ÖVE/ÖNORM EN ISO/IEC 27005

Ausgabe: 2025-01-15

Informationssicherheit, Cybersicherheit und Datenschutz – Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022)

Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés à la sécurité de l'information (ISO/IEC 27005:2022)

Diese österreichische Norm ist qualitätsgeprüft. Diese österreichische Norm beinhaltet EN ISO/IEC 27005:2024 (idente Übernahme).

Komitee 001 – Informationstechnologie

ICS 35.030

Erläuternde Informationen zu ÖNORM und ONR:
https://www.austrian-standards.at/info-oenorm_de

Medieninhaber, Herausgeber und Hersteller
Austrian Standards International
Standardisierung und Innovation
Heinestraße 38, 1020 Wien

OVE Österreichischer Verband für Elektrotechnik
Eschenbachgasse 9, 1010 Wien
E-Mail: verkauf@ove.at
Tel.: +43 1 587 63 73
Internet: http://www.ove.at

Vertrieb und Lizenzierung
Austrian Standards plus GmbH
Heinestraße 38, 1020 Wien

Customer Service
E-Mail: service@austrian-standards.at
Tel.: +43 1 213 00-300
Internet: www.austrian-standards.at

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27005

August 2024

ICS 35.030

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022)

Information security, cybersecurity and privacy protection - Guidance on managing information security risks (ISO/IEC 27005:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Préconisations pour la gestion des risques liés à la sécurité de l'information (ISO/IEC 27005:2022)

Diese Europäische Norm wurde vom CEN am 1. August 2024 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 und elektrotechnischen Komitees 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 Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

Seite

Bilder

Tabellen

Europäisches Vorwort

Der Text von ISO/IEC 27005:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27005:2024 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 Februar 2025, und etwaige entgegenstehende nationale Normen müssen bis Februar 2025 zurückgezogen werden.

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

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 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 27005:2022 wurde von CEN-CENELEC als EN ISO/IEC 27005:2024 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.

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 http://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. In der IEC, siehe www.iec.ch/understanding-standards.

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

Diese vierte Ausgabe ersetzt die dritte Ausgabe (ISO/IEC 27005:2018), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

— der gesamte Leitfaden wurde an ISO/IEC 27001:2022 und ISO 31000:2018 angepasst;

— die Terminologie wurde an die Terminologie in ISO 31000:2018 angepasst;

— die Gliederung der Abschnitte wurde an den Aufbau der ISO/IEC 27001:2022 angepasst;

— Konzepte für Risikoszenarien wurden eingeführt;

— der ereignisbasierte Ansatz wird dem auf Werten basierenden Ansatz zur Risikoidentifizierung gegenübergestellt;

— der Inhalt der Anhänge wurde überarbeitet und in einem einzigen Anhang zusammengefasst.

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.

Einleitung

Dieses Dokument bietet einen Leitfaden für:

— die Implementierung der in ISO/IEC 27001 festgelegten Anforderungen im Hinblick auf Informationssicherheitsrisiken;

— die wesentlichen Verweisungen innerhalb der von ISO/IEC JTC 1/SC 27 entwickelten Normen zur Unterstützung von Maßnahmen im Rahmen der Handhabung von Informationssicherheitsrisiken;

— Aktionen zur Bewältigung von Risiken im Zusammenhang mit der Informationssicherheit (siehe ISO/IEC 27001:2022, 6.1 und Abschnitt 8);

— die Implementierung eines Leitfadens zum Risikomanagement in ISO 31000 im Zusammenhang mit der Informationssicherheit.

Dieses Dokument enthält einen ausführlichen Leitfaden zum Risikomanagement und ergänzt die Leitlinien in ISO/IEC 27003.

Dieses Dokument richtet sich an:

— Organisationen, die beabsichtigen, ein Informationssicherheitsmanagementsystem (ISMS) in Übereinstimmung mit ISO/IEC 27001 einzuführen und umzusetzen;

— Personen, die das Informationssicherheitsrisikomanagement durchführen oder daran beteiligt sind (z. B. Fachkräfte für ISMS, Risikoeigentümer und andere interessierte Parteien);

— Organisation, die ihren Risikomanagementprozess im Bereich der Informationssicherheit verbessern wollen.

1 Anwendungsbereich

Dieses Dokument enthält einen Leitfaden, der Organisationen dabei hilft,

— die Anforderungen der ISO/IEC 27001 in Bezug auf Aktionen zur Bewältigung von Informationssicherheitsrisiken zu erfüllen;

— Maßnahmen zur Handhabung von Informationssicherheitsrisiken, insbesondere zur Risikobeurteilung und -behandlung im Bereich der Informationssicherheit, durchzuführen.

Dieses Dokument gilt für alle Organisationen, unabhängig von ihrer Art, Größe oder Branche.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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*

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 Begriffe im Zusammenhang mit Informationssicherheitsrisiken

3.1.1
externer Kontext
externes Umfeld, in dem die Organisation versucht, ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der externe Kontext kann Folgendes beinhalten:

— soziale, kulturelle, politische, rechtliche, behördliche, finanzielle, technologische, wirtschaftliche, geologische Umgebung, seien sie internationaler, nationaler, regionaler oder lokaler Art;

— Schlüsselfaktoren und Trends, die die Ziele der Organisation beeinflussen;

— die Beziehungen, Wahrnehmungen, Werte, Erfordernisse und Erwartungen externer interessierter Parteien;

— vertragliche Beziehungen und Verpflichtungen;

— die Komplexität der Netzwerke und Abhängigkeiten.

[QUELLE: ISO Guide 73:2009, 3.3.1.1, modifiziert — Anmerkung 1 zum Begriff wurde modifiziert.]