ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 27002:2022

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen

Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information (ISO/IEC 27002:2022)

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

11/2022

Nationales Vorwort

Diese Europäische Norm EN ISO/IEC 27002:2022 wurde als luxemburgische Norm ILNAS-EN ISO/IEC 27002:2022 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN ISO/IEC 27002

November 2022

ICS 35.030

Ersetzt EN ISO/IEC 27002:2017

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Moyens de maîtrise de l'information (ISO/IEC 27002:2022)

Diese Europäische Norm wurde vom CEN am 30. Oktober 2022 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

Europäisches Vorwort

Der Text von ISO/IEC 27002:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27702:2022 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 Mai 2023, und etwaige entgegenstehende nationale Normen müssen bis Mai 2023 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 27002:2017.

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 27002:2022 wurde von CEN-CENELEC als EN ISO/IEC 27002:2022 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-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 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 der IEC-Liste der erhaltenen Patenterklärungen (siehe 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 https://www.iec.ch/understanding-standards.

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

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27002:2013), die technisch überarbeitet wurde. Sie berücksichtigt auch die Berichtigungen ISO/IEC 27002:2013/Cor. 1:2014 und ISO/IEC 27002:2013/Cor. 2:2015.

Die wesentlichen Änderungen sind Folgende:

— der Titel wurde modifiziert;

— die Struktur des Dokuments wurde geändert, indem die Maßnahmen mit einer einfachen Taxonomie und zugehörigen Attributen dargestellt werden;

— einige Maßnahmen wurden zusammengelegt, einige gestrichen und mehrere neue Maßnahmen wurden eingeführt. Die vollständigen Zusammenhänge können Anhang B entnommen werden.

Diese korrigierte Version von ISO/IEC 27002:2022 enthält die folgenden Korrekturen:

— nicht funktionierende Hyperlinks im gesamten Dokument wurden wiederhergestellt;

— in der einleitenden Tabelle in Unterabschnitt 5.22 und in Tabelle A.1 (Zeile 5.22) wurde „#Vertrauenswürdigkeit_in_Bezug_auf_Informationssicherheit“ von der Spalte „Sicherheitsdomänen“ in die Spalte „Betriebsfähigkeit“ verschoben.

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 https://www.iec.ch/national-committees zu finden.

Einleitung

0.1 Hintergrund und Kontext

Dieses Dokument wurde für Organisationen jeder Art und Größe erarbeitet. Es soll als Referenz für die Bestimmung und Implementierung von Maßnahmen zur Behandlung von Informationssicherheitsrisiken in einem Informationssicherheitsmanagementsystem (ISMS) auf der Grundlage von ISO/IEC 27001 verwendet werden. Es kann auch als Anleitung für Organisationen verwendet werden, die allgemein anerkannte Informationssicherheitsmaßnahmen festlegen und umsetzen. Darüber hinaus ist dieses Dokument ebenfalls bestimmt für die Entwicklung von branchen- und organisationsspezifischen Leitlinien zum Management von Informationssicherheit, die deren spezifisches Umfeld der Informationssicherheitsrisiken berücksichtigen. Organisatorische oder umgebungsspezifische Maßnahmen, die nicht in diesem Dokument enthalten sind, können bei Bedarf durch eine Risikobeurteilung festgelegt werden.

Organisationen aller Arten und Größen (einschließlich öffentlicher und privater, kommerzieller und gemeinnütziger) erheben, verarbeiten, speichern, übertragen und vernichten Informationen in vielen Formen, darunter elektronisch, physisch und verbal (z. B. Gespräche und Präsentationen).

Der Informationswert besteht nicht nur aus geschriebenen Wörtern, Zahlen und Bildern: Wissen, Konzepte, Ideen und Marken sind Beispiele für immaterielle Informationsformen. In einer vernetzten Welt verdienen oder erfordern Informationen und andere damit verbundene Werte Schutz vor verschiedenen Risikoquellen, seien sie natürlich, zufällig oder vorsätzlich.

Die Einführung einer Reihe geeigneter Sicherheitsmaßnahmen, darunter Richtlinien, Regeln, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen, sorgt für Informationssicherheit. Um ihre spezifischen Sicherheits- und Geschäftsziele zu erreichen, sollte die Organisation diese Maßnahmen festlegen, umsetzen, überwachen, überprüfen und gegebenenfalls verbessern. Ein Informationssicherheitsmanagementsystem (ISMS), wie in ISO/IEC 27001 näher beschrieben, verfolgt eine ganzheitliche, koordinierte Betrachtung der Risiken in der Informationssicherheit einer Organisation, um eine umfassende Sammlung von Maßnahmen zur Informationssicherheit innerhalb eines einheitlichen Managementsystems bestimmen und einführen zu können.

Viele Informationssysteme, einschließlich ihres Managements und Betriebs, sind nicht so konzipiert, dass sie im Sinne eines ISMS, wie es in ISO/IEC 27001 und diesem Dokument beschrieben ist, als sicher betrachtet werden können. Die Sicherheitsstufe, die allein durch technische Maßnahmen erreicht werden kann, ist begrenzt und sollte durch geeignete Managementaktivitäten und organisatorische Prozesse unterstützt werden. Die Feststellung der benötigten Sicherheitsmaßnahmen erfordert sorgfältige Planung und Detailtreue bei der Risikobehandlung.

Ein erfolgreiches Informationssicherheitsmanagementsystem erfordert die Mitarbeit des gesamten Personals einer Organisation. Sie kann auch die Beteiligung anderer interessierter Parteien, wie z. B. Aktionäre oder Lieferanten, erfordern. Auch der Rat von Fachleuten kann erforderlich sein.

Ein geeignetes, angemessenes und wirksames Managementsystem für die Informationssicherheit bietet der Leitung der Organisation und anderen interessierten Parteien die Vertrauenswürdigkeit, dass ihre Informationen und andere damit verbundenen Werte angemessen sicher und vor Bedrohungen und Schäden geschützt sind, so dass die Organisation ihre erklärten Geschäftsziele erreichen kann.