DIN EN ISO/IEC 27000

DIN

ICS 01.040.03; 01.040.35; 03.100.70; 35.030

Entwurf

Einsprüche bis 2019-09-05
Vorgesehen als Ersatz für
DIN EN ISO/IEC 27000:2017-10

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche und Englische Fassung prEN ISO/IEC 27000:2019

Information technology –
Security techniques –
Information security management systems – Overview and vocabulary
(ISO/IEC 27000:2018);
German and English version prEN ISO/IEC 27000:2019

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire
(ISO/IEC 27000:2018);
Version allemande et anglaise prEN ISO/IEC 27000:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-07-05 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 nia@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 Informationstechnik und Anwendungen (NIA), 10772 Berlin, 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 73 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

Nationales Vorwort

Dieses Dokument (prEN ISO/IEC 27000:2018) wurde im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) vom NA 043-01-27 AA „IT-Sicherheitsverfahren“ erarbeitet.

Der Text von ISO/IEC 27000:2018 wurde von ISO/IEC JTC 1/SC 27 „Information security, cybersecurity and privacy protection“ der Internationalen Organisation für Normung (ISO) und der Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27000:2018 durch das Gemeinsame Technische Komitee CEN/CENELEC/JTC 13 „Cybersicherheit und Datenschutz“, dessen Sekretariat von DIN (Deutschland) gehalten wird, als Europäische Norm übernommen.

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.

Änderungen

Gegenüber DIN EN ISO/IEC 27000:2017-10 wurden folgende Änderungen vorgenommen:

a) die Einleitung wurde umformuliert;

b) einige Begriffe und Definitionen wurden entfernt;

c) Abschnitt 3 wurde auf die High-Level-Struktur für MSS ausgerichtet;

d) Abschnitt 5 wurde überarbeitet, um die Änderungen in den betrachteten Standards zu berücksichtigen;

e) Anhänge A und B wurden entfernt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

– Entwurf –

CEN/TC 13

Datum: 2019-06

prEN ISO/IEC 27000:2019

CEN/TC 13

Sekretariat:

Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie (ISO/IEC 27000:2018)

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité des informations — Vue d'ensemble et vocabulaire (ISO/IEC 27000:2018)

Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

Inhalt

Seite

Europäisches Vorwort 4

Vorwort 5

0 Einleitung 6
0.1 Überblick 6
0.2 Zweck dieser Internationalen Norm 6
0.3 Inhalt dieses Dokumentes 6

1 Anwendungsbereich 7

2 Normative Verweisungen 7

3 Begriffe 7

4 Managementsysteme für Informationssicherheit (ISMS) 20
4.1 Allgemeines 20
4.2 Was ist ein ISMS? 20
4.2.1 Überblick und Grundsätze 20
4.2.2 Informationen 21
4.2.3 Informationssicherheit 21
4.2.4 Management 22
4.2.5 Managementsystem 22
4.3 Prozessorientierter Ansatz 22
4.4 Warum ist ein ISMS wichtig? 22
4.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS 23
4.5.1 Übersicht 23
4.5.2 Identifizierung von Informationssicherheitsanforderungen 24
4.5.3 Beurteilung von Informationssicherheitsrisiken 24
4.5.4 Behandlung von Informationssicherheitsrisiken 25
4.5.5 Auswahl und Umsetzung von Maßnahmen 25
4.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS 26
4.5.7 Fortlaufende Verbesserung 26
4.6 Kritische Erfolgsfaktoren für das ISMS 27
4.7 Nutzen der ISMS-Normenfamilie 28

5 Die ISMS-Normenfamilie 28
5.1 Allgemeine Informationen 28
5.2 Normen, die einen Überblick geben und die Terminologie festlegen: ISO/IEC 27000 (dieses Dokument) 29
5.3 Normen, die Anforderungen festlegen 29
5.3.1 ISO/IEC 27001 29
5.3.2 ISO/IEC 27006 30
5.3.3 ISO/IEC 27009 30
5.4 Normen, die allgemeine Leitfäden beschreiben 31
5.4.1 ISO/IEC 27002 31
5.4.2 ISO/IEC 27003 31
5.4.3 ISO/IEC 27004 31
5.4.4 ISO/IEC 27005 31
5.4.5 ISO/IEC 27007 32
5.4.6 ISO/IEC TR 27008 32
5.4.7 ISO/IEC 27013 32

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

5.4.8 ISO/IEC 27014 33
5.4.9 ISO/IEC TR 27016 33
5.4.10 ISO/IEC FDIS 27021 33
5.5 Normen, die branchenspezifische Leitfäden beschreiben 34
5.5.1 ISO/IEC 27010 34
5.5.2 ISO/IEC 27011 34
5.5.3 ISO/IEC 27017 34
5.5.4 ISO/IEC 27018 35
5.5.5 ISO/IEC FDIS 27019 35
5.5.6 ISO 27799 36
Literaturhinweise 37

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

Europäisches Vorwort

Der Text von ISO/IEC 27000:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27000:2019 durch das Technische Komitee CEN/JTC 13 „Cybersecurity and data protection“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27000:2018 wurde von CEN als prEN ISO/IEC 27000:2019 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

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. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

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).

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).

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/IEC JTC 1, *Information technology,* Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* erarbeitet.

Diese fünfte Ausgabe ersetzt die vierte Ausgabe (ISO/IEC 27000:2016), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

— Die Einleitung wurde umformuliert;

— Einige Begriffe und Definitionen wurden entfernt;

— Abschnitt 3 wurde auf die high-Level Struktur für MSS ausgerichtet;

— Abschnitt 5 wurde überarbeitet um die Änderungen in den betrachteten Standards zu berücksichtigen;

— Anhänge A und B wurden entfernt.

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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

0 Einleitung

0.1 Überblick

Internationale Normen für Managementsysteme stellen ein Vorgehensmodell zum Einrichten und Betreiben eines Managementsystems zur Verfügung. Dieses Modell berücksichtigt die Merkmale, zu denen unter Experten auf dem Gebiet Konsens herrscht, dass diese Merkmale den internationalen Stand der Technik widerspiegeln. ISO/IEC JTC 1/SC 27 unterhält ein Expertengremium, dass sich der Entwicklung von Internationalen Managementsystemnormen für Informationssicherheit, auch bekannt als die Informationssicherheitsmanagementsystem (ISMS) Normenfamilie.

Durch den Einsatz der ISMS-Normenfamilie können Organisationen ein Rahmenwerk zur Handhabung der Sicherheit ihrer Informationswerte einschließlich Finanzinformationen, geistige Eigentumsrechte und Details zu Beschäftigten, oder der ihnen von Kunden oder Dritten anvertrauten Informationen, entwickeln und umsetzen. Diese Standards können auch eingesetzt werden, um eine unabhängige Beurteilung ihres zum Schutz von Informationen eingesetzten ISMS vorzubereiten.

0.2 Zweck dieser Internationalen Norm

Die ISMS-Normenfamilie beinhaltet Normen die:

a) Anforderungen an ein ISMS und an diejenigen, die solche Systeme zertifizieren, festlegen;

b) direkte Unterstützung, detaillierte Leitlinien und/oder Interpretationen für den Gesamtprozess zur Errichtung, Umsetzung, Aufrechterhaltung und Verbesserung eines ISMS anbieten;

c) sektorspezifische Leitlinien für ISMS adressieren; und

d) Konformitätsbewertung für ISMS adressieren.

0.3 Inhalt dieses Dokumentes

In diesem Dokument werden die folgenden Modalverben verwendet:

— „muss“ bezeichnet eine Anforderung

— „sollte“ bezeichnet eine Empfehlung

— „darf“ bezeichnet eine Erlaubnis

— „kann“ bezeichnet eine Möglichkeit oder Fähigkeit

Information, die als „Anmerkung“ gekennzeichnet ist, dient dem Verständnis oder der Klarstellung der dazugehörigen Anforderung. „Anmerkungen zum Begriff“, die in Abschnitt 3 verwendet werden, stellen zusätzliche Information bereit, welche die Terminologische Information ergänzen und Maßnahmen in Bezug zur Verwendung eines Begriffes enthalten können.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

1 Anwendungsbereich

Diese Internationale Norm stellt einen Überblick über Informationssicherheitsmanagementsysteme (ISMS) und Begriffe bereit, die in der ISMS-Normenfamilie üblicherweise verwendet werden. Diese Internationale Norm ist anwendbar für Organisationen aller Arten und Größe (z. B. gewerbliche Unternehmen, Behörden, Nicht-gewinnorientierte Unternehmen).

Die Begriffe und Definitionen, die mit diesem Dokumente bereitgestellt werden,

— decken die gebräuchlichen Begriffe und Definitionen ab, die in der ISMS Normenfamilie verwendet werden;

— deckt nicht sämtliche verwendete Begriffe innerhalb der ISMS Normenfamilie ab; und

— schränkt die Normen aus der ISMS Normenfamilie nicht darin ein neue Begriffe für die Anwendung zu definieren.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

— IEC Electropedia: verfügbar unter http://www.electropedia.org/

3.1
Zugangssteuerung
(en: access control)
Mittel um sicherzustellen, dass der Zugang zu Werten aufgrund von Geschäfts- und Sicherheits*anforderungen* (2.63) befugt und eingeschränkt ist

3.2
Angriff
(en: attack)
Versuch, einen Wert zu zerstören, aufzudecken, zu verändern, außer Funktion zu setzen, zu stehlen, zu diesem unbefugten Zugang zu erhalten oder diesen unbefugt zu verwenden

3.3
Audit
(en: audit)
systematischer, unabhängiger und dokumentierter *Prozess* (3.54) zum Erlangen von Auditnachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit die Auditkriterien erfüllt sind

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

Anmerkung 2 zum Begriff: „Auditnachweise“ und „Auditkriterien“ sind in ISO 19011 definiert.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

3.4
Auditumfang
(en: audit scope)
Ausmaß und Grenzen eines *Audits* (3.3)

[QUELLE: ISO 19011:2011, 3.14, modifiziert — Anmerkung 1 zum Begriff wurde gestrichen]

3.5
Authentisierung
(en: authentication)
Sicherstellung, dass die von einer Entität behaupteten Eigenschaften richtig sind

3.6
Authentizität
(en: authenticity)
Eigenschaft, dass eine Entität das ist, was sie angibt zu sein

3.7
Verfügbarkeit
(en: availability)
Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

3.8
Elementarmessgröße
(en: base measure)
Messgröße (2.42), die mittels eines Attributs und der Methode ihrer Quantifizierung definiert ist

Anmerkung 1 zum Begriff: Eine Elementarmessgröße ist funktional unabhängig von anderen Messgrößen (2.47)

[QUELLE: ISO/IEC 15939:2007, 2.3, modifiziert — Anmerkung 2 zum Begriff wurde gestrichen]

3.9
Kompetenz
(en: competence)
Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

3.10
Vertraulichkeit
(en: confidentiality)
Eigenschaft, dass Information unbefugten Personen, Entitäten oder *Prozessen* (3.54) nicht verfügbar gemacht oder offengelegt wird

3.11
Konformität
(en: conformity)
Erfüllung einer *Anforderung* (3.56)

3.12
Folge
(en: consequence)
Ergebnis eines *Ereignisses* (3.21), welches *Ziele* (3.49) beeinflusst

Anmerkung 1 zum Begriff: Ein Ereignis (2.25) kann eine Reihe von Folgen haben.

Anmerkung 2 zum Begriff: Eine Folge kann gewiss oder ungewiss sein und ist im Kontext von Informationssicherheit (2.33) in der Regel negativ.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

Anmerkung 3 zum Begriff: Folgen können qualitativ oder quantitativ beschrieben werden.

Anmerkung 4 zum Begriff: Ursprüngliche Folgen können sich durch Dominoeffekte verstärken.

[QUELLE: ISO Guide 73:2009, 3.6.1.3, modifiziert – Anmerkung 2 zum Begriff wurde nach dem „und" geändert]

3.13
fortlaufende Verbesserung
(en: continual improvement)
wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.52)

3.14
Maßnahme
(en: control)
Mittel zur Veränderung von *Risiken* (3.61)

Anmerkung 1 zum Begriff: Maßnahmen umfassen Prozesse (3.54), Richtlinien, Geräte, Methoden oder anderweitige Handlungen, die Risiken (3.61) verändern.

Anmerkung 2 zum Begriff: Maßnahmen haben nicht immer den erwünschten oder angenommenen Veränderungseffekt.

[QUELLE: ISO Guide 73:2009 3.8.1.1, modifiziert – Anmerkung 2 zum Begriff wurde geändert]

3.15
Maßnahmenziel
(en: control objective)
Beschreibung dessen, was als Ergebnis umgesetzter *Maßnahmen* (3.14) erzielt werden soll

3.16
Korrektur
(en: correction)
Maßnahme zum Beseitigen einer erkannten *Nichtkonformität* (3.47)

3.17
Korrekturmaßnahme
(en: corrective action)
Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.47) und zum Verhindern des erneuten Auftretens

3.18
abgeleitete Messgröße
(en: derived measure)
Messgröße (3.42), dies als Funktion von zwei oder mehr Werten von *Elementarmessgrößen* (3.8) definiert ist

[QUELLE: ISO/IEC 15939:2007, 2.8 modifiziert — Anmerkung 1 zum Begriff wurde gestrichen]

3.19
dokumentierte Information
(en: documented information)
Information, die von einer *Organisation* (3.50) 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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

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

— das *Managementsystem* (3.41), einschließlich damit verbundener *Prozesse* (3.54);

— Information, die für den Betrieb der *Organisation* (3.50) geschaffen wurden (Dokumentation);

— Nachweise erreichter Ergebnisse (Aufzeichnungen).

3.20
Wirksamkeit
(en: effectiveness)
Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden

3.21
Ereignis
(en: event)
Auftreten oder Veränderung einer bestimmten Menge von Umständen

Anmerkung 1 zum Begriff: Ein Ereignis kann aus einem oder mehreren Vorkommnissen bestehen und verschiedene Gründe haben.

Anmerkung 2 zum Begriff: Ein Ereignis kann darin bestehen, dass etwas nicht passiert,

Anmerkung 3 zum Begriff: Ein Ereignis wird manchmal „Vorfall“ oder „Zwischenfall“ genannt.

[QUELLE: ISO Guide 73:2009, 3.5.1.3, modifiziert — Anmerkung 4 zum Begriff wurde gestrichen]

3.22
externer Kontext
(en: external context)
externes Umfeld, in dem die Organisation versucht ihre *Ziele* (2.56) zu erreichen

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

— die kulturelle, soziale, politische, gesetzliche, regulatorische, finanzielle, technologische, ökonomische, natürliche und wettbewerbliche Umgebung, die internationalen, nationalen, regionalen oder lokalen Charakter haben kann;

— wesentliche Treiber und Trends, die sich auf die *Ziele* (2.56) der *Organisation* (2.57) auswirken;

— Beziehungen zu externen Stakeholdern[N1)] (2.82) sowie deren Auffassungen und Werte.

[QUELLE: ISO Guide 73:2009, 3.3.1.1]

3.23
Steuerung der Informationssicherheit
(en: governance of information security)
System, mittels dessen die Tätigkeiten einer *Organisation* (3.50), die auf Informationssicherheit (3.28) bezogen sind, geführt und überwacht werden

[N1)] Nationale Fußnote: In der ISO/IEC 27001 wird anstatt des Begriffes „Stakeholder“ durchgängig der Begriff „interessierte Partei“ verwendet.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

3.24
Steuerungsgremium
(en: governing body)
Person oder Personengruppe, welche die rechtliche Verantwortung für die *Leistung* (3.52) und Konformität der *Organisation* (3.50) trägt

Anmerkung 1 zum Begriff: Das Steuerungsgremium kann in einigen Rechtssystemen der Aufsichtsrat, der Verwaltungsrat oder der Vorstand sein.

3.25
Indikator
(en: indicator)
Messgröße (3.42), die eine Einschätzung oder Bewertung liefert

3.26
Informationsbedarf
(en: information need)
Verständnis, das erforderlich ist, um Ziele (3.49), Risiken oder Probleme zu handhaben

[QUELLE: ISO/IEC/IEEE 15939:2007, 3.12]

3.27
informationsverarbeitende Einrichtungen
(en: information processing facilities)
jedes informationsverarbeitende System, jeder informationsverarbeitende Dienst oder jede informationsverarbeitende Infrastruktur oder der physische Standort, der diese beherbergt

3.28
Informationssicherheit
(en: information security)
Aufrechterhaltung der *Vertraulichkeit* (3.10), *Integrität* (3.36) und *Verfügbarkeit* (3.7) von Information

Anmerkung 1 zum Begriff: Zusätzlich können auch andere Eigenschaften wie *Authentizität* (3.6), Zurechenbarkeit, *Nichtabstreitbarkeit* (3.48) und *Verlässlichkeit* (3.55) einbezogen werden.

3.29
Aufrechterhaltung der Informationssicherheit
(en: information security continuity)
Prozesse (3.54) und Verfahren, zur Sicherstellung, dass Tätigkeiten beständig durchgeführt werden, welche die *Informationssicherheit* (3.28) fördern

3.30
Informationssicherheitsereignis
(en: information security event)
erkanntes Auftreten eines Zustands eines Systems, Dienstes oder Netzwerks, der eine mögliche Verletzung der *Informationssicherheitspolitik* (3.53) oder die Unwirksamkeit von *Maßnahmen* (3.14) oder eine vorher nicht bekannte Situation, die sicherheitsrelevant sein kann, anzeigt

3.31
Informationssicherheitsvorfall
(en: information security incident)
einzelnes ungewolltes oder unerwartetes *Informationssicherheitsereignis* (3.30) die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die *Informationssicherheit* (3.28) zu bedrohen

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

3.32
Handhabung von Informationssicherheitsvorfällen
(en: information security incident management)
Prozesse (3.54) zum Entdecken von, Berichten über, Bewerten von, Reagieren auf, Umgehen mit und Lernen aus *Informationssicherheitsvorfällen* (3.31)

3.33
Informationssicherheitsmanagementsystem Fachkraft
(en: information security management system professional)
Person, die einen oder mehrere Informationssicherheitsprozesse (3.54) einrichtet, umsetzt, aufrecht erhält und fortlaufend verbessert

3.34
informationsaustauschende Gemeinschaft
Gruppe von Organisationen (3.50), die sich darauf geeinigt haben Information miteinander zu teilen

Anmerkung 1 zum Begriff: Eine *Organisation* (2.57) kann auch eine Einzelperson sein.

3.35
Informationssystem
(en: information system)
Anwendungen, Dienste, informationstechnische Werte oder andere Information bearbeitende Komponenten

3.36
Integrität
(en: integrity)
Eigenschaft der Richtigkeit und Vollständigkeit

3.37
Interessierte Partei
(en: interested party)
Person oder *Organisation* (3.50), die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann, oder die sich davon beeinflusst fühlen kann

3.38
interner Kontext
(en: internal context)
interne Umgebung, innerhalb derer die *Organisation* (3.50) versucht ihre Ziele zu erreichen

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

- Steuerung durch die Unternehmensführung, Organisationsstruktur, Rollen und Verantwortlichkeiten;
- *Richtlinien* (3.53), *Ziele* (3.49) und Strategien, die in Kraft sind mit dem Ziel sie einzuhalten beziehungsweise sie zu erreichen;
- das Potenzial in Form von Ressourcen und Wissen (zum Beispiel Kapital, Zeit, Menschen, *Prozesse* (3.54), Systeme und Technologien);
- *Informationssysteme* (3.35), Informationsflüsse und *Prozesse* zur Entscheidungsfindung (sowohl formell als auch informell);
- Beziehungen zu internen intressierten Parteien (3.37) sowie deren Auffassungen und Werte;
- die Organisationskultur;
- Standards, Leitfäden und Modelle, die von der *Organisation* übernommen worden sind;
- Gestalt und Ausmaß vertraglicher Beziehungen.

[QUELLE: ISO Guide 73:2009, 3.3.1.2]

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

3.39
Risikoniveau
(en: level of risk)
Größe eines *Risikos* (3.61), das mittels einer Kombination von *Folgen* (3.12) und deren *Wahrscheinlichkeit* (3.40) ausgedrückt wird

[QUELLE: ISO Guide 73:2009, 3.6.1.8, modifiziert - „oder Kombination von Risiken“ wurde entfernt.]

3.40
Wahrscheinlichkeit
(en: likelihood)
Möglichkeit, dass etwas passiert

[QUELLE: ISO Guide 73:2009, 3.6.1.1, modifiziert – Anmerkungen 1 und 2 zum Begriff wurden gestrichen.]

3.41
Managementsystem
Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.50), um *Politiken* (3.53), *Ziele* (3.49) und *Prozesse* (3.54) 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, Betrieb, usw.

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.

3.42
Messgröße
(en: measure)
Variable, der ein Wert als Ergebnis einer *Messung* (3.43) zugeordnet wird,

[QUELLE: ISO/IEC/IEEE 15939:2017, 3.15, modifiziert – Anmerkung 2 zum Begriff wurde gelöscht]

3.43
Messung
(en: measurement)
Prozess (3.54) zum Bestimmen eines Wertes

3.44
Messfunktion
(en: measurement function)
Algorithmus oder Berechnung, der bzw. die zwei oder mehr *Elementarmessgrößen* (3.8) kombiniert

[QUELLE: ISO/IEC/IEE 15939:2017, 3.20]

3.45
Messmethode
(en: measurement method)
logische, generisch beschriebene Folge von Handlungen, die durchgeführt wird, um ein Attribut mit Bezug auf eine festgelegte Skala zu quantifizieren

Anmerkung 1 zum Begriff: Der Typ der Messmethode hängt von der Art der Handlungen ab, die durchgeführt werden, um ein Attribut zu quantifizieren. Zwei Typen lassen sich unterscheiden:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

— Subjektiv: Quantifizierung, die menschliches Ermessen einbezieht;

— Objektiv: Quantifizierung, die auf numerischen Regeln basiert.

[QUELLE: ISO/IEC 15939:2007, 2.22, modifiziert —Anmerkung 2 zum Begriff wurde gestrichen]

3.46
Überwachung
(en: monitoring)
Bestimmung des Zustands eines Systems, eines *Prozesses* (3.54) oder einer Tätigkeit

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

3.47
Nichtkonformität
(en: nonconformity)
Nichterfüllung einer *Anforderung* (3.56)

3.48
Nichtabstreitbarkeit
Fähigkeit, das Eintreten eines behaupteten *Ereignisses* (3.21) oder einer behaupteten Handlung samt ihren ursächlichen Entitäten nachzuweisen

3.49
Ziel
(en: objective)
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. finanzielle, gesundheits- und sicherheitsbezogene sowie umweltbezogene Ziele) und für verschiedene Ebenen gelten (z. B. strategische, organisationsweite, Projekt, Produkt und *Prozess* (3.54)).

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

Anmerkung 4 zum Begriff: Im Kontext von Informationssicherheitsmanagementsystemen werden Informationssicherheitsziele von Organisationen im Einklang mit ihrer Informationssicherheitspolitik gesetzt, um bestimmte Ergebnisse zu erreichen.

3.50
Organisation
(en: organization)
Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.49) zu erreichen

Anmerkung 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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

3.51
ausgliedern (Verb)
(en: outsource, verb)
eine Vereinbarung treffen, bei der eine externe *Organisation* (3.50) einen Teil einer Funktion oder eines *Prozesses* (3.54) einer *Organisation* (3.50) wahrnimmt bzw. durchführt

Anmerkung 1 zum Begriff: Eine externe Organisation befindet sich außerhalb des Anwendungsbereichs eines Managementsystems (3.41), obwohl die ausgegliederte Funktion oder der ausgegliederte Prozess (3.54) im Rahmen des Anwendungsbereichs liegen.

3.52
Leistung
(en: performance)
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* (3.54), Produkten (einschließlich Dienstleistungen), Systemen oder *Organisationen* (3.50) beziehen.

3.53
Politik
(en: policy)
Absichten und Ausrichtung einer *Organisation* (3.50), wie von der *obersten Leitung* (3.75) formell ausgedrückt

3.54
Prozess
(en: process)
Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

3.55
Verlässlichkeit
(en: reliablility)
Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

3.56
Anforderung
(en: requirement)
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 üblich oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt wird.

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

3.57
Restrisiko
(en: residual risk)
Risiko (3.61), das nach einer *Risikobehandlung* (3.72) verbleibt

Anmerkung 1 zum Begriff: Das Restrisiko kann nicht identifizierte Risiken beinhalten.

Anmerkung 2 zum Begriff: Das Restrisiko ist auch unter dem Namen „zurückbehaltenes Risiko“ bekannt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

3.58
Überprüfung
(en: review)
Tätigkeit, die durchgeführt wird, um die Eignung, Angemessenheit und *Wirksamkeit* (3.20) eines Gegenstands zu bestimmen, um festgelegte *Ziele* (3.49) zu erreichen

[QUELLE: ISO Guide 73:2009, 3.8.2.2, modifiziert – Anmerkung 1 zum Begriff wurde gestrichen]

3.59
Überprüfungsobjekt
(en: review object)
bestimmter Gegenstand, der überprüft wird

3.60
Ziel der Überprüfung
(en: review objective)
Aussage, die beschreibt, was als Ergebnis der *Überprüfung* (3.58) erreicht werden soll

3.61
Risiko
(en: risk)
Auswirkung von Ungewissheit auf Ziele (3.49)

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten – in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Information im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiko wird häufig durch Bezugnahme auf mögliche Ereignisse (wie in ISO Guide 73:2009, 3.5.1.3 definiert) und Folgen (wie in ISO Guide 73:2009, 3.6.1.3 definiert), oder eine Kombination beider charakterisiert.

Anmerkung 4 zum Begriff: Risiko wird oft häufig mittels der Folgen eines Ereignisses (einschließlich Veränderungen der Umstände) in Verbindung mit der Wahrscheinlichkeit (wie in ISO Guide 73:2009, 3.6.1.1 definiert) seines Eintretens beschrieben..

Anmerkung 5 zum Begriff: Im Kontext von Informationssicherheitsmanagementsystemen können Informationssicherheitsrisiken als Auswirkung von Ungewissheit auf Informationssicherheitsziele beschrieben werden.

Anmerkung 6 zum Begriff: Informationssicherheitsrisiko ist mit der Möglichkeit verbunden, dass Bedrohungen Schwachstellen eines Informationswerts oder einer Gruppe solcher Werte ausnutzen und damit einer Organisation Schaden zufügen.

3.62
Risikoakzeptanz
(en: risk acceptance)
fundierte Entscheidung ein bestimmtes *Risiko* (3.61) zu tragen

Anmerkung 1 zum Begriff: Risikoakzeptanz kann ohne *Risikobehandlung* (3.72) oder während des Risikobehandlungsprozesses (3.54) erfolgen.

Anmerkung 2 zum Begriff: Akzeptierte Risiken werden einer *Überwachung* (3.46) und *Überprüfung* (3.58) unterzogen.

[QUELLE: ISO Guide 73:2009, 3.7.1.6]

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

3.63
Risikoanalyse
(en: risk analysis)
Prozess (3.54), um die Beschaffenheit des *Risikos* (3.61) zu verstehen und das *Risikoniveau* (3.93) zu bestimmen

Anmerkung 1 zum Begriff: Die Risikoanalyse liefert die Grundlage für die *Risikobewertung* (3.67) und die Entscheidungen im Zuge der *Risikobehandlung* (3.72).

Anmerkung 2 zum Begriff: Die Risikoanalyse beinhaltet die Risikoabschätzung.

[QUELLE: ISO Guide 73:2009, 3.6.1]

3.64
Risikobeurteilung
(en: risk assessment)
übergreifender Prozess (3.54), der aus *Risikoidentifizierung* (3.68), *Risikoanalyse* (3.63) und *Risikobewertung* (3.67) besteht

[QUELLE: ISO Guide 73:2009, 3.4.1]

3.65
Risikokommunikation und –absprachen
(en: risk communication and consultation)
Satz fortlaufender und iterativer Prozesse (3.54), den eine Organisation durchführt, um Informationen zu liefern, zu teilen oder zu erhalten und den Dialog mit *interessierten Parteien* (3.37) in Bezug auf die Handhabung von *Risiken* (3.61) zu suchen

Anmerkung 1 zum Begriff: Die Information kann sich auf die Existenz, die Beschaffenheit, die Gestalt, die Wahrscheinlichkeit (3.41), die Signifikanz, die Bewertung, die Akzeptanz und die Behandlung von Risiken beziehen.

Anmerkung 2 zum Begriff: Bei Absprachen handelt es sich um einen bidirektionalen Prozess von fundierter Kommunikation zwischen einer *Organisation* (3.50) und ihren interessierten Parteien zu einer Angelegenheit, bevor eine Entscheidung getroffen oder eine Zielrichtung für diese Angelegenheit bestimmt wird. Eine Absprache ist

— ein Prozess, der sich auf eine Entscheidung eher durch Beeinflussung als durch Machtbefugnis auswirkt;

— eine Eingabe für das Treffen von Entscheidungen, nicht aber das gemeinsame Treffen von Entscheidungen.

3.66
Risikokriterien
(en: risk criteria)
Festlegungen, um die Signifikanz eines *Risikos* (3.61) zu bewerten

Anmerkung 1 zum Begriff: Risikokriterien basieren auf Zielen der Organisation sowie dem externen (3.22) und internen Kontext (3.38).

Anmerkung 2 zum Begriff: Risikokriterien können aus Standards, Gesetzen, Richtlinien und anderen Anforderungen (3.56) abgeleitet werden.

[QUELLE: ISO Guide 73:2009, 3.3.1.3]

3.67
Risikobewertung
(en: risk evaluation)
Prozess (3.54), der die Ergebnisse der *Risikoanalyse* (3.63) mit den *Risikokriterien* (3.66) vergleicht, um zu bestimmen, ob das *Risiko* (3.61) und/oder seine Größe akzeptabel oder tragbar sind

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27000:2019-08

Anmerkung 1 zum Begriff: Die Risikobewertung unterstützt bei der Entscheidung über die *Risikobehandlung* (3.72).

[QUELLE: ISO Guide 73:2009, 3.7.1]

3.68
Risikoidentifizierung
(en: risk identification)
Prozess (3.54) zum Finden, Erkennen und Beschreiben von *Risiken* (3.61)

Anmerkung 1 zum Begriff: Die Risikoidentifizierung beinhaltet die Identifizierung der Risikoquellen, der *Ereignisse* (3.21), ihrer Ursachen und möglichen *Folgen* (3.12).

Anmerkung 2 zum Begriff: Die Risikoidentifizierung kann historische Daten, theoretische Analysen, fundierte Meinungen und Expertenmeinungen sowie Bedürfnisse von *interessierten Parteien* (3.37) umfassen.

[QUELLE: ISO Guide 73:2009, 3.5.1]

3.69
Risikomanagement
(en: risk management)
koordinierte Tätigkeiten zum Zwecke der Führung und Steuerung einer *Organisation* (3.50) in Bezug auf *Risiken* (3.61)

[QUELLE: ISO Guide 73:2009, 2.1]

3.70
Risikomanagementprozess
(en: risk management process)
systematische Anwendung von Managementrichtlinien, -verfahren und –praktiken auf die Tätigkeiten des Kommunizierens, Abstimmens und Festlegens des Kontextes sowie Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von *Risiken* (3.61)

Anmerkung 1 zum Begriff: ISO/IEC 27005 benutzt den Begriff ‚*Prozess*' (3.54), um das *Risikomanagement* (3.69) insgesamt zu beschreiben. Die Elemente des Risikomanagementprozesses werden ‚Tätigkeiten' genannt.

[QUELLE: ISO Guide 73:2009, 3.1, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt]

3.71
Risikoeigentümer
(en: risk owner)
Person oder Entität, die Verantwortung und Berechtigung hat ein *Risiko* (3.61) zu handhaben

[QUELLE: ISO Guide 73:2009, 3.5.1.5]

3.72
Risikobehandlung
(en: risk treatment)
Prozess (3.54) um *Risiken* (3.61) zu verändern

Anmerkung 1 zum Begriff: Die Risikobehandlung kann umfassen:

— Vermeiden des Risikos, indem entschieden wird, die Tätigkeit, die Anlass zu dem Risiko gibt, nicht zu beginnen oder fortzusetzen;

— Eingehen oder Vergrößern des Risikos mit dem Ziel eine Chance wahrzunehmen;

— Beseitigen der Risikoquelle;

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

— Verändern der *Wahrscheinlichkeit* (3.40);

— Verändern der *Folgen* (3.12);

— Teilen des Risikos mit einer anderen Partei oder anderen Parteien (einschließlich Verträgen und Finanzierung von Risiken); und

— Beibehalten des Risikos im Rahmen einer fundierten Wahl.

Anmerkung 2 zum Begriff: Risikobehandlungen, die sich mit negativen *Folgen* (3.12) beschäftigen, heißen manchmal auch „Risikominderung", „Risikoeliminierung" „Risikovorsorge" und „Risikoreduzierung".

Anmerkung 3 zum Begriff: Die Risikobehandlung kann zu neuen *Risiken* (3.61) führen oder vorhandene *Risiken* (3.61) verändern.

[QUELLE: ISO Guide 73:2009, 3.8.1, modifiziert — in Anmerkung 1 zum Begriff wurde Entscheidung durch Wahl ersetzt]

3.73
Standard zur Einführung von Sicherheit
(en: security implementation standard)
Dokument, das genehmigte Wege zur Umsetzung von Sicherheit festlegt

3.74
Bedrohung
(en: threat)
mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder eine *Organisation* (3.50) führen kann

3.75
oberste Leitung
(en: top management)
Person oder Personengruppe, die eine *Organisation* (3.50) auf der obersten Ebene führt und steuert

Anmerkung 1 zum Begriff: Die oberste Leitung ist innerhalb der *Organisation* (3.50) in der Lage Verantwortung zu delegieren und Ressourcen bereitzustellen.

Anmerkung 2 zum Begriff: Wenn der Anwendungsbereich des *Managementsystems* (3.41) nur einen Teil einer *Organisation* (3.50) umfasst, bezieht sich „oberste Leitung" auf diejenigen, die diesen Teil der Organisation führen und steuern.

Anmerkung 3 zum Begriff: Die oberste Leitung wird manchmal executive management genannt und kann Chief Executive Officer, Chief Financial Officer, Chief Informatin Officer und vergleichbare Rollen beinhalten.

3.76
vertrauenswürdige Einheit zur Informationsverbreitung
selbständige *Organisation* (3.50), die den Informationsaustausch innerhalb einer *informationsaustauschenden Gemeinschaft* (3.34) unterstützt

3.77
Schwachstelle
Schwäche eines Wertes oder einer *Maßnahme* (3.14), die durch eine oder mehrere *Bedrohungen* (3.74) ausgenutzt werden kann

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08

4 Managementsysteme für Informationssicherheit (ISMS)

4.1 Allgemeines

Organisationen jeder Art und Größe:

a) sammeln, verarbeiten, speichern und übermitteln Informationen;

b) betrachten Informationen und zugehörige Prozesse, Systeme, Netzwerke und Personen als wichtige Werte, die für das Erreichen der Organisationsziele notwendig sind;

c) sind mit einer Reihe von Risiken konfrontiert, welche die Funktionsfähigkeit von Werten beeinträchtigen können; und

d) begegnen ihrem bekannten Gefährdungspotential mit der Einführung von Informationssicherheitsmaßnahmen.

Sämtliche Informationen, die von einer Organisation gehalten und verarbeitet werden, unterliegen der Bedrohung durch Angriffe, Fehler, Naturereignisse (z. B. Überschwemmung oder Feuer) usw. sowie durch Schwachstellen, die ihre Nutzung grundsätzlich mit sich bringt. Der Begriff Informationssicherheit basiert im Allgemeinen darauf, dass Informationen als Wert angesehen werden, der angemessenen Schutz erfordert, z. B. gegen den Verlust von Verfügbarkeit, Vertraulichkeit und Integrität. Die Ermöglichung, berechtigten Bedarfsträgern korrekte und vollständige Informationen in angemessener Zeit zur Verfügung zu stellen, ist ein Katalysator für betriebliche Wirtschaftlichkeit.

Informationswerte durch Definition, Erlangung, Pflege und Verbesserung von Informationssicherheit wirksam zu schützen, ist erforderlich, um eine Organisation in die Lage zu versetzen, ihre Ziele zu erreichen, und die Einhaltung von gesetzlichen Regelungen sowie ihr Image aufrechtzuhalten und zu verbessern. Diese koordinierten Tätigkeiten, welche die Umsetzung geeigneter Maßnahmen und die Behandlung von unakzeptablen Informationssicherheitsrisiken steuern, werden allgemein als Bestandteile des Informationssicherheitsmanagements bezeichnet.

Da Informationssicherheitsrisiken und die Wirksamkeit der Maßnahmen sich in Abhängigkeit von sich wandelnden Umständen verändern, ist es erforderlich, dass die Organisationen:

a) die Wirksamkeit der umgesetzten Maßnahmen und Verfahren überwachen und bewerten;

b) die aufkommenden Risiken, die behandelt werden müssen, identifizieren; und

c) angemessene Maßnahmen nach Bedarf auswählen, umsetzen und verbessern.

Um solche Tätigkeiten im Bereich der Informationssicherheit zu verknüpfen und zu koordinieren, ist es für jede Organisation notwendig, ihre eigene Informationssicherheitspolitik und -ziele festzulegen und diese Ziele wirksam durch den Einsatz eines Managementsystems zu erreichen.

4.2 Was ist ein ISMS?

4.2.1 Überblick und Grundsätze

Ein Informationssicherheitsmanagementsystem (ISMS) umfasst Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die alle von einer Organisation gesteuert werden, um ihre Informationswerte zu schützen. Ein ISMS ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen. Es basiert auf einer Risikobeurteilung und dem Risikoakzeptanzniveau der Organisation und dient dazu, die Risiken wirksam zu behandeln und zu handhaben. Eine Anforderungsanalyse für den Schutz von Informationswerten und die Anwendung

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27000:2019-08