DIN EN ISO/IEC 27011

ICS 03.100.70; 35.030 Einsprüche bis 2020-05-27

Entwurf

Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen (ISO/IEC 27011:2016); Englische Fassung prEN ISO/IEC 27011:2020

Information technology –
Security techniques –
Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations (ISO/IEC 27011:2016);
English version prEN ISO/IEC 27011:2020

Technologies de l'information –
Techniques de sécurité –
Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications (ISO/IEC 27011:2016);
Version anglaise prEN ISO/IEC 27011:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-03-27 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 43 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

Nationales Vorwort

Der Text von ISO/IEC 27011:2016 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27011:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieses Dokument enthält unter Berücksichtigung des Präsidialbeschlusses 1/2004 nur die englische Originalfassung von ISO/IEC 27011:2016.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

Nationaler Anhang NA
(informativ)

Begriffe

Reihenfolge und Inhalt der folgenden Begriffe sind identisch mit denen in Abschnitt Begriffe der englischen Fassung.

3 Begriffe und Abkürzungen

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

— IEC Electropedia: verfügbar unter http://www.electropedia.org/

3.1 Begriffe

Für die Anwendung dieser Empfehlung/Internationalen Norm gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

3.1.1
Colocation
Installation von Telekommunikationseinrichtungen in den Räumlichkeiten anderer Telekommunikationsunternehmen

3.1.2
Kommunikationszentrum
Gebäude, in dem sich Einrichtungen für die Bereitstellung von Telekommunikationsgeschäften befinden

3.1.3
wesentliche Nachricht
Nachricht, deren Inhalte zur Verhinderung oder Beseitigung von Katastrophen und zur Aufrechterhaltung der öffentlichen Ordnung unter widrigen Umständen erforderlich ist

3.1.4
Geheimhaltung/Vertraulichkeit von Nachrichten
Anforderung, die Existenz, den Inhalt, die Quelle, das Ziel sowie das Datum und die Uhrzeit der übermittelten Informationen nicht offenzulegen

3.1.5
Blitzgespräch
Telekommunikation über bestimmte Endgeräte in Notfällen, die vorrangig durch Einschränkung öffentlicher Anrufe behandelt werden sollte

ANMERKUNG Die spezifischen Endgeräte können verschiedene Dienstleistungen (Voice over Internet Protocol, VoIP), PSTN (Public Switched Telephone Network)-Sprache, Internet Protocol (IP)-Datenverkehr usw.) für drahtgebundene und drahtlose Netzwerke umfassen

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

3.1.6
Telekommunikationsanwendungen
Anwendungen wie Voice over IP (VoIP), die von Endbenutzern verwendet werden und auf netzwerkbasierten Dienstleistungen beruhen

3.1.7
Telekommunikationsgeschäft
Unternehmen, das Telekommunikationsdienstleistungen erbringt, um der Nachfrage anderer gerecht zu werden

3.1.8
Telekommunikationsgeräteraum
sicherer Ort oder Raum innerhalb eines allgemeinen Gebäudes, an dem sich Geräte für die Bereitstellung von Telekommunikationsgeschäften befinden

3.1.9
Telekommunikationseinrichtungen
Maschinen, Ausrüstungen, Drähte und Leitungen, physische Gebäude oder andere elektrische Einrichtungen für den Betrieb der Telekommunikation

3.1.10
Telekommunikationsorganisationen
Unternehmen, das Telekommunikationsdienstleistungen erbringt, um der Nachfrage anderer gerecht zu werden

3.1.11
Telekommunikationsaufzeichnungen
Informationen zu den an einer Kommunikation beteiligten Parteien mit Ausnahme des Kommunikationsinhalts sowie des Zeitpunkts und der Dauer der erfolgten Telekommunikation

3.1.12
Telekommunikationsdienst
Kommunikation über Telekommunikationseinrichtungen oder andere Kommunikationsmittel entweder zwischen Nutzern oder Kunden von Telekommunikationsdienstleistungen

3.1.13
Kommunikationsdienstleistungskunde
Person oder Organisation, die einen Vertrag mit Telekommunikationsorganisationen abschließt, von denen Telekommunikationsdienste anzubieten sind

3.1.14
Kommunikationsdienstleistungsanwender
Person oder Organisation, die Telekommunikationsdienstleistungen nutzt

3.1.15
Anschlussanlagen
Telekommunikationsanlagen, die an ein Ende von Telekommunikationsleitungsanlagen anzuschließen sind und von denen sich ein Teil auf demselben Gelände (einschließlich der als dasselbe Gelände betrachteten Bereiche) oder in demselben Gebäude befindet, in dem auch ein anderer Teil davon zu installieren ist

3.1.16
Anwender
Person oder Organisation, die informationsverarbeitende Einrichtungen oder Systeme nutzt, z. B. Mitarbeiter, Auftragnehmer oder Anwender von dritten Parteien

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

3.2 Abkürzungen

Für die Anwendung dieser Empfehlung/Internationalen Norm gelten die folgenden Begriffe:

CIA	Vertraulichkeit, Integrität und Verfügbarkeit (en: Confidentiality, Integrity and Availability)
CNI	kritische nationale Infrastruktur (en: Critical National Infrastructure)
DDoS	verteilter Überlastangriff (en: Distributed Denial of Service)
DNS	Domain Name System
DoS	Überlastangriff (en: Denial of Service)
HVAC	Heizung, Lüftung und Klimatisierung (en: Heating, Ventilation, and Air Conditioning)
IP	Internet-Protokoll (en: Internet Protocol)
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Centre
ISMS	Informationssicherheitsmanagementsystem (en: Information Security Management System)
NMS	Managementsystem von Netzwerken (en: Network Management System)
OAM&P	Betrieb, Verwaltung, Wartung und Zuteilung (en: Operations, Administration, Maintenance and Provisioning)
PSTN	öffentliches Fernsprechwählnetz (en: Public Switched Telephone Network)
SIP	Sitzungseinleitungsprotokoll (en: Session Initiation Protocol)
SLA	Service Level Agreement
SMS	Kurzmitteilungsdienst (en: Short Message Service)
SOA	Erklärung zur Anwendbarkeit (en: Statement of Applicability)
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

Nationaler Anhang NB
(informativ)

Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

Foreword

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

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

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

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

This second edition cancels and replaces firs edition of ISO/IEC 27011:2008 which has been technically revised.

ISO/IEC 27011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27*, IT Security techniques,* in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.1051.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

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	Information security policies	5
6	Organization of information security	5
	6.1 Internal organization	5
	6.2 Mobile devices and teleworking	6
7	Human resource security	6
	7.1 Prior to employment	6
	7.2 During employment	7
	7.3 Termination or change of employment	7
8	Asset management	7
	8.1 Responsibility for assets	7
	8.2 Information classification	8
	8.3 Media handling	8
9	Access control	8
	9.1 Business requirement for access control	8
	9.2 User access management	9
	9.3 User responsibilities	9
	9.4 System and application access control	9
10	Cryptography	9
11	Physical and environmental security	9
	11.1 Secure areas	9
	11.2 Equipment	10
12	Operations security	12
	12.1 Operational procedures and responsibilities	12
	12.2 Protection from malware	13
	12.3 Backup	13
	12.4 Logging and monitoring	13
	12.5 Control of operational software	13
	12.6 Technical vulnerability management	14
	12.7 Information systems audit considerations	14
13	Communications security	14
	13.1 Network security management	14
	13.2 Information transfer	15
14	System acquisition, development and maintenance	16
	14.1 Security requirements of information systems	16
	14.2 Security in development and support processes	16
	14.3 Test data	16
15	Supplier relationships	16
	15.1 Information security in supplier relationships	16
	15.2 Supplier service delivery management	17
16	Information security incident management	17
	16.1 Management of information security incidents and improvements	17
17	Information security aspects of business continuity management	19

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

Page

17.1 Information security continuity 19
17.2 Redundancies 20
18 Compliance 20
Annex A – Telecommunications extended control set 21
Annex B – Additional guidance for network security 29
B.1 Security measures against network attacks 29
B.2 Network security measures for network congestion 30
Bibliography 31

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27011:2020-05

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), may 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 security objectives and controls described in ISO/IEC 27002, telecommunications organizations may need to implement extra controls to ensure confidentiality, integrity, availability and any other security property of telecommunications in order to manage security risk in an adequate fashion.

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 by the telecommunications organization maintain the confidentiality of any information regarding others that may 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 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 general security control objectives based on ISO/IEC 27002, telecommunications sector-specific controls and information security management guidelines allowing for the selection and implementation of such controls.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27011:2020-05

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

1 Scope

The scope of this Recommendation | International Standard is to define 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 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.*
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

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.

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 may 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 **telecommunications applications**: Applications such as Voice over IP (VoIP) that are consumed by end-users and built upon the network based services.

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

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

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27011:2020-05