DIN EN ISO/IEC 27000

ICS 01.040.03; 01.040.35; 03.100.70; 35.030

Ersatz für
DIN EN ISO/IEC 27000:2017-10

Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020

Information technology –
Security techniques –
Information security management systems –
Overview and vocabulary (ISO/IEC 27000:2018);
German version EN ISO/IEC 27000:2020

Technologies de l'information –
Techniques de sécurité –
Systèmes de management de sécurité de l'information –
Vue d'ensemble et vocabulaire (ISO/IEC 27000:2018);
Version allemande EN ISO/IEC 27000:2020

Gesamtumfang 43 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

www.din.de
www.beuth.de

3144079

Nationales Vorwort

Der Text von ISO/IEC 27000:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27000:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 9000:2015	siehe	DIN EN ISO 9000:2015-11
ISO 19011:2011	siehe	DIN EN ISO 19011:2011-12
ISO 27799	siehe	DIN EN ISO 27799
ISO/IEC 17021:2011	siehe	DIN EN ISO/IEC 17021:2011-07-00
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27009	siehe	DIN ISO/IEC 27009

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 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) Anhang A und Anhang B wurden entfernt;

f) redaktionelle Überarbeitung der Norm.

Frühere Ausgaben

DIN ISO/IEC 27000: 2011-07
DIN EN ISO/IEC 27000: 2017-10

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 9000:2015-11, *Qualitätsmanagementsysteme — Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015*

DIN EN ISO 19011:2011-12, *Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2011); Deutsche und Englische Fassung EN ISO 19011:2011*

DIN EN ISO 27799, *Medizinische Informatik — Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002*

DIN EN ISO/IEC 17021:2011-07-00, *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren (ISO/IEC 17021:2011); Deutsche und Englische Fassung EN ISO/IEC 17021:2011*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-managementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

DIN ISO/IEC 27009, *Informationstechnik — IT-Sicherheitsverfahren — Sektorspezifische Anwendung der ISO/IEC 27001 — Anforderungen*

— Leerseite —

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27000

Februar 2020

ICS 01.040.35; 35.030

Ersetzt EN ISO/IEC 27000:2017

Deutsche Fassung

Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie (ISO/IEC 27000:2018)

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

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

Diese Europäische Norm wurde vom CEN am 20. Oktober 2019 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Ref. Nr. EN ISO/IEC 27000:2020 D

Inhalt

Seite

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) erarbeitet und als EN ISO/IEC 27000:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2020, und etwaige entgegenstehende nationale Normen müssen bis August 2020 zurückgezogen werden.

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

Dieses Dokument ersetzt EN ISO/IEC 27000:2017.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27000:2018 wurde von CEN als EN ISO/IEC 27000:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (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 Themen 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. 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 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/IEC JTC 1, *Information technology,* Unterkomitee SC 27, *IT Security techniques* 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;

— Anhang A und Anhang B wurden entfernt;

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, Rechte an geistigem Eigentum und Details zu Beschäftigten, oder der ihnen von Kunden oder Dritten anvertrauten Informationen entwickeln und umsetzen. Diese Standards können auch eingesetzt werden, um sich auf eine unabhängige Beurteilung ihres zum Schutz von Informationen eingesetzten ISMS vorzubereiten.

0.2 Zweck dieses Dokuments

Die ISMS-Normenfamilie beinhaltet Normen, die:

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

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

c) sektorspezifische Anleitungen für ISMS adressieren; und

d) Konformitätsbewertung für ISMS adressieren.

0.3 Inhalt dieses Dokumentes

In diesem Dokument werden die folgenden Verbformen 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 ergänzt und Maßnahmen in Bezug zur Verwendung eines Begriffes enthalten kann.

1 Anwendungsbereich

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

Die Begriffe, die mit diesem Dokumente bereitgestellt werden,

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

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

— schränken 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* (3.56) 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: Ein internes Audit wird von der Organisation selbst durchgeführt oder durch eine externe Partei in ihrem Auftrag.

Anmerkung 3 zum Begriff: „Auditnachweise“ und „Auditkriterien“ sind in ISO 19011 definiert.

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 (3.42), die mittels eines Attributs und der Methode ihrer Quantifizierung definiert ist

Anmerkung 1 zum Begriff: Eine Elementarmessgröße ist funktional unabhängig von anderen *Messgrößen.*

[QUELLE: ISO/IEC/IEEE 15939:2017, 3.3, 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 kann eine Reihe von Folgen haben.

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

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

Anmerkung 4 zum Begriff: Primäre 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 — 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), die als Funktion von zwei oder mehr Werten von *Elementarmessgrößen* (3.8) definiert ist

[QUELLE: ISO/IEC/IEEE 15939:2017, 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.

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* (3.49) 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* der *Organisation* (3.50) auswirken;

— Beziehungen zu externen Stakeholdern[N1)] (3.37) sowie deren Auffassungen und Werte.

[QUELLE: ISO Guide 73:2009, 3.3.1.1]

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

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

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 unterstützt

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

[QUELLE: ISO/IEC/IEEE 15939:2017, 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)
Bewahrung 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 *Zuverlässlichkeit* (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 *Politik* (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 oder eine Reihe von ungewollten oder unerwarteten *Informationssicherheitsereignissen* (3.30), die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die *Informationssicherheit* (3.28) zu bedrohen

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
Fachkraft für Informationssicherheitsmanagementsysteme
(en: information security management system professional)
Person, die einen oder mehrere Informationssicherheitsmanagementsystem *Prozesse* (3.54) einrichtet, umsetzt, aufrechterhält und fortlaufend verbessert

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

Anmerkung 1 zum Begriff: Eine *Organisation* 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
Stakeholder
(en: interested party)
Person oder *Organisation* (3.50), die eine Entscheidung oder Tätigkeit beeinflussen, davon beeinflusst werden oder 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, *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 (z. B. 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 *interessierten 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]

3.39
Risikoniveau
(en: level of risk)
Höhe 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 — Anmerkung 1 und Anmerkung 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:

— subjektiv: Quantifizierung, die menschliches Ermessen einbezieht;

— objektiv: Quantifizierung, die auf numerischen Regeln basiert.

[QUELLE: ISO/IEC/IEEE 15939:2017, 3.21, 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 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.

3.51
ausgliedern
(en: outsource)
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
Zuverlässichkeit
(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) übrig bleibt

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

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

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* (3.59) 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]

3.63
Risikoanalyse
(en: risk analysis)
Prozess (3.54), um die Beschaffenheit des *Risikos* (3.61) zu verstehen und das *Risikoniveau* (3.39) 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 –absprache
(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 Kontext* (3.22) und dem *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

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;

— 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);

— Beibehalten des Risikos im Rahmen einer fundierten Wahl.

Anmerkung 2 zum Begriff: Risikobehandlungen, die sich mit negativen Folgen beschäftigen, werden manchmal auch als „Risikominderung“, „Risikoeliminierung“, „Risikovorsorge“ und „Risikoreduzierung“ bezeichnet.

Anmerkung 3 zum Begriff: Die Risikobehandlung kann zu neuen Risiken führen oder vorhandene Risiken 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 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 Information Officer“ und vergleichbare Rollen beinhalten.

3.76
vertrauenswürdige Einheit zur Informationsverbreitung
(en: trusted information communication entity)
selbständige *Organisation* (3.50), die den Informationsaustausch innerhalb einer *informationsaustauschenden Gemeinschaft* (3.34) unterstützt

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

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 angemessener Maßnahmen, um den Schutz dieser Informationswerte bedarfsgerecht sicherzustellen, trägt zur erfolgreichen Umsetzung eines ISMS bei. Die folgenden elementaren Grundsätze tragen ebenfalls zur erfolgreichen Umsetzung eines ISMS bei:

a) Bewusstsein für die Notwendigkeit von Informationssicherheit;

b) Übertragung von Verantwortung für Informationssicherheit;

c) Einbeziehung der Verpflichtung der Geschäftsführung und der Interessen der Stakeholder;

d) Förderung sozialer Werte;

e) Risikobeurteilung zum Bestimmen angemessener Maßnahmen, um ein akzeptables Risikoniveau zu erreichen;

f) Aufnahme von Sicherheit als grundlegenden Bestandteil von Informationsnetzwerken und -systemen;

g) aktive Prävention gegen und Erkennung von Informationssicherheitsvorfälle(n);

h) Sicherstellung einer ganzheitlichen Herangehensweise an das Management von Informationssicherheit;

i) fortlaufende Neubeurteilung von Informationssicherheit und Vornahme geeigneter Änderungen.

4.2.2 Informationen

Informationen sind Werte, die wie andere wichtige Wirtschaftsgüter für den Geschäftsbetrieb einer Organisation entscheidend und infolgedessen angemessen zu schützen sind. Informationen können auf vielfältige Weise gespeichert werden: sowohl in digitaler Form (z. B. Dateien, die auf elektronischen oder optischen Medien gespeichert sind), in materieller Form (z. B. auf Papier) als auch in nicht materieller Form als Fachwissen der Mitarbeiter. Informationen können auf unterschiedliche Weise übermittelt werden, wie z. B. per Post, elektronisch oder durch mündliche Kommunikation. Ganz gleich welche Form Information auch immer annimmt, oder auf welchem Weg sie übermittelt wird, sie erfordert immer angemessenen Schutz.

In vielen Organisationen sind Informationen von Informations- und Kommunikationstechnologie abhängig. Diese Technologie ist häufig ein entscheidender Bestandteil der Organisation und trägt zu Erzeugung, Verarbeitung, Speichern, Übermittlung, Schutz und Vernichtung von Informationen bei.

4.2.3 Informationssicherheit

Informationssicherheit stellt die Vertraulichkeit, Verfügbarkeit und Integrität von Information sicher. Informationssicherheit umfasst die Anwendung und das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen mit dem Ziel, anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb (*Business Continuity*) sicherzustellen und Beeinträchtigungen durch Informationssicherheitsvorfälle zu minimieren.

Informationssicherheit wird durch die Umsetzung eines geeigneten Maßnahmenkatalogs erreicht, der durch den festgelegten Risikomanagementprozess ausgewählt und mit Hilfe eines ISMS gesteuert wird, das Richtlinien, Prozesse, Verfahren, Organisationsstrukturen, Software und Hardware zum Schutz von identifizierten Informationswerten umfasst. Diese Maßnahmen müssen festgelegt, umgesetzt, überwacht, überprüft und, wo notwendig, verbessert werden, um sicherzustellen, dass die spezifischen Informationssicherheits- und Geschäftsziele der Organisation erreicht werden. Es wird erwartet, dass relevante Informationssicherheitsmaßnahmen nahtlos in die Geschäftsprozesse der Organisation integriert werden.

4.2.4 Management

Management schließt Tätigkeiten zur Führung, Kontrolle und fortlaufenden Verbesserung der Organisation innerhalb von geeigneten Strukturen ein. Managementaufgaben umfassen den Vorgang sowie die Art und Weise oder Methode, Ressourcen zu organisieren, zu handhaben, zu führen, zu überwachen und zu kontrollieren. Managementstrukturen reichen von einer einzelnen Person in einer kleinen Organisation bis hin zu Managementhierarchien in großen Organisationen, die sich aus vielen Individuen zusammensetzen.

In Bezug auf ein ISMS umfasst Management die Findung und Überwachung von Entscheidungen, die erforderlich sind, um Geschäftsziele durch den Schutz der Informationswerte der Organisation zu erreichen. Das Management von Informationssicherheit findet Ausdruck in der Formulierung und Anwendung von Informationssicherheitspolitik, -verfahren und -richtlinien, die dann in der gesamten Organisation und von allen Personen, die der Organisation angehören, angewendet werden.

4.2.5 Managementsystem

Ein Managementsystem nutzt ein Rahmenwerk von Ressourcen, um die Ziele einer Organisation zu erreichen. Das Managementsystem umfasst Organisationsstrukturen, Richtlinien, Planungstätigkeiten, Verantwortlichkeiten, Methoden, Verfahren, Prozesse und Ressourcen.

Im Hinblick auf Informationssicherheit ermöglicht ein Managementsystem einer Organisation:

a) den Sicherheitsanforderungen von Kunden und anderen Stakeholdern gerecht zu werden;

b) ihre Planungen und Tätigkeiten zu verbessern;

c) ihre Informationssicherheitsziele zu erfüllen;

d) Vorschriften, Gesetze und Branchenstandards einzuhalten; und

e) die Informationswerte in einer organisierten Art und Weise zu steuern, welche die fortlaufende Verbesserung und Anpassung an aktuelle Ziele der Organisation fördert.

4.3 Prozessorientierter Ansatz

Organisationen müssen viele Tätigkeiten identifizieren und lenken, um wirksam und wirtschaftlich zu funktionieren. Jede Tätigkeit, die Ressourcen nutzt, muss gesteuert werden, um Eingaben mittels einer Reihe von zusammenhängenden oder zusammenwirkenden Tätigkeiten in Ergebnisse zu überführen, dies ist auch als „Prozess“ bekannt. Die Ergebnisse eines Prozesses können direkt die Eingaben für einen anderen Prozess bilden; im Allgemeinen erfolgt diese Transformation unter geplanten und kontrollierten Bedingungen. Die Anwendung eines Systems von Prozessen innerhalb einer Organisation zusammen mit der Identifikation und Interaktion dieser Prozesse und ihrer Steuerung kann als „prozessorientierter Ansatz“ bezeichnet werden.

4.4 Warum ein ISMS wichtig ist

Risiken, die mit den Informationswerten der Organisation verbunden sind, müssen betrachtet werden. Das Erreichen von Informationssicherheit erfordert ein Risikomanagement und umfasst Risiken aufgrund von materiellen, menschlichen und technischen Bedrohungen, die mit allen Formen von Informationen, welche die Organisation hat oder nutzt, verbunden sind.

Die Einführung eines ISMS soll eine strategische Entscheidung für eine Organisation sein, und es ist erforderlich, dass diese Entscheidung in Übereinstimmung mit den Anforderungen der Organisation nahtlos integriert, skaliert und aktualisiert wird.

Die Planung und Umsetzung des ISMS einer Organisation wird beeinflusst durch die Anforderungen und Ziele der Organisation, den Sicherheitsbedarf, die angewandten Geschäftsprozesse und die Größe und Struktur der Organisation. Die Planung und der Betrieb eines ISMS erfordern es, den Interessen und Anforderungen an die Informationssicherheit aller Stakeholder der Organisation, einschließlich Kunden, Lieferanten, Geschäftspartnern, Anteilseignern und anderen betroffenen Dritten, Rechnung zu tragen.

In einer vernetzten Welt stellen Informationen und zugehörige Prozesse, Systeme und Netzwerke entscheidende Wirtschaftsgüter dar. Organisationen und ihre Informationssysteme und Netzwerke sind mit Sicherheitsbedrohungen aus einer Vielfalt von Quellen konfrontiert, einschließlich computergestütztem Betrug, Spionage, Sabotage, Vandalismus, Feuer und Überschwemmungen. Schäden an Informationssystemen und Netzwerken, die durch Schadcode, Computer-Hacking, und Denial-of-Service-Angriffe verursacht werden, sind häufiger, ehrgeiziger und immer raffinierter geworden.

Ein ISMS ist sowohl im öffentlichen Bereich als auch in der Privatwirtschaft wichtig. In jeder Branche ist ein ISMS ein Wegbereiter, der E-Business unterstützt und für Risikomanagement-Tätigkeiten unerlässlich ist. Das Zusammenschließen von öffentlichen und privaten Netzwerken und die gemeinsame Nutzung von Informationswerten erhöht die Schwierigkeit, den Zugriff auf und die Verarbeitung von Informationen zu kontrollieren. Darüber hinaus kann die Verbreitung von mobilen Speichergeräten, die Informationswerte enthalten, die Wirksamkeit herkömmlicher Maßnahmen schwächen. Wenn Organisationen die ISMS-Normenfamilie übernehmen, können sie ihre Fähigkeit, einheitliche und gegenseitig erkennbare Prinzipien der Informationssicherheit anzuwenden, Geschäftspartnern und anderen interessierten Parteien unter Beweis stellen.

Informationssicherheit wird bei der Planung und Entwicklung von Informationssystemen nicht immer berücksichtigt. Außerdem wird Informationssicherheit oft als rein technische Lösung angesehen. Das Maß an Informationssicherheit, das durch technische Mittel erreicht werden kann, ist jedoch begrenzt und kann unwirksam sein, wenn es nicht durch ein geeignetes Management und entsprechende Verfahren im Rahmen eines ISMS unterstützt wird. Die nachträgliche Integration von Sicherheit in ein funktionsfähiges geschlossenes Informationssystem kann schwierig und teuer sein. Ein ISMS umfasst die Identifikation der bereits etablierten Maßnahmen und erfordert sorgfältige Planung und die Beachtung von Details. So sind z. B. Zugangssteuerungen, die technischer (logischer), physikalischer, administrativer Art oder eine Kombination dieser Typen sein können, Mittel um sicherzustellen, dass der Zugriff auf Informationswerte nur befugt und eingeschränkt auf Basis der Geschäfts- und Informationssicherheitsanforderungen erfolgt.

Die erfolgreiche Einführung eines ISMS ist wichtig, um Informationswerte zu schützen, und ermöglicht es einer Organisation,

a) größere Gewissheit zu erlangen, dass ihre Informationswerte angemessen und beständig gegen Bedrohungen geschützt sind;

b) ein strukturiertes und umfassendes Rahmenwerk zur Identifizierung und Einschätzung von Informationssicherheitsrisiken, zur Auswahl und Anwendung geeigneter Maßnahmen, sowie zur Messung und Verbesserung der Wirksamkeit dieser Maßnahmen zu unterhalten;

c) fortlaufend ihre Maßnahmenumgebung zu verbessern; und

d) effektiv die Einhaltung gesetzlicher und behördlicher Regelungen zu erreichen.

4.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS

4.5.1 Übersicht

Um ihr ISMS einzuführen, zu überwachen, zu pflegen und zu verbessern, muss eine Organisation die folgenden Schritte durchführen:

a) Identifikation von Informationswerten und der mit ihnen verbundenen Informationssicherheitsanforderungen (siehe 4.5.2);

b) Bestimmung von Informationssicherheitsrisiken (siehe 4.5.3) und Behandeln dieser Informationssicherheitsrisiken (siehe 4.5.4);

c) Auswahl und Umsetzung geeigneter Maßnahmen, um unakzeptable Risiken zu handhaben (siehe 4.5.5);

d) Überwachung, Wartung und Verbesserung der Wirksamkeit der Sicherheitsmaßnahmen in Zusammenhang mit den Informationswerten der Organisation (siehe 4.5.6).

Um sicherzustellen, dass das ISMS die Informationswerte der Organisation wirksam und fortlaufend schützt, ist es erforderlich, dass die Schritte (a) bis (d) beständig wiederholt werden, um Veränderungen der Risiken oder der Strategie und Geschäftsziele der Organisation zu identifizieren.

4.5.2 Identifizierung von Informationssicherheitsanforderungen

Im Rahmen der übergeordneten Strategie und Geschäftsziele einer Organisation und unter Berücksichtigung ihrer Größe und geographischen Ausdehnung können die Anforderungen an die Informationssicherheit durch Einvernehmen über die folgenden Aspekte bestimmt werden:

a) identifizierte Informationswerte und ihr Nutzen;

b) Geschäftsanforderungen an die Verarbeitung, das Speichern und die Kommunikation von Informationen;

c) gesetzliche, behördliche und vertragliche Anforderungen.

Die Durchführung einer systematischen Beurteilung der Risiken, welche die Informationswerte der Organisation betreffen, umfasst die Analyse folgender Aspekte: Bedrohungen der Informationswerte; Schwachstellen von Informationswerten und die Wahrscheinlichkeit, dass eine Bedrohung von Informationswerten tatsächlich eintritt, sowie mögliche Auswirkungen eines Informationssicherheitsvorfalls auf die Informationswerte. Die Aufwendungen für geeignete Maßnahmen sollten im richtigen Verhältnis zur festgestellten Beeinträchtigung des Geschäfts im Fall, dass das Risiko eintritt, stehen.

4.5.3 Beurteilung von Informationssicherheitsrisiken

Das Management von Informationssicherheitsrisiken erfordert eine entsprechende Methode zur Risikobeurteilung und Risikobehandlung, die, soweit erforderlich, eine Schätzung der Kosten und des Nutzens, die gesetzlichen Anforderungen, die Interessen der Stakeholder und andere Vorgaben und Variablen umfassen darf.

Die Risikobeurteilung sollte die Risiken entsprechend den Kriterien der Risikoakzeptanz und den für die Organisation einschlägigen Zielen identifizieren, bemessen und priorisieren. Die Ergebnisse sollten den geeigneten Managementmaßnahmen Richtung geben und Priorisierungen zur Handhabung von Informationssicherheitsrisiken und zum Umsetzen von Maßnahmen, die ausgewählt wurden, um vor diesen Risiken zu schützen, bestimmen.

Die Risikobeurteilung sollte beinhalten:

— das systematische Vorgehensmodell zur Schätzung der Risikohöhen (Risikoanalyse); und

— den Prozess zum Vergleichen der geschätzten Risiken mit den Risikokriterien, um die Bedeutung des Risikos zu bestimmen (Risikobewertung).

Risikobeurteilungen sollten regelmäßig durchgeführt werden und wenn wesentliche Änderungen auftreten, um Veränderungen der Informationssicherheitsanforderungen und der Risikolage, z. B. bei Werten, Bedrohungen, Schwachstellen, Auswirkungen und der Risikobewertung zu berücksichtigen. Diese Risikobeurteilungen sollten methodisch durchführt werden und geeignet sein, vergleichbare und reproduzierbare Ergebnisse zu erbringen.

Damit die Informationssicherheitsrisikobeurteilung leistungsfähig ist, sollte sie einen eindeutig festgelegten Anwendungsbereich haben und, falls erforderlich, die Beziehungen zu Risikobeurteilungen in anderen Gebieten umfassen.

ISO/IEC 27005 liefert eine Anleitung zum Informationssicherheitsrisikomanagement einschließlich Ratschlägen zur Risikobeurteilung, -behandlung, -akzeptanz, -berichterstattung, -überwachung und -überprüfung. Beispiele für Risikobeurteilungsmethodiken sind hier ebenfalls zu finden.

4.5.4 Behandlung von Informationssicherheitsrisiken

Bevor die Risikobehandlung in Betracht gezogen wird, sollte die Organisation Kriterien beschließen, um zu bestimmen, ob Risiken akzeptiert werden können oder nicht. Risiken dürfen akzeptiert werden, z. B. wenn sie als niedrig abgeschätzt werden oder die Kosten für die Behandlung für die Organisation nicht tragbar sind. Solche Entscheidungen sollten aufgezeichnet werden.

Für jedes im Rahmen der Risikobeurteilung identifizierte Risiko muss über eine Risikobehandlung entschieden werden. Mögliche Optionen für die Risikobehandlung umfassen die folgenden:

a) Anwenden geeigneter Maßnahmen, um die Risiken zu reduzieren;

b) bewusstes und sachliches Akzeptieren von Risiken, vorausgesetzt, sie erfüllen offensichtlich die Politik der Organisation und die zugehörigen Kriterien zur Risikoakzeptanz;

c) Vermeiden von Risiken, indem Handlungen, die das Auftreten der Risiken verursachen, untersagt werden;

d) Teilen der zugehörigen Risiken mit anderen Parteien, z. B. Versicherern oder Lieferanten.

Für diejenigen Risiken, für welche gemäß der Entscheidung zur Risikobehandlung geeignete Maßnahmen anzuwenden sind, sollten diese ausgewählt und umgesetzt werden.

4.5.5 Auswahl und Umsetzung von Maßnahmen

Wenn die Informationssicherheitsanforderungen identifiziert (4.5.2), die Informationssicherheitsrisiken für die identifizierten Informationswerte bestimmt und bewertet (4.5.3) und Entscheidungen hinsichtlich der Behandlung von Informationssicherheitsrisiken getroffen worden sind (4.5.4), werden Maßnahmen zur Risikoreduzierung ausgewählt und umgesetzt.

Maßnahmen sollten sicherstellen, dass die Risiken auf ein akzeptables Niveau gesenkt werden, und das Folgende berücksichtigen:

a) Anforderungen und Beschränkungen durch nationale und internationale Gesetze und Vorschriften;

b) Organisationsziele;

c) betriebliche Anforderungen und Beschränkungen;

d) die Kosten ihrer Umsetzung und ihres Betriebs im Verhältnis zur Verminderung der Risiken, wobei ein angemessenes Verhältnis zu den Anforderungen und Beschränkungen der Organisation gewahrt bleibt;

e) sie sollten umgesetzt werden, um zur Unterstützung der Organisationsziele die Wirtschaftlichkeit und Wirksamkeit der Informationssicherheitsmaßnahmen zu überwachen, zu bewerten und zu verbessern. Die Auswahl und Umsetzung von Maßnahmen sollte in einer Erklärung zur Anwendbarkeit dokumentiert werden, um die Einhaltung von Anforderungen zu unterstützen;

f) die Notwendigkeit, das Gleichgewicht zwischen der Investition für Umsetzung und Betrieb von Maßnahmen einerseits und der Verlusterwartung andererseits, die sich aus Informationssicherheitsvorfällen ergibt, zu wahren.

Die in ISO/IEC 27002 festgelegten Maßnahmen sind anerkannt als bewährte Praktiken, die auf die meisten Organisationen anwendbar und leicht anpassbar sind, so dass sie Organisationen unterschiedlicher Größe und Komplexität Rechnung tragen. Andere Normen in der ISMS-Normenfamilie liefern Anleitungen hinsichtlich der Auswahl und Anwendung von Informationssicherheitsmaßnahmen nach ISO/IEC 27002 für das Informationsmanagementsystem.

Informationssicherheitsmaßnahmen sollten bereits beim Systementwurf und bei der Projektanforderungsspezifikation berücksichtigt werden. Andernfalls können daraus zusätzliche Kosten und weniger wirksame Lösungen resultieren, und schlimmstenfalls kann dies dazu führen, dass angemessene Sicherheit nicht erreicht wird. Die Maßnahmen können aus der ISO/IEC 27002 oder aus anderen Maßnahmenkatalogen ausgewählt werden, oder neue Maßnahmen können entworfen werden, um so die speziellen Anforderungen der Organisation zu erfüllen. Es ist nötig zu verstehen, dass manche Maßnahmen möglicherweise nicht auf jedes Informationssystem oder in jeder Umgebung anwendbar oder nicht für jede Organisation umsetzbar sind.

Manchmal braucht es Zeit, einen ausgewählten Satz von Maßnahmen umzusetzen, und das Risikoniveau ist in diesem Zeitraum möglicherweise höher als langfristig tolerierbar. Risikokriterien sollten eine kurzzeitige Tolerierung von Risiken während der Umsetzung der Maßnahmen berücksichtigen. Interessierte Parteien sollten über das eingeschätzte bzw. voraussichtliche Risikoniveau zu verschiedenen Zeitpunkten während der fortschreitenden Umsetzung der Maßnahmen informiert werden.

Es sollte beachtet werden, dass kein Satz von Maßnahmen vollständige Informationssicherheit erreichen kann. Zur Unterstützung der Organisationsziele sollten zusätzliche Managementmaßnahmen umgesetzt werden, um die Wirtschaftlichkeit und Wirksamkeit von Informationssicherheitsmaßnahmen zu überwachen, zu bewerten und zu verbessern.

Die Auswahl und Umsetzung von Maßnahmen sollte in einer Erklärung zur Anwendbarkeit dokumentiert werden, um die Einhaltung von Anforderungen zu unterstützen.

4.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS

Eine Organisation muss ein ISMS durch Überwachung und Bewertung der Leistung gegenüber den Richtlinien und den Zielen der Organisation aufrechterhalten und verbessern und der Leitung die Ergebnisse zur Bewertung vorlegen. Bei dieser ISMS-Bewertung wird untersucht, ob das ISMS angemessene Maßnahmen für eine Risikobehandlung im Rahmen des ISMS-Anwendungsbereichs festlegt. Außerdem wird auf Basis der Aufzeichnungen zu den überwachten Bereichen der Nachweis der Verifizierung und die Nachvollziehbarkeit von Korrektur-, Vorbeugungs- und Verbesserungsmaßnahmen geliefert.

4.5.7 Fortlaufende Verbesserung

Das Ziel der fortlaufenden Verbesserung eines ISMS ist es, die Wahrscheinlichkeit dafür zu erhöhen, dass die Ziele zur Wahrung der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen erreicht werden. Im Mittelpunkt der fortlaufenden Verbesserung steht die Suche nach Verbesserungsmöglichkeiten und nicht die Bestätigung, dass die bestehenden Managementaktivitäten ausreichend oder so gut wie möglich sind.

Verbesserungsmaßnahmen schließen Folgendes ein:

a) Analysieren und Bewerten der vorliegenden Situation, damit Verbesserungspotentiale erkannt werden;

b) Festlegen der Ziele der Verbesserung;

c) Suchen nach möglichen Lösungen, um diese Ziele zu erreichen;

d) Bewerten dieser Lösungen und Treffen einer Auswahl;

e) Umsetzen der ausgewählten Lösung;

f) Messen, Verifizieren, Analysieren und Bewerten der Umsetzungsergebnisse, um zu bestimmen, ob die Ziele erreicht wurden;

g) Formalisieren der Änderungen.

Falls erforderlich, werden die Ergebnisse bewertet, um weitere Verbesserungsmöglichkeiten zu bestimmen. Weil diese Tätigkeiten regelmäßig wiederholt werden, ist Verbesserung ein fortlaufender Prozess. Zum Ermitteln von Verbesserungsmöglichkeiten können auch Rückmeldungen von Kunden und anderen interessierten Parteien, Audits und Überprüfungen des ISMS genutzt werden.

4.6 Kritische Erfolgsfaktoren für das ISMS

Eine große Anzahl von Faktoren ist ausschlaggebend für die erfolgreiche Umsetzung eines ISMS, um einer Organisation das Erreichen ihrer Geschäftsziele zu ermöglichen. Beispiele für kritische Erfolgsfaktoren sind die folgenden:

a) Informationssicherheitspolitik, -ziele und -tätigkeiten sind an diese Ziele angepasst;

b) ein Ansatz und Rahmenwerk für die Planung, Umsetzung, Überwachung, Aufrechterhaltung und Verbesserung der Informationssicherheit in Übereinstimmung mit der Unternehmenskultur;

c) erkennbare Unterstützung und Verpflichtung seitens aller Leitungsebenen, insbesondere der obersten Leitung;

d) ein Einvernehmen über die Anforderungen an den Schutz von Informationswerten, das durch die Anwendung eines Informationssicherheitsrisikomanagements erzielt wird (siehe ISO/IEC 27005);

e) ein wirksames Bewusstseins-, Schulungs- und Fortbildungsprogramm für Informationssicherheit, bei dem alle Beschäftigte und andere betroffene Parteien über ihre Informationssicherheitspflichten, so wie sie in den Informationssicherheitsrichtlinien, -standards, usw. dargelegt sind, informiert werden und motiviert werden, entsprechend zu handeln;

f) ein wirksamer Prozess zur Handhabung von Informationssicherheitsvorfällen;

g) ein wirksamer Ansatz zum Business Continuity Management;

h) ein Messsystem, das genutzt wird, um die Leistung bei der Handhabung der Informationssicherheit zu bewerten und Verbesserungsvorschläge zu erhalten.

Ein ISMS erhöht die Wahrscheinlichkeit, dass eine Organisation durchgängig die kritischen Erfolgsfaktoren erreicht, die zum Schutz ihrer Informationswerte erforderlich sind.

4.7 Nutzen der ISMS-Normenfamilie

Der Nutzen der Umsetzung eines ISMS ergibt sich in erster Linie aus der Verminderung von Informationssicherheitsrisiken (d. h. Senkung der Wahrscheinlichkeit von Informationssicherheitsvorfällen und/oder ihrer Auswirkungen). Der erzielte Nutzen für eine Organisation, um einen nachhaltigen Erfolg aus der Übernahme der ISMS-Normenfamilie zu erreichen, umfasst insbesondere die folgenden Punkte:

a) ein strukturiertes Rahmenwerk, um den Prozess der Bestimmung, der Umsetzung, des Betriebs und der Aufrechterhaltung eines umfassenden, wirtschaftlichen, wertschaffenden, integrierten und angepassten ISMS zu unterstützen, das den Bedarf der Organisation über verschiedene Arbeitsabläufe und Standorte hinweg deckt;

b) Unterstützung der Leitung beim konsistenten und verantwortlichen Führen und Betreiben ihrer Herangehensweise auf dem Gebiet des Informationssicherheitsmanagements im Zusammenhang mit dem Risikomanagement des Unternehmens und mit der Unternehmenssteuerung einschließlich der Ausbildung und Schulung von Geschäfts- und Systemverantwortlichen hinsichtlich der ganzheitlichen Handhabung von Informationssicherheit;

c) Förderung von weltweit anerkannten, guten Informationssicherheitspraktiken in einer nicht-vorschreibenden Art und Weise, die Institutionen den Handlungsspielraum gibt, zutreffende Maßnahmen zu ergreifen und zu verbessern, die ihren speziellen Gegebenheiten entsprechen und diese angesichts von internen und externen Veränderungen aufrecht zu erhalten;

d) Bereitstellung einer gemeinsamen Sprache und konzeptionellen Basis für Informationssicherheit, die es leichter macht, Vertrauen in Geschäftspartner mit einem konformen ISMS zu setzen, insbesondere wenn sie eine Zertifizierung nach ISO/IEC 27001 durch eine akkreditierte Zertifizierungsstelle benötigen;

e) Erhöhung des Vertrauens der Stakeholder in die Organisation;

f) Befriedigung gesellschaftlicher Bedürfnisse und Erwartungen;

g) ein wirksameres ökonomisches Management der Investitionen in Informationssicherheit.

5 Die ISMS-Normenfamilie

5.1 Allgemeine Informationen

Die ISMS-Normenfamilie besteht aus Normen, die zueinander in Beziehung stehen und bereits veröffentlicht oder in Bearbeitung sind. Sie beinhaltet eine Reihe wichtiger struktureller Elemente. Diese Elemente konzentrieren sich auf:

— Normen, die Anforderungen an ISMS (ISO/IEC 27001) beschreiben;

— Anforderungen an Zertifizierungsstellen (ISO/IEC 27006), welche die Konformität mit ISO/IEC 27001 zertifizieren, darlegen; und

— zusätzliches Anforderungsrahmenwerk zur sektorspezifischen Umsetzung des ISMS (ISO/IEC 27009).

Weitere Normen geben Anleitung für verschiedene Aspekte einer ISMS-Umsetzung. Sie befassen sich mit einem allgemeingültigen Prozess, maßnahmenbezogenen Leitfäden und sektorspezifischer Anleitung.

Bild 1 zeigt die Zusammenhänge innerhalb der ISMS-Normenfamilie.

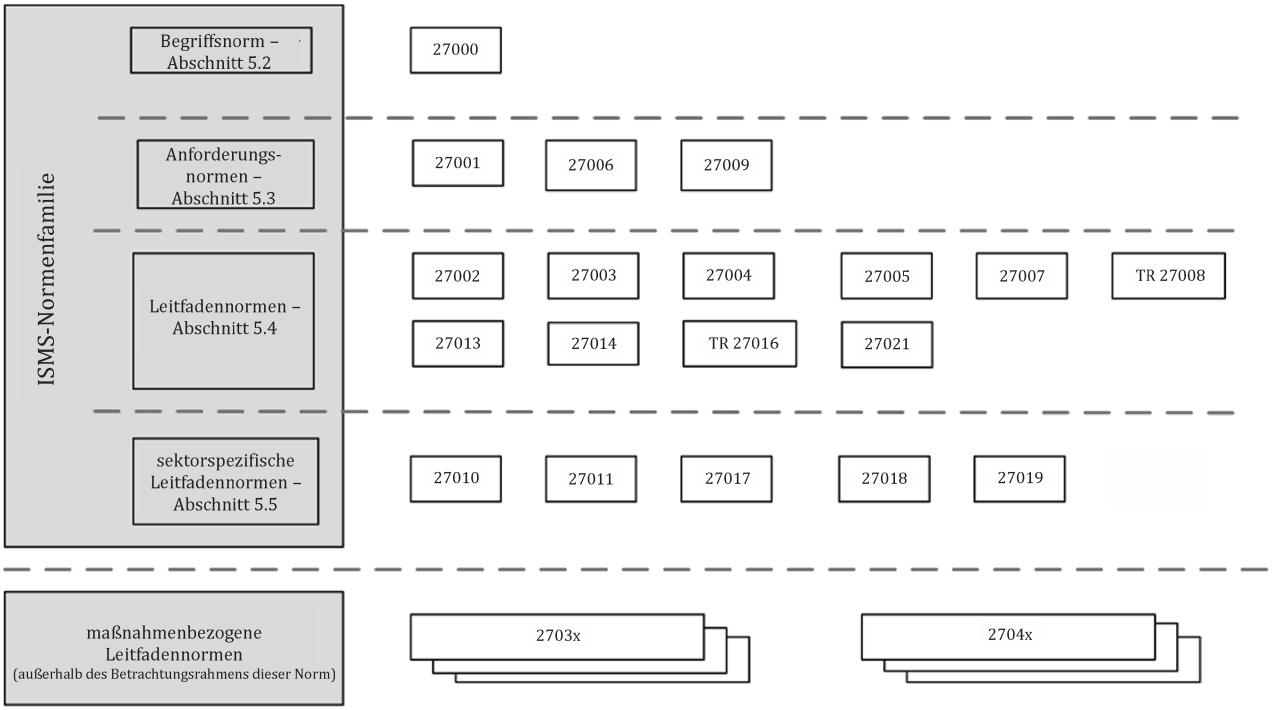

Bild 1 — Zusammenhänge der ISMS-Normenfamilie

Die Normen der ISMS-Normenfamilie werden unten anhand ihres Typs (oder ihrer Rolle) innerhalb der ISMS-Normenfamilie und ihrer Normnummer beschrieben.

5.2 Norm, die einen Überblick und die Terminologie beschreibt: ISO/IEC 27000 (dieses Dokument)

Information technology — Security techniques — Information security management systems — Overview and vocabulary (Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie)

Anwendungsbereich: Dieses Dokument liefert Organisationen und Einzelpersonen:

a) einen Überblick über die ISMS-Normenfamilie;

b) eine Einführung zu Informationssicherheitsmanagementsystemen (ISMS); und

c) Begriffe, die durchgehend in der ISMS-Normenfamilie verwendet werden.

Zweck: Dieses Dokument beschreibt die Grundlagen von Informationssicherheitsmanagementsystemen, die Gegenstand der ISMS-Normenfamilie sind, und definiert die zugehörigen Begriffe.

5.3 Normen, die Anforderungen festlegen

5.3.1 ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements (Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen)

Anwendungsbereich: Dieses Dokument legt die Anforderungen an die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Aufrechterhaltung und Verbesserung von formalisierten Informationssicherheitsmanagementsystemen (ISMS) im Zusammenhang mit den übergreifenden Unternehmensrisiken einer Organisation fest. Sie legt Anforderungen an die Umsetzung von Informationssicherheitsmaßnahmen fest, die auf die Bedürfnisse der jeweiligen Organisation oder Teilbereiche der Organisation zugeschnitten sind. Dieses Dokument kann für alle Arten von Organisationen unabhängig von ihrer Art, Größe oder Erscheinungsform, verwendet werden.

Zweck: ISO/IEC 27001 stellt normative Anforderungen an die Entwicklung und den Betrieb eines ISMS, einschließlich eines Maßnahmenkatalogs für die Steuerung und Minderung der Risiken, die mit den Informationswerten verbunden sind, welche die Organisation durch den Betrieb ihres ISMS zu schützen sucht. Organisationen, die ein ISMS betreiben, können sich ihre Konformität auditieren und zertifizieren lassen. Die Maßnahmenziele und Maßnahmen aus ISO/IEC 27001:2013, Anhang A, müssen als Teil dieses ISMS-Prozesses so ausgewählt werden, dass die identifizierten Anforderungen abgedeckt werden. Die Maßnahmenziele und Maßnahmen, die in ISO/IEC 27001:2013 Tabelle A.1, aufgelistet sind, sind direkt abgeleitet von und angeglichen an diejenigen, welche in ISO/IEC 27002:2013, Abschnitt 5 bis Abschnitt 18, aufgeführt sind.

5.3.2 ISO/IEC 27006

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (Informationstechnik —Sicherheitsverfahren — Anforderungen an Stellen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten)

Anwendungsbereich: Dieses Dokument legt zusätzlich zu den Anforderungen, die in ISO/IEC 17021 enthalten sind, Anforderungen fest und gibt Anleitung für Stellen, die Audits und ISMS-Zertifizierungen nach ISO/IEC 27001 anbieten. Es verfolgt in erster Linie den Zweck, die Akkreditierung von Zertifizierungsstellen zu unterstützen, welche die Zertifizierung von ISMS nach ISO/IEC 27001 anbieten.

Die in diesem Dokument enthaltenen Anforderungen müssen zur Darlegung der Kompetenz und Zuverlässlichkeit von jedem der ISMS Zertifizierungen anbietet nachgewiesen werden und die Hilfestellungen die in diesem Dokument enthalten sind stellen zusätzliche Interpretationen dieser Anforderungen bereit für jeden der ISMS Zertifizierungen anbietet.

Zweck: ISO/IEC 27006 ergänzt ISO/IEC 17021 dahingehend, dass die Anforderungen für die Akkreditierung von Zertifizierungsstellen bereit gestellt werden, so dass es diesen Organisationen ermöglicht wird, Konformitätsbewertungen in Bezug auf die in ISO/IEC 27001 festgelegten Anforderungen einheitlich durchzuführen.

5.3.3 ISO/IEC 27009

Information technology — Security techniques — Sector-specific applications of ISO/IEC 27001 — Requirements (Informationstechnik — IT-Sicherheitsverfahren — Sektorspezifische Anwendung der ISO/IEC 27001 — Anforderungen)

Anwendungsbereich: Dieses Dokument legt die Anforderungen für die Anwendung der ISO/IEC 27001 in jedwedem spezifischen Sektor fest (Bereich, Anwendungsgebiet oder Marktsegment). Es erklärt wie Anforderungen zusätzlich zu denen aus ISO/IEC 27001 aufgenommen werden, wie Anforderungen aus ISO/IEC 27001 verfeinert werden und wie Maßnahmen oder Maßnahmenpakete zusätzlich zum ISO/IEC 27001:2013, Anhang A, aufgenommen werden.

Zweck: ISO/IEC 27009 stellt sicher, dass zusätzliche oder verfeinerte Anforderungen nicht im Konflikt mit den Anforderungen aus ISO/IEC 27001 stehen.

5.4 Normen, die allgemeine Leitfäden beschreiben

5.4.1 ISO/IEC 27002

Information technology — Security techniques — Code of practice for information security management controls (Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen)

Anwendungsbereich: Dieses Dokument stellt eine Liste von allgemein anerkannten Maßnahmenzielen und bewährten Maßnahmen als Anleitung für die Auswahl und Umsetzung von Maßnahmen zur Erreichung von Informationssicherheit zur Verfügung.

Zweck: ISO/IEC 27002 ist eine Anleitung für die Umsetzung von Informationssicherheitsmaßnahmen. Insbesondere Abschnitt 5 bis Abschnitt 18 geben spezifische Ratschläge und Anleitung für bewährte Praktiken zur Umsetzung der Maßnahmen, die in ISO/IEC 27001:2013, A.5 bis A.18, festgelegt sind.

5.4.2 ISO/IEC 27003

Information technology — Security techniques — Information security management system implementation guidance (Informationstechnik —Sicherheitsverfahren — Anleitung)

Anwendungsbereich: Dieses Dokument stellt Erläuterungen und Hilfestellungen zur ISO/IEC 27001:2013 bereit.

Zweck: ISO/IEC 27003 bietet einen Hintergrund zur erfolgreichen Umsetzung des ISMS in Übereinstimmung mit ISO/IEC 27001.

5.4.3 ISO/IEC 27004

Information technology — Security techniques — Information security management — Monitoring measurement, analysis and evaluation (Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Management — Überwachung, Messung, Analyse und Evaluation)

Anwendungsbereich: Dieses Dokument gibt Hilfestellung um Organisationen zu unterstützen die Informationssicherheitsleistung und Wirksamkeit des ISMS zu evaluieren um die Anforderungen aus ISO/IEC 27001:2013, 9.1, zu erfüllen. Es adressiert dabei:

a) die Überwachung und Messung der Informationssicherheitsleistung;

b) die Überwachung und Messung der Wirksamkeit eines Informationssicherheitsmanagementsystems einschließlich seiner Prozesse und Maßnahmen;

c) die Analyse und Evaluation der Ergebnisse der Überwachung und Messung

Zweck: ISO/IEC 27004 liefert ein Rahmenwerk, das es ermöglicht, die Wirksamkeit von ISMS gemäß ISO/IEC 27001 zu messen und zu bewerten.

5.4.4 ISO/IEC 27005

Information technology — Security techniques — Information security risk management (Informations-technik — IT-Sicherheitsverfahren — Informationssicherheits-Risikomanagement)

Anwendungsbereich: Dieses Dokument liefert Leitfäden für das Informationssicherheitsrisikomanagement. Der in diesem Dokument beschriebene Ansatz unterstützt die allgemeinen Konzepte, die in ISO/IEC 27001 festgelegt sind.

Zweck: ISO/IEC 27005 gibt Anleitung für die Umsetzung eines prozessorientierten Risikomanagementansatzes, der die Umsetzung und die Einhaltung der Anforderungen des Informationssicherheits-Risikomanagements gemäß ISO/IEC 27001 zufriedenstellend unterstützt.

5.4.5 ISO/IEC 27007

Information technology — Security techniques — Guidelines for information security management systems auditing (Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für Informationssicherheits-Managementsystemaudits)

Anwendungsbereich: Dieses Dokument gibt zusätzlich zu der Anleitung, die in ISO 19011 enthalten ist und die für Managementsysteme im Allgemeinen gilt, Anleitung sowohl für die Durchführung von ISMS-Audits als auch bezüglich der Kompetenz von ISMS-Auditoren.

Zweck: ISO/IEC 27007 stellt eine Anleitung für Organisationen zur Verfügung, die interne oder externe Audits eines ISMS durchführen oder ein ISMS-Auditprogramm nach den in ISO/IEC 27001 festgelegten Anforderungen handhaben müssen.

5.4.6 ISO/IEC TR 27008

Information technology — Security techniques — Guidelines for auditors on information security controls (Informationstechnik — IT-Sicherheitsverfahren — Richtlinien für Auditoren von Informationssicherheits-maßnahmen

Anwendungsbereich: Dieses Dokument gibt Anleitung zur Überprüfung der Umsetzung und des Betriebs von Maßnahmen, einschließlich der Prüfung der Übereinstimmung von Maßnahmen für das Informationssicherheitssystem auf technischer Ebene in Übereinstimmung mit den Informationssicherheitsstandards der Organisation.

Zweck: Dieses Dokument richtet das Augenmerk auf die Überprüfung von Informationssicherheitsmaßnahmen einschließlich der Übereinstimmung auf technischer Ebene in Bezug auf einen von der Organisation erstellten Standard zur Umsetzung von Informationssicherheit. Er ist nicht als spezielle Anleitung zur Prüfung der Übereinstimmung mit Messungen, Risikobeurteilung oder Auditierung eines ISMS nach ISO/IEC 27004, ISO/IEC 27005 oder ISO/IEC 27007 gedacht. Dieses Dokument ist nicht für Managementsystemaudits gedacht.

5.4.7 ISO/IEC 27013

Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (Informationstechnik — Sicherheitsverfahren — Anleitung für die gemeinsame Einführung von ISO/IEC 27001 und ISO/IEC 20000-1)

Anwendungsbereich: Dieses Dokument liefert eine Anleitung zur integrierten Umsetzung von ISO/IEC 27001 und ISO/IEC 20000-1 für Organisationen, die:

a) ISO/IEC 27001 umsetzen, nachdem ISO/IEC 20000-1 bereits umgesetzt wurde oder umgekehrt;

b) ISO/IEC 27001 und ISO/IEC 20000-1 gemeinsam umsetzen;

c) bereits vorhandene Managementsysteme nach ISO/IEC 27001 und ISO/IEC 20000-1 integrieren.

Dieses Dokument konzentriert sich ausschließlich auf die integrierte Umsetzung eines Informationssicherheitsmanagementsystems (ISMS), wie es in ISO/IEC 27001 festgelegt ist, und eines Servicemanagementsystems (SMS), wie es in ISO/IEC 20000-1 festgelegt ist.

In der Praxis können ISO/IEC 27001 und ISO/IEC 20000-1 auch mit anderen Managementsystemstandards, wie ISO 9001 und ISO 14001, integriert werden.

Zweck: Unterstützung von Organisationen beim besseren Verständnis der Merkmale, Gemeinsamkeiten und Unterschiede von ISO/IEC 27001 und ISO/IEC 20000-1 und bei der Planung eines integrierten Managementsystems, das mit beiden internationalen Normen übereinstimmt.

5.4.8 ISO/IEC 27014

Information technology — Security techniques — Governance of information security (Informationstechnik — IT-Sicherheitsverfahren — Governance von Informationssicherheit)

Anwendungsbereich: Dieses Dokument liefert Anleitung zu den Grundlagen und Prozessen der Steuerung von Informationssicherheit, mit denen Organisationen das Informationssicherheitsmanagement bewerten, führen und überwachen können.

Zweck: Informationssicherheit ist für Organisationen zu einem Schlüsselthema geworden. Einerseits gibt es immer mehr regulatorische Anforderungen, andererseits kann ein Fehler bei den Informationssicherheitsmaßnahmen direkte Auswirkung auf den guten Ruf einer Organisation haben. Deshalb sind Steuerungsgremien in ihren Steuerungsverantwortlichkeiten zunehmend gefordert, den Überblick über die Informationssicherheit zu wahren, um sicherzustellen, dass die Ziele der Organisation erreicht werden.

5.4.9 ISO/IEC TR 27016

Information technology — Security techniques — Information security management — Organizational economics (Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheitsmanagement — organisationsbezogene Wirtschaftlichkeit)

Anwendungsbereich: Dieses Dokument liefert Organisationen eine Methodik zum besseren ökonomischen Verständnis für die genaue Bewertung ihrer ermittelten Informationswerte und der für diese vorhandenen Risiken sowie beim Wertschätzen des Nutzens, den Informationssicherheitsmaßnahmen für diese Informationswerte beitragen und bei der Bestimmung des optimalen Niveaus von Ressourcen zum Schutz dieser Informationswerte.

Zweck: Dieses Dokument ergänzt die ISMS-Normenfamilie um eine ökonomische Perspektive hinsichtlich des Schutzes der Informationswerte der Organisation im Kontext mit dem größeren gesellschaftlichen Umfeld, in dem die Organisation tätig ist, und gibt anhand von Modellen und Beispielen eine Anleitung, wie Informationssicherheit im Hinblick auf die betriebliche Wirtschaftlichkeit eingesetzt wird.

5.4.10 ISO/IEC 27021

Information technology — Security techniques — Information security management — Competence requirements for information security management systems professionals

Anwendungsbereich: Dieses Dokument legt die Anforderungen an die Kompetenz von ISMS Fachkräften fest, die die Einführung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines oder mehrerer Informationssicherheitsmanagmentsysteme auf Basis von ISO/IEC 27001:2013 leiten oder darin eingebunden sind.

Zweck: Dieses Dokument ist vorgesehen zum Gebrauch durch:

a) Personen, die ihre Kompetenz als Fachkraft für Informationssicherheitsmanagementsysteme nachweisen möchten oder die erforderlichen Kompetenzen verstehen und erlangen möchten, um in diesem Bereich tätig zu werden oder ihr Wissen vertiefen möchten;

b) Organisationen, die potentielle ISMS Fachkräfte suchen, um die geforderten Kompetenzen für Positionen mit ISMS Bezug festzulegen;

c) Stellen, die Zertifizierungen für ISMS Fachkräfte entwickeln und einen Wissensfundus (en: body of knowledge (BOK)) für die Quellensuche benötigen; und

d) Organisationen für Aus- und Weiterbildung, wie etwa Universitäten und Berufsschulen, um ihre Lehrpläne und Kurse an den Kompetenzen für ISMS Fachkräfte auszurichten

5.5 Normen, die branchenspezifische Leitfäden beschreiben

5.5.1 ISO/IEC 27010

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications (Informationstechnik — Sicherheitsverfahren – Informationssicherheits-management für sektor- und organisationsübergreifende Kommunikation)

Anwendungsbereich: Dieses Dokument liefert ergänzend zu den Anleitungen der Normenfamilie ISO/IEC 27000 Leitfäden zur Umsetzung des Informationssicherheitsmanagements in informationsteilenden Gemeinschaften.

Dieses Dokument liefert Maßnahmen und Anleitung zum Einführen, Umsetzen, Aufrechterhalten und Verbessern der Informationssicherheit bei der Kommunikation, speziell zwischen Organisationen und Sektoren.

Zweck: Dieses Dokument ist anwendbar auf alle Formen des Austauschs und des Teilens sensibler Information, sowohl öffentlich als auch privat, national wie international, innerhalb derselben Branche oder desselben Marktsektors oder zwischen den Branchen oder Sektoren. Insbesondere kann sie auf den Austausch und das Teilen von Information in Bezug auf Bereitstellung, Instandhaltung und Schutz der kritischen Infrastruktur einer Organisation oder eines Nationalstaates anwendbar sein.

5.5.2 ISO/IEC 27011

Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations (Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen)

Anwendungsbereich: Dieses Dokument liefert Leitlinien, welche die Umsetzung von Informationssicherheitsmaßnahmen für Telekommunikationsunternehmen unterstützen.

Zweck: ISO/IEC 27011 ermöglicht es Telekommunikationsunternehmen, Mindestanforderungen für Informationssicherheitsmanagement hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit und anderer zutreffender Sicherheitseigenschaften zu erfüllen.

5.5.3 ISO/IEC 27017

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Informationstechnik — Sicherheitsverfahren — Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud-Dienste)

Anwendungsbereich: ISO/IEC 27017 bietet Leitlinien für Informationssicherheitsmaßnahmen, die anwendbar für die Erbringung und Nutzung von Cloud-Diensten sind, durch Bereitstellen von:

— einer zusätzlichen Anleitung zur Umsetzung von relevanten Maßnahmen, die in ISO/IEC 27002 festgelegt sind;

— zusätzlichen Maßnahmen mit Anleitung zur Umsetzung, die speziell Cloud-Dienste betreffen.

Zweck: Dieses Dokument liefert Maßnahmen und eine Anleitung zur Umsetzung, sowohl für Cloud-Dienstleister als auch für Cloud-Dienst-Kunden.

5.5.4 ISO/IEC 27018

Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors (Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung

Anwendungsbereich: ISO/IEC 27018 legt allgemein anerkannte Maßnahmenziele, Maßnahmen und Leitlinien für die Umsetzung von Maßnahmen zum Schutz personenbezogener Daten (pbD) nach den in ISO/IEC 29100 festgelegten Datenschutzprinzipien für die Public-Cloud-Computing-Umgebung fest.

Zweck: Dieses Dokument ist auf Organisationen einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisationen anwendbar, die als Verarbeiter von personenbezogenen Daten anderen Organisationen im Rahmen eines Vertrags Informationsverarbeitungsdienste mittels Cloud-Computing zur Verfügung stellen. Die in diesem Dokument

festgelegten Leitlinien können auch für Organisationen von Bedeutung sein, die als verantwortliche Stellen fungieren; diese verantwortlichen Stellen können jedoch weiteren Gesetzen, Vorschriften und Verpflichtungen zum Schutz von personenbezogenen Daten unterliegen, die nicht für Verarbeiter von personenbezogenen Daten gelten. Dieses Dokument ist nicht dafür vorgesehen, auch derartige zusätzliche Verpflichtungen abzudecken.

5.5.5 ISO/IEC 27019

Information technology — Security techniques — Information security controls for the energy utility industry (Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmaßnahmen für die Energieversorgung)

Anwendungsbereich: Dieses Dokument gibt eine auf ISO/IEC 27002:2013 basierende Anleitung zur Anwendung bei Prozesssteuerungssystemen, die von der Energieversorgungsindustrie genutzt werden, die zur Steuerung und Überwachung von Produktion oder Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas, Öl und Wärme und für die Steuerung von verbundenen unterstützenden Prozessen dienen. Dies umfasst insbesondere folgendes:

— zentrale und dezentrale Prozess-, Leit-, Automatisierungs- und Überwachungs-technik sowie die für ihren Betrieb genutzten Informations-Systeme, wie z. B. Programmier- und Parametriergeräte;

— digitale Steuerungs- und Automatisierungskomponenten wie Leit- und Feldgeräte, Controller oder SPSen inklusive digitaler Sensor- und Aktorelemente;

— alle weiteren in der Prozesstechnik genutzten unterstützenden Informations-Systeme, zum Beispiel für ergänzende Aufgaben der Visualisierung und Steuerung, zur Überwachung, Datenarchivierung, Berichtswesen und Dokumentationszwecke;

— Kommunikationstechnik, die im Bereich der Prozesssteuerung eingesetzt wird, zum Beispiel Netzwerk-, Telemetrie-, Fernwirk- und Fernsteuertechnik;

— digitale Mess- und Zählvorrichtungen, z. B. zur Verbrauchs-, Erzeugungs- und Emissionswerterfassung;

— Messgeräte zum Beispiel für Emissionswerte;

— digitale Schutz- und Safety-Systeme, z. B. Schutzgeräte, Sicherheits-PLCs oder Maschinenschutzkomponenten;

— Energiemanagementsysteme, zum Beispiel verteilte Energiesysteme, elektrische Ladeinfrastrukturen, in privaten Haushalten, Wohngebäuden oder Industriekundeneinrichtungen;

— verteilte Komponenten zukünftiger Smart-Grid-Umgebungen, zum Beispiel in Energieversorgungsnetzen in privaten Haushalten, Wohngebäuden oder Industriekundeneinrichtungen;

— alle Programme und Anwendungen, die auf den vorgenannten Systemen eingesetzt werden, zum Beispiel Anwendungen für verteilte Managementsysteme oder Schwarzfallmanagementsysteme;

— jedwede Liegenschaft, die oben aufgeführte Einrichtungen oder Systeme beherbergt;

— Fernwartungssysteme für die oben aufgeführten Systeme

Dieses Dokument ist nicht anwendbar im Bereich der Nukleartechnik. Dieser Bereich wird durch IEC 62645 abgedeckt.

Dieses Dokument beinhaltet ebenso eine Anforderung, die in ISO/IEC 27001:2013 beschriebenen Risikobeurteilungs- und-behandlungsprozesse an den in diesem Dokument bereitgestellten Leitfaden für die Energieversorgung anzupassen.

Zweck: Zusätzlich zu den Sicherheitszielen und –maßnahmen, die in ISO/IEC 27002 dargelegt sind, liefert dieses Dokument Leitlinien zu Informationssicherheitsmaßnahmen, die sich mit weiteren speziellen Anforderungen befassen, für Systeme, die in der Energieversorgung genutzt werden.

5.5.6 ISO 27799

Health informatics — Information security management in health using ISO/IEC 27002 (*Medizinische Informatik — Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002)*

Anwendungsbereich: Dieses Dokument gibt eine Hilfestellung für organisatorische Informationssicherheitsstandards und Informationssicherheitspraktiken, einschließlich der Auswahl, Umsetzung und Handhabung von Maßnahmen, welche die Informationssicherheitsrisiko-Umgebung der jeweiligen Organisation berücksichtigt.

Dieses Dokument gibt eine Umsetzungshilfestellung für die Maßnahmen nach ISO/IEC 27002 und ergänzt diese, wo notwendig, so dass sie wirksam zur Handhabung von Gesundheitsinformationssicherheit eingesetzt werden können.

Zweck: ISO 27799 stellt Organisationen im Gesundheitswesen eine Anpassung der Leitlinien der ISO/IEC 27002 für ihren Bereich bereit, die ergänzend zu der Anleitung geliefert wird, um die Anforderungen nach ISO/IEC 27001:2013, Anhang A, zu erfüllen.

Literaturhinweise

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO/IEC/IEEE 15939:2017, *Systems and software engineering — Measurement process*

[3] ISO/IEC 17021:2011, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[4] ISO 19011:2011, *Guidelines for auditing management systems*

[5] ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

[6] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[7] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[8] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[9] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[10] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[11] ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[12] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[13] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[14] ISO/IEC 27009, *Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements*

[15] ISO/IEC 27010, *Information technology — Security techniques — Information security management guidelines for inter-sector and inter-organizational communications*

[16] ISO/IEC 27011, *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[17] ISO/IEC 27013, *Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

[18] ISO/IEC 27014, *Information technology — Security techniques — Governance of information security*

[19] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[20] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[21] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for PII protection of personally identifiable information (PII) in public clouds acting as PII processors*

[22] ISO/IEC 27019, *Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

[23] ISO/IEC 27021, *Information technology — Security techniques — Competence requirements for information security management systems professionals*

[24] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*

[25] ISO/IEC Guide 73:2009, *Risk Management — Vocabulary*