

DIN ISO/IEC 27009



ICS 35.030

Entwurf

Einsprüche bis 2021-11-17
Vorgesehen als Ersatz für
DIN ISO/IEC 27009:2016-11

**Informationstechnik – IT-Sicherheitsverfahren –
Sektorspezifische Anwendung der ISO/IEC 27001 –
Anforderungen (ISO/IEC 27009:2020);
Text Deutsch und Englisch**

Information security, cybersecurity and privacy protection –
Sector-specific application of ISO/IEC 27001 –
Requirements (ISO/IEC 27009:2020);
Text in German and English

Sécurité de l'information, cybersécurité et protection des données personnelles –
Application de l'ISO/IEC 27001 à un secteur spécifique –
Exigences (ISO/IEC 27009:2020);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-09-17 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 Am DIN-Platz, Burggrafenstr. 6, 10787 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 48 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
Vorwort	5
1 Anwendungsbereich.....	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Übersicht zu dieser Internationalen Norm	7
4.1 Allgemeines	7
4.2 Aufbau dieser Internationalen Norm.....	8
4.3 Erweiterung von Anforderungen nach ISO/IEC 27001 oder Maßnahmen nach ISO/IEC 27002.....	9
5 Ergänzende, verfeinerte oder interpretierte Anforderungen nach ISO/IEC 27001	9
5.1 Allgemeines	9
5.2 Ergänzende Anforderungen zur ISO/IEC 27001	9
5.3 Verfeinerte Anforderungen der ISO/IEC 27001.....	9
5.4 Interpretierte Anforderungen der ISO/IEC 27001.....	10
6 Ergänzende oder geänderte Anleitung nach ISO/IEC 27002.....	10
6.1 Allgemeines	10
6.2 Ergänzende Anleitung.....	10
6.3 Geänderte Anleitung.....	11
Anhang A (normativ) Vorlage für die Erarbeitung sektorspezifischer Normen mit Bezug zu ISO/IEC 27001 und optional ISO/IEC 27002	12
Anhang B (normativ) Vorlage für die Erarbeitung sektorspezifischer Normen mit Bezug zu ISO/IEC 27002.....	16
Anhang C (informativ) Erklärung der Vor- und Nachteile der innerhalb von Anhang B verwandten Nummerierungsansätze.....	25
Literaturhinweise.....	27

Nationales Vorwort

Das internationale Dokument ISO/IEC 27009:2020 ist in der deutschen Sprachfassung unverändert in diesen Norm-Entwurf übernommen worden. Fachlich zuständig ist für diese deutsche Norm der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss „Informationstechnik und Anwendungen“ (NIA).

Die dieser Norm zugrundeliegende Internationale Norm ISO/IEC 27009:2020 wurde von ISO/IEC JTC 1 „ISO/IEC Gemeinschaftskomitee für Informationstechnik“ erarbeitet, dessen Sekretariat von ANSI (USA) gehalten wird. Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27018	siehe	DIN EN ISO/IEC 27018
ISO/IEC 27019	siehe	DIN EN ISO/IEC 27019

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

Änderungen

Gegenüber DIN ISO 27009:2016-11 wurden folgende Änderungen vorgenommen:

- a) der Anwendungsbereich wurde angepasst um den Inhalt des Dokumentes deutlicher herauszustellen;
- b) Anhang A wurde aufgeteilt in Anhang A und Anhang B;
- c) Anhang C wurde hinzugefügt;
- d) redaktionelle Überarbeitung der Norm.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

DIN EN ISO/IEC 27018, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung*

DIN EN ISO/IEC 27019, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmaßnahmen für die Energieversorgung*

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.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

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. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27009:2016), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- der Anwendungsbereich wurde angepasst um den Inhalt des Dokumentes deutlicher herauszustellen;
- Anhang A wurde aufgeteilt in Anhang A und Anhang B;
- Anhang C wurde hinzugefügt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

1 Anwendungsbereich

Dieses Dokument legt die Anforderungen zur Erstellung von sektorspezifischen Standards fest, die ISO/IEC 27001 erweitern und ISO/IEC 27002 vervollständigen oder ergänzen, um einen spezifischen Sektor (Bereich, Fachgebiet oder Marktsektor) zu unterstützen.

Dieses Dokument erläutert, wie:

- ergänzende Anforderungen zu den in ISO/IEC 27001 enthaltenen aufgenommen;
- Anforderungen nach ISO/IEC 27001 verfeinert oder interpretiert;
- Maßnahmen in Ergänzung zu ISO/IEC 27001:2013, Anhang A, und ISO/IEC 27002 einbezogen;
- Maßnahmen von ISO/IEC 27001:2013, Anhang A, und ISO/IEC 27002 verändert;
- Anleitungen hinzugefügt oder Anleitung aus ISO/IEC 27002 verändert

werden müssen.

Dieses Dokument legt fest, dass ergänzende oder verfeinerte Anforderungen nicht im Widerspruch zu den Anforderungen nach ISO/IEC 27001 stehen.

Dieses Dokument ist für all diejenigen anwendbar, die sektorspezifische Normen erarbeiten.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

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

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

3.1

Interpretation

Erklärung einer Anforderung nach ISO/IEC 27001 in einem sektorspezifischen Kontext, die keine der Anforderungen nach ISO/IEC 27001 außer Kraft setzt

Anmerkung 1 zum Begriff: Diese Erklärung kann entweder eine Anforderung oder eine Anleitung betreffen.

3.2

Verfeinerung

Ergänzung oder Anpassung einer Anforderung nach ISO/IEC 27001 in einem sektorspezifischen Kontext, die keine der Anforderungen nach ISO/IEC 27001 beseitigt oder außer Kraft setzt

4 Übersicht zu dieser Internationalen Norm

4.1 Allgemeines

ISO/IEC 27001 definiert die Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems. Sie enthält die Aussage, dass die in ihr festgelegten Anforderungen allgemein gehalten sind und auf alle Organisationen, ungeachtet ihrer Art, Größe oder Natur, anwendbar sein sollen.

ISO/IEC 27001:2013, Anhang A, stellt Maßnahmenziele und Maßnahmen bereit. ISO/IEC 27001 fordert von einer Organisation, „alle Maßnahmen, die zur Umsetzung der gewählte(n) Option(en) für die Informationssicherheitsrisikobehandlung erforderlich sind, festzulegen [siehe 6.1.3 b)]“ und „die nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in [ISO/IEC 27001:2013] Anhang A zu vergleichen und zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden“ [siehe 6.1.3 c)].

Die Maßnahmenziele und Maßnahmen nach ISO/IEC 27001:2013, Anhang A sind in ISO/IEC 27002 enthalten.

ISO/IEC 27002 stellt Leitfäden für Informationssicherheitsmanagementpraktiken bereit, einschließlich Auswahl, Umsetzung und Management der Maßnahmen unter Berücksichtigung der Risikoumgebung für die Informationssicherheit der Organisation. Die Leitfäden haben einen hierarchischen Aufbau aus Abschnitten, Maßnahmenzielen, Maßnahmen, Anleitungen zur Umsetzung und weiteren Informationen. Die Richtlinien nach ISO/IEC 27002 sind allgemein gehalten und sollen auf alle Organisationen, ungeachtet ihrer Art, Größe oder Natur, anwendbar sein.

Während ISO/IEC 27001 und ISO/IEC 27002 in Organisationen, einschließlich Wirtschaftsunternehmen, Behörden und gemeinnützigen Organisationen, weitgehend anerkannt sind, gibt es einen aufkommenden Bedarf für sektorspezifische Versionen dieser Normen.

BEISPIELE

Die folgenden Dokumente, die erarbeitet wurden, um mit diesem sektorspezifischen Bedarf umzugehen, sind:

- ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*;
- ISO/IEC 27011, *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*;
- ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*;
- ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processor*;

- ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*.

Andere Organisationen haben auch Standards erstellt, die sektorspezifische Anforderungen behandeln.

Die sektorspezifischen Normen sollten mit den Anforderungen des Informationssicherheitsmanagementsystems in Einklang stehen. Dieses Dokument legt die Anforderungen fest, wie sektorspezifische Normen, die ISO/IEC 27001 erweitern und ISO/IEC 27002 vervollständigen oder ergänzen, erstellt werden müssen (siehe Abschnitt 1).

Dieses Dokument geht davon aus, dass alle Anforderungen nach ISO/IEC 27001, die nicht verfeinert oder interpretiert wurden und alle Maßnahmen nach ISO/IEC 27002, die nicht geändert wurden, im sektorspezifischen Kontext unverändert anwendbar sind.

4.2 Aufbau dieser Internationalen Norm

Abschnitt 5 stellt Anforderungen und Anleitungen dazu bereit, wie Anforderungen festgelegt werden müssen, die Anforderungen nach ISO/IEC 27001 ergänzen, verfeinern oder interpretieren.

Abschnitt 6 stellt Anforderungen und Anleitungen dazu bereit, wie Maßnahmenabschnitte, Maßnahmenziele, Maßnahmen, Anleitungen zur Umsetzung oder weitere Informationen, die den Inhalt von ISO/IEC 27002 ergänzen oder ändern, bereitgestellt werden müssen.

Anhang A enthält eine Vorlage, die für sektorspezifische Normen mit Bezug zu ISO/IEC 27001 verwendet werden muss.

Anhang B enthält zwei Vorlagen, die für sektorspezifische Normen mit Bezug zu ISO/IEC 27002 verwendet werden müssen.

Für sektorspezifische Normen mit Bezug zu sowohl ISO/IEC 27001 (siehe Abschnitt 5) und ISO/IEC 27002 (siehe Abschnitt 6), gelten sowohl Anhang A als auch Anhang B.

Anhang C enthält Erklärungen über Vor- und Nachteile von zwei verschiedenen Nummerierungsansätzen in den zwei Vorlagen in Anhang B.

Im Rahmen dieses Dokumentes werden die folgenden Konzepte verwendet, um die Anforderungen nach ISO/IEC 27001 für einen Sektor anzupassen:

- Ergänzung – siehe 5.2;
- Verfeinerung – siehe 5.3;
- Interpretation – siehe 5.4.

Im Rahmen dieses Dokumentes werden die folgenden Konzepte verwendet, um die Anleitung nach ISO/IEC 27002 für einen Sektor anzupassen:

- Ergänzung – siehe 6.2;
- Änderung – siehe 6.3.

4.3 Erweiterung von Anforderungen nach ISO/IEC 27001 oder Maßnahmen nach ISO/IEC 27002

Sektorspezifische Normen mit Bezug zu ISO/IEC 27001 dürfen Anforderungen oder Anleitungen zu denen nach ISO/IEC 27001 oder ISO/IEC 27002 hinzufügen. Diese Ergänzungen können die Anforderungen über die Informationssicherheit hinaus auf ihren sektorspezifischen Bereich erweitern.

BEISPIEL ISO/IEC 27018, verwendet solche Erweiterungen. ISO/IEC 27018:2019, Anhang A, enthält einen Maßnahmen-katalog zum Schutz personenbezogener Daten und erweitert damit den Anwendungsbereich von ISO/IEC 27018, um zusätzlich zur Informationssicherheit auch den Datenschutz zu behandeln.

5 Ergänzende, verfeinerte oder interpretierte Anforderungen nach ISO/IEC 27001

5.1 Allgemeines

Bild 1 stellt dar, wie sektorspezifische Anforderungen in Zusammenhang mit ISO/IEC 27001 erstellt werden.



Bild 1 — Erstellung von sektorspezifischen Anforderungen

5.2 Ergänzende Anforderungen zur ISO/IEC 27001

Die Festlegung ergänzender Anforderungen nach ISO/IEC 27001 ist zulässig.

BEISPIEL Ein Sektor, der ergänzende Anforderungen für eine Informationssicherheitspolitik hat, kann diese den Anforderungen an die Politik nach ISO/IEC 27001:2013, 5.2, hinzufügen.

Keine Anforderung, die die Anforderungen nach ISO/IEC 27001 ergänzt, darf eine der nach ISO/IEC 27001 definierten Anforderungen beseitigen oder außer Kraft setzen.

Sektorspezifische Ergänzungen von Anforderungen nach ISO/IEC 27001 müssen, soweit möglich, den Anforderungen und Anleitungen nach Anhang A entsprechen.

5.3 Verfeinerte Anforderungen der ISO/IEC 27001

Die Verfeinerung von Anforderungen nach ISO/IEC 27001 ist zulässig.

ANMERKUNG Anforderungen nach ISO/IEC 27001 werden durch derartige Verfeinerungen weder beseitigt noch außer Kraft gesetzt (siehe 3.2).

Sektorspezifische Verfeinerungen von Anforderungen nach ISO/IEC 27001 müssen, soweit möglich, den Anforderungen und Anleitungen nach Anhang A entsprechen.

BEISPIEL 1 Eine sektorspezifische Norm könnte Maßnahmen enthalten, die ISO/IEC 27001:2013, Anhang A, ergänzen. In diesem Fall müssen die Anforderungen bezüglich der Informationssicherheitsrisikobehandlung nach ISO/IEC 27001:2013, 6.1.3 c) und d) verfeinert werden, um die in der sektorspezifischen Norm angegebenen, ergänzenden Maßnahmen einzuschließen.

Die Festlegung eines bestimmten Ansatzes, um Anforderungen nach ISO/IEC 27001 zu erfüllen, ist ebenfalls zulässig.

BEISPIEL 2 Ein bestimmter Sektor hat eine vorgeschriebene Weise zur Bestimmung der Kompetenz von Personen, die im Anwendungsbereich des sektorspezifischen Managementsystems arbeiten. Diese Anforderung könnte die allgemeine Anforderung nach ISO/IEC 27001:2013, 7.2, verfeinern.

5.4 Interpretierte Anforderungen der ISO/IEC 27001

Die Interpretation der Anforderungen nach ISO/IEC 27001 ist zulässig.

ANMERKUNG Derartige Interpretationen setzen keine Anforderungen nach ISO/IEC 27001 außer Kraft, sondern erklären diese oder ordnen sie in den sektorspezifischen Kontext ein (siehe 3.1).

Sektorspezifische Interpretationen von Anforderungen nach ISO/IEC 27001 müssen, soweit möglich, den Anforderungen und Anleitungen nach Anhang A entsprechen.

6 Ergänzende oder geänderte Anleitung nach ISO/IEC 27002

6.1 Allgemeines

Bild 2 stellt dar, wie ISO/IEC 27002-Anleitungen hinzugefügt oder geändert werden können.



Bild 2 — Erstellung von sektorspezifischen Anleitungen

Jede „Maßnahme“ darf ausschließlich einmal das Wort „sollte“ enthalten.

ANMERKUNG Die Informationssicherheitsrisikobehandlung nach ISO/IEC 27001 erfordert, dass eine Organisation festgelegte Maßnahmen und Begründungen für die Auswahl und den Ausschluss von Maßnahmen nach ISO/IEC 27001:2013, Anhang A, angibt. Die Einmalige Verwendung des Wortes „sollte“ je Maßnahme vermeidet Mehrdeutigkeiten hinsichtlich des Geltungsbereichs der Maßnahme.

6.2 Ergänzende Anleitung

Das Ergänzen von Abschnitten Maßnahmenzielen, Maßnahmen, Anleitungen zur Umsetzung und weiteren Informationen zu ISO/IEC 27002 ist zulässig.

Abschnitte, Maßnahmenziele, Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen, die ISO/IEC 27002 ergänzen, müssen, soweit möglich, den Anforderungen und Anleitungen nach Anhang B entsprechen.

Vor der Festlegung ergänzender Abschnitte, Maßnahmenziele oder Maßnahmen sollten Einheiten, die sektorspezifische Normen mit Bezug zu ISO/IEC 27001 erarbeiten, erwägen, ob es als Ansatz effektiver ist, bestehende Inhalte von ISO/IEC 27002 zu ändern oder das gewünschte Ergebnis durch Ergänzung sektorspezifischer Maßnahmenziele (statt der Ergänzung von Abschnitten), Maßnahmen (statt der Ergänzung von Maßnahmenzielen), Anleitungen zur Umsetzung oder weiteren Informationen (statt von Maßnahmen) zum bestehenden Inhalt von ISO/IEC 27002 erreicht werden kann.

6.3 Geänderte Anleitung

In ISO/IEC 27002 enthalten Abschnitte, Maßnahmen und ihre Maßnahmenziele dürfen nicht geändert werden.

Falls es einen sektorspezifischen Bedarf gibt, ein Maßnahmenziel aufzunehmen, das einem in ISO/IEC 27002 enthaltenen Maßnahmenziel widerspricht, muss ein neues sektorspezifisches Maßnahmenziel eingeführt werden. Dieses neue Maßnahmenziel muss mindestens eine sektorspezifische Maßnahme enthalten. Falls es einen sektorspezifischen Bedarf gibt, eine Maßnahme aufzunehmen, die einer in ISO/IEC 27002 enthaltenen Maßnahme widerspricht, muss eine neue sektorspezifische Maßnahme eingeführt werden.

Die Veränderung von Anleitungen zur Umsetzung oder weiterer Informationen aus ISO/IEC 27002 ist erlaubt.

Abschnitte, Maßnahmenziele, Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen, die ISO/IEC 27002 entnommen und geändert wurden, müssen, soweit möglich, den Anforderungen und Anleitungen nach Anhang B entsprechen.

Anhang A (normativ)

Vorlage für die Erarbeitung sektorspezifischer Normen mit Bezug zu ISO/IEC 27001 und optional ISO/IEC 27002

A.1 Entwurfsanweisungen

In A.2 wird folgende Formatierungskonvention verwendet:

- Text in spitzen Klammern sollte durch geeigneten sektorspezifischen Text ersetzt werden.

BEISPIEL Für den Sektor „Telekommunikation“ sollte die in Abschnitt A.2 angegebene Überschrift von Abschnitt 4 „(Bezeichnung des Sektors)-spezifische ISMS-Anforderungen“ lauten: „Telekommunikationsspezifische ISMS-Anforderungen“.

- Text, der in Kursivschrift und in geschweifte Klammern gesetzt ist, gibt an, wie dieser Teil der Vorlage zu verwenden ist; dieser Text sollte in der Endfassung der sektorspezifischen Norm gelöscht werden.
- Text ohne besondere Formatierung sollte im Wortlaut übernommen werden.

A.2 Vorlage

Einleitung

{Die Art und Weise, wie die Anforderungen innerhalb dieses Dokumentes sich auf die Anforderungen nach ISO/IEC 27001 und optional, wenn sich die sektorspezifische Norm auch auf ISO/IEC 27002 bezieht, wie die Anleitung innerhalb dieser Norm sich auf die Anleitungen nach ISO/IEC 27002 beziehen, wird eingefügt.}

{Der folgende Text wird eingefügt:}

Dieses Dokument ist KEINE neue, von ISO/IEC 27001 unabhängige Managementsystemnorm, sondern legt die <Bezeichnung des Sektors>-spezifischen Anforderungen fest, die aus Verfeinerungen von und/oder Ergänzungen zu den Anforderungen von ISO/IEC 27001 bestehen.

{Falls die sektorspezifische Norm auch einen Bezug zu ISO/IEC 27002 hat, wird statt vorherigem folgender Text eingefügt:}

Dieses Dokument ist KEINE neue, von ISO/IEC 27001 unabhängige Managementsystemnorm, sondern:

- a) legt die <Bezeichnung des Sektors>-spezifischen Anforderungen fest, die aus Verfeinerungen von und/oder Ergänzungen zu den Anforderungen der ISO/IEC 27001 bestehen; und
- b) legt die <Bezeichnung des Sektors>-spezifische Anleitung fest, die Ergänzungen zu und/oder Veränderungen von ISO/IEC 27002 unterstützen (siehe Abschnitt 6).

1 Anwendungsbereich

{Die zutreffenden Aussagen zum Anwendungsbereich einschließlich des Zusammenhangs dieser Norm mit der ISO/IEC 27001 und optional der ISO/IEC 27002, wenn sich die sektorspezifische Norm auch auf ISO/IEC 27002 bezieht, werden eingefügt.}

2 Normative Verweisungen

{Die entsprechenden zutreffenden normativen Verweisungen, einschließlich ISO/IEC 27001 und optional ISO/IEC 27002, werden eingefügt.}

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

3 Begriffe

{Der folgende Text wird eingefügt, um sicherzustellen, dass ISO/IEC 27000 enthalten ist.}

Für die Anwendung dieses Dokuments gelten die Begriffe und Definitionen nach ISO/IEC 27000 [und die folgenden Begriffe und Definitionen].

4 <Bezeichnung des Sektors>-spezifische Anforderungen mit Bezug zu ISO/IEC 27001:2013

4.1 Allgemeines

{Der folgende Text ist einzufügen.}

Alle Anforderungen nach ISO/IEC 27001:2013, Abschnitt 4 bis Abschnitt 10 gelten unverändert, sofern sie im Folgenden nicht aufgeführt sind.

{Sämtliche sektorspezifische Anforderungen werden hinzugefügt. Beim Ergänzen einer Anforderung wird zuerst überprüft, ob sie in Zusammenhang mit einer bereits bestehenden Anforderung nach ISO/IEC 2700 steht. Wenn ein Zusammenhang zu bestehenden Anforderungen nach ISO/IEC 27001 besteht, wird ein Titel mit einem Präfix von mindestens drei Buchstaben für den Sektor, gefolgt von einer Unterabschnittsnummer und dem ursprünglichen Titel des Unterabschnitts nach ISO/IEC 27001 hinzugefügt.}

BEISPIEL **4.2 CLD 4.1 Verstehen der Organisation und ihres Kontextes.**

Wenn kein Bezug zu einer bestehenden Anforderung besteht, wird die zusätzliche Anforderung als neuer Unterabschnitt am Ende nach allen Unterabschnitten in Abschnitt 4 der sektorspezifischen Norm eingefügt.}

{Optional darf eine sektorspezifische Norm über eine Tabelle verfügen, die den Zusammenhang zwischen den (Unter-)Abschnitten der sektorspezifischen Norm und denen nach ISO/IEC 27001 anzeigt. Eine Tabelle ist ein nützliches Werkzeug, das Lesern beim Verständnis der Anordnung der Abschnitte von sektorspezifischen Normen im Vergleich zu denen nach ISO/IEC 27001 hilft.}

Tabelle 1 — Entsprechung der <Name des Sektors>-spezifischen Anforderungen zu denen nach ISO/IEC 27001

Unterabschnitt in ISO/IEC 27001:2013	Titel	Unterabschnitt in diesem Dokument	Anmerkungen

{Sektorspezifische Anforderungen, die die Anforderungen nach ISO/IEC 27001 ergänzen, werden durch Einfügen des folgenden Textes angegeben.}

Eine Anforderung, die ISO/IEC 27001:2013 {Abschnitts- | Unterabschnittsnummer} ergänzt, ist:

{Sektorspezifische Anforderungen, die die Anforderungen nach ISO/IEC 27001:2013 verfeinern, werden durch Einfügen des folgenden Textes angegeben:}

Die Anforderung nach ISO/IEC 27001:2013 {Abschnitts- | Unterabschnittsnummer} wird wie folgt verfeinert:

{Sektorspezifische Anforderungen, die die Anforderungen nach ISO/IEC 27001:2013 interpretieren, werden durch Einfügen des folgenden Textes angegeben:}

Die Anforderung nach ISO/IEC 27001:2013 {Abschnitts- | Unterabschnittsnummer} wird wie folgt interpretiert:

{Nach Möglichkeit wird ergänzter, verfeinerter oder interpretierter Text durch Kursivschrift kenntlich gemacht:}

{Falls die sektorspezifische Norm sektorspezifische Maßnahmen enthält, wird der folgende Text eingefügt:}

Die Anforderung nach ISO/IEC 27001:2013, 6.1.3 c) wird wie folgt verfeinert:

Die in 6.1.3 b) festgelegten Maßnahmen sind mit den Maßnahmen in ISO/IEC 27001:2013, Anhang A, und mit Anhang A zu vergleichen und zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden.

Die Anforderung nach ISO/IEC 27001:2013, 6.1.3 d) wird wie folgt verfeinert:

Es ist eine Erklärung zur Anwendbarkeit zu erstellen, die folgendes enthält:

- die erforderlichen Maßnahmen [siehe ISO/IEC 27001:2013, 6.1.3 b) und c)];
- Gründe für deren Einbeziehung;
- ob sie umgesetzt sind oder nicht; und
- Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A und ISO/IEC 27001:2013, Anhang A.

{Die Maßnahmen in ISO/IEC 27001:2013, Anhang A, sind keine Anforderungen. Es ist allerdings möglich, Maßnahmen anzuordnen. Es gibt zwei Arten von Quellen für angeordnete Maßnahmen. Falls die Gruppe der angeordneten Maßnahmen aus einer externen Quelle kommt, dann wird eine Anforderung hinzugefügt, die die Gruppe der Maßnahmen anordnet, indem sie die externe Quelle referenziert. Falls sie in diesem Dokument eingeführt werden, werden sie explizit angegeben. Solche angeordneten Maßnahmen sollten in den am ehesten relevanten Abschnitten (d. h. Abschnitt 4 bis Abschnitt 10) dieses Dokumentes abgelegt werden, beispielsweise Abschnitt 8. Der folgende Text wird eingefügt, um festzulegen, dass die angeordneten Maßnahmen als eine Verfeinerung nach ISO/IEC 27001 als ein zusätzlicher Abschnitt festgelegt sind:}

Eine Anforderung, die ISO/IEC 27001:2013 {Abschnittnummer} ergänzt, ist:

{Falls sich die sektorspezifische Norm auch auf ISO/IEC 27002 bezieht, wird die Vorlage erstellt, indem Abschnitt 4 dieser Vorlage und Abschnitt 4 bis Abschnitt 6 in B.2 oder Abschnitt 4 bis Abschnitt 18 in B.3 geeignet kombiniert werden, so dass die Struktur der sektorspezifischen Norm für seinen Zweck geeignet ist.}

{Falls eine sektorspezifische Norm sektorspezifische Maßnahmen enthält, muss ein normativer Anhang A auf die gleiche Art wie in ISO/IEC 27001:2013, Anhang A, mit dem folgenden Text erstellt werden:}

Anhang A für die <Bezeichnung des Sektors>-spezifischen Maßnahmenziele und –maßnahmen auf, die zusätzlich zu ISO/IEC 27001:2013, Anhang A, wie in 4.1 festgelegt, angewandt werden müssen.

Anhang A

(normativ)

<Bezeichnung des Sektors>-spezifische Referenzmaßnahmenziele und Maßnahmen

{Die Tabelle A.1 muss im gleichen Format wie ISO/IEC 27001:2013, Anhang A, mit folgendem Text eingeführt werden.}

Die in Tabelle A.1 aufgeführten zusätzlichen oder veränderten Maßnahmenziele und Maßnahmen sind direkt aus diesem Dokument abgeleitet und mit diesem abgeglichen und müssen im Zusammenhang mit ISO/IEC 27001:2013, 6.1.3, wie in diesem Dokument verfeinert, verwendet werden.