DIN ISO 28000

DIN

ICS 03.100.01; 03.100.70

Einsprüche bis 2021-05-19
Vorgesehen als Ersatz für
DIN ISO 28000:2015-08

Entwurf

Sicherheit und Belastbarkeit – Sicherheitsmanagementsysteme – Anforderungen für die Lieferkette (ISO/DIS 28000:2021); Text Deutsch und Englisch

Security and resilience –
Security management systems –
Requirements for the supply chain (ISO/DIS 28000:2021);
Text in German and English

Sûreté et résilience –
Systèmes de management de la sûreté –
Exigences pour la chaîne d'approvisionnement (ISO/DIS 28000:2021);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-03-19 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 info@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 Organisationsprozesse (NAOrg), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 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 58 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

Bilder

Tabellen

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung des internationalen Norm-Entwurfes ISO/DIS 28000:2021, der vom Technischen Komitee ISO/TC 292 „Security and resilience“ erarbeitet wurde, dessen Sekretariat von SIS (Schweden) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitsausschuss NA 175-00-05 GA „Sicherheit und Business Continuity“ im DIN-Normenausschuss Organisationsprozesse (NAOrg).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. 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 9001	siehe	DIN EN ISO 9001
ISO 14001	siehe	DIN EN ISO 14001
ISO 22300	siehe	DIN EN ISO 22300
ISO 22301	siehe	DIN EN ISO 22301
ISO 31000	siehe	DIN ISO 31000
ISO 45001	siehe	DIN ISO 45001
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001

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 28000:2015-08 wurden folgende Änderungen vorgenommen:

a) ISO-Richtlinien, Anhang L, Anlage 2, wurden eingehalten;

b) Empfehlungen zu Grundsätzen wurden in Abschnitt 4 hinzugefügt, um eine bessere Koordination mit ISO 31000 zu bieten;

c) in Abschnitt 8 wurden zur besseren Übereinstimmung mit ISO 22301 Empfehlungen hinzugefügt, die die Integration ermöglichen, einschließlich:

   — Sicherheitsstrategien, -verfahren, -prozesse und -behandlungen;

   — Sicherheitspläne.

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 14001, *Umweltmanagementsysteme — Anforderungen mit Anleitung zur Anwendung*

DIN EN ISO 22300, *Sicherheit und Resilienz — Vokabular*

DIN EN ISO 22301, *Sicherheit und Resilienz — Business Continuity Management System — Anforderungen*

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

DIN ISO 31000, *Risikomanagement — Leitlinien*

DIN ISO 45001, *Managementsysteme für Sicherheit und Gesundheit bei der Arbeit — Anforderungen mit Anleitung zur Anwendung*

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

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. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten 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 ist 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/TC 292, *Security and resilience,* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 28000:2007), die technisch überarbeitet wurde, jedoch bestehende Anforderungen beibehält, um Kontinuität für Organisationen zu gewährleisten, die die vorherige Ausgabe verwenden. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

— ISO-Richtlinien, Anhang L, Anlage 2, wurden eingehalten;

— Empfehlungen zu Grundsätzen wurden in Abschnitt 4 hinzugefügt, um eine bessere Koordination mit ISO 31000 zu bieten;

— in Abschnitt 8 wurden zur besseren Übereinstimmung mit ISO 22301 Empfehlungen hinzugefügt, die die Integration ermöglichen, einschließlich:

  — Sicherheitsstrategien, -verfahren, -prozesse und -behandlungen;

  — Sicherheitspläne.

Eine Auflistung aller Teile der Normenreihe ISO 28000 ist auf der ISO-Internetseite abrufbar.

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.

Einleitung

Die meisten Organisationen erfahren eine zunehmende Unsicherheit und Volatilität in der Sicherheitsumgebung. Als Folge daraus stellen sich ihnen Sicherheitsfragen, die sich auf ihre Ziele auswirken, und sie möchten diese innerhalb ihres Managementsystems systematisch behandeln. Eine formale Herangehensweise an das Sicherheitsmanagement kann zu den geschäftlichen Fähigkeiten und der Glaubwürdigkeit der Organisation direkt beitragen.

Dieses Dokument legt die Anforderungen für ein Sicherheitsmanagementsystem fest, einschließlich der Aspekte, die für die Sicherheitsgewährleistung der Lieferkette von hoher Wichtigkeit sind. Es erfordert von der Organisation:

— Bewerten der Sicherheitsumgebung, in der es arbeitet, einschließlich ihrer Lieferkette (einschließlich Abhängigkeiten und Wechselbeziehungen);

— Feststellen, ob angemessene Sicherheitsmaßnahmen vorhanden sind, um sicherheitsrelevante Risiken effektiv zu behandeln;

— Einhalten von gesetzlichen, behördlichen und freiwilligen Verpflichtungen, denen sich die Organisation unterwirft; und

— Anpassen von Sicherheitsprozessen und -steuerungen, einschließlich der relevanten vor- und nachgelagerten Prozesse und Kontrollen der Lieferkette, um die Ziele der Organisation zu erreichen.

Es erfordert von der Organisation, die Sicherheitsumgebung, in der sie arbeitet, zu bewerten und festzustellen, ob angemessene Sicherheitsmaßnahmen vorhanden sind, um sicherheitsrelevante Risiken effektiv zu behandeln, und ob bereits andere gesetzliche sicherheitsrelevante Anforderungen bestehen, die die Organisation erfüllt.

Wenn Sicherheitsziele identifiziert sind, implementiert die Organisation Kontrollen, um diese Ziele zu erreichen.

Sicherheitsmanagement ist mit vielen Aspekten der Geschäftsführung verbunden. Sie beinhalten alle Aktivitäten, die von Organisationen kontrolliert oder beeinflusst werden, einschließlich, aber nicht beschränkt auf diejenigen, die sich auf die Lieferkette auswirken. Alle Aktivitäten, Funktionen und Tätigkeiten sollten berücksichtigt werden, die eine Auswirkung auf das Sicherheitsmanagement der Organisation haben, einschließlich (aber nicht beschränkt auf) dessen Lieferkette.

Hinsichtlich der Lieferkette muss berücksichtigt werden, dass Lieferketten dynamischer Natur sind. Daher dürfen einige Organisationen, die mehrere Lieferketten verwalten, von ihren Anbietern verlangen, dass sie die entsprechenden Sicherheitsstandards als Bedingung für die Aufnahme in diese Lieferkette erfüllen, um die Anforderungen an das Sicherheitsmanagement zu erfüllen.

Dieses Dokument wendet das „Plan-Do-Check-Act"-Modell (PDCA, de: Planen-Durchführen-Prüfen-Handeln) an, um die Effektivität des Sicherheitsmanagementsystems einer Organisation zu planen, einzurichten, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und fortlaufend zu verbessern.

Tabelle 1 — Erläuterung des PDCA-Modells

Planen (Einführen)	Einführen von Sicherheitsleitlinie, -zielen, -einzelzielen, -kontrollen, -prozessen und -verfahren, die für die Verbesserung der Sicherheit relevant sind, um Ergebnisse zu erzielen, die sich mit der übergeordneten Leitlinie und den übergeordneten Zielen der Organisation in Übereinstimmung befinden.