# DIN ISO/IEC 27009

ICS 35.030

Ersatz für
DIN ISO/IEC 27009:2016-11

## Informationssicherheit, Cybersicherheit und Datenschutz – Sektorspezifische Anwendung der ISO/IEC 27001 – Anforderungen (ISO/IEC 27009:2020)

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

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)

Gesamtumfang 26 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN ISO/IEC 27009:2022-09

# 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 diesem Dokument ... 7
4.1 Allgemeines ... 7
4.2 Aufbau dieses Dokuments ... 8
4.3 Erweiterung von Anforderungen nach ISO/IEC 27001 oder Maßnahmen nach ISO/IEC 27002 ... 8
5 Ergänzende, verfeinerte oder interpretierte Anforderungen nach ISO/IEC 27001 ... 9
5.1 Allgemeines ... 9
5.2 Ergänzende Anforderungen zu ISO/IEC 27001 ... 9
5.3 Verfeinerte Anforderungen zu ISO/IEC 27001 ... 9
5.4 Interpretierte Anforderungen zu ISO/IEC 27001 ... 9
6 Ergänzende oder geänderte Anleitung nach ISO/IEC 27002 ... 10
6.1 Allgemeines ... 10
6.2 Ergänzende Anleitung ... 10
6.3 Geänderte Anleitung ... 10
Anhang A (normativ) Vorlage für die Erarbeitung sektorspezifischer Normen mit Bezug zu ISO/IEC 27001 und optional ISO/IEC 27002 ... 11
Anhang B (normativ) Vorlage für die Erarbeitung sektorspezifischer Normen mit Bezug zu ISO/IEC 27002 ... 15
Anhang C (informativ) Erklärung der Vor- und Nachteile der innerhalb von Anhang B verwendeten Nummerierungsansätze ... 24
Literaturhinweise ... 26



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09

# Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO/IEC 27009:2020, die vom Technischen Komitee ISO/IEC JTC 1 „ISO/IEC Gemeinschaftskomitee für Informationstechnik“ erarbeitet wurde, dessen Sekretariat von ANSI (USA) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-04-27-01 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 | siehe | DIN EN ISO/IEC 27001 |
| ISO/IEC 27002 | siehe | DIN EN ISO/IEC 27002 |
| ISO/IEC 27011 | siehe | DIN EN ISO/IEC 27011 |
| ISO/IEC 27017 | siehe | DIN EN ISO/IEC 27017 |
| 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/IEC 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.

**Frühere Ausgaben**

DIN ISO/IEC 27009: 2016-11



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09

# Nationaler Anhang NA
(informativ)

# Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagement-systeme — 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 27011, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen*

DIN EN ISO/IEC 27017, *Informationstechnik —Sicherheitsverfahren —Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste*

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*



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09

# 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.



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09

# 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.

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/



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09

**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 diesem Dokument

## 4.1 Allgemeines

ISO/IEC 27001 definiert die Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems. ISO/IEC 27001 enthält die Aussage, dass die dort 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 Leitlinien 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*.



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09

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 (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 dieses Dokuments

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 Maßnahmenkatalog zum Schutz personenbezogener Daten und erweitert damit den Anwendungsbereich von ISO/IEC 27018, um zusätzlich zur Informationssicherheit auch den Datenschutz zu behandeln.



Documents
Document Sharing Hub
Full document details: DIN ISO/IEC 27009:2022-09