

DIN EN ISO/IEC 27011

ICS 03.100.70; 35.030

**Informationstechnik –
Sicherheitsverfahren –
Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von
ISO/IEC 27002 für Telekommunikationsorganisationen
(ISO/IEC 27011:2016);
Deutsche Fassung EN 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);
German version EN 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 allemande EN ISO/IEC 27011:2020

Gesamtumfang 54 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

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 EN 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).

Für die in diesem Dokument zitierten 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

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (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*

Deutsche Fassung

Informationstechnik —
Sicherheitsverfahren —
Leitfaden für Informationssicherheitsmaßnahmen
auf Grundlage von ISO/IEC 27002 für Telekommunikations-
organisationen (ISO/IEC 27011:2016)

Information technology —
Security techniques —
Code of practice for Information security controls based
on ISO/IEC 27002 for telecommunications organizations
(ISO/IEC 27011:2016)

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)

Diese Europäische Norm wurde vom CEN am 3. Mai 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort.....	5
Vorwort	6
Einleitung.....	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe und Abkürzungen	9
3.1 Begriffe	9
3.2 Abkürzungen	11
4 Übersicht.....	12
4.1 Aufbau dieser Empfehlung Internationalen Norm.....	12
4.2 Informationssicherheits-Managementsysteme in Telekommunikationsorganisationen	12
4.2.1 Ziel.....	12
4.2.2 Sicherheitsbetrachtungen in der Telekommunikation.....	13
4.2.3 Zu schützende Informationswerte	14
4.2.4 Einrichtung des Informationssicherheitsmanagements.....	15
5 Informationssicherheitsrichtlinien	16
6 Organisation der Informationssicherheit.....	16
6.1 Interne Organisation	16
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten	16
6.1.2 Aufgabentrennung.....	16
6.1.3 Kontakt mit Behörden	16
6.1.4 Kontakt mit speziellen Interessensgruppen.....	17
6.1.5 Informationssicherheit im Projektmanagement.....	17
6.2 Mobilgeräte und Telearbeit.....	17
7 Personalsicherheit	17
7.1 Vor der Beschäftigung.....	17
7.1.1 Sicherheitsüberprüfung.....	17
7.1.2 Beschäftigungs- und Vertragsbedingungen.....	18
7.2 Während der Beschäftigung	18
7.3 Beendigung oder Änderung der Beschäftigung.....	18
8 Verwaltung der Werte.....	19
8.1 Verantwortlichkeit für Werte	19
8.1.1 Inventarisierung der Werte.....	19
8.1.2 Zuständigkeit für Werte.....	19
8.1.3 Zulässiger Gebrauch von Werten.....	19
8.1.4 Rückgabe von Werten	19
8.2 Informationsklassifizierung	19
8.2.1 Leitlinien für die Klassifizierung	19
8.2.2 Kennzeichnung von Information	20
8.2.3 Handhabung von Werten.....	20
8.3 Handhabung von Datenträgern.....	20
9 Zugangssteuerung.....	20

9.1	Geschäftsanforderungen an die Zugangsteuerung.....	20
9.1.1	Zugangssteuerungsrichtlinie.....	20
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten.....	21
9.2	Benutzerzugangsverwaltung	21
9.3	Benutzerverantwortlichkeiten	21
9.4	Zugangssteuerung für Systeme und Anwendungen.....	21
10	Kryptographie	21
11	Physische und umgebungsbezogene Sicherheit.....	21
11.1	Sicherheitsbereiche.....	21
11.1.1	Physische Sicherheitsperimeter.....	21
11.1.2	Physische Zutrittssteuerung.....	22
11.1.3	Sichern von Büros, Räumen und Einrichtungen.....	22
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen.....	22
11.1.5	Arbeiten in Sicherheitsbereichen.....	23
11.1.6	Anlieferungs- und Ladebereiche.....	23
11.2	Geräte und Betriebsmittel.....	23
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln.....	23
11.2.2	Versorgungseinrichtungen.....	23
11.2.3	Sicherheit der Verkabelung.....	24
11.2.4	Instandhaltung von Geräten und Betriebsmitteln.....	24
11.2.5	Entfernen von Werten	24
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten.....	24
11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln.....	24
11.2.8	Unbeaufsichtigte Benutzergeräte.....	24
11.2.9	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	24
12	Betriebssicherheit.....	25
12.1	Betriebsabläufe und -verantwortlichkeiten.....	25
12.1.1	Dokumentierte Betriebsabläufe.....	25
12.1.2	Änderungssteuerung.....	25
12.1.3	Kapazitätssteuerung.....	25
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....	26
12.2	Schutz vor Schadsoftware	26
12.3	Datensicherung.....	26
12.4	Protokollierung und Überwachung.....	26
12.4.1	Ereignisprotokollierung	26
12.4.2	Schutz der Protokollinformation.....	27
12.4.3	Administratoren- und Bedienerprotokolle	27
12.4.4	Uhrensynchronisation.....	27
12.5	Steuerung von Software im Betrieb.....	27
12.5.1	Installation von Software auf Systemen im Betrieb	27
12.6	Handhabung technischer Schwachstellen.....	28
12.6.1	Handhabung von technischen Schwachstellen.....	28
12.6.2	Einschränkungen von Softwareinstallation	28
12.7	Audits von Informationssystemen.....	28
13	Kommunikationssicherheit.....	28
13.1	Netzwerksicherheitsmanagement.....	28
13.1.1	Netzwerksteuerungsmaßnahmen.....	28
13.1.2	Sicherheit von Netzwerkdiensten	29
13.1.3	Trennung in Netzwerken.....	29
13.2	Informationsübertragung.....	30
13.2.1	Richtlinien und Verfahren für die Informationsübertragung.....	30
13.2.2	Vereinbarungen zur Informationsübertragung.....	30
13.2.3	Elektronische Nachrichtenübermittlung.....	30

13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	30
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	30
14.1	Sicherheitsanforderungen an Informationssysteme	30
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	30
14.3	Testdaten	30
15	Lieferantenbeziehungen	30
15.1	Informationssicherheit in Lieferantenbeziehungen	30
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	30
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	31
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	31
15.2	Steuerung der Dienstleistungserbringung von Lieferanten	32
16	Handhabung von Informationssicherheitsvorfällen	32
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	32
16.1.1	Verantwortlichkeiten und Verfahren	32
16.1.2	Meldung von Informationssicherheitsereignissen	33
16.1.3	Meldung von Schwächen in der Sicherheit	33
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	34
16.1.5	Reaktion auf Informationssicherheitsvorfälle	34
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	34
16.1.7	Sammeln von Beweismaterial	35
17	Informationssicherheitsaspekte beim Business Continuity Management	35
17.1	Aufrechterhalten der Informationssicherheit	35
17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit	35
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit	35
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	36
17.2	Redundanzen	36
17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	36
18	Compliance	36
Anhang A (normativ)	Telekommunikationsspezifischer Maßnahmenkatalog	37
TEL.9	Zugangssteuerung	37
TEL.9.5	Steuerung des Netzwerkzugangs	37
TEL.11	Physische und umgebungsbezogene Sicherheit	38
TEL.11.1	Sicherheitsbereiche	38
TEL.11.3	Sicherheit im Verantwortungsbereich von Dritten	41
TEL.13	Kommunikationssicherheit	42
TEL.13.1	Netzwerksicherheitsmanagement	42
TEL.18	Compliance	45
TEL.18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	45
Anhang B (informativ)	Weitere Leitlinien für die Netzwerksicherheit	49
B.1	Sicherheitsmaßnahmen zum Schutz vor Netzwerkangriffen	49
B.1.1	Schutz vor Netzwerkangriffen	49
B.1.2	Anwender informieren	50
B.2	Netzwerksicherheitsmaßnahmen zum Schutz vor Netzwerküberlastung	50
B.2.1	Sammeln von Informationen	50
B.2.2	Maßnahmen gegen Netzwerküberlastungen	50
Literaturhinweise		52

Europäisches 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 EN ISO/IEC 27011:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2020, und etwaige entgegenstehende nationale Normen müssen bis November 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27011:2016 wurde von CEN als EN ISO/IEC 27011:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe der gemeinsamen Technischen Komitees besteht in dem Erarbeiten von Internationalen Normen. Die von den gemeinsamen Technischen Komitees angenommenen Norm-Entwürfe werden den Mitgliedsorganisationen zur Umfrage zur Verfügung gestellt. Für eine Veröffentlichung als Internationale Norm wird eine Zustimmung von mindestens 75 % der Mitgliedsländer, die abgestimmt haben, benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27011:2008), die technisch überarbeitet wurde.

ISO/IEC 27011 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*, in Zusammenarbeit mit ITU-T erarbeitet. Der identische Text wird veröffentlicht als Rec. ITU-T X.1051

Einleitung

Diese Empfehlung | Internationale Norm bietet in Anlehnung an ISO/IEC 27002 Interpretationsrichtlinien für die Umsetzung und das Management von Informationssicherheitsmaßnahmen für Telekommunikationsorganisationen.

Telekommunikationsorganisationen bieten Telekommunikationsdienste an, indem sie Kunden die Kommunikation über ihre Infrastruktur ermöglichen. Um Telekommunikationsdienste anbieten zu können, müssen Telekommunikationsorganisationen ihre Dienste und Einrichtungen vernetzen und/oder freigeben und/oder die Dienste und Einrichtungen anderer Telekommunikationsorganisationen nutzen. Darüber hinaus haben nicht nur die Mitarbeiter der Organisation, sondern auch externe Auftragnehmer und Anbieter Zugriff auf die Standorte, wie z. B. Funkstandorte, Antennenstandorte, Erdkabel und Versorgungseinrichtungen (Strom, Wasser).

Daher ist das Informationssicherheitsmanagement in Telekommunikationsorganisationen komplex und potentiell von Folgendem geprägt:

- Abhängigkeit von externen Parteien;
- Notwendigkeit der Abdeckung aller Bereiche der Netzwerkinfrastruktur, Serviceanwendungen und weiterer Einrichtungen;
- Abdeckung mehrerer Telekommunikationstechnologien (z. B. kabelgebunden, drahtlos oder Breitband);
- Unterstützung eines breiten Spektrums an Dienstleistungsumfängen, -bereichen und -typen.

Zusätzlich zur Anwendung der in ISO/IEC 27002 beschriebenen Sicherheitsziele und -maßnahmen müssen Telekommunikationsorganisationen möglicherweise zusätzliche Maßnahmen implementieren, um die Vertraulichkeit, Integrität, Verfügbarkeit und andere Sicherheitseigenschaften der Telekommunikation zu gewährleisten und das Sicherheitsrisiko in angemessener Weise zu verwalten.

1) Vertraulichkeit

Schutz der Vertraulichkeit von Informationen vor unberechtigter Offenlegung bei der Telekommunikation. Dies schließt die Geheimhaltung der Kommunikation in Bezug auf das Vorhandensein, den Inhalt, die Quelle, das Ziel sowie das Datum und die Uhrzeit der übermittelten Informationen ein.

Es ist von entscheidender Bedeutung, dass Telekommunikationsorganisationen Geheimhaltungsverstöße im Zusammenhang mit der von ihnen gehandhabten Kommunikation verhindern. Dazu gehört auch, dass die von der Telekommunikationsorganisation beauftragten Personen die Vertraulichkeit von Informationen Dritter wahren, von denen sie während ihrer Arbeitstätigkeit Kenntnis erlangt haben.

ANMERKUNG Im Zusammenhang mit der „Geheimhaltung von Kommunikation“ wird in einigen Ländern der Begriff „Kommunikationsgeheimnis“ verwendet.

2) Integrität

Der Schutz der Integrität von Telekommunikationsinformationen umfasst die Kontrolle der Installation und Nutzung von Telekommunikationseinrichtungen, um die Authentizität, Genauigkeit und Vollständigkeit von Informationen zu gewährleisten, die per Kabel, Funk oder auf anderem Wege übertragen, weitergeleitet oder empfangen werden.

3) Verfügbarkeit

Die Verfügbarkeit von Telekommunikationsinformationen umfasst die Sicherstellung, dass der Zugang zu Einrichtungen und zu dem für die Bereitstellung von Kommunikationsdiensten genutzten Medium autorisiert ist, unabhängig davon, ob die Kommunikation über Kabel, Funk oder auf anderem Wege erfolgt. Typischerweise geben Telekommunikationsorganisationen in Notfällen der kritischen Kommunikation die höchste Priorität und verwalten die Nichtverfügbarkeit weniger wichtiger Kommunikation in Übereinstimmung mit den gesetzlichen Bestimmungen.

Zielgruppe

Diese Empfehlung | Internationale Norm richtet sich an Telekommunikationsorganisationen sowie an Verantwortliche für die Informationssicherheit, einschließlich Sicherheitsdienstleister, Auditoren, Anbieter von Telekommunikationsendgeräten und Anbieter von Anwendungsinhalten. Diese Empfehlung | Internationale Norm beschreibt in Anlehnung an ISO/IEC 27002 eine Reihe allgemeiner Ziele von Sicherheitsmaßnahmen sowie für den Telekommunikationssektor spezifische Maßnahmen und liefert Leitlinien für das Informationssicherheitsmanagement, um Anwender zur Auswahl und Umsetzung solcher Maßnahmen zu befähigen.

1 Anwendungsbereich

Diese Empfehlung | Internationale Norm legt Leitlinien fest, welche die Umsetzung von Informationssicherheitsmaßnahmen für Telekommunikationsorganisationen unterstützen.

Durch die Anwendung dieser Empfehlung | Internationalen Norm können Telekommunikationsorganisationen Mindestanforderungen an das Informationssicherheitsmanagement hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie weiterer relevanter Sicherheitseigenschaften erfüllen.

2 Normative Verweisungen

Die folgenden Empfehlungen | Internationalen Normen enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil der vorliegenden Empfehlung | Internationalen Norm sind. Zum Zeitpunkt der Veröffentlichung dieser Empfehlung | Internationalen Norm waren die angegebenen Ausgaben aktuell. Alle Empfehlungen und Normen unterliegen der Überarbeitung. Vertragspartner, deren Vereinbarungen auf dieser Empfehlung | Internationalen Norm basieren, werden gebeten, die Möglichkeit zu prüfen, ob die jeweils neuesten Ausgaben der im folgenden genannten Empfehlungen und Normen angewendet werden können. Die Mitglieder von IEC und ISO führen Verzeichnisse der gegenwärtig gültigen Internationalen Normen. Der Standardisierungs-Sektor der Internationalen Fernmeldeunion (ITU-T) führt ein Verzeichnis der aktuell gültigen ITU-T-Empfehlungen.

- 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 Begriffe und Abkürzungen

3.1 Begriffe

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

3.1.1

Co-Lokation

Installation von Telekommunikationseinrichtungen auf den Liegenschaften anderer Telekommunikationsanbieter

3.1.2

Kommunikationszentrale

Gebäude, in dem Einrichtungen für das Telekommunikationsgeschäft untergebracht sind

3.1.3

kritische Kommunikation

Kommunikation, deren Inhalt für die Vermeidung von oder die Abhilfe gegen Katastrophen und für die Aufrechterhaltung der öffentlichen Ordnung unter widrigen Umständen erforderlich ist

3.1.4

Geheimhaltung von Kommunikation

Anforderung, das Vorhandensein, den Inhalt, die Quelle, das Ziel sowie das Datum und die Uhrzeit der übermittelten Informationen nicht offenzulegen

3.1.5

priorisierte Kommunikation

Telekommunikation von bestimmten Endgeräten bei Notfällen, die durch Einschränkung öffentlicher Anrufe vorrangig behandelt werden sollten

Anmerkung 1 zum Begriff: Die spezifischen Endgeräte können verschiedene Dienste (Sprache über Internetprotokoll (VoIP, en: voice over Internet protocol), Sprache über das öffentliche Telefonnetz (PSTN, en: public switched telephone network), Datenverkehr über Internetprotokoll usw.) für drahtgebundene und drahtlose Netzwerke umfassen.

3.1.6

Telekommunikationsanwendung

Anwendung wie Sprache über Internetprotokoll (VoIP, en: voice over Internet protocol), die von Endanwendern genutzt wird und auf den netzbasierten Diensten aufbaut

3.1.7

Telekommunikationsgeschäft

Geschäft der Bereitstellung von Telekommunikationsdienstleistungen, um die Nachfrage anderer zu decken

3.1.8

Raum für Telekommunikationsbetriebsmittel

sicherer Ort oder Raum innerhalb eines allgemeinen Gebäudes, in dem Ausrüstung für die Bereitstellung von Telekommunikationsdienstleistungen untergebracht ist

3.1.9

Telekommunikationseinrichtung

Maschine, Betriebsmittel, elektrische Leitung und Kabel, physisches Gebäude oder andere elektrische Einrichtung für den Betrieb der Telekommunikation

3.1.10

Telekommunikationsorganisation

Geschäftseinheit, die Telekommunikationsdienstleistungen bereitstellt, um die Nachfrage anderer zu decken

3.1.11

Telekommunikationsaufzeichnung

Informationen über die an einer Kommunikation beteiligten Parteien mit Ausnahme des Inhalts der Kommunikation sowie des Zeitpunkts und der Dauer der stattgefundenen Telekommunikation

3.1.12

Telekommunikationsdienstleistung

Kommunikation unter Verwendung von Telekommunikationseinrichtungen oder einem anderen Kommunikationsmittel zwischen Anwendern von Telekommunikationsdienstleistungen oder Kunden von Telekommunikationsdienstleistungen

3.1.13

Kunde von Telekommunikationsdienstleistungen

Person oder Organisation, die einen Vertrag mit Telekommunikationsorganisationen abschließt, um von diesen Telekommunikationsdienstleistungen angeboten zu bekommen

3.1.14

Anwender von Telekommunikationsdienstleistungen

Person oder Organisation, die Telekommunikationsdienstleistungen verwendet

3.1.15

Endstelleneinrichtung

Telekommunikationseinrichtung, die an einem Ende der einer Telekommunikationsschaltung angeschlossen wird und von der ein Teil auf derselben Liegenschaft (einschließlich der Bereiche, die als dieselbe Liegenschaft gelten) oder in demselben Gebäude installiert wird, in dem auch jeglicher anderer Teil davon installiert wird

3.1.16

Anwender

Person oder Organisation, die Einrichtungen oder Systeme zur Informationsverarbeitung nutzt, z. B. Mitarbeiter, Auftragnehmer oder Drittanwender

3.2 Abkürzungen

Für die Anwendung dieser Empfehlung | Internationalen Norm gelten die folgenden Abkürzungen:

CIA	Confidentiality, Integrity and Availability (Vertraulichkeit, Integrität und Verfügbarkeit)
CNI	Critical National Infrastructure (kritische nationale Infrastruktur)
DDoS	Distributed Denial of Service (dezentrale Dienstverweigerung)
DNS	Domain Name System (Domännennamensystem)
DoS	Denial of Service (Dienstverweigerung)
HLK	Heizung, Lüftung, Klimatechnik
IP	Internet Protocol (Internetprotokoll)
IRC	Internet Relay Chat (Gespräch über Internet-Relaisstationen)
ISAC	Information Sharing and Analysis Centre (Informationsaustausch- und Analysezentrum)
ISMS	Informationssicherheits-Managementsystem
NMS	Netzwerk-Managementsystem
OAM&P	Operations, Administration, Maintenance and Provisioning (Betrieb, Administration, Wartung und Bereitstellung)
PSTN	Public Switched Telephone Network (öffentliches Telefonnetz)
SIP	Session Initiation Protocol (Sitzungsaufbauprotokoll)
SLA	Service Level Agreement (Dienstgütevereinbarung)
SMS	Short Message Service (Kurznachrichtendienst)
SOA	Statement of Applicability (Erklärung zur Anwendbarkeit)
URL	Uniform Resource Locator (einheitlicher Ressourcenzeiger)
VoIP	Voice over Internet Protocol (Sprache über Internetprotokoll)

4 Übersicht

4.1 Aufbau dieser Empfehlung | Internationalen Norm

Diese Empfehlung | Internationale Norm ist ähnlich wie die Norm ISO/IEC 27002 aufgebaut. Wenn die in ISO/IEC 27002 festgelegten Ziele und Maßnahmen gültig sind, ohne dass zusätzliche Informationen erforderlich sind, wird lediglich auf ISO/IEC 27002 verwiesen. Für den Telekommunikationssektor spezifische Leitlinien für Maßnahmen und die Umsetzung sind im normativen Anhang A beschrieben.

Wenn für Maßnahmen zusätzliche für den Telekommunikationssektor spezifische Leitlinien erforderlich sind, wird die Maßnahme zunächst unverändert nach ISO/IEC 27002 angegeben, gefolgt von den Telekommunikationsspezifischen Leitlinien zu dieser Maßnahme. Für den Telekommunikationssektor spezifische Leitlinien und Informationen sind in den folgenden Abschnitten enthalten:

- Organisation der Informationssicherheit (Abschnitt 6)
- Personalsicherheit (Abschnitt 7)
- Verwaltung der Werte (Abschnitt 8)
- Zugangssteuerung (Abschnitt 9)
- Physische und umgebungsbezogene Sicherheit (Abschnitt 11)
- Betriebssicherheit (Abschnitt 12)
- Kommunikationssicherheit (Abschnitt 13)
- Anschaffung, Entwicklung und Instandhaltung von Systemen (Abschnitt 14)
- Lieferantenbeziehungen (Abschnitt 15)
- Handhabung von Informationssicherheitsvorfällen (Abschnitt 16)
- Informationssicherheitsaspekte beim Business Continuity Management (Abschnitt 17)

4.2 Informationssicherheits-Managementsysteme in Telekommunikationsorganisationen

4.2.1 Ziel

Informationen sind für jede Organisation von entscheidender Bedeutung. Bei der Telekommunikation bestehen Informationen aus Daten, die in einer elektronischen Anordnung zwischen zwei beliebigen Punkten übertragen werden, sowie aus Metadaten für jede Übertragung, z. B. Positionsdaten von Sender und Empfänger. Unabhängig davon, wie die Informationen übertragen werden und ob sie während der Übertragung zwischengespeichert oder gespeichert werden, sollten Informationen immer angemessen geschützt werden.

Telekommunikationsorganisationen und ihre Informationssysteme und -netzwerke sind Sicherheitsbedrohungen aus einer Vielzahl von Quellen ausgesetzt, z. B. Abhören, fortgeschrittene andauernde Bedrohung, Terrorismus, Spionage, Sabotage, Vandalismus, Informationslecks, Fehler und Ereignisse höherer Gewalt. Diese Sicherheitsbedrohungen können von innerhalb oder außerhalb der Telekommunikationsorganisation ausgehen und der Organisation schaden.

Sobald die Informationssicherheit verletzt wird, z. B. durch Abhören der Telekommunikationsleitungen, kann die Organisation Schaden nehmen. Daher ist es für eine Organisation unerlässlich, ihre Informationssicherheit

durch die kontinuierliche Verbesserung ihres Informationssicherheits-Managementsystems (ISMS) zu gewährleisten.

Eine effektive Informationssicherheit wird durch die Umsetzung einer Reihe geeigneter Sicherheitsmaßnahmen erreicht, die auf den in dieser Empfehlung | Internationalen Norm beschriebenen Maßnahmen beruhen. Diese Sicherheitsmaßnahmen müssen in Telekommunikationseinrichtungen, -dienstleistungen und -anwendungen eingeführt, verwirklicht, überwacht, überprüft und verbessert werden. Diese Aktivitäten ermöglichen es einer Organisation, ihre Sicherheitsziele und damit ihre Geschäftsziele zu erreichen.

Telekommunikationsorganisationen stellen verschiedenen Anwendertypen Einrichtungen zur Verarbeitung, Übertragung und Speicherung von Informationen bereit. Bei diesen Informationen könnte es sich um personenbezogene Informationen oder um vertrauliche private und geschäftliche Daten handeln. In allen Fällen sollten die Informationen mit dem richtigen Maß an Sorgfalt und Aufmerksamkeit behandelt werden, und es sollte ein angemessener Schutz bereitgestellt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit (CIA, en: confidentiality, integrity and availability) zu gewährleisten, wobei Datenschutz und Sensibilität an erster Stelle stehen.

4.2.2 Sicherheitsbetrachtungen in der Telekommunikation

Die Forderung nach einem generischen Sicherheitsframework in der Telekommunikation hat ihren Ursprung in verschiedenen Quellen:

- a) Kunden/Anschlussinhaber, die Vertrauen in das Netz und die zu erbringenden Dienstleistungen benötigen, einschließlich der Verfügbarkeit von Dienstleistungen (insbesondere Notdiensten) im Falle größerer Katastrophen;
- b) Behörden, die Sicherheit in Form von Richtlinien, Vorschriften und Gesetzen einfordern, um die Verfügbarkeit von Dienstleistungen, einen fairen Wettbewerb und den Schutz der Privatsphäre zu gewährleisten;
- c) Netzbetreiber und Dienstanbieter selbst, die Sicherheit benötigen, um ihre betrieblichen und geschäftlichen Interessen zu wahren und ihre Verpflichtungen gegenüber ihren Kunden und der Öffentlichkeit zu erfüllen.

Darüber hinaus sollten Telekommunikationsorganisationen die folgenden umweltbedingten und operativen Sicherheitsvorfälle berücksichtigen.

- a) Telekommunikationsdienstleistungen sind in hohem Maße von verschiedenen untereinander verbundenen Einrichtungen abhängig, z. B. von Routern, Switches, Domänennamenservern, Übertragungsvermittlungssystemen und einem Netzwerk-Managementsystem (NMS). Daher können Sicherheitsvorfälle in der Telekommunikation verschiedene Betriebsmittel/Einrichtungen betreffen, und die Vorfälle können sich über das Netzwerk schnell auf andere Betriebsmittel/Einrichtungen ausbreiten.
- b) Zusätzlich zu den Telekommunikationseinrichtungen können Schwachstellen in Netzwerkprotokollen und in der Netzwerktopologie zu schwerwiegenden Sicherheitsvorfällen führen. Insbesondere die Konvergenz von drahtgebundenen und drahtlosen Netzwerken kann bei der Entwicklung von interoperablen Protokollen eine erhebliche Herausforderung darstellen.
- c) Ein besonderes Augenmerk von Telekommunikationsorganisationen liegt auf dem Potential, dass Sicherheitslücken zu Netzausfällen führen. Solche Ausfallzeiten können in Bezug auf Kundenbeziehungen, Einnahmehausfälle und Wiederherstellungskosten extrem kostspielig sein. Vorsätzliche Angriffe auf die Verfügbarkeit der nationalen Telekommunikationsinfrastruktur können als ein nationales Sicherheitsrisiko angesehen werden.

- d) Netzwerke und Systeme für das Telekommunikationsmanagement sind anfällig für Eindringversuche von Hackern. Ein häufiges Motiv für solche Eindringversuche ist der Diebstahl von Telekommunikationsdienstleistungen. Ein solcher Diebstahl kann auf verschiedene Weise erfolgen, z. B. durch das Aufrufen von Diagnosefunktionen, das Manipulieren von Abrechnungsdatensätzen, das Verändern von Bereitstellungsdatenbanken und das Abhören von Teilnehmeranrufen.
- e) Neben dem Eindringen von außen haben die Netzbetreiber auch Sicherheitsbeeinträchtigungen durch interne Quellen im Blick, z. B. ungültige Änderungen an Netzwerkverwaltungsdatenbanken und -konfigurationen durch nicht autorisiertes Personal. Solche Vorkommnisse können versehentlich oder absichtlich erfolgen.
- f) Telekommunikationsdienstleistungen können durch Schadsoftware wie Würmer und Viren gestört werden, die Endsysteme oder die Kommunikationsinfrastruktur angreifen. DoS-/DDoS-Angriffe sind eine der Hauptursachen für Vorfälle in der Kommunikation und können Verfahren umfassen, bei denen Kommunikationssignale unterbrochen oder blockiert oder Daten von vielen hundert Systemen gleichzeitig an ein System oder Netzwerk gesendet werden, um es zu überlasten (siehe TEL 13.1.6 in Anhang A).

Zum Schutz von Informationswerten in der Telekommunikation, die aus unterschiedlichen Quellen in verschiedenen Telekommunikationsumgebungen stammen, sind Sicherheitsrichtlinien für die Telekommunikation unabdingbar, um die Implementierung des Informationssicherheitsmanagements in Telekommunikationsorganisationen zu unterstützen.

Die Sicherheitsrichtlinien sollten für folgende Instanzen und Zwecke gelten:

- a) Telekommunikationsorganisationen, die darauf vertrauen wollen, dass die Informationssicherheitsanforderungen aller Beteiligten (z. B. Lieferanten, Kunden, Regulierungsbehörden) erfüllt werden;
- b) Telekommunikationsorganisationen, die sich mit der Implementierung eines ISMS einen Geschäftsvorteil verschaffen möchten;
- c) Anwender und Lieferanten der mit der Informationssicherheit im Zusammenhang stehenden Produkte und Dienstleistungen für die Telekommunikationsbranche;
- d) Personen innerhalb oder außerhalb der Telekommunikationsorganisation, die das ISMS auf Konformität mit den Anforderungen nach ISO/IEC 27001 beurteilen und auditieren;
- e) Personen innerhalb oder außerhalb der Telekommunikationsorganisation, die Beratung oder Schulungen zum ISMS für die jeweilige Organisation durchführen;
- f) die Sicherstellung der Einhaltung grenzüberschreitender und landesinterner gesetzlicher und behördlicher Anforderungen in allen Ländern, in denen die Organisation tätig ist oder die als Transitländer dienen.

4.2.3 Zu schützende Informationswerte

Um ein Informationssicherheitsmanagement einzurichten, ist es für eine Organisation unerlässlich, alle Werte der Organisation zu klären und zu bestimmen. Die Klärung der Attribute und der Bedeutung der Werte ermöglicht es, geeignete Maßnahmen zu implementieren.

Informationswerte, die Telekommunikationsorganisationen schützen sollten, sind in Abschnitt 8.1.1 enthalten.

4.2.4 Einrichtung des Informationssicherheitsmanagements

4.2.4.1 Bestimmung der Sicherheitsanforderungen

Für Telekommunikationsorganisationen ist es unerlässlich, ihre Sicherheitsanforderungen zu bestimmen. Es gibt die folgenden drei Hauptarten von Sicherheitsanforderungen:

- a) Sicherheitsanforderungen, die aus der Risikobeurteilung für einen Telekommunikationsanbieter unter Berücksichtigung seiner gesamten Geschäftsstrategie und -ziele abgeleitet werden. Bei der Risikobeurteilung werden die Bedrohungen für Werte bestimmt, die Anfälligkeit für das Auftreten sowie die Wahrscheinlichkeit des Auftretens werden evaluiert, und die potentiellen Auswirkungen werden abgeschätzt.
- b) Die gesetzlichen, behördlichen und vertraglichen Anforderungen, die Telekommunikationsorganisationen erfüllen müssen, einschließlich Anforderungen zur grenzüberschreitenden Einhaltung von gesetzlichen und behördlichen Bestimmungen und zur Berücksichtigung des soziokulturellen Umfelds. Beispiele für gesetzliche Anforderungen an Telekommunikationsorganisationen sind die Geheimhaltung der Kommunikation (TEL.18.1.6, Anhang A) und die Sicherstellung der kritischen Kommunikation (TEL.18.1.7, Anhang A). Beispiele für soziokulturelle Anforderungen sind die Sicherstellung der Integrität der Telekommunikation, unabhängig davon, mit welchen Mitteln sie übertragen, weitergeleitet und empfangen wird, sowie die Verfügbarkeit von drahtgebundenen oder drahtlosen Telekommunikationseinrichtungen durch autorisierte Personen und die Nicht-beeinträchtigung anderer Telekommunikationseinrichtungen.
- c) Die spezifischen Grundsätze, Ziele und Geschäftsanforderungen für die Informationsverarbeitung, die ein Telekommunikationsanbieter zur Unterstützung seines Betriebs entwickelt hat.

4.2.4.2 Beurteilung von Sicherheitsrisiken

Die Sicherheitsanforderungen werden durch eine systematische Beurteilung der Sicherheitsrisiken ermittelt. Die Kosten für Maßnahmen müssen gegen den geschäftlichen Schaden abgewogen werden, der durch Sicherheitsmängel entstehen kann. Die Ergebnisse der Risikobeurteilung helfen dabei, das geeignete Management der Informationssicherheitsrisiken und die damit verbundenen Prioritäten zu bestimmen sowie die zum Schutz vor diesen Risiken ausgewählten Maßnahmen zu implementieren.

Die Risikobeurteilung sollte in regelmäßigen Abständen, mindestens jedoch jährlich, wiederholt werden, um alle Änderungen zu berücksichtigen, die die Ergebnisse der Risikobeurteilung beeinflussen könnten.

4.2.4.3 Auswahl von Maßnahmen

Nachdem die Sicherheitsanforderungen und -risiken bestimmt und Entscheidungen für die Behandlung der Risiken getroffen wurden, sollten geeignete Maßnahmen ausgewählt und implementiert werden, um die Risiken auf ein annehmbares Niveau zu mindern.

Diese Empfehlung | Internationale Norm bietet zusätzliche Leitlinien und, zusätzlich zum allgemeinen Informationssicherheitsmanagement, telekommunikationsspezifische Maßnahmen unter Berücksichtigung der telekommunikationsspezifischen Anforderungen. Daher wird Telekommunikationsorganisationen empfohlen, Maßnahmen aus dieser Empfehlung | Internationalen Norm auszuwählen und zu implementieren. Darüber hinaus können nach Bedarf neue Maßnahmen entwickelt werden, um spezifische Anforderungen zu erfüllen.

Die Auswahl der Sicherheitsmaßnahmen ist abhängig von organisatorischen Entscheidungen, denen die Kriterien für Risikoakzeptanz, Risikobehandlungsmöglichkeiten und die allgemeine Haltung der Telekommunikationsorganisation bezüglich des Risikomanagements zugrunde liegen. Die Auswahl sollte zudem alle relevanten nationalen und internationalen Gesetze und Vorschriften berücksichtigen.