

DIN ISO 28000



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 Saathöfener 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

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Kontext der Organisation	12
4.1 Verstehen der Organisation und ihres Kontextes	12
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	12
4.2.1 Allgemeines	12
4.2.2 Rechtliche, gesetzliche und andere behördliche Sicherheitsanforderungen	13
4.2.3 Grundsätze	13
4.3 Festlegen des Anwendungsbereichs des Sicherheitsmanagementsystems	15
4.4 Sicherheitsmanagementsystem	16
5 Führung	16
5.1 Führung und Verpflichtung	16
5.2 Leitlinien	16
5.2.1 Festlegung der Sicherheitsleitlinien	16
5.2.2 Anforderungen an die Sicherheitsleitlinien	17
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	17
6 Planung	17
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	17
6.1.1 Allgemeines	17
6.1.2 Bestimmung von Sicherheitsrisiken und Identifizierung von Möglichkeiten	18
6.1.3 Bestimmung von Sicherheitsrisiken und Nutzung von Möglichkeiten	18
6.2 Sicherheitsziele und Planung zu deren Erreichung	19
6.2.1 Festlegung von Sicherheitszielen	19
6.2.2 Bestimmung von Sicherheitszielen	19
6.3 Planung von Änderungen am Sicherheitsmanagementsystem	19
7 Unterstützung	20
7.1 Ressourcen	20
7.2 Kompetenz	20
7.3 Bewusstsein	20
7.4 Kommunikation	20
7.5 Dokumentierte Information	21
7.5.1 Allgemeines	21
7.5.2 Erstellen und Aktualisieren	21
7.5.3 Kontrolle	21
8 Betrieb	22
8.1 Betriebliche Planung und Steuerung	22
8.2 Identifikation von Prozessen und Aktivitäten	22
8.3 Risikobewertung und -behandlung	23
8.4 Kontrollen	23
8.5 Sicherheitsstrategien, -verfahren, -prozesse und -behandlungen	23
8.5.1 Identifikation und Auswahl der Strategien und Behandlungen	23
8.5.2 Festlegen des Ressourcenbedarfs	24
8.5.3 Umsetzung von Behandlungen	24
8.6 Sicherheitspläne	24
8.6.1 Allgemeines	24
8.6.2 Reaktionsstruktur	24

8.6.3	Warnung und Kommunikation	25
8.6.4	Inhalt des Sicherheitsplans	26
8.6.5	Wiederherstellung	27
9	Bewertung der Leistung	27
9.1	Überwachung, Messung, Analyse und Bewertung	27
9.2	Internes Audit	27
9.2.1	Durchführen interner Audits	27
9.2.2	Auditprogramm	27
9.3	Managementbewertung	28
9.3.1	Allgemeines	28
9.3.2	Ergebnisse der Managementbewertung	28
9.3.3	Eingaben für die Managementbewertung	28
10	Verbesserung	29
10.1	Nichtkonformität und Korrekturmaßnahmen	29
10.2	Fortlaufende Verbesserung	30
	Literaturhinweise	31

Bilder

Bild 1 — PDCA-Modell, angewandt auf das Sicherheitsmanagementsystem	8
Bild 2 — Grundsätze	14

Tabellen

Tabelle 1 — Erläuterung des PDCA-Modells	7
--	---

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 beigelegt. 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.
-----------------------	---

Tabelle 1 (fortgesetzt)

Durchführen (Umsetzen und Betreiben)	Umsetzen und Betreiben der Sicherheitsleitlinie, -kontrollen, -prozesse und -verfahren.
Prüfen (Überwachen und Überprüfen)	Überwachen und Überprüfen der Leistung vor dem Hintergrund von Sicherheitsleitlinie und -zielen, 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 (SMS) durch die Ergreifung von Korrekturmaßnahmen, basierend auf den Ergebnissen der Managementbewertung und der Neubewertung des Anwendungsbereichs des SMS sowie der Sicherheitsleitlinie und -ziele.

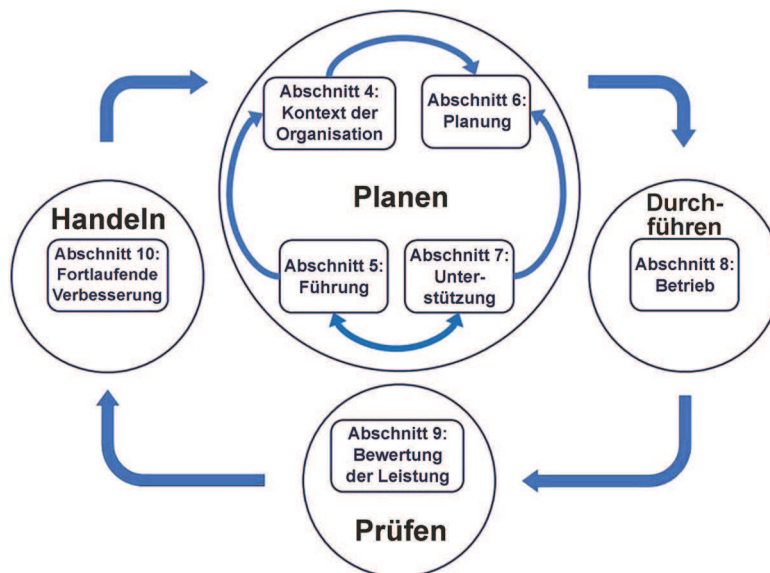


Bild 1 — PDCA-Modell, angewandt auf das Sicherheitsmanagementsystem

Dies gewährleistet eine gewisse Übereinstimmung mit anderen Managementsystem-Normen, wie z. B. ISO 9001, Quality management systems — Requirements, ISO 14001, Environmental management systems — Requirements with guidance for use, ISO 22301, Security and resilience — Business continuity management systems — Requirements, ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirement, ISO 45001, Occupational health and safety management systems — Requirements with guidance for use, usw., wodurch die konsistente und integrierte Umsetzung und der Betrieb mit verwandten Managementsystemen unterstützt wird.

Die Einhaltung einer Internationalen Norm verleiht an sich keine Immunität hinsichtlich rechtlicher Pflichten. Für Organisationen, die dies wünschen, kann die Einhaltung des Sicherheitsmanagementsystems dieser Internationalen Norm durch einen externen oder internen Audit-Prozess verifiziert werden.

1 Anwendungsbereich

Diese Internationale Norm 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 gemeinsamen Ansatz und ist nicht branchen- oder sektorspezifisch.

Dieses Dokument kann während der gesamten Lebensdauer der Organisation genutzt und auf alle internen und externen Aktivitäten 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*

ISO 31000, *Risk management — Guidelines*

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 <http://www.electropedia.org/>

3.1

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.8) zu erreichen

Anmerkung 1 zum Begriff: Der Begriff 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.

3.2

interessierte Partei (bevorzugter Begriff)

Anspruchsgruppe (zulässige Benennung)

Person oder *Organisation* (3.1), die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann, oder die sich davon beeinflusst fühlen kann

3.3

Anforderung

Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist

Anmerkung 1 zum Begriff: „Üblicherweise vorausgesetzt“ bedeutet, dass es für die Organisation und andere interessierte Parteien übliche oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt wird.

Anmerkung 2 zum Begriff: Eine festgelegte Anforderung ist eine, die z. B. in dokumentierter Information enthalten ist.

3.4

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.1), um *Leitlinien* (3.7), *Ziele* (3.8) und *Prozesse* (3.12) zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln.

Anmerkung 2 zum Begriff: Die Elemente des Systems beinhalten die Struktur der Organisation, Rollen und Verantwortlichkeiten, Planung sowie Betrieb.

Anmerkung 3 zum Begriff: Der Anwendungsbereich eines Managementsystems kann die ganze Organisation bestimmte Funktionen der Organisation, bestimmte Bereiche der Organisation oder eine oder mehrere Funktionen über eine Gruppe von Organisationen hinweg umfassen.

3.5

oberste Leitung

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

Anmerkung 1 zum Begriff: Die oberste Leitung ist innerhalb der Organisation in der Lage, Verantwortung zu delegieren und Ressourcen bereitzustellen.

Anmerkung 2 zum Begriff: Wenn der Anwendungsbereich des *Managementsystems* (3.4) nur einen Teil einer Organisation umfasst, bezieht sich „oberste Leitung“ auf diejenigen, die diesen Teil führen und steuern.

3.6

Wirksamkeit

Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden

3.7

Leitlinie

Absichten und Ausrichtung einer *Organisation* (3.1), wie sie von der *obersten Leitung* (3.5) formell ausgedrückt sind

3.8

Ziel

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Ein Ziel kann strategisch, taktisch oder operativ sein.

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen beziehen (z. B. Finanz-, Gesundheits- und Sicherheits- und Umweltziele) und auf verschiedenen Ebenen gelten (z. B. strategisch, organisationsweit, Projekt, Produkt und *Prozess* (3.12)).

Anmerkung 3 zum Begriff: Ein Ziel kann auf andere Weise ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, als Zweck, als betriebliches Kriterium, als Sicherheitsziel oder durch die Verwendung anderer Wörter mit ähnlicher Bedeutung (en: aim, goal, target).

Anmerkung 4 zum Begriff: Im Kontext von Sicherheitsmanagementsystemen werden Sicherheitsziele von Organisationen im Einklang mit ihren Sicherheitsleitlinien gesetzt, um bestimmte Ergebnisse zu erreichen.

3.9

Risiko

Auswirkung von Unsicherheit auf Ziele

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten. Sie kann positiv, negativ oder beides sein und Möglichkeiten und Bedrohungen ansprechen, schaffen oder zu ihnen führen.

Anmerkung 2 zum Begriff: Ziele können unterschiedliche Aspekte und Kategorien haben und auf verschiedenen Ebenen angewendet werden.

Anmerkung 3 zum Begriff: Das Risiko wird üblicherweise anhand der Risikoquellen, der potenziellen Ereignisse, ihrer Folgen und ihrer Wahrscheinlichkeit dargestellt.

3.10

Kompetenz

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

3.11

dokumentierte Information

Information, die von einer *Organisation* (3.1) gelenkt und aufrechterhalten werden muss, und das Medium, auf dem sie enthalten ist

Anmerkung 1 zum Begriff: Dokumentierte Information kann in jeglichem Format oder Medium vorliegen sowie aus jeglicher Quelle stammen.

Anmerkung 2 zum Begriff: Dokumentierte Information kann sich beziehen auf:

- das *Managementsystem* (3.4), einschließlich damit verbundener *Prozesse* (3.12);
- Informationen, die für den Betrieb der *Organisation* (3.1) geschaffen wurden (Dokumentation);
- Nachweise erreichter Ergebnisse (Aufzeichnungen).

[QUELLE: ISO/IEC 27000, 3.19]

3.12

Prozess

Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

3.13

Leistung

messbares Ergebnis

Anmerkung 1 zum Begriff: Leistung kann sich entweder auf quantitative oder qualitative Feststellungen beziehen.

Anmerkung 2 zum Begriff: Leistung kann sich auf das Führen und Steuern von Tätigkeiten, *Prozessen* (3.12), Produkten (einschließlich Dienstleistungen), Systemen oder *Organisationen* (3.1) beziehen.

3.14

ausgliedern (Verb)

Treffen einer Vereinbarung, bei der eine externe *Organisation* (3.1) einen Teil einer Funktion oder eines *Prozesses* (3.12) einer Organisation wahrnimmt bzw. durchführt

Anmerkung 1 zum Begriff: Eine externe Organisation befindet sich außerhalb des Anwendungsbereichs des *Managementsystems* (3.4), obwohl die ausgegliederte Funktion oder der ausgegliederte Prozess im Rahmen des Anwendungsbereichs liegen.

3.15

Überwachung

Bestimmung des Zustands eines Systems, eines *Prozesses* (3.12) oder einer Tätigkeit

Anmerkung 1 zum Begriff: Zur Bestimmung des Zustands kann es erforderlich sein, zu prüfen, zu beaufsichtigen oder kritisch zu beobachten.

3.16

Messung

Prozess (3.12) zum Bestimmen eines Wertes

3.17

Audit

systematischer, unabhängiger und dokumentierter *Prozess* (3.12) zum Erlangen von Auditnachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit Auditkriterien erfüllt sind

Anmerkung 1 zum Begriff: Ein Audit kann ein internes Audit (Erstparteien-Audit) oder externes Audit (Zweit- oder Drittparteien-Audit) sein und es kann ein kombiniertes Audit sein (Verbindung zweier oder mehrerer Disziplinen).

Anmerkung 2 zum Begriff: Ein internes Audit wird von der Organisation selbst durchgeführt, oder von einer externen Stelle in ihrem Auftrag.

Anmerkung 3 zum Begriff: „Auditnachweis“ und „Auditkriterium“ sind in ISO 19011 definiert.

3.18

Konformität

Erfüllung einer *Anforderung* (3.3)

3.19

Nichtkonformität

Nichterfüllung einer *Anforderung* (3.3)

3.20

Korrekturmaßnahme

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.19) und zum Verhindern des erneuten Auftretens

3.21

fortlaufende Verbesserung

wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.13)

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Sicherheitsmanagementsystems zu erreichen.

4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien

4.2.1 Allgemeines

Die Organisation muss

- die interessierten Parteien, die für ihr Sicherheitsmanagementsystem relevant sind,
- die relevanten Anforderungen dieser interessierten Parteien

bestimmen.

4.2.2 Rechtliche, gesetzliche und andere behördliche Sicherheitsanforderungen

Die Organisation muss:

- a) einen Prozess umsetzen und aufrechterhalten, um die geltenden rechtlichen und behördlichen Anforderungen in Bezug auf die Sicherheit zu ermitteln, und Zugang zu diesen rechtlichen und behördlichen Anforderungen erhalten und diese bewerten;
- b) sicherstellen, dass diese anzuwendenden rechtlichen, behördlichen und anderen Anforderungen bei der Umsetzung und Aufrechterhaltung ihres Sicherheitsmanagements berücksichtigt werden;
- c) diese Informationen dokumentieren und auf dem aktuellen Stand halten; und
- d) diese Informationen gegenüber relevanten interessierten Parteien kommunizieren.

4.2.3 Grundsätze

4.2.3.1 Allgemeines

Der Zweck des Sicherheitsmanagements innerhalb der Organisation ist die Erschaffung und insbesondere der Schutz von Wert.

Die Organisation sollte die folgenden Grundsätze anwenden:



Bild 2 — Grundsätze

4.2.3.2 Führung

Führungskräfte auf allen Ebenen sollten einen einheitlichen Zweck und eine einheitliche Richtung festlegen und Bedingungen schaffen, um die Strategien, Leitlinien, Prozesse und Ressourcen der Organisation auf das Erreichen ihrer Ziele auszurichten. Abschnitt 5 über Führung erläutert die Anforderungen in Bezug auf dieses Prinzip.

4.2.3.3 Strukturierter und umfassender Prozessansatz basierend auf den besten verfügbaren Informationen

Eine strukturierte und umfassende Herangehensweise an das Sicherheitsmanagement einschließlich der Lieferkette muss zu konsistenten und vergleichbaren Ergebnissen beitragen, die effektiver und effizienter erreicht werden, wenn Aktivitäten verstanden und als zusammenhängende, als kohärentes System funktionierende Prozesse verstanden werden.

4.2.3.4 Individuelle Anpassung

Das Sicherheitsmanagementsystem sollte an den externen und internen Zusammenhang und an die Bedürfnisse einer Organisation individuell angepasst und diesen angemessen sowie mit den Zielen der Organisation verbunden sein

4.2.3.5 Einbeziehung von Personen

Die Organisation sollte interessierte Parteien angemessen und rechtzeitig einbeziehen und deren Kenntnisse, Ansichten und Wahrnehmungen angemessen berücksichtigen, um das Bewusstsein für ein informiertes Sicherheitsmanagement zu verbessern und es zu erleichtern. Die Organisation sollte sicherstellen, dass jeder auf allen Ebenen respektiert und einbezogen wird.

4.2.3.6 Integrierter Ansatz

Das Sicherheitsmanagement ist ein integraler Bestandteil aller Aktivitäten einer Organisation. Es sollte mit allen anderen Managementsystemen der Organisation integriert werden.

Das Risikomanagement der Organisation – ob formell, informell oder intuitiv – sollte in das Sicherheitsmanagementsystem integriert werden.

4.2.3.7 Dynamische und fortlaufende Verbesserung

Die Organisation sollte einen Fokus fortlaufend auf Verbesserung durch Lernen und Erfahrung richten, um das Leistungsniveau zu halten, auf Veränderungen zu reagieren und neue Möglichkeiten zu schaffen, wenn sich der externe und interne Kontext der Organisation ändert.

4.2.3.8 Berücksichtigen menschlicher und kultureller Faktoren

Das menschliche Verhalten und kulturelle Faktoren haben einen wesentlichen Einfluss auf alle Aspekte des Sicherheitsmanagements und sollten auf allen Ebenen und in jeder Phase berücksichtigt werden. Entscheidungen sollten auf der Analyse und Bewertung von Daten und Informationen basieren, um sicherzustellen, dass sie zu mehr Objektivität und Vertrauen in die Entscheidungsfindung führen und mit größerer Wahrscheinlichkeit zu den gewünschten Ergebnissen führen. Individuelle Wahrnehmungen sollten berücksichtigt werden.

4.2.3.9 Beziehungsmanagement

Für nachhaltigen Erfolg sollte die Organisation ihre Beziehungen zu allen relevanten interessierten Parteien pflegen, da sie die Leistung der Organisation beeinflussen könnten.

4.3 Festlegen des Anwendungsbereichs des Sicherheitsmanagementsystems

Die Organisation muss die Grenzen und die Anwendbarkeit des Sicherheitsmanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.

Bei der Festlegung des Anwendungsbereichs muss die Organisation

- die unter 4.1 aufgeführten externen und internen Themen,
- die unter 4.2 aufgeführten Anforderungen

berücksichtigen.

Der Anwendungsbereich muss als dokumentierte Information verfügbar sein.

Wenn sich eine Organisation für einen Prozess entscheidet, der die Konformität mit ihrem Sicherheitsmanagementsystem beeinflusst, muss die Organisation die Kontrolle derartiger Prozesse sicherstellen. Die notwendi-

gen Kontrollen für derartige ausgegliederte Prozesse und die Verantwortlichkeiten für diese müssen im Sicherheitsmanagementsystem festgelegt sein.

4.4 Sicherheitsmanagementsystem

Die Organisation muss entsprechend den Anforderungen dieses Dokuments ein Sicherheitsmanagementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihren Wechselwirkungen.

5 Führung

5.1 Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das Sicherheitsmanagementsystem Führung und Verpflichtung zeigen, indem sie:

- sicherstellt, dass die Sicherheitsleitlinie und die Sicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind;
- sicherstellt, dass die Anforderungen und Erwartungen der interessierten Parteien der Organisation festgelegt und überwacht werden und dass angemessene und rechtzeitige Maßnahmen ergriffen werden, um diese Erwartungen zu erfüllen, wobei die Integration der Anforderungen an das Sicherheitsmanagementsystem in die Geschäftsprozesse der Organisation sichergestellt wird;
- sicherstellt, dass die für das Sicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;
- die Bedeutung eines wirksamen Sicherheitsmanagements sowie die Wichtigkeit der Erfüllung der Anforderungen des Sicherheitsmanagements vermittelt;
- sicherstellt, dass das Sicherheitsmanagementsystem sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt;
- sicherstellt, dass die Ziele, Einzelziele und Programme des Sicherheitsmanagements realisierbar sind;
- sicherstellt, dass jegliche von anderen Teilen der Organisation entwickelten Programme das Sicherheitsmanagementsystem ergänzen;
- Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Sicherheitsmanagementsystems beitragen können;
- die fortlaufende Verbesserung des Sicherheitsmanagementsystems der Organisation fördert; und
- andere relevante Führungskräfte unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen.

ANMERKUNG Wenn in diesem Dokument das Wort „Geschäft“ (en: business) verwendet wird, kann dieses im weiteren Sinne verstanden werden und bezieht sich auf Tätigkeiten, die für den Zweck der Organisation bzw. deren Existenz entscheidend sind.

5.2 Leitlinien

5.2.1 Festlegung der Sicherheitsleitlinien

Die oberste Leitung muss eine Sicherheitsleitlinie vorgeben, die:

- a) für den Zweck der Organisation angemessen ist;

- b) einen Rahmen zum Festlegen von Sicherheitszielen bietet;
- c) eine Verpflichtung zur Erfüllung anwendbarer Anforderungen enthält;
- d) eine Verpflichtung zur fortlaufenden Verbesserung des Sicherheitsmanagementsystems enthält; und
- e) die negative Auswirkung berücksichtigt, die die Leitlinie, Ziele, Einzelziele, Programme usw. zum Sicherheitsmanagement auf andere Aspekte der Organisation haben kann.

5.2.2 Anforderungen an die Sicherheitsleitlinien

Die Sicherheitsleitlinien muss:

- mit anderen Leitlinien der Organisation im Einklang stehen;
- mit der allgemeinen Bewertung der Sicherheitsrisiken des Unternehmens im Einklang stehen;
- ihre Prüfung im Falle einer Übernahme von oder einer Fusion mit anderen Organisationen, oder anderer Änderungen des Geschäftsrahmens der Organisation vorsehen, die das Fortbestehen oder die Relevanz des Sicherheitsmanagementsystems beeinflussen können;
- die primäre Rechenschaftspflicht und Verantwortlichkeit für Ergebnisse beschreiben und zuweisen;
- als dokumentierte Information verfügbar sein;
- innerhalb der Organisation bekanntgemacht werden;
- für interessierte Parteien verfügbar sein, soweit angemessen.

ANMERKUNG Organisationen können sich für eine detaillierte Sicherheitsmanagement-Leitlinie für den internen Gebrauch entscheiden, die ausreichend Informationen und Leitung bietet, um das Sicherheitsmanagementsystem (von dem Teile vertraulich sein können) zu fördern und über eine zusammenfassende (nicht vertrauliche) Version zu verfügen, die zur Weitergabe an ihre Anspruchsgruppe und andere interessierte Parteien die allgemeinen Zielsetzungen umfasst.

5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für relevante Rollen zugewiesen und innerhalb der Organisation bekannt gemacht werden.

Die oberste Leitung muss die Verantwortlichkeit und Befugnis zuweisen für:

- a) das Sicherstellen, dass das Sicherheitsmanagementsystem die Anforderungen dieses Dokuments erfüllt;
- b) das Berichten an die oberste Leitung über die Leistung des Sicherheitsmanagementsystems.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten

6.1.1 Allgemeines

Bei Planungen für das Sicherheitsmanagementsystem muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie die Risiken und Möglichkeiten bestimmen, die behandelt werden müssen, um:

- sicherzustellen, dass das Sicherheitsmanagementsystem seine angestrebten Ergebnisse erzielen kann;

- unerwünschte Auswirkungen zu verhindern oder zu verringern;
- fortlaufende Verbesserung zu erreichen.

Die Organisation muss planen:

- a) Maßnahmen zum Umgang mit diesen Risiken und Möglichkeiten;
- b) wie:
 - die Maßnahmen in die Sicherheitsmanagementsystem-Prozesse der Organisation integriert und dort umgesetzt werden;
 - die Wirksamkeit dieser Maßnahmen bewertet wird.

ANMERKUNG Der Zweck des Risikomanagements ist die Erschaffung und der Schutz von Wert, und das Risikomanagement muss in das Sicherheitsmanagementsystem integriert werden. Risiken in Bezug auf die Sicherheit der Organisation und ihrer interessierten Parteien werden in 8.3 behandelt.

6.1.2 Bestimmung von Sicherheitsrisiken und Identifizierung von Möglichkeiten

Die Bestimmung von Sicherheitsrisiken und die Identifizierung und Nutzung von Möglichkeiten erfordert eine proaktive Risikobewertung, die folgende Punkte berücksichtigen sollte, ohne auf diese beschränkt zu sein:

- a) physische oder funktionale Ausfälle und böswillige oder kriminelle Handlungen;
- b) Umwelt-, menschliche und kulturelle Faktoren und andere interne oder externe Zusammenhänge, einschließlich Faktoren außerhalb der Kontrolle der Organisation, die die Sicherheit der Organisation beeinträchtigen;
- c) die Auslegung, Installation, Wartung und den Austausch von Sicherheitseinrichtungen;
- d) das Informations-, Daten-, Wissens- und Kommunikationsmanagement der Organisation;
- e) Informationen in Bezug auf Sicherheitsbedrohungen und Schwachstellen.

6.1.3 Bestimmung von Sicherheitsrisiken und Nutzung von Möglichkeiten

Die Bewertung der identifizierten Sicherheitsrisiken muss einen Beitrag leisten zu (ohne darauf beschränkt zu sein):

- a) dem gesamten Risikomanagement der Organisation;
- b) der Risikobehandlung;
- c) den Zielen des Sicherheitsmanagements;
- d) den Sicherheitsmanagement-Prozessen;
- e) der Auslegung, Spezifikation und Umsetzung des Sicherheitsmanagementsystems;
- f) der Bestimmung angemessener Ressourcen, einschließlich Personalbeständen; und
- g) der Identifikation von Schulungsbedarf und dem erforderlichen Kompetenzniveau.