web security, network security and cybersecurity.

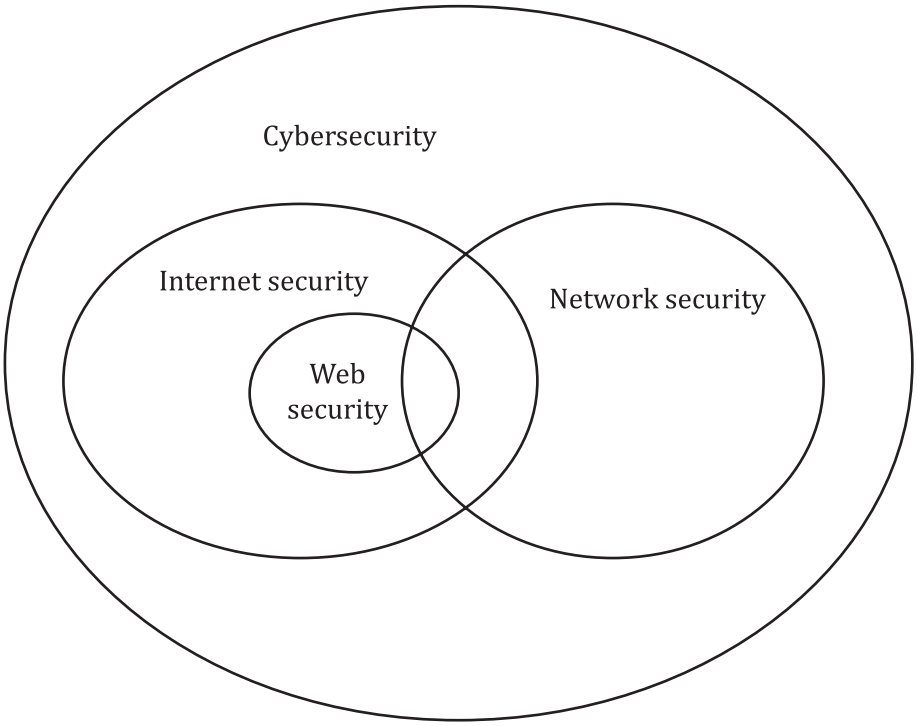

Figure 1 — Relationship between Internet security, web security, network security and cybersecurity

The Internet is a global system of inter-connected digital networks in the public domain. The information exchange on the Internet also uses the mobile telephony network that is hence part of the Internet. This global network connects billions of servers, computers, and other hardware devices. Each device is connected with any other device through its connection to the Internet. The Internet creates an environment which is conducive to information sharing.

Internet security is concerned with protecting Internet-related services and related ICT systems and networks as an extension of network security. These efforts aim to reduce Internet related security risks for organizations, customers and other relevant stakeholders.

Internet security also ensures the availability and reliability of Internet services. Over the Internet, various services are on offer, such as file transfer services, mail services or any services that can be publicly shared with the end users. In this context, Internet security deals with the secure delivery of these services over the public network.

The web is one of the ways information is shared on the Internet [others include email, file transfer protocol (FTP), and instant messaging services]. The web is composed of billions of connected digital documents that can be viewed using a web browser. A website is a set of related web pages that are prepared and maintained as a collection in support of a single purpose.

Web security deals with information security in the context of World Wide Web (WWW) and with web services accessed over the public network. The web service is enabled by the use of HTTP protocol in which any registered publicly available URL can be accessed. Web security also deals with security of this HTTP connection used for information exchange.

A network can include components such as routers, hubs, cabling, telecommunications controllers, key distribution centres, and technical control devices. Network security broadly covers all kinds of networks that exist within an organization from local area network, wide area network, personal area network and wireless networks.

Network security is concerned with the design, implementation, operation and improvement of networks, as well as the identification and treatment of network-related security risks within organizations, between organizations, and between organizations and users.

Cybersecurity concerns managing information security risks when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

Cybersecurity also deals with protecting Internet-connected systems including hardware, software, programs and data from potential attacks. Many of these attacks are characterized by targeted and blended attacks with a high degree of sophistication and persistence. The threats can be Internet-based and/or threats due to connectivity with other networks and systems within the organization or customer and service provider's network, to which the organization communicates during the normal course of business.

6 Overview of Internet security

The personally identifiable information (PII) of Internet users is captured by many sites and services offered on the Internet. This includes application service providers who closely track user activities and use artificial intelligence (AI) techniques to provide recommendations for purchases, healthcare, time management and a host of other feedback intending to make their lives and tasks easier to manage. Many of these sites collect this data without the users' permission and provide this data to other third parties for monetary gain, again without the users' knowledge. Interested parties have been establishing their presence on the Internet through websites, conducting e-Commerce on a global scale, providing digital services on the Internet, using public cloud services to deliver services and using web-based business applications and services.

Many uses of the Internet involve exchange of information and provision of services that do not concern people and PII. PII varies by jurisdiction. The security of such information and services can be critical to interested parties. Furthermore, the range of hardware connected to the Internet as either individual devices or private networks is increasing rapidly in the so-called Internet of things. Autonomy and application of artificial intelligence within the Internet of things creates challenging Internet security requirements.

While the Internet can facilitate significant business outcomes, there are always many security risks to be managed. It is important to remember that the Internet was not originally designed with security features in mind. Organizations rely heavily on the use of the Internet to conduct their business. Owing to a low level of trust associated with the Internet, business operations can face significant adverse consequences from the loss of confidentiality, integrity, and availability of information and services, if not adequately controlled.

While some individuals are careful in managing their online identity, most people upload 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 interested parties on the Internet. Thus, risks can be associated with loss of privacy over the Internet.

The convergence of information and communication technologies, the ease of getting into the Internet from desktops, laptops to mobile and IoT devices, and the narrowing of personal space between individuals, are gaining the attention of malicious actors and criminal organizations.

These entities are using mechanisms such as phishing, spam and spyware, as well as developing attack techniques like zero-day attacks, vishing, malicious websites and other deception techniques to exploit any weaknesses they can discover on the Internet.

In recent years, security attacks on the Internet 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.

Many of these tools are also available on public software repositories and other publicly available resources. The objectives of an attack range from personal attacks, identity theft, financial frauds or thefts, to hacktivism and information manipulation on the Internet. Much of the stolen personal data and customer data are also made available on the dark net, which can be publicly accessible. Organizations, and SMEs in particular, should understand the real consequences of "manipulating" information on the Internet. These security risks are the cyber risks to the users accessing the Internet.

As the Internet is a global public network, transactions can originate from any part of the world, as can attacks. The multiple modes of business transactions that are carried out on the Internet 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.

Another complexity arises from the fact that all interested parties, even when they are not malicious, have a different view on their needs, requirements and threats, hence they have a different list of risks and controls to counter them. This means that there is no "one size fits all" solution.

Criteria such as what constitutes a transaction or an agreement are dependent on the specific legal and regulatory environments across jurisdictions. These criteria also depend on the interpretation of the law and how each party in the relationship manages their liability. Often, the issue of using 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 Internet issues are far-reaching and global in nature. The challenges can only be addressed through collaboration between the information security technical community, legal community and different regions to adopt a coherent strategy. This strategy should take into account the role of each interested party and existing initiatives, within a framework of international cooperation.

Information travels through the Internet instantly, meaning that attacks can also happen instantly. As these speeds are not easily apprehended by human mind, the attack is always discovered a long time after it occurred, and damages are already potentially huge. In most cases, the identity of the attackers is hidden. Therefore, the use of artificial intelligence (AI) is frequently proposed to counter the attacks.

7 Interested parties

7.1 General

Interested parties of Internet security include those who:

— use services over the Internet;

— use the Internet to provide services;

— provide the infrastructure and communicating capabilities of the Internet;

— globally coordinate the operation of the Internet;

— provide and enforce laws and regulations.

The interested parties of Internet security can be categorized as users (7.2), coordinators and standardization organizations (7.3), government authorities (7.4), law enforcement agencies (7.5) and Internet service providers (7.6).

7.2 Users

Users is a term that refers to individuals, end-users as well as private and public organizations using the Internet. Private organizations include small and medium enterprises (SMEs), as well as large enterprises. Government and other public agencies are collectively referred to as public organizations. An individual or an organization becomes a user when they access the Internet or any services available over the Internet. Users can make use of Internet services, view or collect information. They can also provide certain specific information which is within an application's space, or open to limited members or groups within the application's space, or the general public.

User roles can include, but are not limited to, the following:

— general Internet application user, or general user, such as online game player, instant messenger user, or web surfer;

— buyer/seller, involved in placing goods and services on online auction and marketplace sites for interested buyers, and vice versa;

— blogger and other contents contributor (for example, an author of an article on a wiki), in which information in text and multimedia (for example, video clips) are published for general public or limited audience's consumption;

— member of an organization (such as an employee of a company, or other form of association with a company);

— other roles, whereby a user can be assigned a role unintentionally or without their consent.

EXAMPLE 1 When a user visits a site which requires authorization, and intentionally or unintentionally gains access, the user can be labelled as an intruder.

EXAMPLE 2 An individual, acting as buyer or seller, can unknowingly participate in criminal transactions of selling stolen goods or money laundering activities.

Organizations often use the Internet to publicize company and related information, as well as market related products and services. Organizations also utilize the Internet as part of their network for delivery and receipt of electronic messages (for example, emails) and other documents (for example, file transfer).

In line with the same principles of being a good corporate citizen, these organizations should extend their corporate responsibilities to the Internet by proactively ensuring that their practices and actions in the Internet usage do not introduce further security risks into the Internet user community.

Some proactive measures include:

— information security management by implementing and operating an effective information security management system (ISMS) (see ISO/IEC 27001 for requirements for information security management systems);

— implementing controls based on ISO/IEC 27002 and other relevant standards, without operating an ISMS;

— security monitoring and incident response;

— incorporating security as part of the software development life-cycle (SDLC), where the level of security built into systems should be determined based on the organization's criticality of data;

— regular security education of users in the organization through continuous technology and process updates and keeping track of latest technology developments; and

— understanding and using proper channels in communicating with vendors and service providers on security issues discovered during usage.

7.3 Coordinator and standardization organisations

Coordinator and standardization organisations (ICANN, IETF, W3C etc.) develop technical standards on the use of the Internet and the services provided by the service providers. They advise organizations of their roles and responsibilities on the Internet.

7.4 Government authorities

Governments hold information on national security, strategic, military, intelligence issues among many other elements relating to the government and state, but also a vast array of information on individuals, organizations and society as a whole.

Governments should protect their own country's infrastructure and information from unauthorized access and exploitation. There is a growing and expanding trend of offering e-government services using the Internet. This is a new channel, among others, to launch attacks and access the abovementioned information which, if successful, can result in serious impact to a region, its government and society.

Government authorities play a coordination role between law enforcement agencies and are the primary coordinator for disseminating information and orchestrating any required resources, both at national-level and corporate level, in times of crisis arising from a massive cyber-attack. This also includes authorities like CERT and similar organizations that are entrusted with such responsibilities depending on the specific region in context.

Governments mandate cybersecurity education programmes for universities and high schools, and ensure that an appropriate public-private-partnership is organized with the necessary legal structure, that organizes the law enforcement agencies and defines their missions.

7.5 Law enforcement agencies

Law enforcement agencies enforce the regulations and hold all interested parties accountable in terms of their compliance to the relevant regulations within its national jurisdiction.

7.6 Internet service providers

Service providing organizations can include two categories:

— providers of access to the Internet for employees and partners;

— providers of services to consumers of the Internet.

These services are provided either to a closed community (for example, registered users), or the general public, through the delivery of applications including cloud-service providers over the Internet. A consumer can also be a service provider, if it in turn provides a service over the Internet or enables another consumer to access the Internet.

Service providers can also be understood as carriers or wholesalers, versus distributors and retailers of access services. This distinction is important from a security and, especially, law enforcement perspective. In the event that a distributor or retailer is unable to provide adequate security or lawful access, support services often default back to the carrier or wholesaler. Internet service providers (ISPs) can provide support by supervising the "traffic" and providing alternative routes or hosts for traffic control. They also can look for "dangerous" transfers over the Internet. With the necessary legal authorizations and those of the users, they can filter what is dangerous, as it is the case with solutions providing "sand boxes" to verify transferred files for malware. ISPs can warn their customers when they discover threat patterns.

8 Internet security risk assessment and treatment

8.1 General

ISO 31000 provides principles and generic guidelines on risk management while ISO/IEC 27005 provides guidelines and processes for information security risk management in an organization, supporting the requirements of an ISMS according to ISO/IEC 27001. The guidelines and processes provided by these documents are recommended for addressing risk management in the context of the Internet. It is the responsibility of the interested parties to define their approach for risk management. Several existing methodologies can be used under the framework described in ISO/IEC 27005 to conduct a risk assessment and manage the risks associated with the organization's use of the Internet, considering the relevant threats and vulnerabilities and the Internet security issues.

In organizations where there are limited resources available, the controls are required to take into account the rationality between the organizational needs for security and resources to avoid errors in the selection of controls. An inappropriate selection of controls may result in additional risks or ineffective controls.

8.2 Threats

A threat agent is an individual or group of individuals who have any role in the execution or support of an attack. Thorough understanding of their motives (religious, political, economic, etc.), capabilities (knowledge, funding, size, etc.) and intentions (fun, crime, espionage, etc.) is critical in the assessment of vulnerabilities and risks, as well as in the development and deployment of controls.

Malware can result in the compromise of security controls (e.g. capture and disclosure of passwords), unintended disclosure of information, unintended changes to information, destruction of information, and/or unauthorized use of system resources. Malware is commonly delivered through viruses, worms, and trojans with far-reaching consequences.

A virus is an executable and replicable program that inserts its own code into legitimate programs with the objective of damaging the host computer (i.e. deleting files and programs, corrupting storage and operating systems). In its simplest state, a worm is a computer program meant to self-replicate and spread to other computers through outbound messages to all the addresses in a user's contact list to drain a system's resources. Additionally, just like a virus, a worm can propagate code that can damage its host. Such code is referred to as a payload (e.g. the ability to encrypt files in ransomware and the installation of system backdoors that enable remote access). A trojan is a malicious program disguised as or embedded within legitimate software that has similar objectives to viruses and worms, but, unlike either of them, does not replicate or propagate on its own.

Internet security threats to personally identifiable information (PII) of Internet users revolve mainly around identity issues, posed by the leakage or theft of personal information. If a person's online identity is stolen or masqueraded, the person can be deprived of access to key services and applications. In more serious scenarios, the consequences can range from financial to national level incidents. Unauthorized access to a person's financial information also opens up the possibility of theft of the person's money and fraud.

EXAMPLE 1 Credit information can be sold on the black market or darknet, which can facilitate online identity theft.

EXAMPLE 2 Other examples of threats that in turn equate to threats to life include cyber bullying, online stalking and exploitation crimes including child exploitation and human trafficking.

Another threat is the possibility of the endpoint including personal devices and bring your own device (BYOD) being made a zombie or a bot. Computing devices can become compromised and thereby part of a larger botnet. The online presence and online business of an organization are often targeted by miscreants whose intent is more than plain mischief.

On a larger scale, the infrastructure that supports the Internet can be targeted as well. While this does not affect the functioning of the Internet permanently, it affects the reliability and availability of the infrastructure, which contributes to the security of the Internet.

On a national or international level, the Internet is an area in which illegal behaviour in a given jurisdiction thrives. Due to the nature of the Internet, specifically the challenges in defining boundaries and borders, it is difficult to regulate and control the way that it can be used.

Criminals can either legitimately buy the applications, services and resources that facilitate their cause, or they can resort to illegal means of securing these resources to avoid detection and tracking. This can include acquiring massive computing resources through botnets.

Another threat relates to the deliberate modification of publicly available or proprietary information, or creation of fake information and hoaxes that, if relied upon, can generate serious damage.

8.3 Vulnerabilities

Vulnerability is weaknesses of an asset or control that can be exploited by a threat. Manufacturers, software developers and other technology developers produce security updates and patches to fix these weaknesses once they are found and solved. As systems receive patches, updates or new elements are added. As systems become outdated or unsupported by the vendor or not patched to the latest version, new vulnerabilities can be introduced. Interested parties should have a thorough knowledge and understanding of the asset or control in question, as well as the threats, threat agents and risks involved, in order to perform a comprehensive assessment. Interested parties should be aware of the zero-day vulnerabilities for which there is no patch available.

Web applications accessed over the Internet are susceptible to a variety of vulnerabilities that are introduced by poor design, poorly written code and poorly built production libraries and executables. Examples of such vulnerabilities include the authentication bypass, database injection attacks and cross-site scripting attacks. In these attacks, requests can be manipulated to abuse the webserver functionality.

8.4 Attack vectors

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

Port scanners are one of the oldest and still very effective tools used by attackers. They scan all ports available on the Internet-facing system to confirm which ports are open. This normally is one of the first steps executed by a prospective attacker on the target Internet-facing system. While the initial attack always targets a publicly facing system (e.g. router, server, firewall, website, etc.), attackers can also seek to exploit assets residing inside the private network that are connected to these publicly facing systems.

Listening to communication channels is a simple and easy attack vector. It is also one of the oldest. Copying and analysing the traffic can be extremely valuable for detecting entry points and initiate other threat vectors. An attacker can also use communication hijacking (by tailgating or piggy-backing) and disguise themselves behind the identity or credentials, and at the expense of the legitimate user without them knowing.

Many of the attacks on the Internet are carried out using malicious software, such as spyware, worms and viruses. Information is often gathered through phishing techniques. An attack can occur as a singular attack vector or carried out as a blended attack or a targeted attack. These attacks can be propagated via, for example, suspicious websites, unverified downloads, spam emails, remote exploitation, zero-day exploitation, and infected removable media.

Other mechanisms growing in use and sophistication, for carrying out attacks, are those based on social networking websites and the use of corrupted files on legitimate websites. Legitimate websites can also be hacked into and have some of their files corrupted and used as a means for perpetrating attacks. Individuals tend to implicitly trust commonly visited websites. Attackers can apply the waterhole

technique to compromise a specific group of end users by infecting frequently visited websites. Besides the attacks launched by human attackers, malware infected computers also launch various attacks to surrounding connected computers.

With the proliferation of peer-to-peer applications, commonly used to share files such as digital music, video, photos, etc., attackers are becoming increasingly sophisticated in how to disguise themselves and their malicious code using the exchanged files as a Trojan for their attacks. Once an attacker, through identity theft, can disguise themselves as a legitimate contact, the attacker can engage others, and a new avenue is open for launching the various types of attacks.

Another technique is IP spoofing, in which the attacker manipulates the IP address associated with their messages in an attempt to disguise it as a known, trusted source, thus gaining unauthorized access to systems.

The attacker does not always use the same attack vector. It uses multiple vectors and changes them frequently. Some attacks are hidden to such an extent that they are not detected until it is already too late for the user. Defenders should consider this and look for defence against multiple vectors and not only those already used against them.

IoT devices, smart phones, etc. can be connected to the Internet. These devices can act as an additional attack vector just like any other Internet-connected device, if they are not adequately controlled when connected to the organization's network.

An advanced persistent threat (APT) is a method of attack with a goal of stealing information over a long period of time whereby attackers gain ongoing access to an organization's network, establish themselves undetected, move laterally, look, learn and remain in the network.

Another old attack method is brute force. This uses trial and error to guess login credentials, encryption keys, finding hidden web pages whereby attackers work through all possible combinations hoping to guess correctly to gain access to an organization's network and information.

9 Security guidelines for the Internet

9.1 General

Interested parties can assess risks by taking into account threats that apply to their assets. This analysis can aid in the selection of controls to counter the risks and reduce them to an acceptable level. Controls are implemented to reduce the likelihood or consequences of such risks, and to meet security requirements of the interested parties (either directly or indirectly by providing direction to other parties).

Vulnerabilities can remain after the implementation of controls. Such vulnerabilities can be exploited by threat agents. Interested parties seek to minimize the risk, given other constraints. Interested parties should be confident that the controls are adequate to counter the threats to assets before they allow exposure of assets to the specified threats. If the interested parties do not possess the capability to evaluate all aspects of the controls, they can seek evaluation of the controls using external organizations.

An effective way to confront Internet security risks involves a combination of multiple strategies, taking into consideration the various interested parties.

These strategies include:

— industry specific approaches, with collaboration of all interested parties to identify and address Internet issues and risks;

— broad consumer and employee education, providing a trusted resource for how to identify and address specific Internet risks within the organization as well as in the community of Internet users;

— innovative technology solutions to help protect consumers from known Internet-based attacks, to stay current and be prepared against new exploitations;

— updated legislation and regulations to enable justice to prevail across jurisdictions.

9.2 Controls for Internet security

9.2.1 General

Most organizations use the Internet for various purposes, from web surfing, blogging, social networking and accessing public cloud services, to information sharing and doing e-commerce business. This involves sharing of classified business information including personal information while executing online transactions. The Internet being a public network is prone to certain unique threats. If not addressed, these threats result in attacks that can be difficult to manage.

Organizations should develop policies, procedures and response capability to:

a) define the rules for acceptable use of the Internet by personnel;

b) define what services may be exposed over the Internet;

c) identify the threats, vulnerabilities, attack vectors and their associated risks;

d) define the roles and responsibilities of various users of the Internet;

e) conduct user awareness on the safe practices for Internet usage;

f) specify the responsible departments for handling Internet security issues;

g) establish a response mechanism for cybersecurity incidents;

h) conduct security drills to test the response mechanism towards attacks originating from the Internet.

Based on risk assessment, one can uncover the various relevant Internet security risks that can be addressed through various controls as explained below.

9.2.2 Policies for Internet security

An organization should prepare and publish a policy concerning Internet usage by personnel and other relevant parties in alignment with security objectives. This determines which Internet services are used, who is authorized to use them, and what the security objectives are. This policy directs all other guidelines for the secure connection to, and use of, the Internet.

Policies for Internet security should be defined, approved by management, published and communicated to, and acknowledged by, the relevant personnel, contractors and external parties. The Internet security policies should stipulate the personnel authorized to access the Internet, the content they can view, prohibited conduct on the Internet, among others. Responsibilities should be allocated for all activities pertaining to the Internet, and for the design, approval, implementation, operation and monitoring of all the specific controls applicable to Internet security.

ISO/IEC 27002 provides further guidance on policies for Internet security.

9.2.3 Access control

Access control includes access rights not only for users, but also other entities such as devices, applications or automated processes. Therefore, every connection should be authenticated, and every activity duly authorized, based on the roles and permissions established according to the business and security rules, and each entity should be assigned the least privileged permissions. This enhances the traceability of access to information and assets, and reduces anonymity to increase security.

Rules to control physical and logical access to information and assets, other assets associated with the Internet and information processing facilities should be established and implemented based on business and information value. Rules regarding access to essential information and assets, other assets associated with information and information processing facilities should be in line with an established access control policy and information classification policy.

Accounts should only be restricted to users who are authorized due to their job role or function. Each user should have separate accounts and they should not be shared, nor should the same password be used for more than one account.

Access rights to information, systems, applications and services should be provisioned, reviewed, adjusted, modified and removed according to the organization's policy and procedure on access control. The allocation and use of privileged access rights should be restricted and controlled. Secure authentication technologies and procedures should be implemented based on information access restrictions and related access control rules. Password management systems should be put in place to manage and support the process of password creation and the quality thereof.

Information systems directly connected to the Internet (e.g. firewall infrastructure, network perimeter devices, etc.) can have one or more privileged utility programs that can be capable of overriding system and application controls. If an attacker gets access to any of the systems, then these privileged utility programs, if not properly controlled, can result in privileged access by the attacker.

These programs should be adequately controlled by the organization so that intruders do not get access to such privileged utility programs and override system and application controls. Effective access management should include:

— regular review of all access rights;

— regular review of administrative logs.

ISO/IEC 27002 and ISO/IEC 29146 provide further guidance on access management.

9.2.4 Education, awareness and training

Organization's personnel (including top management, system admin, IT staff and privileged users etc.) should be regularly updated on the main threats (e.g. phishing and vishing) and the actions to be taken to prevent them and respond in case of improper action.

Numerous new threats are launched on the Internet daily and are continuously evolving and becoming more stealthy and sophisticated. When implementing a control to counter an attack, it is possible users are not aware that they are the victim of an attack that is new or more sophisticated.

Organizations should provide regular awareness and training material for personnel using a variety of formats such as email communications, online training and messaging through intranets, to inform personnel of online threats as well as their obligations of acceptable use and reporting incidents. This provides a level of understanding and catches their attention to protect both themselves and the organization.

ISO/IEC 27002 provides further guidance on education, awareness and training.

9.2.5 Security incident management

Security incidents on the Internet can range from a wide variety of cyber-attacks on Internet-facing organizational resources, as well as servers, databases and applications that are behind the Internet facing resources. Security incidents can be triggered from anywhere on the Internet. Sometimes the host that is carrying the attack can be a compromised host. Some incidents can be sophisticated in nature and involve special skills to adequately respond. Incidents often cross national, geographical and organizational boundaries, and the speed of information flow and changes from the unfolding incident often gives limited time for the responding individuals and organizations to act.

An incident management team (IMT) with a supporting incident response team (IRT) should be established to provide the organization with capability for assessing, responding to and learning from such incidents. Incident response procedures should consider detecting and reporting the occurrence of security events like potential and actual incidents by human or automatic means. Monitoring tools implemented by the organization can detect and send security events for incident response. Threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. Information security personnel should continuously scan threat intelligence sources like social media intelligence, human intelligence, technical intelligence or intelligence from the deep and dark web, collect the information and then analyse it.

A technical solution to support information sharing and coordination should be established to help prepare and respond to security events and cyber incidents. This is an important step that organizations should take as part of their security controls. Such a solution should involve information sharing and coordination that should be secure, effective, reliable and efficient.

Incidents pertaining to Internet security should be responded to by a nominated contact and other relevant persons of the organization or interested parties. Any external requirements on reporting of incidents to relevant interested parties within the defined time frame (e.g. incident notification requirements to regulators within defined time frames) should be considered when implementing incident management procedures. The organization should establish and maintain contact with the relevant legal, regulatory, and supervisory authorities. The organizations should also maintain contact with special interest groups and other specialist security forums and professional associations.

There is a need for efficient and effective information sharing, coordination and incident handling among interested parties in Internet security. This collaboration should be in a secure and reliable manner that also protects the privacy of individuals concerned. Many of the interested parties can reside in different geographical locations and time zones and are likely to be governed by different regulatory requirements.

Information sharing and collaboration includes:

— key elements of considerations for establishing trust;

— necessary processes for collaboration and information exchange and sharing;

— technical requirements for systems integration and interoperability between different interested parties.

The organization using the Internet should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence in case of a security incident. It is expected that evidence is collected in a manner that is admissible in the appropriate national courts of law or international authorities in case the incident is proved to have originated from another country as per the monitoring logs and other digital evidence.

Digital evidence can transcend organizational or jurisdictional boundaries in case of a security incident. In such cases, it should be ensured that the organization is entitled to collect the required information as digital evidence for future course of action. The correct setting of computer clocks is important to ensure the accuracy of audit logs, which can be expected for investigations in case of any attacks from over the Internet or expected as evidence in possible legal action.

The information gained from the evaluation of security incidents of Internet-facing systems should be used to identify recurring or related incidents in order to plan and implement changes to reduce the likelihood or impact of future similar incidents. Tools like IPS and SIEM can be re-configured based on the evaluation of the security incidents and relevant policy amendments can be initiated to prevent future incidents.

ISO/IEC 27002 and the ISO/IEC 27035 series provide further guidance on incident management.

9.2.6 Asset management

ICT components containing critical information and applications should be identified. Traditionally, organizations have been expected to know where their assets are physically located in order to protect them adequately. Organizations should not only keep an inventory of up-to-date ICT assets within their control but should also maintain an information asset register of where their information is processed, stored, transferred, whether it is on their internal network or uses cloud/Internet-based hosting solutions. In this manner, the organization can manage the risks to their information wherever it resides and make risk-based decisions regarding whether it is appropriate for that information to be stored outside the organization's control environment. Similarly, for network components, organizations are expected to know where the sensitive assets are located with regards to the entry points for potential attackers. This can be the official Internet access — via the firewall — and all the other connections with devices, (e.g. smartphones, IoT). Organizations should also identify critical paths used to access sensitive ICT assets or to transport sensitive information within the organization’s network. These paths should not be visible, accessible or monitorable by intruders. Without this knowledge, no adequate segregation of networks is possible. This inventory should take the form of network architecture (location of the functionalities) and infrastructure, both clearly indicating the entry/connection points with the Internet (all the interconnected networks).

Rules for the acceptable use and procedures for the handling of assets, other assets associated with the Internet and related processing facilities should be identified, documented and implemented. Organizations should have and use a procedure to evaluate the criticality of information and ICT assets that hold and transfer them. This would allow the organization to clearly identify what should be protected and at what level in terms of generic policies and network security.

ISO/IEC 27002 provides further guidance on asset management.

9.2.7 Supplier management

Processes and procedures should be identified and implemented to manage the Internet security risks associated with the use of suppliers. All relevant information security requirements should be established and agreed with each supplier based on the type of supplier and associated risks. Risk management in relation with the ICT suppliers and the information they store, exploit or can have access to, is key for preparing contracts that ensure that the organization’s information security objectives are continuously achieved.

Agreement with suppliers relevant to the Internet (like ISPs and cloud service providers over the Internet) should be established and documented to ensure that there is a clear understanding between the organization and the suppliers regarding both parties’ obligations to fulfil relevant information security requirements. Organizations should have open partnerships with the ISPs, telecommunication service providers, cloud service providers and partners to inform/warn of detections of incoming threats. The ability of the Internet service provider to manage agreed services in a secure way should be determined and regularly monitored. It is expected that the organization and the service provider reach an agreement on the right to audit.

For cloud services accessible over the Internet and as subscribed by the organization, the organization is expected to review and negotiate the cloud service agreements with the cloud service provider(s). The organization should undertake the relevant risk assessment to identify the risks associated with using the cloud services and manage the risks for the duration of the agreement. It is expected that the cloud service agreement addresses the confidentiality, integrity, availability and PII handling requirements of the organization. For any cloud services where an organization is unable to negotiate the terms of the agreement, it is expected that the organization enters the agreement with eyes wide open, understanding the risks of using the service and how to manage these risks for the duration of the agreement.

Cloud-based tools like web meeting tools, web chatting tools and cloud storage tools pose the risk to an organization if these tools have inherent security bugs that can be exploited by bad actors, therefore it is important for the organization to establish security controls for usage of these cloud-based tools.

The following can be considered for inclusion in the agreements in order to satisfy the identified Internet security requirements:

a) legal and regulatory requirements, including information protection requirements at the ISP's end like protection from DDoS and other attacks;

b) obligation of each contractual party to implement an agreed set of controls including access control, network and system monitoring, reporting and auditing; as well as the supplier's obligations to comply with the organization's security requirements;

c) incident management requirements and procedures (especially notification and collaboration during incident remediation);

d) monitoring, review and change management of supplier services to ensure that the information security terms and conditions of the agreements are being adhered to, and that they allow the monitoring of service performance levels to verify adherence to the agreements, monitor changes made by suppliers and monitor changes in supplier services.

ISO/IEC 27002, the ISO/IEC 27036 series, ISO/IEC TR 23187 and ISO/IEC 27017 provide further guidance related to suppliers.

9.2.8 Business continuity over the Internet

Some business activities like Internet based trading and other e-commerce activities depend on the organization's Internet infrastructure within the organization. Disruptions to Internet services can be caused by DoS and DDoS attacks from bad actors, perimeter device malfunction or any disruption from the ISP end. DoS and DDoS attacks can also be conducted by bad actors on the ISP end that can result in complete outage of the Internet backbone. Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Any disruptions in the Internet infrastructure constitute continuity risks to the organization and should be addressed by the organization. Organizations should plan for procurement of Internet services from different ISPs for basic continuity measures. Organizations should deploy security measures to avoid disruptions like anti-DDoS measures for continuity of network devices. Organizations can also require respective ISPs to deploy anti-DDoS measures within the ISP network. Regardless of the continuity service, organizations should continue to consider information security in any solution even when in business continuity mode.

ISO/IEC 27002, ISO 22301 and ISO/IEC 27031 provide further guidance related to ICT continuity.

9.2.9 Privacy protection over the Internet

Most service providers control or process PII. When this information is used for purposes different to the interests of the data principal, privacy concerns are raised. A hosting service provider processes PII on their network and data centre as part of their business services. These services, which include websites and other online applications, are often re-packaged and resold by hosting subscribers to other consumers, such as small businesses and end-users and made accessible over the Internet.

Should the hosting subscribers set up an insecure server, or host malicious contents in their sites or applications, the security of the consumers including PII stored by such online applications, will be adversely affected. As such, it is important that services, at a minimum, meet best practice standards by complying with the minimum terms of agreements that covers the privacy requirements of the users. In addition to the data protection and personal privacy provisions on the Internet-facing site or application, service providers should require such sites or applications hosted on their networks to implement a set of best practice security controls at the application level before they go live. Prior to signing up to a service on the Internet, organizations should undertake a privacy impact assessment (PIA) to identify the personal information that can be used, collected, processed, stored or transmitted and the associated privacy risks to determine whether they are acceptable to the organization and manage these accordingly. This does not only include collecting customer data to provide a service but can also include collecting metadata such as IP addresses or geolocation data of individuals browsing

websites. Organizations should publish a privacy notice on their site to clearly inform all their users of the requirements of interacting with the organization's online services. Data masking should be used according to the organization's policy on access control and business requirements, taking legal requirements into consideration. DLP measures should be applied to systems and networks that process, store or transmit sensitive information. There are technological features in some Internet browsers, that allow privacy settings to be changed by the user.

ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29100 and ISO/IEC 27018 provide further guidance related to privacy.

9.2.10 Vulnerability management

Information about vulnerabilities of ICT systems being used should be obtained in a timely fashion. The organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken to address the associated risk. Configurations, including security configurations of hardware, software, services and networks should be established, documented, implemented, and monitored and reviewed.

Organizations that supply technology products (firewall, IDS, IPS etc.) and services (network services, VoIP services, managed security services etc.) should consistently and effectively implement measures to identify, handle and disclose vulnerabilities of the products and services they supply. Based on the vulnerabilities disclosed by the product and service vendors, appropriate protection measures are implemented to address the vulnerabilities.

With the increasing proliferation of malware on the Internet, a service providing organization can receive reports relating to malware and spyware infections and other security issues. Such information is important and useful for relevant vendors to assess the risk of malware infection, and provide updates to necessary tools to ensure that any new malware or spyware detected can be removed or disabled effectively. In this regard, an organization should establish contact with security vendors and submit relevant reports and malware samples to the vendors for follow-up, particularly if there appears to be a spike in prevalence. Most vendors maintain an email list for receiving such reports or samples for analysis and follow-up.

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities. The organization should define and enforce strict policy on which types of software users can install. Software patches should be applied when they can help to remove or reduce security vulnerabilities.

Vendor supplied software used in operational systems over the Internet should be maintained at a level supported by the supplier. Over time, software vendors cease to support older versions of software. The organization should consider the risks of relying on unsupported software including open-source software when used in operational systems. Open-source software used in operational systems should be maintained to the latest appropriate release of the software.

Other mitigations for vulnerabilities include:

a) changing the operational practices;

b) reconfiguring the technical systems;

c) avoiding the risk by managing Internet access;

d) training staff and users;

e) applying defence in-depth measures i.e. where one controls fails, there is another independent method in place to continue to defend;

f) system security testing, secure SDLC and testing of patches, updates before deployment.

ISO/IEC 27002, ISO/IEC 30111 and ISO/IEC 29147 provide further guidance related to vulnerability management.

9.2.11 Network management

Reducing the exposure of assets connected to Internet reduces risks related to unauthorized access, tampering or damage. Controls should be implemented to ensure the security of information connected to the Internet and to the protection of connected services from unauthorized access. Controls should be established to safeguard the confidentiality and integrity of data passing over the Internet and to protect the connected systems and applications. Systems that can be connected to the Internet should be restricted and where permitted, should be authenticated. Logging and monitoring of network devices and systems associated with the organization's Internet infrastructure, should be applied for recording and detecting actions that can affect, or are relevant to, Internet security. The organization should consider managing the security of systems connected to the Internet by segregating the same from other organizational networks like private networks and DMZ. The perimeter of this segregated network should be well defined and should be controlled using a gateway (e.g. firewall, filtering router).

The following should be considered for network security implementation:

— Ensure there is a monitored and reliable interface between the organization’s network and the Internet, that also ensures access control of all entities, and not only authorized people. Information and applications should also be controlled before granting both access to and from the internal infrastructure.

— Structure the internal network to isolate highly critical assets from general use assets, by creating kind of silos or clusters with adequate access control. Ensure sub-networks with filtering routers and imbedded sub-networks to avoid having a straight path to critical assets.

— Monitor and analyse internal traffic to detect and block illicit activities.

— Ensure the access and use of Internet and its services (including the communication with personnel working outside the physical facilities) is preserved.

— Ensure that the internal network is sufficiently segregated with internal border protections to isolate critical or crucial components from the entry-points and easy to access internal transfer channels.

Rules should be formulated on the use of Internet and services accessed over the Internet to cover the following aspects at a minimum:

a) the network services over the Internet that may be accessed by the user and authorization procedures for such services;

b) network management and technological controls and procedures to protect access to Internet connections and network services over the Internet;

c) the means used to access Internet and services over the Internet (e.g. HTTPS, VPN);

d) monitoring of the services accessed over the Internet (e.g. bandwidth monitoring, SIEM).

A firewall is a critical network perimeter device and organizations should consider firewall technologies that can better address the Internet-based attacks. The aim of this device is to provide a protection from the threats coming from the Internet and prevent the uncontrolled transfer of proprietary information to the Internet. Router technologies can be deployed with in-built features or add-on modules to enhance network security and can address cyber risks like DoS and DDoS attacks.

Network-based IDS and network-based IPS technologies can be deployed with artificial intelligence and machine learning to deal with advanced Internet-based attacks including attacks with known signature patterns and behaviour. Depending upon their network setup, organizations can consider network appliances that come with in-built various network security modules like firewall, IPS, DLP and protection from attacks targeting DNS.

ISO/IEC 27002 and the ISO/IEC 27033 series provide further guidance on network security.

9.2.12 Protection against malware

Anti-malware software scans data and programs to identify suspicious patterns associated with malware. To enable detection of new malicious code, it is very important to ensure that the scanning software is always kept up to date, desirably through daily updates.

Given the potential for new malware to target zero-day vulnerabilities, software exists that can identify known variants. This includes technology that can identify potential attack patterns. While not fool proof, this software does provide a higher level of protection than not using it. Several popular operating systems have some embedded features to protect against common malware but should still be supplemented with anti-malware technology for higher risk environments.

Anti-malware implementation should be expanded to the protection of unwanted Internet traffic and exchange (in both directions), as users generally receive and send malware without knowing it. Prevention, detection, correction and recovery measures to protect against malware should be implemented, combined with appropriate user awareness.

The following guidance should be considered by the organization:

a) using anti-malware software on the gateways to the Internet, for scanning all traffic to and from the Internet, including all network protocols authorized for use;

b) using anti-malware software on all client systems, especially those used for Internet access by employees;

c) scanning files, emails, instant messaging attachments, webpages and external links for viruses, ransomware, trojans and other forms of malware;

d) blocking suspicious pop-ups, web advertisements, known or suspected malicious websites, and using blocklists for unauthorized services, e.g. chat channels or web mail services;

e) making users aware that there are greater risks associated with malware when dealing with external parties over external links;

f) verifying that accurate information relating to malware comes from qualified and reputable sources (e.g. reliable Internet sites or suppliers of anti-malware software);

g) implementing logging and monitoring for all services which allow the possibility to transfer data towards the Internet;

h) restricting the use of unauthorised services which enable the transfer of big amounts of data;

i) implementing filters for non-authorized protocols, e.g. peer-to-peer networking protocols;

j) patching known system vulnerabilities within time frames based on vulnerability criticality, with focus on all systems receiving Internet traffic;

k) configuring systems and applications accessed over the Internet, to disable functions that are not necessary (e.g. macros);

l) preparing appropriate plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery arrangements.

ISO/IEC 27002 provides further guidance on protection against malware.

9.2.13 Change management

Change management policies and processes should be established to ensure that it is easier for organizations to roll out changes to the IT infrastructure, manage changes to IT systems and applications in order to prevent unscheduled disruption, data corruption or loss. Organizations should include Internet security related changes for systems hosted on the Internet in its change management process. These processes help the organization to request, prioritize, authorize, approve, schedule

and implement any changes. Change management policies include statements on responsibilities and duties of system managers, importing software and files, access control, among others. All changes (modifications, moves, removals or additions) of network components or structure should be managed to keep the architecture and the infrastructure drawings up to date.

ISO/IEC 27002 provides further guidance on change management.

9.2.14 Identification of applicable legislation and compliance requirements

The Internet is increasingly used as a platform to deploy many online transaction services. There can be data security, cybersecurity and privacy laws and regulations on protection of confidentiality, integrity and availability of transaction details.

Banking transactions, payment channels, mobile app-based transactions and other e-commerce activities are usually regulated due to involvement of money in digital form. All information security and cyber security relevant legal, statutory, regulatory and contractual requirements and the organization's approach to meet these requirements should be identified, documented and kept up to date.

It is expected that records maintained on online systems accessed over the Internet, are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legal, statutory, regulatory, contractual and business requirements. Records can be required as evidence that an organization operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organization to interested parties.

ISO/IEC 27002 provides further guidance on legislation and compliance requirements.

9.2.15 Use of cryptography

Cryptography is one of the ways to ensure the protection of the transmitted information and prevent traffic analysis. A virtual private network (VPN) is a simple solution. Cryptography has some constraints associated with the management of the ciphering and deciphering keys, and the management of the cryptographic devices, which should be considered as confidential and critical.

Cryptography should be used to protect the confidentiality, authenticity and/or integrity of information transmitted over the Internet. Implementation of VPN and HTTPS (hypertext transfer protocol secure) uses cryptography for secure connections. Cryptographic algorithms, key lengths and usage practices should be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use, as well as disclosure. Equipment used to generate, store and archive keys should be physically protected where relevant. When using cryptography, it should be kept in mind that different regulations and national restrictions can apply to the use of cryptographic techniques and the issues of trans-border flow of encrypted information.

ISO/IEC 27002 provides further guidance on use of cryptography.

9.2.16 Application security for Internet-facing applications

New technology can be adopted for systems that are part of the internet infrastructure. The new technology should be analysed for security risks and the design should be reviewed against known attack patterns. Security should be embedded while designing the system. The systems should also be regularly reviewed to ensure that they remain up to date in terms of combatting any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

Organizations should adopt secure engineering principles including implementing a secure development life cycle to identify and mitigate risks in products and solutions being developed. This should consider threat modelling, user authentication techniques, supply chain components, secure session control and data validation, sanitization and a security-oriented design review to help identify

security vulnerabilities on Internet-facing systems. Application code for Internet-facing applications is best designed from the security perspective based upon the assumption that it is always subject to attack, through either error or malicious events.

Organizations should establish rules for safe and appropriate use of resources over the Internet, including any restriction to undesirable or inappropriate websites and web-based applications, and inform its personnel accordingly. This discourages personnel from trying to access such sites. The rules should be kept up to date. Such websites can contain illegal information, viruses and phishing materials. A technique for restricting an undesirable or inappropriate website is blocking the IP address or domain of the website concerned. Some browser and anti-malware technologies can do this automatically or can be configured to do so.

Secure coding standards should be followed to design and develop applications. If the application owner can access scripts by direct remote access to the server, so can an attacker in principle. Web servers should be configured to prevent directory browsing in such cases. The OWASP guidelines[23, 24] can be a useful reference to secure application design and testing.

Organizations should document code behaviour and make an assessment as to whether the behaviour can fall into potential areas that can be considered as spyware or deceptive software. In the latter case, organizations should engage a suitably qualified assessor to evaluate whether the code falls within anti-spyware vendors objective criteria that adheres to best practices. This can ensure that the software tools provided by organizations for the end-users would not be labelled as spyware by anti-spyware vendors. Many anti-spyware vendors publish the criteria by which they rate software.

Organizations should implement digital code signing for their binaries so that anti-malware and anti-spyware vendors can easily determine the owner of a file. Software consistently produced by ISVs using best practices including digital code signing, can be categorized as likely to be secure. Should an organization discover useful software techniques that can help to reduce the spyware or malware problem, the organization should consider partnering and working with the vendor to make them broadly available.

For applications where the transactions are processed over the Internet, the following should be considered:

— requirements for the level of protection required to maintain the confidentiality and integrity of transaction details;

— transmitting transaction details over the Internet with adequate security controls (e.g. encrypted transmission path, digital certification);

— storing transaction details outside of any publicly accessible environment and ensuring the storage medium is not directly accessible from the Internet;

— resilience requirements against attacks, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service;

— where there is the need for a high degree of reliance on the security of software products, the products should be independently validated under the Common Criteria scheme, as described in the ISO/IEC 15408 series.

Security testing should be an integral part of the testing for system or components before exposure to the Internet. The organization can leverage automated tools, such as code analysis tools and vulnerability scanners, and should verify the remediation of security related defects before making the systems live on the Internet.

Security testing should include testing of:

a) security functions, e.g. user authentication, access restriction, secure use of APIs and use of cryptography;

b) secure configurations including that of operating systems, firewalls and other security components.

The ISO/IEC 15408 series provides guidance on application assurance. ISO/IEC 27002 and the ISO/IEC 27034 series provide guidance related to application security.

9.2.17 Endpoint device management

Information stored on, processed by or accessible via endpoint devices (e.g. IoT devices, USB devices, BYOD) should be protected. Carrying and using endpoint devices in secure areas should be appropriately controlled. A security strategy for endpoint device management should be developed and implemented. This strategy should include the management of device firewalls, email specific filtering tools, Internet security and filtering, mobile device management and security tools, encryption and intrusion detection tools.

Endpoint security has become even more important, as endpoints are moving outside the organizational perimeter and users may use the Internet to access the cloud and resources within the organization's network. Compromise at the endpoint should be responded with immediate action to block the attacker and to limit further damage. Organizations should deploy technical capabilities at the endpoints to detect any bad traffic from unknown sources and bad actors, and respond. Such technologies are also known as endpoint detection and response (EDR) technologies. Organizations should have a mechanism to ensure that all the organizational security policies applicable to the end user systems and devices are enabled at all times. Such technologies should make sure that the end user is not able to disable or bypass the security features installed on their endpoint.

Loss or compromise of the endpoint can be a significant risk to the data residing on the endpoint including mobile devices. Organizations should deploy techniques to ensure that they can track these devices and in case of any loss or compromise of the device, they should be able to remotely wipe the contents of the devices even before the data are stolen by the bad actors.

ISO/IEC 27002 provides further guidance on endpoint device management.

9.2.18 Monitoring

Logs that record activities, exceptions, faults and other relevant events should be produced, protected, kept and analysed. Logs should be protected and kept in a secure location for log analysis and audit. Some regulations require storing logs for a certain period of time. Internet-facing networks, systems, and applications should be monitored for anomalous behaviour and appropriate actions should be taken to evaluate potential information security incidents.

ISO/IEC 27002 provides further guidance on monitoring.

Annex A
(informative)

Cross-references between this document and ISO/IEC 27002

Table A.1 shows the correspondence between the controls for Internet security cited in 9.2 of this document and the controls contained in ISO/IEC 27002. Each column contains the relevant subclause number and subheading.

Table A.1 — Mapping between controls for Internet security

ISO/IEC 27032	ISO/IEC 27002:2022
9.2.2 Policies for Internet security	5.1 Policies for information security 5.4 Management responsibilities
9.2.3 Access control	5.15 Access control 5.16 Identity management 5.18 Access rights 8.2 Privileged access rights 8.18 Use of privileged utility programs
9.2.4 Education, awareness and training	6.3 Information security awareness, education and training
9.2.5 Security incident management	5.7 Threat intelligence 5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence 6.8 Information security event reporting
9.2.6 Asset management	5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets 5.12 Classification of information
9.2.7 Supplier management	5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services

Table A.1 *(continued)*

ISO/IEC 27032	ISO/IEC 27002:2022
9.2.8 Business continuity over the Internet	5.29 Information security during disruption 5.30 ICT readiness for business continuity 8.13 Information backup 8.14 Redundancy of information processing facilities
9.2.9 Privacy protection over the Internet	5.34 Privacy and protection of PII 8.11 Data masking
9.2.10 Vulnerability management	8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems
9.2.11 Network management	8.16 Monitoring activities 8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks
9.2.12 Protection against malware	8.7 Protection against malware
9.2.13 Change management	8.32 Change management
9.2.14 Identification of applicable legislation and compliance requirements	5.28 Collection of evidence 5.31 Legal, statutory, regulatory and contractual requirements 5.33 Protection of records
9.2.15 Use of cryptography	8.24 Use of cryptography
9.2.16 Application security for Internet-facing applications	8.23 Web filtering 8.24 Use of cryptography 8.25 Secure development life cycle 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.29 Security testing in development and acceptance
9.2.17 Endpoint device management	8.1 User endpoint devices 8.9 Configuration management
9.2.18 Monitoring	8.15 Logging 8.16 Monitoring activities

Bibliography

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO/IEC 15408 (all parts)

[3] ISO 19101-1:2014, *Geographic information — Reference model — Part 1: Fundamentals*

[4] ISO 22301:2019, *Security and resilience — Business continuity management systems — Requirements*

[5] ISO/IEC/TR 23187:2020, *Information technology — Cloud computing — Interacting with cloud service partners (CSNs)*

[6] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[7] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[8] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[9] ISO/IEC 27017:2015, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[10] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[11] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[12] ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*

[13] ISO/IEC 27034 (all parts), *Information technology — Application security*

[14] ISO/IEC 27035 (all parts), *Information technology — Security techniques — Information security incident management*

[15] ISO/IEC 27036 (all parts), *Cybersecurity — Supplier relationships*

[16] ISO/IEC/TS 27100:2020, *Information technology — Cybersecurity — Overview and concepts*

[17] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[18] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[19] ISO/IEC 29146:2016, *Information technology — Security techniques — A framework for access management*

[20] ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

[21] ISO/IEC 30111:2019, *Information technology — Security techniques — Vulnerability handling processes*

[22] ISO 31000:2018, *Risk management — Guidelines*

[23] OPEN WEB APPLICATION SECURITY PROJECT (OWASP), OWASP Web Security Testing Guide, [online] [viewed 2020-12-03]. Available at https://owasp.org/www-project-web-security-testing-guide/

[24] OPEN WEB APPLICATION SECURITY PROJECT (OWASP), OWASP Top 10, [online] [viewed 2022-10-29]. Available at https://owasp.org/Top10/

ICS 35.030

Price based on 28 pages