International Standard

ISO/IEC 27011

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002

Third edition
2024-03

Reference number
ISO/IEC 27011:2024(en)

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

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 (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 ITU-T (as ITU-T Recommendation X.1051) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27011-1:2016), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 27011-1:2016/Cor 1:2018.

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.

INTERNATIONAL STANDARD ISO/IEC 27011
RECOMMENDATION ITU-T X.1051

Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations

Summary

This Recommendation | International Standard:

a) establishes guidelines and general principles for initiating, implementing, maintaining and improving information security controls in telecommunications organizations based on ISO/IEC 27002;

b) provides an implementation baseline of information security controls within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.

As a result of implementing this Recommendation | International Standard, telecommunications organizations, both within and between jurisdictions, will:

a) be able to ensure the confidentiality, integrity and availability of global telecommunications facilities, services and the information handled, processed or stored within global facilities and services;

b) have adopted secure collaborative processes and controls ensuring the lowering of risks in the delivery of telecommunications services;

c) be able to deliver information security in an effective and efficient manner;

d) have adopted a consistent holistic approach to information security;

e) be able to improve the security culture of organizations, raise staff awareness and increase public trust.

History[*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1051	2004-07-29	17	11.1002/1000/7286
2.0	ITU-T X.1051	2008-02-13	17	11.1002/1000/9332
3.0	ITU-T X.1051	2016-04-29	17	11.1002/1000/12845
3.1	ITU-T X.1051 (2016) Cor. 1	2017-09-06	17	11.1002/1000/13407
4.0	ITU-T X.1051	2023-06-13	17	11.1002/1000/15559

Keywords

Information security controls and telecommunications extended controls, information security management, information security risk assessment, information security risk treatment, ISO/IEC 27002.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

CONTENTS

		Page
1	Scope	1
2	Normative references	1
3	Definitions and abbreviations	1
	3.1 Definitions	1
	3.2 Abbreviations	2
4	Overview	2
	4.1 Structure of this Recommendation | International Standard	2
	4.2 Information security management systems in telecommunications organizations	3
5	Organizational controls	5
	5.1 Policies for information security	5
	5.2 Information security roles and responsibilities	5
	5.3 Segregation of duties	6
	5.4 Management responsibilities	6
	5.5 Contact with authorities	6
	5.6 Contact with special interest groups	6
	5.7 Threat intelligence	6
	5.8 Information security in project management	6
	5.9 Inventory of information and other associated assets	6
	5.10 Acceptable use of information and other associated assets	6
	5.11 Return of assets	6
	5.12 Classification of information	7
	5.13 Labelling of information	7
	5.14 Information transfer	7
	5.15 Access control	7
	5.16 Identity management	7
	5.17 Authentication information	7
	5.18 Access rights	7
	5.19 Information security in supplier relationships	7
	5.20 Addressing information security within supplier agreements	8
	5.21 Managing information security in the ICT supply chain	8
	5.22 Monitoring, review and change management of supplier services	8
	5.23 Information security for use of cloud services	8
	5.24 Information security incident management planning and preparation	8
	5.25 Assessment and decision on information security events	9
	5.26 Response to information security incidents	9
	5.27 Learning from information security incidents	9
	5.28 Collection of evidence	9
	5.29 Information security during disruption	9
	5.30 ICT readiness for business continuity	10
	5.31 Legal, statutory, regulatory and contractual requirements	10
	5.32 Intellectual property rights	10
	5.33 Protection of records	10
	5.34 Privacy and protection of PII	10
	5.35 Independent review of information security	10

Page

5.36 Compliance with policies, rules and standards for information security 10
5.37 Documented operating procedures 10
5.38 TEL – Interconnected telecommunications services 10
5.39 TEL – Security management of telecommunications services delivery 11
5.40 TEL – Response to spam 12
5.41 TEL – Response to DoS/DDoS attacks 12
5.42 TEL – Non-disclosure of communications 13
5.43 TEL – Essential communications 14
5.44 TEL – Legality of emergency actions 15
5.45 TEL – Coordination for information security incident management 15
6 People controls 16
6.1 Screening 16
6.2 Terms and conditions of employment 16
6.3 Information security awareness, education and training 16
6.4 Disciplinary process 16
6.5 Responsibilities after termination or change of employment 16
6.6 Confidentiality or non-disclosure agreements 16
6.7 Remote working 17
6.8 Information security event reporting 17
7 Physical controls 17
7.1 Physical security perimeter 17
7.2 Physical entry 17
7.3 Securing offices, rooms and facilities 17
7.4 Physical security monitoring 17
7.5 Protecting against physical and environmental threats 17
7.6 Working in secure areas 17
7.7 Clear desk and clear screen 17
7.8 Equipment siting and protection 18
7.9 Security of assets off-premises 18
7.10 Storage media 18
7.11 Supporting utilities 18
7.12 Cabling security 18
7.13 Equipment maintenance 18
7.14 Secure disposal or re-use of equipment 18
7.15 TEL – Securing communication centres 18
7.16 TEL – Securing telecommunications equipment room 19
7.17 TEL – Securing physically isolated operation areas 20
7.18 TEL – Equipment sited in other carriers' premises 21
7.19 TEL – Equipment sited in user premises 21
8 Technological controls 22
8.1 User endpoint devices 22
8.2 Privileged access rights 22
8.3 Information access restriction 22
8.4 Access to source code 22
8.5 Secure authentication 22

Page

8.6 Capacity management 22
8.7 Protection against malware 22
8.8 Management of technical vulnerabilities 22
8.9 Configuration management 22
8.10 Information deletion 22
8.11 Data masking 22
8.12 Data leakage prevention 22
8.13 Information backup 22
8.14 Redundancy of information processing facilities 22
8.15 Logging 23
8.16 Monitoring activities 23
8.17 Clock synchronization 23
8.18 Use of privileged utility programs 23
8.19 Installation of software on operational systems 23
8.20 Network security 23
8.21 Security of network services 23
8.22 Segregation of networks 24
8.23 Web filtering 24
8.24 Use of cryptography 24
8.25 Secure development lifecycle 24
8.26 Application security requirements 24
8.27 Secure system architecture and engineering principles 24
8.28 Secure coding 24
8.29 Security testing in development and acceptance 24
8.30 Outsourced development 24
8.31 Separation of development, test and production environments 24
8.32 Change management 24
8.33 Test information 25
8.34 Protection of information systems during audit testing 25
8.35 TEL – Telecommunications carrier identification and authentication by users 25

Annex A Additional guidance for network security 26
A.1 Security measures against network attacks 26
A.2 Network security measures for network congestion 27

Bibliography 28

Introduction

This Recommendation | International Standard provides interpretation guidelines for the implementation and management of information security controls in telecommunications organizations based on ISO/IEC 27002.

Telecommunications organizations provide telecommunications services by facilitating the communications of customers through their infrastructure. In order to provide telecommunications services, telecommunications organizations need to interconnect and/or share their services and facilities and/or use the services and facilities of other telecommunications organizations. Furthermore, the site location, such as radio sites, antenna locations, ground cables and utility provision (power, water), can be accessed not only by the organization's staff, but also by contractors and providers external to the organization.

Therefore, the management of information security in telecommunications organizations is complex, potentially:

- depending on external parties;
- having to cover all areas of network infrastructure, services applications and other facilities;
- including a range of telecommunications technologies (e.g., wired, wireless or broadband);
- supporting a wide range of operational scales, service areas and service types.

In addition to the application of information security controls described in ISO/IEC 27002, telecommunications organizations can implement extra information security controls to ensure confidentiality, integrity, availability and any other information security property of telecommunications in order to manage information security risk in an adequate fashion. The security properties specialized for telecommunications can be described below (in no order of priority).

1) *Confidentiality*

   Protecting confidentiality of information related to telecommunications from unauthorized disclosure. This implies non-disclosure of communications in terms of the existence, the content, the source, the destination and the date and time of communicated information.

   It is critical that telecommunications organizations ensure that the non-disclosure of communications being handled by them is not breached. This includes ensuring that persons engaged in the telecommunications organization maintain the confidentiality of any information regarding others that can have come to be known during their work duties.

   NOTE – The term "secrecy of communications" is used in some countries in the context of "non-disclosure of communications".

2) *Integrity*

   Protecting the integrity of telecommunications information includes controlling the installation and use of telecommunications facilities to ensure the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other method.

3) *Availability*

   Availability of telecommunications information includes ensuring that access to facilities and the medium used for the provision of communication services is authorized, regardless of whether communications is provided by wire, radio or any other method. Typically, telecommunications organizations give priority to essential communications in case of emergencies, managing unavailability of less important communications in compliance with statutory and regulatory requirements.

Audience

The audience of this Recommendation | International Standard consists of telecommunications organizations and those responsible for information security; together with security vendors, auditors, telecommunications terminal vendors and application content providers. This Recommendation | International Standard provides a common set of information security controls based on ISO/IEC 27002, telecommunications sector-specific information security controls and information security management guidelines allowing for the selection and implementation of such controls.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations

1 Scope

The scope of this Recommendation | International Standard is to provide guidelines supporting the implementation of information security controls in telecommunications organizations.

The adoption of this Recommendation | International Standard will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant information security property.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Recommendation | International Standard, the definitions given in ISO/IEC 27000 and the following apply:

3.1.1 co-location: Installation of telecommunications facilities on the premises of other telecommunications carriers.

3.1.2 communication centre: Building where facilities for providing telecommunications business are sited.

3.1.3 essential communications: Communications whose contents are necessary for the prevention of or relief from disasters and for the maintenance of public order in adverse conditions.

3.1.4 non-disclosure of communications: Requirement not to disclose the existence, the content, the source, the destination and the date and time of communicated information.

NOTE – Communication information can include both data in motion and data at rest.

3.1.5 priority call: Telecommunications made by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls.

NOTE – The specific terminals can span different services (voice over Internet protocol (VoIP), public switched telephone network (PSTN) voice, Internet protocol (IP) data traffic, etc.) for wired and wireless networks.

3.1.6 resilience: Ability to absorb and adapt in a changing environment.

3.1.7 telecommunications applications: Applications such as voice over Ip (VoIP) that are utilized by end-users and built upon the network-based services.

3.1.8 telecommunications business: Business to provide telecommunications services in order to meet the demand of others.

3.1.9 telecommunications equipment room: A secure location or room within a general building where equipment for providing telecommunications business are sited.

3.1.10 telecommunications facilities: Machines, equipment, wire and cables, physical buildings or other electrical facilities for the operation of telecommunications.

3.1.11 telecommunications organizations: Business entities who provide telecommunications services in order to meet the demand of others.

3.1.12 telecommunication records: Information concerning the parties in a communication including the metadata such as the time, and duration of the telecommunication that took place but excluding the contents of the communication.

3.1.13 telecommunications services: Communications using telecommunications facilities, or any other means of providing communications either between telecommunications service users or telecommunications service customers.

3.1.14 telecommunications service customer: Person or organization who enters into a contract with telecommunications organizations to be offered telecommunications services by them.

NOTE – A telecommunication service customer is a contractor with telecommunication organization and can be a telecommunication service user.

3.1.15 telecommunications service user: Person or organization who utilizes telecommunications services.

3.1.16 terminal facilities: Telecommunications facilities which are to be connected to one end of telecommunications circuit facilities and part of which is to be installed on the same premises (including the areas regarded as the same premises) or in the same building where any other part thereof is also to be installed.

3.2 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

CIA	Confidentiality, Integrity and Availability
CNI	Critical National Infrastructure
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
HVAC	Heating, Ventilation, and Air Conditioning
IP	Internet Protocol
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Centre
ISMS	Information Security Management System
NMS	Network Management System
OAM&P	Operations, Administration, Maintenance and Provisioning
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
VoIP	Voice over Internet Protocol

4 Overview

4.1 Structure of this Recommendation | International Standard

This Recommendation | International Standard has been structured in a format similar to ISO/IEC 27002:2022. In cases where the information security control, attribute table, purpose, guidance and other information specified in ISO/IEC 27002:2022 are applicable without a need for any additional information, only a reference is provided to ISO/IEC 27002.

The following clauses include telecommunication sector specific information according to the control layout from ISO/IEC 27002:2022.

- Organizational controls (clause 5)
- People controls (clause 6)
- Physical controls (clause 7)
- Technological controls (clause 8)

Annex A provides additional guidance for network security.

4.2 Information security management systems in telecommunications organizations

4.2.1 Goal

Information is critical to every organization. In the case of telecommunications, information consists of data transmitted between any two points in an electronic form as well as metadata of each transmission, e.g., positioning data of sender and receiver. Information in telecommunications organizations includes that information necessary for the organization to operate as well as information associated with telecommunications services. Regardless of how the information is transmitted and whether it is cached or stored during transmission, information should always be appropriately protected.

Telecommunications organizations and their information systems and networks are exposed to information security threats from a wide range of sources, including: wire-tapping; advanced persistent threats; terrorism; espionage; sabotage; vandalism; information leakage; errors; and force majeure events. These security threats can originate from inside or outside the telecommunications organization, resulting in damage to the organization and can also affect their customers.

Once information security is violated, e.g., by wire-tapping the telecommunications lines, the organization can suffer damage. Therefore, it is essential for an organization to ensure its information security by continual improvement of its information security management system (ISMS).

Effective information security is achieved by implementing a suitable set of information security controls based on those described in this Recommendation | International Standard. These controls need to be established, implemented, monitored, reviewed and improved in telecommunications facilities, services and applications. These activities will enable an organization to meet its information security objectives and therefore business objectives.

Telecommunications organizations provide facilities to various user types to process, transmit and store information. This information could be personally identifiable information, or confidential private and business data. In all cases, information should be handled with the correct level of care and attention, and the appropriate levels of protection provided to ensure confidentiality, integrity and availability (CIA), with privacy and sensitivity being paramount.

4.2.2 Telecommunications organizations

"Telecommunications Organizations" has evolved extensively to provide communication infrastructure and/or communication services. The following telecommunication organizations can be identified for providing communication infrastructure and/or services which can be forms of various businesses for telecommunications organizations.

a) Telecommunication organizations providing network facilities and the related services (network facility service providers) – are the owners/providers of network facilities, namely infrastructure such as, cables, towers, satellite earth stations, broadband fibre optic cables, telecommunications lines and exchanges, radiocommunications transmission equipment, mobile communications base stations and broadcasting transmission towers and equipment. These represent the fundamental building blocks of the convergence model upon which network, applications and content services are provided.

b) Telecommunication organizations providing network services (network service providers) – provide the basic connectivity and bandwidth to support a variety of network services. Network services enable connectivity or transport between different networks. A network service provider usually owns/deploys the network facilities or use the network facilities owned by another licensee providing connectivity services (e.g., message communication service).

c) Telecommunication organizations providing applications services (application service providers) – provide particular functions such as voice services, data services, Internet access and electronic commerce. Applications services are essentially the functions or capabilities, which are delivered to end-users. They do not install transmission line equipment by themselves and use the network facilities owned by another licensee providing connectivity services (e.g., ISP service, MVNO service, CDN service).

d) Telecommunication organizations providing content applications (content application service providers) – represent a special subset of applications service providers such as television and radio broadcast services, and services such as online publishing (currently exempt from licensing requirements) and the provisioning of information services.

e) Telecom organizations that provide industry-oriented services (e.g., 5G and 6G solution providers) – provide industry-oriented solutions to the entire business ecosystem. For example, current 5G industry solutions include smart healthcare, smart factories, smart grid, VR gaming, etc. Besides meeting the networking needs of various industries for ultra-high bandwidth, ultra-low latency, reliability, safety, and isolated logical private networks, 5G can also provide self-help purchasing, automatic opening, customized private networks, etc. to accelerate the evolution of these industries.

4.2.3 Information security considerations in telecommunications

The requirement for information security in telecommunications has originated from the different relevant parties as follows:

a) customers/subscribers needing confidence in the network and the services to be provided, including availability of services (especially emergency services) in case of major catastrophes;

b) public authorities demanding security by directives, regulation and legislation, in order to ensure availability of services, fair competition and privacy protection;

c) network operators and service providers themselves needing information security to safeguard their operational and business interests, and to meet their obligations to their customers and the public.

Furthermore, telecommunications organizations should consider the following environmental and operational information security incidents.

a) Telecommunications services are heavily dependent on various interconnected facilities, such as routers, switches, domain name servers, transmission relay systems and a network management system (NMS). Therefore, telecommunications security incidents can occur to various equipment/facilities and the incidents can propagate rapidly through the network into other equipment/facilities.

b) In addition to telecommunications facilities, vulnerabilities in network protocols and topology can result in serious information security incidents. In particular, convergence of wired and wireless networks can impose significant challenges for developing interoperable protocols.

c) A major concern of telecommunications organizations is the possibility of compromised information security that causes interruption of network services. Such compromised security can be extremely costly in terms of customer relations, lost revenue and recovery costs. Deliberate attacks on the availability of the national telecommunications infrastructure can be viewed as a national security concern.

d) Telecommunications management networks and systems are susceptible to hacker penetrations. A common motivation for such penetrations is theft of telecommunications services. Such theft can be engineered in various ways, such as invoking diagnostic functions, manipulating accounting records, altering provisioning databases and eavesdropping on subscriber calls.

e) In addition to external penetrations, carriers are concerned about information security compromises from internal sources, such as incorrect and/or authorized changes to network management databases and configurations on the part of unauthorized personnel. Such occurrences can be accidental or deliberate.

f) Telecommunications services can be disrupted by malware such as worms and viruses attacking end systems or communications infrastructure. DoS/DDoS is a major cause of incidents on communications and can be caused by various methods to interrupt or block communication signals including sending data to one system or network from many hundreds of systems at the same time to overload it (see TEL 5.41).

For the purpose of meeting the information security requirements for telecommunications originating from the different parties and protecting information assets in telecommunications from information security incidents occurring in various telecommunications environments, information security controls with their guidance for telecommunications are indispensable to support the implementation of information security management in telecommunications organizations.

This document should be applicable to the following:

a) telecommunications organizations seeking confidence that the information security requirements of their interested parties (e.g., suppliers, customers, regulators) will be satisfied;

b) telecommunications organizations seeking a business advantage through the implementation of an ISMS;

c) users and suppliers of the information security related products and services for the telecommunications industry;

d) those internal or external parties to the telecommunications organizations who give advice or training on the ISMS appropriate to that organization;

e) those internal or external parties to ensure compliance with trans-border legal and regulatory requirements, and with statutory requirements in all countries of operation or transit.

4.2.4 Information assets to be protected

In order to establish information security management, it is essential for an organization to clarify and identify all organizational information assets. The identification and assessment of information security risks associated with these information assets makes it possible to prioritise and implement controls.

Information assets which telecommunications organizations should protect can be found in clause 5.9.

4.2.5 Establishment of information security management

4.2.5.1 How to establish information security requirements

It is essential for telecommunications organizations to determine their information security requirements. There are three main sources of security requirements as follows.

a) Those derived from assessing information security risks to a telecommunications carrier, taking into account its overall business strategy and objectives. Through information security risk assessment, threats to and vulnerability of information assets are determined, and likelihood of information security incident occurrences is assessed and potential impact as consequence is estimated.

b) The legal, statutory, regulatory, and contractual requirements that telecommunications organizations have to ensure, trans-border legal and regulatory compliance, and the socio-cultural environment. Examples of legislative requirements for telecommunications organizations are non-disclosure of communications (TEL.5.42) and ensuring essential communications (TEL.5.43). Examples of socio-cultural requirements are ensuring the integrity of telecommunications that are transmitted, relayed and received by any means, the availability of wired or wireless telecommunications facilities by authorized persons and not harming other telecommunications facilities.

c) The particular set of principles, objectives and business requirements for information processing that a telecommunications carrier has developed to support its operations.

4.2.5.2 Assessing information security risks

Information security requirements are determined by a methodical assessment of information security risks. Expenditure on information security controls needs to be balanced against the business harm likely to result from information security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing information security controls selected to protect against these risks.

NOTE – Further information on managing information security risks can be found in ISO/IEC 27005.

Information security risk assessment should be repeated periodically and at least annually, to address any changes that can influence the risk assessment results.

4.2.5.3 Selecting information security controls

Once information security requirements and risks have been determined and decisions for the treatment of risks have been made, appropriate information security controls should be selected and implemented to ensure information security risks are reduced to an acceptable level.

This Recommendation | International Standard provides telecommunications-specific guidance and information security controls with guidance, in addition to the information security controls of ISO/IEC 27002, taking account of telecommunications-specific information security requirements. Therefore, telecommunications organizations are recommended to select information security controls from this Recommendation | International Standard and implement them. In addition, new information security controls can be designed to meet specific needs as appropriate.

The selection of information security controls is dependent upon organizational decisions based on the criteria for information security risk acceptance, risk treatment options and the information security risk management approach applied to telecommunications organizations; additionally, the selection should be subject to all relevant national and international legislation and regulations.

5 Organizational controls

5.1 Policies for information security

Control 5.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.2 Information security roles and responsibilities

Control 5.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

When appointing telecommunication engineers and other staff, telecommunication organizations should ensure they also have appropriate knowledge and skills in the area of cybersecurity and information security. Telecom engineers and other staff should also be notified of and formally agree on the assigned roles and responsibilities they have in the context of cybersecurity and information security measures.

Where cryptography is used, there should be specific crypto-custodian roles and personnel in these positions should be properly trained in the management of cryptographic material and the use and protection of cryptographic systems.

5.3 Segregation of duties

Control 5.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.4 Management responsibilities

Control 5.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.5 Contact with authorities

Control 5.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

When telecommunications organizations receive enquiries from law-enforcement agencies or investigative organizations regarding information relating to telecommunications service users, these telecommunications organizations need to confirm that the enquiries have gone through legitimate processes and procedures according to relevant applicable laws and regulations before any information is disclosed.

The applications and infrastructure of telecommunications organizations can be considered part of critical infrastructure and can be essential for the functioning of the community, society and economy as a whole. Operators of such systems and telecommunications organizations should therefore maintain contact with all of the relevant authorities.

5.6 Contact with special interest groups

Control 5.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.7 Threat intelligence

Control 5.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.8 Information security in project management

Control 5.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.9 Inventory of information and other associated assets

Control 5.9, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

When developing and maintaining the inventory of assets, clear responsibilities between the telecommunications facilities of the organization and those of other connected or related organizations (including telecommunications organizations) should be specified and clearly documented.

The list of assets should be comprehensive, covering all telecommunications assets of value including information assets for network facilities, network services and applications.

5.10 Acceptable use of information and other associated assets

Control 5.10, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.11 Return of assets

Control 5.11, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.12 Classification of information

Control 5.12, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

In classifying information, in addition to the general requirements for organizational sensitive and critical information, telecommunications organizations should also take into account the following:

a) situations where information can be subject to legally regulated disclosure requirements;

b) distinction between information relating to essential communications that need to be handled with priority in an emergency or possible emergency and non-essential communications (see TEL.5.43);

c) awareness of the effects of aggregation, where classified or sensitive information can be deduced by searching large amount of data.

5.13 Labelling of information

Control 5.13, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.14 Information transfer

Control 5.14, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.15 Access control

Control 5.15, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should implement role-based access controls, with a limited number of profiles and controlled sets of user access permissions as applicable.

As telecommunication companies are regularly exposed to different suppliers that cannot support the same security features or standards, it is essential to ensure all access is tracked for amendments and timely removal.

Only the authorized users should have access to use the communications services, such as a particular phone number, voicemail or other data services that have been assigned to them.

5.16 Identity management

Control 5.16, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.17 Authentication information

Control 5.17, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.18 Access rights

Control 5.18, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.19 Information security in supplier relationships

Control 5.19, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

If supplier's access to sensitive information (e.g., personally identifiable information and telephone records) is to be granted, telecommunications organizations should:

– ensure that the supplier is capable of adequately protecting that information;

– include handling of such sensitive information in a confidentiality or non-disclosure agreement with the supplier (see 6.6 in ISO/IEC 27002);

– meet all legal and regulatory requirements including trans-border requirements.

5.20 Addressing information security within supplier agreements

Control 5.20, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should consider the following terms for inclusion in the agreement in order to satisfy the identified security requirements:

a) a clear statement regarding protection against damaged or impaired telecommunications service facilities or those of other telecommunications users connected to these facilities in relation to other telecommunications organizations;

b) a clear demarcation of responsibilities between the telecommunications organizations regarding their telecommunication service facilities and those of other organizations.

c) a clear statement regarding the availability and priority requirements especially for emergency/essential services.

5.21 Managing information security in the ICT supply chain

Control 5.21, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Supplier agreements between a telecommunication organization and its customers should include appropriate controls to ensure the non-disclosure of sensitive customer data. For instance, if directory assistance services are provided by third parties, the suppliers' agreements should include requirements concerning disclosure of customer data, such as their telephone numbers or IDs.

When essential communications together with other communications are provided by suppliers, the telecommunications organizations should ensure existing agreements are fulfilled regarding prioritization of essential communications throughout the supply chain.

In cases where components provided by the supply chain are integrated into a telecommunications network, the organization should ensure the integrity and communications functionality of sourced components. Particular attention should be paid to maintenance and "call home" or "trouble reporting" functionalities.

Where services provided by a supplier involve sensitive information, there should be supplier agreements in place. These should include terms prohibiting any sub-contract that allows access to information in scope of the agreement, without prior agreement of the data owner. When it is necessary for a supplier to sub-contract work, telecommunications organizations should ensure that the appropriate levels of protection for that sensitive information have been previously agreed and are maintained throughout the entire supply chain.

5.22 Monitoring, review and change management of supplier services

Control 5.22, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.23 Information security for use of cloud services

Control 5.23, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.24 Information security incident management planning and preparation

Control 5.24, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should define criteria to be used to evaluate if customer-initiated issues constitute an information security incident. If the agreed service level is no longer met by the evaluation, telecommunications organizations should escalate the customer-initiated issues that can affect both customer and employees regarding the operation of existing customer configurations.

Incident response procedures should include criteria and timing requirements for providing information about information security incidents to customers.

All customers should be made fully aware of problem escalation procedures and have the relevant documentation available to them.

For example, customer-initiated issues can be prioritized according to the criteria provided:

a) sensitive customer data such as customer related PII data is compromised;

b) customer site is completely down or is failing to meet service level agreement (SLA) requirements;

c) customer site is being significantly impacted by the outage – one or more systems down or significant packet loss and/or latency;

d) customer service degraded;

e) customer requests.

Telecommunications organizations, responsible for the provision of telecommunications services as an important utility, should establish mechanisms and/or procedures for containing, eradicating and recovering from information security incidents, as well as those for detecting and analysing incidents in telecommunications systems accurately and in a timely manner.

Such mechanisms and/or procedures should include the following:

a) report the incident to the appropriate internal personnel and external organizations, including regulators, emergency services and those involved in critical infrastructure, as required;

b) isolate the telecommunication system, if possible, use of it should be stopped, or if the system is to be examined, it should be disconnected from any telecommunications operation networks before being re-powered;

c) recover from the incident with a confirmation that the affected systems are functioning normally; if necessary, implement additional monitoring to look for future related activity.

Other information for telecommunications

Telecommunications organizations should share information regarding information security incidents with the relevant organizations such as the Telecom Information Sharing and Analysis Centre (Telecom-ISAC).

5.25 Assessment and decision on information security events

Control 5.25, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should consider the impact on customers when classifying security events as incidents.

5.26 Response to information security incidents

Control 5.26, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations, if necessary, should promptly report incidents to the related customers through appropriate communications channels or other forms of communication.

The need to inform customers will depend on the nature of the service provided.

5.27 Learning from information security incidents

Control 5.27, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should establish mechanisms and/or procedures for sharing the lessons learnt and improving the incident management, taking account of the following actions:

a) hold a post-incident meeting with affected stakeholders (can include impacted customer representatives);

b) collect incident data, such as, total hours on involvement and costs, and use it for improvement of the incident management scheme.

5.28 Collection of evidence

Control 5.28, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.29 Information security during disruption

Control 5.29, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.30 ICT readiness for business continuity

Control 5.30, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Plan for graceful degradation of service with priority given to emergency services and the least critical services being degraded or stopped in priority order.

The business continuity plan should contain provisions for maintaining availability of telecommunications services. In developing and implementing the business continuity plan, telecommunications organizations should consider the inclusion of a disaster recovery plan for telecommunications services and ensuring essential communications of telecommunications service customers.

Telecommunications organizations should also consider when to dispatch their staff to telecommunication operating areas for disaster recovery.

5.31 Legal, statutory, regulatory and contractual requirements

Control 5.31, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.32 Intellectual property rights

Control 5.32, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.33 Protection of records

Control 5.33, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.34 Privacy and protection of PII

Control 5.34, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.35 Independent review of information security

Control 5.35, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.36 Compliance with policies, rules and standards for information security

Control 5.36, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.37 Documented operating procedures

Control 5.37, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

In the operating procedures, telecommunications organizations should specify under which criteria and conditions customer-initiated issues require the invocation of incident, emergency or crisis handling procedures.

5.38 TEL – Interconnected telecommunications services

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control

In the provision of interconnected telecommunications services, the telecommunications organizations should specify a well-defined boundary and interface with other telecommunications organizations, so that each organization can be partitioned and isolated in a timely manner in order to evade an identified risk.

Purpose

To ensure secure provision of interconnected telecommunications services.

Guidance

Appropriate controls should be in place to check whether the service of interconnected telecommunications organizations is in normal operation or not.

In order to diagnose problems and take corrective actions, the organizations should have means to isolate the facilities of the organization from those of other organizations and to re-connect to them at the point of interconnection.

The telecommunications organizations should consistently monitor the traffic conditions at the point of interconnection.

Telecommunications organizations should specify in an agreement or a contract that the provision of telecommunications services for the customers can be suspended, whose communications pose a problem for the smooth service provision of the interconnected telecommunications organizations.

5.39 TEL – Security management of telecommunications services delivery

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Telecommunications organizations should set the security level for the various business propositions of telecommunications services provided, announce it to their customers prior to service delivery, and maintain and manage their telecommunications services properly.

Purpose

To ensure proper security management for delivery of telecommunications services.

Guidance

Telecommunications organizations should conduct the following activities for telecommunications service customers:

a) specification of security features, service levels, and management requirements of telecommunications services, and provision of their clear statement;

b) awareness activities to protect communications service users from unsolicited communications, cybercrime, malware and similar.

Telecommunications organizations should also consider the following:

c) implementation of controls compliant with relevant laws and regulations, such as prevention of unauthorized interception and ensuring interconnection with other telecommunications service providers;

d) provision of communications required for special service levels, such as essential communications in emergency situations (see TEL.5.43);

e) implementation of security controls for each service provided like the following;

IP connecting services/Data centre services:

1) controls against unsolicited communications such as email, fax, short message service (SMS) deliveries and automated calls (see TEL.5.40);

2) controls against DoS/DDoS attack (see TEL.5.41);

3) controls for management of technical vulnerabilities (see 8.8 in ISO/IEC 27002);

Telephone services/mobile-phone services:

4) handling of essential communications;

5) ensuring priority calls in an emergency;

6) traffic congestion of telephone calls;

Managed services:

7) utilization of authentication/encryption;

8) deliberate handling of privileged mode;

f) implementation of security controls in order to strictly maintain the following items in the management of information on service delivery:

1) ensuring non-disclosure of communications, including telephone call details;

2) protection of personally identifiable information.

Telecommunications service delivery should include appropriate controls to prevent the display of corruptly modified uniform resource locators (URLs). Upon detection of such an attack, service delivery should be suspended to minimize the impact of the attack and the relevant customer advised.

In order to maintain the telecommunications services provided, telecommunications organizations should apply the following controls:

g) appropriate maintenance of transmission facilities such as transmission cables and prompt repair in emergency situations;

h) appropriate maintenance of switching facilities for telecommunications services, or constant monitoring of their traffic load; changeover to back-up facilities or other routes in order to avoid traffic congestion in emergency situations;

i) methods and procedures to maintain the functions of telecommunications facilities in the case of DoS attacks which can force the switching facilities like routers to process a larger amount of traffic compared with ordinary situations;

j) appropriate management of Internet routing information and control information such as the domain name system (DNS) and the deployment of their security extensions (DNSSEC).

5.40 TEL – Response to spam

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Information_security_event_management	#Governance_and_Ecosystem

Control

Telecommunications organizations should stipulate the policies for responding to spam and implement appropriate controls.

Purpose

To establish and maintain a secure environment in messaging communications (for example, email, SMS).

Guidance

When telecommunications organizations recognize spam from a telecommunications service user's complaint and the relevant spammer is their own customer, telecommunications organizations should request the relevant customer to stop the sending of spam.

In the case of a determined spammer attack, telecommunications organizations should suspend their services to the relevant customer, in order to minimize the impact of the attack.

When spam is sent out from the network of other telecommunications organizations with which telecommunications organizations interconnect its telecommunications facilities, the organization should request the relevant organization to take necessary measures in order to block spam, and the relevant organization should take appropriate actions, responding to such a request.

In order to take effective measures against spam, telecommunications organizations should work in close cooperation with other telecommunications organizations and spam-fighting organizations at home and abroad.

Telecommunications organizations should develop and implement their policies against spam in line with national law and regulations and make them available to the public.

5.41 TEL – Response to DoS/DDoS attacks

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Information_security_event_management	#Defence

Control

Telecommunications organizations should stipulate the policies for responding to DoS/DDoS attacks and implement appropriate controls.

Purpose

To establish and maintain an environment for telecommunications services where DoS/DDoS attacks are minimised.

Guidance

When telecommunications organizations recognize the incidence of DoS/DDoS attacks e.g., detection of abnormal traffic patterns or unstable operation status of telecommunications facilities, telecommunications organizations should take appropriate countermeasures in order to ensure the ongoing stable operation of telecommunications facilities.

Although specific measures required depend upon the type of DoS/DDoS attacks, telecommunications organizations should take account of the following countermeasures:

a) filtering of packets heading for the target site under attack;

b) restriction of communication port used for DoS/DDoS attacks;

c) reduction or suspension of operation of target telecommunications facilities.

When the DoS/DDoS attacker is their own customer, telecommunications organizations should suspend telecommunications services to the relevant customer in order to block DoS/DDoS attacks to telecommunications facilities.

When the DoS/DDoS attack comes from the network of other telecommunications organizations with which telecommunications organizations interconnect its telecommunications facilities, the organization should request the relevant organization to take necessary measures in order to stop DoS/DDoS attacks, and the relevant organization should take appropriate actions to respond to such requests.

In order to take effective measures against DoS/DDoS attacks, telecommunications organizations should work in close cooperation with other telecommunications organizations and anti-cyber terrorism organizations at home and abroad.

5.42 TEL – Non-disclosure of communications

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection	#Governance_and_Ecosystem

Control

Non-disclosure requirements of communications being handled by telecommunications organizations should be defined and maintained throughout confidentiality or non-disclosure of agreement in communicated information.

Purpose

To ensure non-disclosure of communications being handled by telecommunications organizations.

Guidance

To identify requirements for confidentiality or non-disclosure agreements, telecommunications organizations should consider the need to protect against disclosure of:

a) the existence;

b) the content;

c) the source;

d) the destination;

e) the date and time;

in communicated information.

Telecommunications organizations should take account of the following guidelines:

a) maintaining telecommunications facilities properly to ensure non-disclosure of communications;

b) take necessary measures to prevent unintentional disclosure of other communications during normal use at the connection point between equipment and facilities of telecommunications service users and telecommunications carriers;

c) taking necessary measures to prevent unauthorized access, destruction or falsification of records and data of telecommunications service users stored in telecommunications facilities;

d) prohibiting the unauthorized or unlawful utilization by staff of the telecommunications organizations of any information related to customer communication;

e) setting the appropriate retention period of telecommunications data, which is within the time period required for carrying out the purposes for retaining data, and delete them at the end of retention period or at the attainment of the purposes without any delay;

f) prohibiting provision of any secrets in communications to third parties, without legal enforcement or the consent of telecommunications service users themselves;

g) offering the functionality in which telecommunications service users can decide on a case-by-case basis whether they send their caller ID in the provision of caller ID services;

h) prohibiting the provision of caller ID to third parties, without legal enforcement or the consent of telecommunications service users themselves;

i) prohibiting provision of PII in communications to third parties, without legal enforcement or the consent of telecommunications service users themselves;

j) offering telecommunications service customers a choice as to whether to list their telephone numbers or ID related to other services, in the provision of directory assistance services – when users request their numbers to be unlisted, telecommunications organizations should exclude their information from directory assistance services without any delay;

k) when telecommunications organizations are requested to submit information related to telecommunications service users including non-disclosure of communications, they need to confirm that the request from law-enforcement agencies or other investigative bodies has gone through a legitimate procedure in accordance with the applicable national laws and regulations.

5.43 TEL – Essential communications

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Continuity #Legal_and_compliance	#Resilience #Governance_and_Ecosystem

Control

Telecommunications organizations should, when a natural disaster, accident or any other emergency occurs, or at a risk of occurrence thereof, give priority to essential communications whose contents are necessary for the prevention of or relief or recovery from such incidents and for the maintenance of public order.

Purpose

To prioritize important communications for responding to the occurrence of natural disasters, accidents and other emergencies, and to ensure preparedness against their occurrence.

Guidance

Telecommunications organizations should take account of suspending or restricting part of their telecommunications activities implementing graceful failure in order of importance or priority, in order to ensure that essential communications can be carried out by, for example, the following organizations and/or in agreement with national law and regulations:

a) meteorological organizations;

b) flood prevention organizations;

c) fire and rescue service organizations;

d) disaster relief organizations;

e) organizations directly associated with preservation of public order;

f) organizations directly associated with defence;

g) organizations directly associated with maritime safety;

h) organizations directly associated with ensuring transportation;

i) organizations directly associated with communications services;

j) organizations directly associated with electric power supply;

k) organizations directly associated with water supply;

l) organizations directly associated with gas supply;

m) election administration organizations;

n) journalistic organizations;

o) financial institutions;

p) medical institutions;

q) organizations directly associated with the food supply chain;

r) government agencies that provide essential services;

s) other national or local organizations that handle essential communications;

t) any other organizations operating essential communications as defined by national laws, regulations or other requirements.

Telecommunications organizations should, in the case where they interconnect their telecommunications facilities with other telecommunications organizations, take the necessary measures to conclude an agreement for preferential treatment of essential communications in order to ensure their smooth and continuous operation.

5.44 TEL – Legality of emergency actions

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Legal_and_compliance	#Governance_and_Eco system

Control

All measures that telecommunications organizations take in emergency situations should be confined only to those necessary and sufficient measures for legitimate self-defence or emergency evacuation. Such measures should be appropriate and not be excessive.

Purpose

To legally implement necessary measures taken in emergency actions.

Guidance

Telecommunications organizations should institute procedures in advance for contingency, including information security incidents, and get advice and guidance from legal experts whether the defined emergency measures are not excessive and that they are necessary and sufficient for legitimate self-defence or emergency evacuation.

Telecommunications organizations should make aware and advise their telecommunications service customers that they can take the necessary action, such as suspension of telecommunications services to respond to incidents. For example, the connection with telecommunications service customers' facilities interfere with the functioning of telecommunications organizations facilities or other telecommunications service customers' facilities or other building sites and that can have an impact on human security and safety.

5.45 TEL – Coordination for information security incident management

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Legal_and_compliance #Information_security_event_management	#Governance_and_Eco system #Resilience

Control

Telecommunication organization should appropriately conduct information security incident management for coordinating with relevant parties both within and outside the organization.

Purpose

To manage information security incident with appropriate coordination(s).

Guidance

For telecommunications organizations, coordination is an important aspect in information security incident management. Incidents crossing organizational boundaries frequently occur and cannot be easily resolved by a single

telecommunication organization. Especially emerging threats nowadays have a variety of ways or methods of attack and a wider range of impacts. The characteristics of emerging threats and attacks make it more urgent than ever to coordinate incidents across organizations.

Coordination should be carried out with relevant parties both inside and outside of the organization. For example, internal interested parties include representatives from business, administrative, IT and other required departments; external interested parties include cybersecurity specialised organisations, external incident response teams (IRTs), law enforcement and relevant authorities.

6 People controls

6.1 Screening

Control 6.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should consider detailed checks on candidates for job positions that give employees access to sensitive information. This should also apply to positions giving employees access to telecommunications equipment or to communications information as this could provide unrestricted access to data which can become sensitive as a result of aggregation.

NOTE – Any person who is involved with critical national infrastructure (CNI) aspects of communications systems should be subjected to formal screening and criminal records checks before being given access.

6.2 Terms and conditions of employment

Control 6.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

The legal rights and responsibilities of employees regarding non-disclosure of communications and essential communications, which telecommunications organizations should take into account, are included in the laws and regulations.

Telecommunications organizations should clarify and state the responsibilities for maintaining the communications service provided by telecommunications organizations in addition to the protection and non-disclosure of personally identifiable and other confidential information in the terms and conditions of employment.

Telecommunications organizations should make sure that any person engaged in their telecommunications services is aware and up-to date on:

a) their responsibilities for protecting the personally identifiable information and other confidential information of users of their service;

b) their responsibilities concerning the non-disclosure of information confidentiality obtained through their operational activities on telecommunications services.

6.3 Information security awareness, education and training

Control 6.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

6.4 Disciplinary process

Control 6.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

6.5 Responsibilities after termination or change of employment

Control 6.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

6.6 Confidentiality or non-disclosure agreements

Control 6.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

6.7 Remote working

Control 6.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

6.8 Information security event reporting

Control 6.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7 Physical controls

7.1 Physical security perimeter

Control 7.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should consider and implement the following guidelines where appropriate for physical security perimeters:

a) telecommunications operations centres should be equipped with adequate physical intruder detection systems;

b) facilities for telecommunications services, e.g., transmission facilities, switching facilities and telecommunications infrastructure, should be physically separated and sited away from other facilities, e.g., customer facilities in managed data centres;

c) physical barriers should be effectively installed, with all local security policies rigorously enforced to ensure the protection of information and other associated assets at all times; if a physical barrier is malfunctioning or a policy is not followed, it is imperative that the issue be resolved immediately by management with the appropriate level of responsibility.

7.2 Physical entry

Control 7.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should consider the following guidelines:

a) appropriate physical security controls should be applied to all telecommunication operation rooms and control centres;

b) upon entry, relevant visitor data should be recorded and adequately protected from unauthorized disclosure;

c) visitor records should be physically and electronically protected to preserve the CIA of the information they contain.

7.3 Securing offices, rooms and facilities

Control 7.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.4 Physical security monitoring

Control 7.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.5 Protecting against physical and environmental threats

Control 7.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.6 Working in secure areas

Control 7.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.7 Clear desk and clear screen

Control 7.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 2024 apply.

7.8 Equipment siting and protection

Control 7.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

If the systems of several organizations are sited in the same data centre as telecommunications facilities, the telecommunications organizations should implement appropriate measures to protect customers' information stored in their systems. Such systems should have additional security in place, e.g., by being located in a separate secured area.

7.9 Security of assets off-premises

Control 7.9, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.10 Storage media

Control 7.10, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.11 Supporting utilities

Control 7.11, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

In particular, power supply facilities in isolated areas, such as mobile base stations, should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries can be augmented with a private electric generator, especially in isolated areas.

As for the associated requirements for fuel reserves, the following should be considered.

a) adequate and usable fuel should always be available for emergency power generators;

b) fuel for emergency power generators should be stored in a location and in a manner that minimises the risk in case of fire or natural disaster affecting the communications facility.

Any equipment room should have adequate heating, ventilation and air conditioning (HVAC) services to ensure external environmental conditions do not result in equipment operating outside manufacturers' guidelines.

7.12 Cabling security

Control 7.12, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Cabling should be implemented to ensure that wire-tapping and eavesdropping devices or any alteration to the cabling can be detected either using active means or regular audits of access points.

7.13 Equipment maintenance

Control 7.13, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.14 Secure disposal or re-use of equipment

Control 7.14, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.15 TEL – Securing communication centres

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Physical security of communication centres, where telecommunications facilities such as switching facilities for providing telecommunications business are housed, should be designed, developed and implemented.

Purpose

To protect communication centres from any physical hazards and to prevent unauthorized physical access and damage of communication centres.

Guidance

To protect telecommunications facilities such as switching facilities for providing telecommunications business (hereafter referred to as communication centres), the following should take place:

a) communication centres should be on level ground away from causes of vibration or natural hazards such as land movement;

b) communication centres should be well above the water table and any flood plains;

c) communication centres should be clear of man-made hazards such as chemical plants;

d) a site whose environment is least susceptible to damage from the environment should be selected for communication centres – where a site is chosen that is vulnerable to environmental damage, appropriate measures should be taken against known hazards including: natural disasters [see g)] and temperature extremes;

e) a site whose environment is least susceptible to damage from strong electromagnetic fields should be selected for communication centres – where a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect telecommunications equipment rooms with electromagnetic shields;

f) communication centres should not be located at sites adjacent to facilities used for storing dangerous articles that pose a danger of explosion or combustion;

g) communication centre buildings should be designed to minimize the impact of natural disasters and/or events including:

- earthquakes;
- fires;
- lightning;
- floods;
- water leakage.

h) communication centre buildings should have adequate structural stability to meet the necessary floor load;

i) automatic fire alarms should be installed in communication centres;

j) HVAC controls should be deployed to ensure that all communications equipment is operated within manufacturers' guidelines.

7.16 TEL – Securing telecommunications equipment room

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_managment	#Protection

Control

Physical security of equipment rooms, where telecommunications facilities are set for providing telecommunications business, should be designed, developed and implemented.

Purpose

To ensure provision of secure telecommunications equipment rooms.

Guidance

All telecommunications equipment rooms and facilities should be subject to the application of appropriate physical and environmental security controls, such as use of access control systems, CCTV, alarm systems, as well as protection against fire and adverse environmental conditions.

To protect a room in which facilities are located for providing telecommunications services (hereafter referred to as telecommunications equipment room), the following guidance should be considered:

a) the telecommunications equipment room should be located where it is least susceptible to external effects, such as natural disasters;

b) the telecommunications equipment room should be located where it is least susceptible to intrusion by unauthorized personnel – adequate measures should be taken to prevent such intrusions;

c) the telecommunications equipment room should be located where it is least susceptible to flooding – if the room needs to be located where it is susceptible to flooding, then necessary measures should be taken such as raising the floor level, installing a water blockade and installing special water drainage facilities;

d) the telecommunications equipment room should be located where it is least susceptible to damage from strong electromagnetic fields – if the room needs to be located where it is susceptible to strong electromagnetic fields, it should be protected by electromagnetic shields or some other measures – especially, if power supply facilities are installed within the telecommunications equipment room, measures should be appropriately taken to prevent interference from electromagnetic fields;

e) important facilities should be placed in an exclusive telecommunications equipment room with appropriate physical protection;

f) measures should be taken to prevent the materials used for the floor, walls, ceiling etc. from collapsing and falling, e.g., due to earthquakes of a normally predictable magnitude;

g) materials used for the floor, walls, ceiling etc. should be non-combustible or fire-resistant;

h) measures should be taken to deal with static electricity;

i) ducts connecting telecommunications equipment rooms should be designed to slow down or prevent the spread of fire;

j) fire suppression systems should be fit for use in equipment rooms such as clean agent and inert gas systems designed to slow down or prevent the spread of fire;

k) if necessary, measures should be taken to protect the data storage room and data safe from electromagnetic interference;

l) fire-proofing measures should be taken for the data storage room and dedicated data warehouses, as needed;

m) automatic fire alarms should be installed in the telecommunications equipment room and the air-conditioning facility room;

n) fire extinguishers should be installed in the telecommunications equipment room and the air-conditioning facility room;

o) the telecommunications equipment room should be air conditioned;

p) air-conditioning of telecommunications equipment room housing important facilities should be provided by a separate system from that for offices and other rooms;

q) HVAC controls should be connected to an uninterruptable power supply to ensure loss of power does not impact the operating environment.

7.17 TEL – Securing physically isolated operation areas

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

For physically isolated operating areas, where telecommunications facilities are located for providing telecommunications business, physical security controls should be designed, developed and implemented.

Purpose

To ensure provision of secure physically isolated operation areas.

Guidance

To protect physically isolated operating areas (e.g., mobile base stations) in which telecommunications facilities are located for providing telecommunications business (hereafter referred to as isolated operating areas), the following controls should be considered:

a) isolated operating areas should be earthquake-proof to meet the mandated national or regional standards;

b) isolated operating areas should be equipped with automatic fire control equipment;

c) isolated operating areas should be monitored by a remote office for the purpose of detecting facility failures, power failures, fire, humidity and temperature etc.;

d) physically secure perimeters should be provided in a proper manner, e.g., using secure fencing to cover the isolated operating area; since it is normally operated in an unmanned way, it should be equipped with an automatic alert function to the operation centre in the event of an incident.

7.18 TEL – Equipment sited in other carriers' premises

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_managment	#Protection

Control

When telecommunications organizations install equipment outside their own premises, the equipment should be sited in a protected area.

Purpose

To ensure secure provision of equipment sited in other carrier locations.

Guidance

To protect the equipment of one telecommunications organization sited in the premises of another, the following controls should be considered:

a) the boundary and interface with the other telecommunications organization should be specified, and the equipment should be easily isolated from that of the other organization, if required;

b) an agreement for the supply of support utilities should be made with the other telecommunications organization;

c) management should confirm that the location where the equipment is to be installed is appropriate in order to ensure the desired level of security.

Other information

In order to make the security level of the other organization's premises consistent with that of the telecommunications organization's own premises, an agreement and rules for achieving the desired level of security with other telecommunications organizations should be checked beforehand.

7.19 TEL – Equipment sited in user premises

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_managment	#Protection

Control

When telecommunications organizations install equipment within the telecommunications service customer premises in order to connect with the customer equipment, the organizations' equipment should be protected.

Purpose

To ensure secure provision of equipment sited in user locations.

Guidance

To protect equipment located at a telecommunications service customer site, the following controls should be considered:

a) the equipment, such as cabinet, installed at the customer site should be sturdy, and be adequately protected against unauthorized access;

b) modification or attempted modification of equipment should be detectable;

c) the boundary and interface with the customer should be specified, and the equipment should be easily isolated from the customer, if required;

d) it should be possible to remotely monitor the status of the equipment or to operate the equipment.

8 Technological controls

8.1 User endpoint devices

Control 8.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.2 Privileged access rights

Control 8.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.3 Information access restriction

Control 8.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.4 Access to source code

Control 8.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.5 Secure authentication

Control 8.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.6 Capacity management

Control 8.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.7 Protection against malware

Control 8.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.8 Management of technical vulnerabilities

Control 8.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.9 Configuration management

Control 8.9, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.10 Information deletion

Control 8.10, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.11 Data masking

Control 8.11, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.12 Data leakage prevention

Control 8.12, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.13 Information backup

Control 8.13, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.14 Redundancy of information processing facilities

Control 8.14, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications facilities for providing essential communications and supporting critical infrastructure (see 5.43 TEL) should have sufficient redundancies to ensure that a loss of availability does not impact the provision of the service.

8.15 Logging

Control 8.15, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should set the appropriate retention time period for retaining telecommunications data (e.g., accounting, billing, attending to complaints, as well as protection from abuse and lawful access by the authorities) and to delete the data at the end of the retention period or at the attainment of the purposes without any delay. This should be done in accordance with any applicable business, legal and regulatory requirements.

8.16 Monitoring activities

Control 8.16, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.17 Clock synchronization

Control 8.17, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.18 Use of privileged utility programs

Control 8.18, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.19 Installation of software on operational systems

Control 8.19, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should minimize the risk of corruption to operational systems by considering the following guidelines to control changes:

a) changes to critical systems' applications or operating system software should be fully tested and procedures for rolling back such an upgrade should be included;

b) if application software is sensitive, then at least three generations of software should be retained;

c) regression test of any updates, patches and changes on a test system, and ensure they operate correctly before they are implemented in an operational environment.

For sensitive systems such as network elements or operations systems, only verified and permitted software should be installed.

Only authorized maintenance personnel should be able to install software on sensitive systems. This restriction should also be applied on the terminals used to administer the sensitive systems.

Software that can adversely affect sensitive systems performance and/or security should be controlled and monitored.

8.20 Network security

Control 8.20, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.21 Security of network services

Control 8.21, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

For telecommunications organizations, securing the services that are provided to the users of the network includes the following:

a) securing the operations, administration, maintenance and provisioning (OAM&P) as well as configuration of network services;

b) securing the control and signalling information used by the network service (e.g., the session initiation protocol (SIP) for VoIP service);

c) securing the end user data and voice as it uses the network service (e.g., VoIP traffic).

8.22 Segregation of networks

Control 8.22, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Specific attention should be paid to adequate segregation of production and management networks.

Hosted customer networks and associated data require adequate segregation from other parts of operational networks and other data.

8.23 Web filtering

Control 8.23, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.24 Use of cryptography

Control 8.24, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.25 Secure development lifecycle

Control 8.25, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.26 Application security requirements

Control 8.26, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.27 Secure system architecture and engineering principles

Control 8.27, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.28 Secure coding

Control 8.28, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.29 Security testing in development and acceptance

Control 8.29, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.30 Outsourced development

Control 8.30, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.31 Separation of development, test and production environments

Control 8.31, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

In telecommunications organizations, the content of the data used in test and development environments should be adequate to test the system and service in a real telecommunications context.

Development staff should only have access to operational passwords or other authentication tokens where controls are in place for temporary authorization used for the support of operational systems. Controls should ensure that such authorizations are revoked or authentication tokens are changed after use.

8.32 Change management

Control 8.32, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for telecommunications

Telecommunications organizations should consider the procedures and records for installation, relocation and removal of facilities.

Changes to infrastructure, including both physical and logical modifications, should be subject to a change management process. When applicable, this process should seek approval from a designated risk owner. Output from the change process, including risk assessments, should be subject to regular security audits.

8.33 Test information

Control 8.33, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.34 Protection of information systems during audit testing

Control 8.34, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.35 TEL – Telecommunications carrier identification and authentication by users

Control type	Information security properties	Cybersecurity Concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Identity_and_access_ management	#Governance_and_Eco system

Control

Telecommunications organizations should provide adequate controls for users to be able to identify and authenticate telecommunications organizations.

Purpose

To ensure users of telecommunications services are connecting to the correct provider of those services and to prevent unauthorized access to telecommunication services.

Guidance

Where telecommunications services are used by remote users or via mobile links, such use is subject to the possibility of breach of confidentiality. This could be caused by a person impersonating a legitimate user of the service or malware compromising the service. Therefore, appropriate controls should be in place for telecommunications users to mutually authenticate their communications with telecommunications organizations.

If telecommunications users cannot authenticate telecommunications organizations, the telecommunications organizations should remind users that the authentication function is unavailable together with the generally incurred possible risks.

Other information

There are several alternatives utilizing encryption technology for identification and authentication.

One of the possible threats if users cannot correctly identify and authenticate telecommunications organizations is man-in-the-middle attacks.

Annex A

Additional guidance for network security

(This annex does not form an integral part of this Recommendation | International Standard.)

A.1 Security measures against network attacks

A.1.1 Protection against network attack

a) Protection of network facilities

Telecommunications facilities should be appropriately protected in order to avoid significant interference to telecommunications services delivery caused by unexpected behaviour that is provoked by telecommunications service users or telecommunications facilities of other organizations. For example, such unintended behaviour could be caused by malwares.

In order to protect IP network facilities, such as servers and routers, from attacks (e.g., DDoS attack), telecommunications organizations should have mechanisms to filter communications or limit communication bands in IP addresses, communication ports and application protocols. Depending on telecommunications services, such mechanisms of communications filters should be implemented associated with signal processing control, user authentication and access controls.

b) Measures against source impersonation

Telecommunications organizations should implement measures to protect against impersonation of IP addresses (IP spoofing).

In order to prevent source impersonation by means of a stepping stone, appropriate security controls against unauthorized access should be implemented at the systems providing user authentication by introducing strict password controls and/or strong authentication functions, e.g., mandatory use of unpredictable passwords above a certain length, and introduction of one-time-password and strong token authentication.

Telecommunications facilities dealing with essential communications should implement mechanisms to prevent source (caller) ID impersonation. For example, it is recommended that terminals based on hard-coding ID or mechanisms to verify caller ID in telecommunications network facilities by using a registered password at the time of registration and connection request be introduced.

c) Measures against malformed communication signal

Telecommunications organizations should implement measures to protect against malformed communication signals (e.g., illegally long packet).

For example, since malformed packets (that are often produced by network attacks) can cause IP network facilities failure, telecommunication organizations should drop such packets in order to protect telecommunications service or facilities.

A.1.2 Drawing attention of users

a) Drawing the attention of telecommunications services users

In order to deter attacks from telecommunications service users' PCs infected with malwares or associated with deliberate malicious actions of users, or to promptly and properly respond to network attacks, telecommunications organizations should clearly specify in the terms and conditions of service delivery that the use of telecommunications services can be restricted in the case where telecommunications facilities are overloaded.

Telecommunications organizations should draw the attention of telecommunications service users to such threats (e.g., viruses and botnets) that can lead to network attacks and encourage them to take the necessary measures by themselves.

NOTE – The term "botnet" is generally used to refer to a group of compromised computers (called zombie computers) running programs, usually referred to as worms, Trojan horses or backdoors, under a common command and control infrastructure. A botnet's originator ("bot herder") can control the group remotely, usually through means, such as internet relay chat (IRC), and usually for nefarious purposes.

A.2 Network security measures for network congestion

A.2.1 Gathering information

a) Collection in advance of information that can cause congestion

Operating rules to collect information concerning disaster and planned events that can cause network congestion should be stipulated by telecommunications organizations, e.g., the establishment of a framework to collect weather information and planned events information. Mechanisms and procedures to report the collected information should be set up, and the information should keep relevant personnel informed.

b) Advance gathering of information that can trigger malfunction

Since disaster, accidents and social phenomena tend to be the cause of telecommunications facilities failures and network congestions, telecommunications organizations should consider measures in advance by gathering the relevant information and accumulating the know-how on a regular basis.

A.2.2 Measures against network congestion

a) Mechanisms of detecting and restricting network congestion

Telecommunications facilities should have mechanisms to detect network congestion and avoid concentration of communications in case of network congestion.

Telecommunications systems dealing with essential communications should have performance resilience to ensure that congestion control processes such as filtering do not adversely affect the provision of those essential services.

Telecommunications organizations should recognize the performance limits of the relevant communication facilities and implement mechanisms to control a number of communications requests before reaching the limits. Furthermore, traffic should be processed by distributed facilities, if possible.

b) Measures to improve temporary throughput

Taking account of the scale of potential disruption and disaster, the use of distributed processing centres and implementation of supplementary facilities, as well as adaptive configuration changes, should be considered, where necessary.

Bibliography

[1] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection– Information security management systems – Requirements*.

[2] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection – Information security controls*.

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

[4] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[5] ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security*.

[6] ISO/IEC 27033-3:2010, *Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues*.

[7] ISO/IEC 27033-4:2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

[8] ISO/IEC 27033-5:2013, *Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*.

[9] ISO/IEC 27035-1:2023, *Information technology – Information security incident management – Part 1: Principles and process*.

[10] ISO/IEC 27035-2:2023, *Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*.

[11] ISO/IEC 27036-1:2021, *Cybersecurity – Supplier relationships – Part 1: Overview and concepts*.

[12] ISO/IEC 27036-2:2022, *Cybersecurity – Supplier relationships – Part 2: Requirements*.

[13] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.

[14] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*.

ICS 35.030
Price based on 28 pages

iso.org