

DIN ISO 28000

ICS 03.100.01; 03.100.70

Ersatz für
DIN ISO 28000:2015-08**Sicherheit und Belastbarkeit –
Sicherheitsmanagementsysteme –
Anforderungen (ISO 28000:2022)**Security and resilience –
Security management systems –
Requirements (ISO 28000:2022)Sûreté et résilience –
Systèmes de management de la sûreté –
Exigences (ISO 28000:2022)

Gesamtumfang 32 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Kontext der Organisation	13
4.1 Verstehen der Organisation und ihres Kontextes	13
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	13
4.2.1 Allgemeines	13
4.2.2 Rechtliche, behördliche und andere Anforderungen	14
4.2.3 Grundsätze	14
4.3 Festlegen des Anwendungsbereichs des Sicherheitsmanagementsystems	16
4.4 Sicherheitsmanagementsystem	17
5 Führung	17
5.1 Führung und Verpflichtung	17
5.2 Verbindliche Sicherheitsleitlinie	17
5.2.1 Festlegung der verbindlichen Sicherheitsleitlinie	17
5.2.2 Anforderungen an die verbindliche Sicherheitsleitlinie	18
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	18
6 Planung	18
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	18
6.1.1 Allgemeines	18
6.1.2 Bestimmung von sicherheitsbezogenen Risiken und Identifizierung von Chancen	19
6.1.3 Befassung mit sicherheitsbezogenen Risiken und Nutzung von Chancen	19
6.2 Sicherheitsziele und Planung zu deren Erreichung	20
6.2.1 Festlegung von Sicherheitszielen	20
6.2.2 Bestimmung von Sicherheitszielen	20
6.3 Planung von Änderungen	20
7 Unterstützung	21
7.1 Ressourcen	21
7.2 Kompetenz	21
7.3 Bewusstsein	21
7.4 Kommunikation	21
7.5 Dokumentierte Information	22
7.5.1 Allgemeines	22
7.5.2 Dokumentierte Informationen erstellen und aktualisieren	22
7.5.3 Kontrolle von dokumentierter Information	22
8 Betrieb	23
8.1 Betriebliche Planung und Steuerung	23
8.2 Identifikation von Prozessen und Aktivitäten	23
8.3 Risikobewertung und -behandlung	23
8.4 Steuerung	24
8.5 Sicherheitsstrategien, -verfahren, -prozesse und -behandlungen	24
8.5.1 Identifikation und Auswahl der Strategien und Behandlungen	24
8.5.2 Festlegen des Ressourcenbedarfs	25
8.5.3 Umsetzung von Behandlungen	25
8.6 Sicherheitspläne	25
8.6.1 Allgemeines	25
8.6.2 Reaktionsstruktur	25

8.6.3 Warnung und Kommunikation 26

8.6.4 Inhalt der Sicherheitspläne 26

8.6.5 Wiederherstellung 27

9 Bewertung der Leistung 28

9.1 Überwachung, Messung, Analyse und Bewertung 28

9.2 Internes Audit 28

9.2.1 Allgemeines 28

9.2.2 Internes Auditprogramm 28

9.3 Managementbewertung 29

9.3.1 Allgemeines 29

9.3.2 Eingaben für die Managementbewertung 29

9.3.3 Ergebnisse der Managementbewertung 30

10 Verbesserung 30

10.1 Fortlaufende Verbesserung 30

10.2 Nichtkonformität und Korrekturmaßnahmen 30

Literaturhinweise 32

Bilder

Bild 1 — PDCA-Modell, angewandt auf das Sicherheitsmanagementsystem 9

Bild 2 — Grundsätze 15

Tabellen

Tabelle 1 — Erläuterung des PDCA-Modells 8

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO 28000:2022, die vom Technischen Komitee ISO/TC 292 „Security and Resilience“ erarbeitet wurde, dessen Sekretariat von SIS (Schweiden) gehalten wird. Das internationale Dokument ist unverändert in diese Norm übernommen worden.

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

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

Dieser Text wurde mithilfe der von ISO eingeführten Grundstruktur für Managementsystemnormen („Harmonized Structure“) erarbeitet, welche in *ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2021, Procedures specific to ISO, Annex SL, Appendix 2*, festgelegt ist. Mit der Grundstruktur für Managementsystemnormen wird das Ziel verfolgt, Normen mit einheitlicher Struktur mit identischen Abschnittsnummern, Abschnittstiteln und gemeinsamen Benennungen und Basisdefinitionen zur Verfügung zu stellen.

Hinweise zur Übersetzung:

Diese Übersetzung von ISO 28000 als DIN ISO 28000 folgt dem Technischen Report DIN/TR 36601:2023-02, welcher die Übersetzung der ISO Harmonized Structure ins Deutsche festlegt. Die deutsche Übersetzung der Grundstruktur wurde zwischen Deutschland, Österreich und der Schweiz abgestimmt und wird für alle Übersetzungen von Managementsystemnormen, die vollständig oder teilweise der ISO-Grundstruktur folgen, angewendet. Ausnahmen bestehen in DIN ISO 28000 da, wo ISO 28000 von der Harmonized Structure abweicht und beim Begriff „Politik“ (3.6), dem die zweite Vorzugsbenennung „verbindliche Leitlinie“ hinzugefügt wurde.

Für die in diesem Dokument zitierten internationalen 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 19011	siehe	DIN EN ISO 19011
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:

- ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2021, Procedures specific to ISO, Annex SL, Appendix 2*, in der Fassung von 2021 eingehalten; die Übersetzungen der ISO Harmonized Structure aus dem Technischen Report DIN/TR 36601:2023-02 wurden angewendet;
- 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;
 - Sicherheitsplänen;
- d) Norm redaktionell überarbeitet.

Frühere Ausgaben

DIN ISO 28000: 2015-08

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

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

DIN EN ISO 19011, *Leitfaden zur Auditierung von Managementsystemen*

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

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*

ISO 10241-2:2012, *Terminological entries in standards — Part 2: Adoption of standardized terminological
entries*

DIN/TR 36601:2023-02, *Harmonisierte Struktur für Managementsystemnormen mit Anleitung zur Anwendung
(ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2021, Procedures specific to ISO, Annex SL, Appendix 2)*

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 sicherzustellen, die die vorherige Ausgabe verwenden. Die wesentlichen Änderungen sind folgende:

- 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;
 - Sicherheitsplänen.

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 folgendes von der Organisation:

- Bewerten der Sicherheitsumgebung, in der sie arbeitet, einschließlich ihrer Lieferkette (einschließlich Abhängigkeiten und Wechselbeziehungen);
- Feststellen, ob angemessene Sicherheitsmaßnahmen vorhanden sind, um sicherheitsbezogene Risiken effektiv zu behandeln;
- Einhalten von gesetzlichen, behördlichen und freiwilligen Verpflichtungen, denen sich die Organisation unterwirft;
- Anpassen von Sicherheitsprozessen und -steuerungen, einschließlich der relevanten vor- und nachgelagerten Prozesse und Kontrollen der Lieferkette, um die Ziele der Organisation 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, siehe Tabelle 1 und Bild 1.

Tabelle 1 — Erläuterung des PDCA-Modells

Planen (Einführen)	Einführen von verbindlichen Sicherheitsleitlinien, Sicherheitszielen, -vorgaben, -kontrollen, -prozessen und -verfahren, die für die Verbesserung der Sicherheit relevant sind, um Ergebnisse zu erzielen, die sich mit der übergeordneten Unternehmensgrundsätzen und Zielen der Organisation in Übereinstimmung befinden.
Durchführen (Umsetzen und Betreiben)	Umsetzen und Betreiben der verbindlichen Sicherheitsleitlinie, -sowie der Sicherheitskontrollen, -prozesse und -verfahren.

Tabelle 1 (fortgesetzt)

Prüfen (Überwachen und Überprüfen)	Überwachen und Überprüfen der Leistung vor dem Hintergrund der verbindlichen Sicherheitsleitlinie und den Sicherheitszielen, Berichten der Ergebnisse an die Leitung zum Zweck der Überprüfung, Festlegung und Autorisierung von Maßnahmen zur Korrektur und Verbesserung.
Handeln (Aufrechterhalten und Verbessern)	Aufrechterhalten und Verbessern des Sicherheitsmanagementsystems durch die Ergreifung von Korrekturmaßnahmen, basierend auf den Ergebnissen der Managementbewertung und der Neubewertung des Anwendungsbereichs des Sicherheitsmanagementsystems sowie der verbindlichen Sicherheitsleitlinie und der Sicherheitsziele.

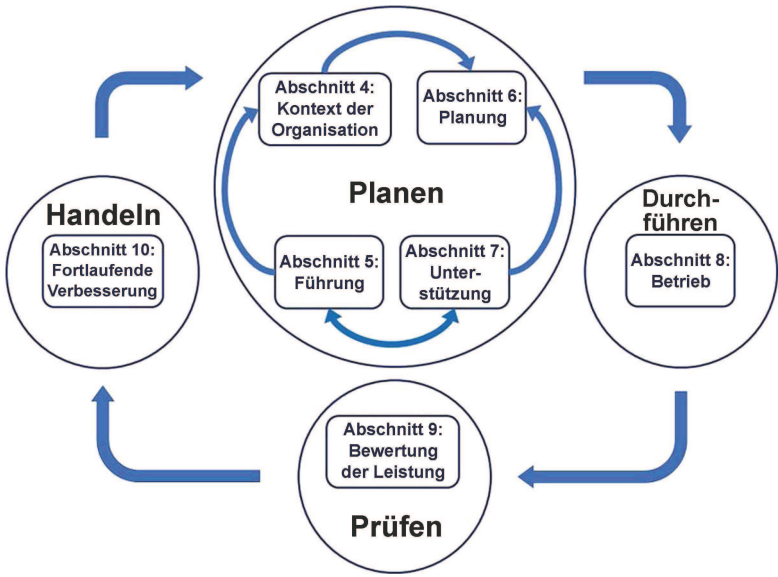


Bild 1 — PDCA-Modell, angewandt auf das Sicherheitsmanagementsystem

Dies stellt eine gewisse Übereinstimmung mit anderen Managementsystem-Normen, wie z. B. ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001 usw. sicher, wodurch die konsistente und integrierte Umsetzung und der Betrieb mit verwandten Managementsystemen unterstützt wird.

Für Organisationen, die dies wünschen, kann die Konformität des Sicherheitsmanagementsystems mit diesem Dokument durch einen externen oder internen Audit-Prozess verifiziert werden.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen für ein Sicherheitsmanagementsystem fest, einschließlich der für die Lieferkette relevanten Aspekte.

Dieses Dokument ist für alle Arten und Größen von Organisationen anwendbar (z. B. kommerzielle Unternehmen, staatliche oder andere öffentliche Einrichtungen und gemeinnützige Organisationen), die beabsichtigen, ein Sicherheitsmanagementsystem einzurichten, zu implementieren, aufrechtzuerhalten und zu verbessern. Es bietet einen ganzheitlichen und allgemeinen Ansatz und ist nicht branchen- oder sektorspezifisch.

Dieses Dokument kann während der gesamten Lebensdauer der Organisation genutzt und auf alle internen oder externen Aktivitäten auf allen Ebenen angewendet werden.

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 22300, *Security and resilience — Vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 22300 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

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.7) zu erreichen

Anmerkung 1 zum Begriff: Der Begriff einer Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

Anmerkung 2 zum Begriff: Wenn die Organisation Teil einer größeren Einheit ist, bezieht sich die Benennung „Organisation“ nur auf den Teil der größeren Einheit, der im Anwendungsbereich des *Sicherheitsmanagementsystems* (3.5) liegt.

3.2

interessierte Partei

Anspruchsgruppe

Person oder *Organisation* (3.1), die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon betroffen ist, oder die sich davon betroffen fühlt

3.3

oberste Leitung

Person oder Personengruppe, die eine *Organisation* (3.1) auf der obersten Ebene führt und steuert

Anmerkung 1 zum Begriff: Die oberste Leitung hat die Macht innerhalb der Organisation Befugnisse zu delegieren und Ressourcen bereitzustellen.