DIN EN ISO/IEC 27001

ICS 03.100.70; 35.030

Ersatz für
DIN EN ISO/IEC 27001:2017-06

Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023

Information security, cybersecurity and privacy protection –
Information security management systems –
Requirements (ISO/IEC 27001:2022);
German version EN ISO/IEC 27001:2023

Sécurité de l'information, cybersécurité et protection de la vie privée –
Systèmes de management de la sécurité de l'information –
Exigences (ISO/IEC 27001:2022);
Version allemande EN ISO/IEC 27001:2023

Gesamtumfang 31 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27001:2024-01

Nationales Vorwort

Der Text von ISO/IEC 27001:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27001:2023 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 Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ 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 27002:2022	siehe	DIN EN ISO/IEC 27002:2024-01
ISO 31000:2018	siehe	DIN ISO 31000:2018-10

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 EN ISO/IEC 27001:2017-06 wurden folgende Änderungen vorgenommen:

a) der Text wurde an die harmonisierte Struktur für Managementsystemnormen und an ISO/IEC 27002:2022 angepasst.

Frühere Ausgaben

DIN ISO/IEC 27001: 2008-09, 2015-03
DIN ISO/IEC 27001 Berichtigung 1: 2017-03
DIN EN ISO/IEC 27001: 2017-06

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27001:2024-01

Nationaler Anhang NA
(informativ)

Literaturhinweise

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

DIN EN ISO/IEC 27002:2024-01, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche Fassung EN ISO/IEC 27002:2022*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27001:2024-01

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27001:2024-01

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27001

Juli 2023

ICS 03.100.70; 35.030

Ersetzt EN ISO/IEC 27001:2017

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2022)

Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences (ISO/IEC 27001:2022)

Diese Europäische Norm wurde vom CEN am 23. Juli 2023 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-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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27001:2024-01

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Kontext der Organisation 7
4.1 Verstehen der Organisation und ihres Kontextes 7
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien 7
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems . 8
4.4 Informationssicherheitsmanagementsystem 8
5 Führung 8
5.1 Führung und Verpflichtung 8
5.2 Politik 9
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation 9
6 Planung 9
6.1 Maßnahmen zum Umgang mit Risiken und Chancen 9
6.1.1 Allgemeines 9
6.1.2 Informationssicherheitsrisikobeurteilung 10
6.1.3 Informationssicherheitsrisikobehandlung 10
6.2 Informationssicherheitsziele und Planung zu deren Erreichung 11
6.3 Planung von Änderungen 12
7 Unterstützung 12
7.1 Ressourcen 12
7.2 Kompetenz 12
7.3 Bewusstsein 12
7.4 Kommunikation 13
7.5 Dokumentierte Information 13
7.5.1 Allgemeines 13
7.5.2 Erstellen und Aktualisieren 13
7.5.3 Steuerung dokumentierter Information 13
8 Betrieb 14
8.1 Betriebliche Planung und Steuerung 14
8.2 Informationssicherheitsrisikobeurteilung 14
8.3 Informationssicherheitsrisikobehandlung 14
9 Bewertung der Leistung 14
9.1 Überwachung, Messung, Analyse und Bewertung 14
9.2 Internes Audit 15
9.2.1 Allgemeines 15
9.2.2 Internes Auditprogramm 15
9.3 Managementbewertung 16
9.3.1 Allgemeines 16
9.3.2 Eingaben für die Managementbewertung 16
9.3.3 Ergebnisse der Managementbewertung 16
10 Verbesserung 16
10.1 Fortlaufende Verbesserung 16
10.2 Nichtkonformität und Korrekturmaßnahmen 16
Anhang A (normativ) Verweisung auf Informationssicherheitsmaßnahmen 18
Literaturhinweise 27

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27001:2024-01

Tabellen

Tabelle A.1 — Informationssicherheitsmaßnahmen 18

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27001:2024-01

Europäisches Vorwort

Der Text von ISO/IEC 27001:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27001:2023 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 Januar 2024, und etwaige entgegenstehende nationale Normen müssen bis Januar 2024 zurückgezogen werden.

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

Dieses Dokument ersetzt EN ISO/IEC 27001:2017.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN und CENELEC abrufbar.

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 27001:2022 wurde von CEN-CENELEC als EN ISO/IEC 27001:2023 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27001:2024-01

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.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC Directives, 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 Directives, Teil 2, erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

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) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe https://patents.iec.ch).

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. Diesbezügliche Informationen der IEC sind unter www.iec.ch/understanding-standards verfügbar.

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

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27001:2013), die technisch überarbeitet wurde. Sie enthält auch die Technischen Berichtigungen ISO/IEC 27001:2013/Cor 1:2014 und ISO/IEC 27001:2013/Cor 2:2015.

Die wesentlichen Änderungen sind folgende:

— der Text wurde an die harmonisierte Struktur für Managementsystemnormen und an ISO/IEC 27002:2022 angepasst.

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 und www.iec.ch/national-committees zu finden.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27001:2024-01

Einleitung

0.1 Allgemeines

Dieses Dokument wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Umsetzung eines Informationssicherheitsmanagementsystems innerhalb einer Organisation richten sich nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern.

Das Informationssicherheitsmanagementsystem wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Es ist wichtig, dass das Informationssicherheitsmanagementsystem als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt wird. Es wird erwartet, dass die Umsetzung eines Informationssicherheitsmanagementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Dieses Dokument kann von internen und externen Parteien dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu beurteilen.

Die Reihenfolge, in der die Anforderungen in diesem Dokument aufgeführt sind, spiegelt nicht deren Bedeutung wider noch die Abfolge, in der sie umzusetzen sind. Die Listeneinträge sind lediglich zu Referenzierungszwecken nummeriert.

ISO/IEC 27000 liefert einen Überblick und die Begrifflichkeiten von Informationssicherheitsmanagementsystemen und verweist auf die Informationssicherheitsmanagementsystem-Normenfamilie (einschließlich ISO/IEC 27003 [2], ISO/IEC 27004 [3] und ISO/IEC 27005 [4]), einschließlich deren Begriffe.

0.2 Kompatibilität mit anderen Managementsystemnormen

Dieses Dokument wendet die übergeordnete Struktur, die identischen Unterabschnittsnummern, den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen an, die in Anhang SL der ISO/IEC Directives, Teil 1, „Consolidated ISO Supplement“ festgelegt sind, und stellt so die Übereinstimmung mit anderen Managementsystemnormen her, die ebenfalls den Anhang SL anwenden.

Diese in Anhang SL festgelegte gemeinsame Herangehensweise nützt jenen Organisationen, die sich für den Betrieb eines einzigen Managementsystems entscheiden, das die Anforderungen von zwei oder mehr Normen für Managementsysteme erfüllt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27001:2024-01