DEUTSCHE NORM Juli 2011

DIN ISO/IEC 27000

DIN

ICS 01.040.35; 35.040

Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2009)

Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2009)

Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité des informations – Vue d'ensemble et vocabulaire (ISO/CEI 27000:2009)

Gesamtumfang 26 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Preisgruppe 13
www.din.de
www.beuth.de

a 1769120

Inhalt

Nationales Vorwort

Die Internationale Norm ISO/IEC 27000:2009 (1. Ausgabe) wurde in deutscher Sprachfassung unverändert in das Deutsche Normenwerk übernommen. Fachlich zuständig ist für diese Deutsche Norm der Arbeitsausschuss NA 043-01-27 AA „IT-Sicherheitsverfahren“ des Normenausschusses Informationstechnik und Anwendungen (NIA) im DIN.

Die dieser Norm zugrunde liegende Internationale Norm ISO/IEC 27000:2009 wurde von ISO/IEC JTC 1/SC 27 (International Organization for Standardization/International Electrotechnical Commission — Joint Technical Committee 1 „Information Technology; Subcommittee 27 „Security techniques“) erarbeitet.

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

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 9000	siehe	DIN EN ISO 9000
ISO/IEC 17021	siehe	DIN EN ISO/IEC 17021
ISO 19011	siehe	DIN EN ISO 19011
ISO/IEC 27001	siehe	DIN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN ISO/IEC 27002
ISO 27799	siehe	DIN EN ISO 27799

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 9000, *Qualitätsmanagementsysteme — Grundlagen und Begriffe*

DIN EN ISO/IEC 17021, *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren*

DIN EN ISO 19011, *Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen*

DIN ISO/IEC 27001, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen*

DIN ISO/IEC 27002, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management*

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

Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie

0 Einleitung

0.1 Überblick

Internationale Normen für Managementsysteme stellen ein Modell zur Verfügung, dem bei der Einrichtung und dem Betrieb eines Managementsystems gefolgt werden kann. Dieses Modell berücksichtigt die Merkmale über die Experten dieses Gebietes Konsens darüber erzielt haben, dass sie dem aktuellen internationalen Stand der Technik entsprechen. ISO/IEC JTC1 SC27 unterhält ein Experten-Komitee, das sich der Entwicklung von Internationalen Normen für Managementsysteme für die Informationssicherheit widmet, welche auch als ISMS-Normenfamilie bekannt sind.

Durch die Anwendung der ISMS-Normenfamilie können Institutionen eine Rahmenstruktur für das Management der Sicherheit ihrer Informationswerte entwickeln und umsetzen und sich auf eine unabhängige Bewertung ihres ISMS im Hinblick auf den Schutz von Informationen, wie z. B. Finanzdaten, geistiges Eigentum, Personaldaten, usw., oder Informationen, die ihnen von Kunden oder Dritten anvertraut wurden, vorbereiten.

0.2 ISMS-Normenfamilie

Die ISMS-Normenfamilie[1)] soll Institutionen jeder Art und Größe dabei unterstützen, ein ISMS umzusetzen und zu betreiben. Die ISMS-Normenfamilie besteht aus den folgenden Normen mit dem allgemeinen Titel *Information technology — Security techniques*:

ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information security management systems — Requirements*

ISO/IEC 27002:2005, *Code of practice for information security management*

ISO/IEC 27003, *Information security management system implementation guidance*

ISO/IEC 27004, *Information security management — Measurement*

ISO/IEC 27005:2008, *Information security risk management*

ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems*

ISO/IEC 27007, *Guidelines for information security management systems auditing*

1) In diesem Abschnitt genannte Normen, bei denen kein Erscheinungsjahr angegeben wurde, sind noch in Arbeit.

ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

ANMERKUNG Der allgemeine Titel „*Information technology — Security techniques*“ weist darauf hin, dass diese Normen vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*, ausgearbeitet wurden.

Internationale Normen ohne den gleichen allgemeinen Titel, die auch Teil der ISMS-Normenfamile sind, sind folgende:

ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

0.3 Ziel dieser Internationalen Norm

Diese Internationale Norm bietet einen Überblick über Managementsysteme für die Informationssicherheit, die Gegenstand der ISMS-Normenfamilie sind und definiert die zugehörige Terminologie.

ANMERKUNG Anhang A stellt klar, wie aufgrund der Wortwahl Anforderungen und/oder Anleitung in der ISMS-Normenfamilie ausgedrückt werden.

Die ISMS-Normenfamilie umfasst Normen, die

a) Anforderungen an ein ISMS und deren Zertifizierungsstellen definieren;

b) Direkte Unterstützung, detaillierte Anleitung und/oder Interpretation für die übergeordneten Plan-Do-Check-Act[N1)] (PDCA)-Prozesse und für die Anforderungen zur Verfügung stellen;

c) branchenspezifische Richtlinien für ISMS behandeln; und

d) Konformitätsprüfungen für ISMS behandeln.

Die Terminologie und Definitionen, die in dieser Internationalen Norm zur Verfügung gestellt werden:

— umfassen Begriffe und Definitionen, die häufig in der ISMS-Normenfamilie verwendet werden;

— umfassen nicht alle Begriffe und Definitionen, die in der ISMS-Normenfamilie angewendet werden; und

— schränken nicht die ISMS-Normenfamilie in der Definition von Begriffen zur eigenen Verwendung ein.

Normen, die lediglich die Umsetzung von Maßnahmen nach ISO/IEC 27002 behandeln, im Gegensatz zur Behandlung aller Maßnahmen, sind von der ISMS-Normenfamilie ausgeschlossen.

Um die Entwicklung der ISMS-Normenfamilie widerzuspiegeln, ist zu erwarten, dass diese Internationale Norm kontinuierlich und häufiger aktualisiert wird, als dies üblicherweise bei anderen ISO/IEC-Normen der Fall ist.

N1) Nationale Fußnote: „Plan-Do-Check-Act process“ ist der Kreislauf des Planens, Durchführens, Prüfens und Handelns.

1 Anwendungsbereich

Diese Internationale Norm bietet:

a) einen Überblick über die ISMS-Normenfamilie;

b) eine Einführung in das Thema Informationssicherheitsmanagementsysteme (ISMS);

c) eine Kurzbeschreibung des Plan-Do-Check-Act (PDCA)-Prozesses; und

d) Terminologie und Definitionen zum Gebrauch in der ISMS-Normenfamilie.

Diese Internationale Norm gilt für alle Arten von Institutionen (z. B. Wirtschaftsunternehmen, Behörden, gemeinnützige Institutionen).

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG Wird in einer Definition oder Anmerkung ein Begriff verwendet, der an einer anderen Stelle in diesem Abschnitt definiert wird, so wird dies durch Fettdruck gefolgt von der in Klammern gesetzten Nummer des Eintrags angezeigt. Ein solcher fett gedruckter Begriff kann in der Definition durch seine vollständige Definition ersetzt werden.

BEISPIEL

Angriff (2.4) ist definiert als „Versuch, einen **Wert** (2.3) zu zerstören, offen zu legen, zu verändern, unbrauchbar zu machen, zu stehlen oder nicht autorisierten Zugriff auf ihn zu erlangen oder ihn ohne Berechtigung zu nutzen“;

Wert ist wiederum definiert als „alles, was für die Institution von Wert ist“.

Wenn der Begriff „**Wert**“ durch seine Definition ersetzt wird:

wird aus dem Begriff „**Angriff**“ ein „Versuch, alles, was für die Institution von Wert ist, zu zerstören, offen zu legen, zu verändern, unbrauchbar zu machen, zu stehlen oder nicht autorisierten Zugriff darauf zu erlangen oder es ohne Berechtigung zu nutzen“.

2.1
Zugriffskontrolle
Sicherstellung, dass der Zugriff auf **Werte** (2.3) autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt

2.2
Zurechenbarkeit
Verantwortung einer Einheit für ihre Handlungen und Entscheidungen

2.3
Wert
alles, was für die Institution von Wert ist

ANMERKUNG Es gibt viele Arten von Werten, einschließlich:

a) **Informationen** (2.18);
b) Software, z. B. Computerprogramme;
c) materielle Werte, z. B. Computer;
d) Dienstleistungen;
e) Menschen und ihren Qualifikationen, Fähigkeiten und Erfahrung; und
f) immaterielle Werte, z. B. Reputation und Image.

2.4
Angriff
Versuch, einen **Wert** (2.3) zu zerstören, offen zu legen, zu verändern, unbrauchbar zu machen, zu stehlen oder nicht autorisierten Zugriff auf ihn zu erlangen oder ihn ohne Berechtigung zu nutzen

2.5
Authentisierung
Sicherstellung, dass die von einer Einheit behauptete Eigenschaft korrekt ist

2.6
Authentizität
Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt

2.7
Verfügbarkeit
Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein

2.8
Business Continuity
Prozesse (2.31) und/oder **Verfahren** (2.30), die der Sicherstellung eines kontinuierlichen Geschäftsbetriebs dienen

2.9
Vertraulichkeit
Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder **Prozessen** (2.31) nicht verfügbar gemacht oder enthüllt werden

2.10
Maßnahme
Mittel zum Management von **Risiken** (2.34), einschließlich von **Leitlinien** (2.28), **Verfahren** (2.30), **Richtlinien** (2.16), Methoden oder Organisationsstrukturen, die verwaltender, technischer, leitender oder gesetzlicher Natur sein können

ANMERKUNG Der Begriff „Maßnahme“ wird auch als Synonym für „Sicherheitsmaßnahme“ oder „Gegenmaßnahme“ benutzt.

2.11
Maßnahmenziel
Beschreibung, was durch die Umsetzung von **Maßnahmen** (2.10) als Ergebnis erreicht werden soll

2.12
Korrekturmaßnahme
Maßnahme zur Beseitigung der Ursache eines erkannten Fehlers oder einer anderen erkannten unerwünschten Situation

[ISO 9000:2005]

2.13
Wirksamkeit
Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden

[ISO 9000:2005]

2.14
Effizienz
Beziehung zwischen den erzielten Ergebnissen und dem Grad der Nutzung der Ressourcen

2.15
Ereignis
Auftreten von ungewöhnlichen Umständen

[ISO/IEC Guide 73:2002]

2.16
Richtlinie
Empfehlung dessen, was an Umsetzung erwartet wird, um ein Ziel zu erreichen

2.17
Auswirkung
Verschlechterung des Niveaus der erreichten Unternehmensziele

2.18
Informationswert
Wissen oder Daten, die von Wert für die Institution sind

2.19
Informationssicherheit
Aufrechterhaltung der **Vertraulichkeit** (2.9), **Integrität** (2.25) und **Verfügbarkeit** (2.7) von Informationen

ANMERKUNG Zusätzlich können auch andere Eigenschaften wie **Authentizität** (2.6), **Zurechenbarkeit** (2.2), **Nicht-Abstreitbarkeit** (2.27) und **Verlässlichkeit** (2.33) einbezogen werden.

2.20
Informationssicherheits-Ereignis
erkanntes Auftreten eines System-, Service- oder Netzwerkzustands, der einen möglichen Verstoß gegen die **Leitlinie** (2.28) zur **Informationssicherheit** (2.19), das Versagen von **Maßnahmen** (2.10) oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt

2.21
Informationssicherheits-Vorfall
einzelnes oder eine Reihe von unerwünschten oder unerwarteten **Informationssicherheits-Ereignissen** (2.20), bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die **Informationssicherheit** (2.19) bedroht wird

2.22
Management von Informationssicherheits-Vorfällen
Prozesse (2.31) der Entdeckung, Berichterstattung, Bewertung von, Reaktion auf, Behandlung von und des Lernens aus **Informationssicherheits-Vorfällen** (2.21)

2.23
Informationssicherheitsmanagementsystem
ISMS
Teil des gesamten **Managementsystems** (2.26), der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der **Informationssicherheit** (2.19) abdeckt

2.24
Informationssicherheits-Risiko
Möglichkeit, dass eine vorhandene **Bedrohung** (2.45) die eine **Schwachstelle** (2.46) eines **Wertes** (2.3) oder einer Gruppe von Werten ausnutzt und dadurch der Institution Schaden zufügen könnte

2.25
Integrität
Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von **Werten** (2.3)

2.26
Managementsystem
Rahmenwerk von **Leitlinien** (2.28), **Verfahren** (2.30), **Richtlinien** (2.16) und den zugehörigen Ressourcen, um die Ziele der Institution zu erreichen

2.27
Nicht-Abstreitbarkeit
Fähigkeit, das Auftreten eines behaupteten **Ereignisses** (2.15) oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des **Ereignisses** (2.15) oder der Handlung und die Beteiligung von Einheiten an dem **Ereignis** (2.15) zu entscheiden

2.28
Leitlinie
vom Management formell ausgedrückte Gesamtintention und -richtung

2.29
Vorbeugungsmaßnahme
Maßnahme zur Beseitigung der Ursache eines möglichen Fehlers oder einer anderen möglichen unerwünschten Situation

[ISO 9000:2005]

2.30
Verfahren
festgelegte Art und Weise, eine Tätigkeit oder einen **Prozess** (2.31) auszuführen

[ISO 9000:2005]

2.31
Prozess
Satz von in Wechselbeziehung oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt

[ISO 9000:2005]

2.32
Aufzeichnung
Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt

[ISO 9000:2005]

2.33
Verlässlichkeit
Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

2.34
Risiko
Kombination aus der Wahrscheinlichkeit eines **Ereignisses** (2.15) und dessen Auswirkungen

[ISO/IEC Guide 73:2002]

2.35
Risikoakzeptanz
Entscheidung, ein **Risiko** (2.34) zu akzeptieren

[ISO/IEC Guide 73:2002]

2.36
Risikoanalyse
systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des **Risikos** (2.34)

[ISO/IEC Guide 73:2002]

ANMERKUNG Die Risikoanalyse bildet die Grundlage der **Risikobewertung** (2.41), **Risikobehandlung** (2.43) und **Risikoakzeptanz** (2.35).

2.37
Risikoeinschätzung
gesamter **Prozess** (2.31) der **Risikoanalyse** (2.36) und **Risikobewertung** (2.41)

[ISO/IEC Guide 73:2002]

2.38
Risikokommunikation
Austausch oder gemeinsame Nutzung von Informationen über **Risiken** (2.34) zwischen Entscheidungsträgern und anderen Stakeholdern

[ISO/IEC Guide 73:2002]

2.39
Risikokriterien
Bezugsrahmen für die Einschätzung der Bedeutung eines **Risikos** (2.34)

[ISO/IEC Guide 73:2002]

2.40
Risikobestimmung
Tätigkeit, bei der der Wahrscheinlichkeit und den Auswirkungen eines **Risikos** (2.34) Werte zugeordnet werden

[ISO/IEC Guide 73:2002]

2.41
Risikobewertung
Prozess (2.31), in dem das eingeschätzte **Risiko** (2.34) mit den festgelegten Risikokriterien (2.39) verglichen wird, um die Bedeutung des **Risikos** (2.34) zu bestimmen

[ISO/IEC Guide 73:2002]

2.42
Risikomanagement
koordinierte Tätigkeit zur Leitung und Kontrolle einer Institution in Bezug auf **Risiken** (2.34)

[ISO/IEC Guide 73:2002]

ANMERKUNG Risikomanagement beinhaltet normalerweise **Risikoeinschätzung** (2.37), **Risikobehandlung** (2.43), **Risikoakzeptanz** (2.35), **Risikokommunikation** (2.38), Risikoüberwachung und Risikoüberprüfung.

2.43
Risikobehandlung
Prozess (2.31) der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des **Risikos** (2.34)

[ISO/IEC Guide 73:2002]

2.44
Erklärung zur Anwendbarkeit
Dokument, das die **Maßnahmenziele** (2.11) und **Maßnahmen** (2.10) beschreibt, die für das **ISMS** (2.23) einer Institution relevant und anwendbar sind

2.45
Bedrohung
möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden des Systems oder der Institution führen kann

2.46
Schwachstelle
Schwäche eines **Werts** (2.3) oder einer **Maßnahme** (2.10), die von einer **Bedrohung** (2.45) ausgenutzt werden kann

3 Managementsysteme für die Informationssicherheit

3.1 Einleitung

Institutionen jeder Art und Größe:

a) sammeln, verarbeiten, speichern und übermitteln große Datenmengen;

b) betrachten Informationen und zugehörige Prozesse, Systeme, Netzwerke und Personen als wichtige Werte, die für die Erreichung ihrer Ziele notwendig sind;

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

d) ändern diese Risiken durch die Umsetzung von Informationssicherheits-Maßnahmen.

Sämtliche Informationen, die von einer Institution erfasst und verarbeitet werden, unterliegen der Bedrohung durch Angriffe, Fehler, Naturereignisse (z. B. Überschwemmung oder Feuer), usw., sowie Schwachstellen, die ihre Nutzung grundsätzlich mit sich bringt. Der Begriff Informationssicherheit basiert im Allgemeinen darauf, dass Informationen als ein Wirtschaftsgut angesehen werden, welches 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 Leistungsfähigkeit.

Informationswerte durch Definition, Erlangung, Pflege und Verbesserung von Informationssicherheit wirksam zu schützen ist grundlegend, um eine Institution in die Lage zu versetzen, ihre Ziele zu erreichen und die Einhaltung von gesetzlichen Regelungen sowie ihr Image aufrecht zu halten und zu verbessern. Diese koordinierten Tätigkeiten, die die Umsetzung geeigneter Maßnahmen und die Behandlung von unakzeptablen Informationssicherheits-Risiken steuern, werden allgemein als Bestandteile des Informationssicherheits-management bezeichnet.

Da Informationssicherheits-Risiken und die Wirksamkeit der Maßnahmen sich in Abhängigkeit von sich wandelnden Umständen verändern, ist es erforderlich, dass die Institutionen:

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

b) die auftretenden Risiken, die behandelt werden müssen, identifizieren; „und“

c) angemessene, bedarfsgerechte Maßnahmen implementieren und verbessern.

Um solche Tätigkeiten im Bereich der Informationssicherheit zu verknüpfen und zu koordinieren, muss jede Institution ihre eigene Leitlinie und ihre Ziele für die Informationssicherheit festlegen und diese Ziele wirksam durch den Einsatz eines Managementsystems erreichen.

3.2 Was ist ein ISMS?

3.2.1 Übersicht und Grundsätze

Ein ISMS (Informationssicherheitsmanagementsystem) liefert ein Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung des Schutzes von Informationswerten, um auf der Basis einer Risikoeinschätzung und des Risikoakzeptanzniveaus der Institution, das so gestaltet ist, die Risiken wirksam zu behandeln und zu managen, Unternehmensziele zu erreichen. Eine Anforderungsanalyse für den Schutz von Informationswerten und die Anwendung angemessener Maßnahmen, um den Schutz dieser Informationswerte bedarfsgerecht sicherzustellen, trägt zu der erfolgreichen Implementierung 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 von gesellschaftlichen Werten;

e) Risikoeinschätzungen, die angemessene Maßnahmen festlegen, um ein akzeptables Risikoniveau zu erreichen;

f) Einbeziehung von Sicherheit als grundlegendem Bestandteil von Informationsnetzwerken und -systemen;

g) aktive Prävention gegen und Entdeckung von Informationssicherheits-Vorfälle(n);

h) Sicherstellung einer umfassenden Herangehensweise an das Management von Informationssicherheit; und

i) kontinuierliche Neubewertung von Informationssicherheit und der Umsetzung geeigneter Änderungen.

3.2.2 Informationen

Informationen sind Werte, die wie andere wichtige Wirtschaftsgüter für den Geschäftsbetrieb einer Institution entscheidend sind und infolgedessen angemessen geschützt werden müssen. 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 wie das 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.

Der Informationsstand einer Institution hängt von der Informations- und Kommunikationstechnologie ab. Diese Technologie ist ein entscheidender Bestandteil jeder Institution und trägt zu der Erzeugung, der Verarbeitung, dem Speichern, der Übermittlung, dem Schutz und der Vernichtung von Informationen bei. Dort wo der Umfang des miteinander verbundenen globalen wirtschaftlichen Umfelds wächst, wächst auch die Notwendigkeit, Informationen zu schützen, da diese nun einer größeren Vielfalt von Bedrohungen und Schwachstellen ausgesetzt sind.

3.2.3 Informationssicherheit

Informationssicherheit umfasst drei Hauptaspekte: Vertraulichkeit, Verfügbarkeit und Integrität. Mit dem Ziel, anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb (*Business Continuity*) sicherzustellen und durch die Minimierung von Beeinträchtigungen bedingt Informationssicherheit die Anwendung und das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen.

Informationssicherheit wird durch die Umsetzung eines geeigneten Katalogs von Maßnahmen erreicht, die durch einen festgelegten Risikomanagementprozess ausgewählt und mit Hilfe eines ISMS organisiert werden, welches Leitlinien, 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 Sicherheits- und Unternehmensziele der Institution erreicht werden. Relevante Informationssicherheits-Maßnahmen sollen nahtlos in die Geschäftsprozesse der Institution integriert werden.

3.2.4 Management

Management schließt Tätigkeiten zur Führung, Kontrolle und kontinuierlichen Verbesserung der Institution 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 Institution bis hin zu Managementhierarchien in großen Institutionen, die sich aus vielen Individuen zusammensetzen.

In Bezug auf ein ISMS umfasst Management die Findung und Überwachung von Entscheidungen, die erforderlich sind, um Unternehmensziele durch den Schutz der Informationswerte der Institution zu erreichen. Das Management von Informationssicherheit findet Ausdruck in der Formulierung und Anwendung von Informationssicherheits-Leitlinien, -Standards, -Verfahren und -Richtlinien, die dann in der gesamten Institution und von allen Personen, die der Institution angehören, angewendet werden.

ANMERKUNG Der Begriff „Management“ kann sich manchmal auf Personen beziehen (d. h. eine Person oder Gruppe von Personen mit der Befugnis und Verantwortung für das Verhalten und die Leitung einer Institution). Der Begriff „Management“ wird in diesem Abschnitt nicht in diesem Sinne gebraucht.

3.2.5 Managementsystem

Ein Managementsystem nutzt ein System von Ressourcen, um die Ziele einer Institution zu erreichen. Das Managementsystem umfasst Organisationsstrukturen, Leitlinien, Planungstätigkeiten, Zuständigkeiten, Methoden, Verfahren, Prozesse und Ressourcen.

Im Hinblick auf Informationssicherheit ermöglicht ein Managementsystem einer Institution:

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

b) ihre Pläne und Tätigkeiten zu verbessern;

c) ihre Informationssicherheitsziele zu erfüllen;

d) Vorschriften, Gesetze und gewerbliche Verfügungen einzuhalten; und

e) die Informationswerte in einer organisierten Art und Weise zu managen, die die kontinuierliche Verbesserung und Anpassung an aktuelle Ziele der Institution und an das Umfeld fördert.

3.3 Prozessorientierter Ansatz

Institutionen müssen viele Tätigkeiten identifizieren und managen, um erfolgreich und leistungsfähig zu funktionieren. Jede Tätigkeit, die Ressourcen nutzt, muss gesteuert werden, um die Umwandlung von Eingaben zu Ergebnissen mittels einer Reihe von zusammenhängenden oder zusammenwirkenden Tätigkeiten zu ermöglichen — 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 Institution zusammen mit der Identifikation und Interaktion dieser Prozesse und ihrer Steuerung kann als „prozessorientierter Ansatz“ bezeichnet werden.

Der prozessorientierte Ansatz für ein ISMS, der in der ISMS-Normenfamilie dargelegt wird, basiert auf dem Regelkreis, der in den ISO-Normen für Managementsysteme zugrunde gelegt wird und der unter der Bezeichnung „Plan-Do-Check-Act-Prozess“ („Planen, Durchführen, Prüfen, Handeln“) bzw. „PDCA-Prozess“ bekannt ist.

a) Planen — lege Ziele fest und erstelle Pläne (analysiere die Situation der Institution, lege übergreifende Ziele fest, lege Vorgaben fest und entwickle Pläne, um sie zu erreichen);

b) Durchführen — setze Pläne um (tu, was geplant war);

c) Prüfen — erfasse Ergebnisse (messe/überwache, in welchem Maße die Ergebnisse den geplanten Zielen entsprechen); und

d) Handeln — korrigiere und verbessere die Tätigkeiten (lerne aus Fehlern, wie die Tätigkeiten verbessert und bessere Ergebnisse erzielt werden können).

3.4 Warum ist ein ISMS wichtig?

Ein Bestandteil des ISMS einer Institution ist die Beschäftigung mit den Risiken, die mit den Informationswerten der Institution verbunden sind. Das Erreichen von Informationssicherheit erfordert es, Risikomanagement zu betreiben und umfasst Risiken aufgrund von materiellen, menschlichen und technischen Bedrohungen, die mit allen Formen von Informationen, die die Institution hat oder nutzt, verbunden sind.

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

Die Planung und Umsetzung des ISMS einer Institution wird beeinflusst durch die Anforderungen und Ziele der Institution, den Sicherheitsbedarf, die angewandten Geschäftsprozesse und die Größe und Struktur der Institution. Die Konzeption und der Betrieb eines ISMS erfordern es, den Interessen und Anforderungen an die Informationssicherheit aller Stakeholder der Institution, einschließlich von 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. Institutionen und ihre Informationssysteme und Netzwerke sind mit Sicherheitsbedrohungen aus einer Vielfalt von Quellen konfrontiert, einschließlich von computergestütztem Betrug, Spionage, Sabotage, Vandalismus, Feuer und Überschwemmungen. Schäden an Informationssystemen und Netzwerken, die durch Schadcode, Computer-Hacking, und Denial-of-Service-Attacken 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 Institutionen die ISMS-Normenfamilie übernehmen, können sie ihre Fähigkeit, einheitliche und gegenseitig erkennbare Prinzipien der Informationssicherheit anzuwenden, Geschäftspartnern und anderen interessierten Dritten unter Beweis stellen.

Informationssicherheit wird bei der Planung und Entwicklung von Informationssystemen nicht immer berücksichtigt. Weiterhin wird Informationssicherheit oft als rein technische Lösung angesehen. Das Maß an Sicherheit, 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 Informationssystem kann mühevoll und teuer sein. Ein ISMS umfasst die Identifikation der bereits etablierten Maßnahmen und erfordert sorgfältige Planung und die Beachtung von Details. Zum Beispiel sind Zugangskontrollen, die sowohl technischer (logischer), physikalischer, administrativer Art oder eine Kombination dieser Typen sein können, ein Mittel um sicherzustellen, dass der Zugriff auf Informationswerte nur autorisiert und eingeschränkt auf Basis der Unternehmens- und Sicherheitsanforderungen erfolgt.

Die erfolgreiche Einführung eines ISMS ist wichtig, um Informationswerte zu schützen, die es einer Institution ermöglichen:

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

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

c) kontinuierlich ihre Maßnahmenumgebung zu verbessern; und

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

3.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS

3.5.1 Übersicht

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

a) Identifikation von Informationswerten und der mit ihnen verbundenen Sicherheits-Anforderungen (siehe 3.5.2);

b) Bestimmung von Informationssicherheits-Risiken (siehe 3.5.3);

c) Auswahl und Umsetzung geeigneter Maßnahmen, um unakzeptable Risiken zu handhaben (siehe 3.5.4); und

d) Überwachung, Wartung und Verbesserung der Wirksamkeit der Sicherheitsmaßnahmen in Zusammenhang mit den Informationswerten der Institution (siehe 3.5.5).

Um sicherzustellen, dass das ISMS wirksam die Informationswerte der Institution in einem laufenden Prozess schützt, ist es erforderlich, dass die Schritte (a) bis (d) fortlaufend wiederholt werden, um Veränderungen der Risiken oder der Strategie und Unternehmensziele der Institution zu identifizieren.

3.5.2 Identifizierung von Informationssicherheits-Anforderungen

Im Rahmen der übergeordneten Strategie und Unternehmensziele einer Institution 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) Unternehmensanforderungen an die Verarbeitung und das Speichern von Informationen; und

c) gesetzliche, behördliche und vertragliche Anforderungen.

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

3.5.3 Bestimmung von Informationssicherheits-Risiken

Das Management von Informationssicherheits-Risiken erfordert eine entsprechende Methode zur Risikoeinschätzung und Risikobehandlung, die soweit erforderlich eine Abschätzung der Kosten und des Nutzens, die gesetzlichen Anforderungen, soziale, wirtschaftliche und Umweltaspekte, die Interessen der Stakeholder, Prioritäten und anderen Vorgaben und Variablen umfassen kann. Die Ergebnisse dieser Einschätzung des Informationssicherheits-Risikos werden dabei helfen, die geeigneten Managemententscheidungen für die Tätigkeit und die Priorisierung des Managements von Informationssicherheits-Risiken festzulegen, und die geeigneten Sicherheitsmaßnahmen zum Schutz gegen diese Risiken umzusetzen. ISO/IEC 27005 liefert eine Anleitung zum Informationssicherheits-Risikomanagement, einschließlich von Hinweisen zur Risikoeinschätzung, -behandlung, -akzeptanz, -kommunikation, -überwachung und -überprüfung.

3.5.4 Auswahl und Umsetzung von Informationssicherheits-Maßnahmen

Wenn die Informationssicherheits-Anforderungen identifiziert und die Informationssicherheits-Risiken für die identifizierten Informationswerte bestimmt und bewertet wurden (einschließlich der Entscheidungen hinsichtlich der Behandlung von Informationssicherheits-Risiken), müssen angemessene Maßnahmen ausgewählt und umgesetzt werden, um sicherzustellen, dass die Informationssicherheits-Risiken auf ein für die Institution akzeptables Niveau gesenkt werden. Die Maßnahmen können der ISO/IEC 27002 entnommen, aus anderen geeigneten Maßnahmenkatalogen ausgewählt oder neu konzipiert werden, um je nach Bedarf spezielle Anforderungen zu erfüllen. Die Auswahl von Sicherheitsmaßnahmen ist abhängig von den Sicherheitsanforderungen, wobei die Kriterien für die Akzeptanz von Informationssicherheits-Risiken, Alternativen der Risikobehandlung und der allgemeine Risikomanagement-Ansatz der Institution in Betracht gezogen werden. Die Auswahl und Umsetzung von Maßnahmen kann durch eine Erklärung zur Anwendbarkeit dokumentiert werden, um die Einhaltung von Anforderungen zu fördern.

Die in ISO/IEC 27002 festgelegten Maßnahmen sind als Leitfaden anerkannt, der auf die meisten Institutionen angewendet und leicht so angepasst werden kann, dass er Institutionen unterschiedlicher Größe und Komplexität Rechnung trägt. Andere Normen in der ISMS-Normenfamilie liefern Anleitungen hinsichtlich der Auswahl und Anwendung von Informationssicherheits-Maßnahmen nach ISO/IEC 27002 für das Managementsystem (ISO/IEC 27001).

3.5.5 Überwachung, Pflege und Verbesserung der Wirksamkeit eines ISMS

Eine Institution muss ein ISMS warten und es durch Überwachung und Bewertung der Leistung gegenüber der Leitlinie und den Zielen der Institution verbessern, und die Ergebnisse dem Management zur Überprüfung zu berichten. Diese Überprüfung des ISMS wird den Nachweis der Gültigkeit, Richtigkeit und der Nachvollziehbarkeit von fehlerbehebenden, vorbeugenden und verbessernden Maßnahmen auf der Basis der Aufzeichnungen der überwachten Bereiche einschließlich der Überwachung von Informationssicherheits-Maßnahmen ermöglichen.

3.6 Kritische Erfolgsfaktoren für ein ISMS

Eine große Anzahl von Faktoren ist ausschlaggebend für die erfolgreiche Implementierung eines ISMS, um der Institution das Erreichen ihrer Unternehmensziele zu ermöglichen. Beispiele für kritische Erfolgsfaktoren sind:

a) eine an die Ziele angepasste Informationssicherheits-Leitlinie, mit Zielsetzungen und Tätigkeiten;

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

c) erkennbare Unterstützung und Engagement seitens aller Managementebenen, insbesondere der Unternehmensspitze;

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

e) ein nachhaltiges Bewusstsein für Informationssicherheit, Schulungs- und Fortbildungsprogramme, bei denen alle Mitarbeiter und andere betroffene Parteien über ihre Verpflichtungen im Bereich der Informationssicherheit nach den Leitlinien und Normen zur Informationssicherheit informiert werden und motiviert werden, entsprechend zu handeln;

f) ein leistungsfähiger Prozess zur Handhabung von Informationssicherheits-Vorfällen;

g) ein leistungsfähiger Ansatz zum Business Continuity-Management; und

h) ein Messsystem, das genutzt wird, um die Leistungsfähigkeit des Informationssicherheitsmanagements zu bewerten und Verbesserungsvorschläge zurück zu melden.

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

3.7 Vorteile der ISMS-Normenfamilie

Die Vorteile der Umsetzung eines ISMS resultieren in erster Linie aus der Verminderung von Informationssicherheits-Risiken (d. h. Senkung der Wahrscheinlichkeit von Informationssicherheits-Vorfällen und/oder ihrer Auswirkungen). Insbesondere umfassen die Vorteile der Übernahme der ISMS-Normenfamilie die folgenden Punkte:

a) Unterstützung des Prozesses der Festlegung, der Umsetzung, des Betriebs und der Pflege eines ganzheitlichen und kostengünstig integrierten und angepassten ISMS, das den Bedarf der Institution über verschiedene Arbeitsabläufe und Standorte hinweg deckt;

b) Unterstützung des Managements bei der Strukturierung der Herangehensweise an das Informationssicherheitsmanagement im Zusammenhang mit dem Risikomanagement des Unternehmens und der Unternehmensführung, einschließlich der Ausbildung und Schulung von Geschäfts- und Systeminhabern hinsichtlich des ganzheitlichen Managements von Informationssicherheit;

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

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

4 Aufbau der ISMS-Normenfamilie

4.1 Allgemeines

Die ISMS-Normenfamilie besteht aus in Wechselbeziehung stehenden Normen, die entweder schon veröffentlicht oder in Arbeit sind, und umfasst eine Anzahl von wichtigen strukturellen Komponenten. Diese Komponenten legen den Schwerpunkt auf normative Normen, die die Anforderungen an ISMS (ISO/IEC 27001) und die Anforderung an Zertifizierungsstellen (ISO/IEC 27006) für die beschreiben, die die Einhaltung von ISO/IEC 27001 zertifizieren. Andere Normen liefern Anleitungen für verschiedene Aspekte der Umsetzung eines ISMS und befassen sich mit einem generischen Prozess, maßnahmenbezogenen Richtlinien sowie mit branchenspezifischen Anleitungen. Die Beziehungen zwischen den einzelnen Normen der ISMS-Normenfamilie[2)] sind in Bild 1 dargestellt.

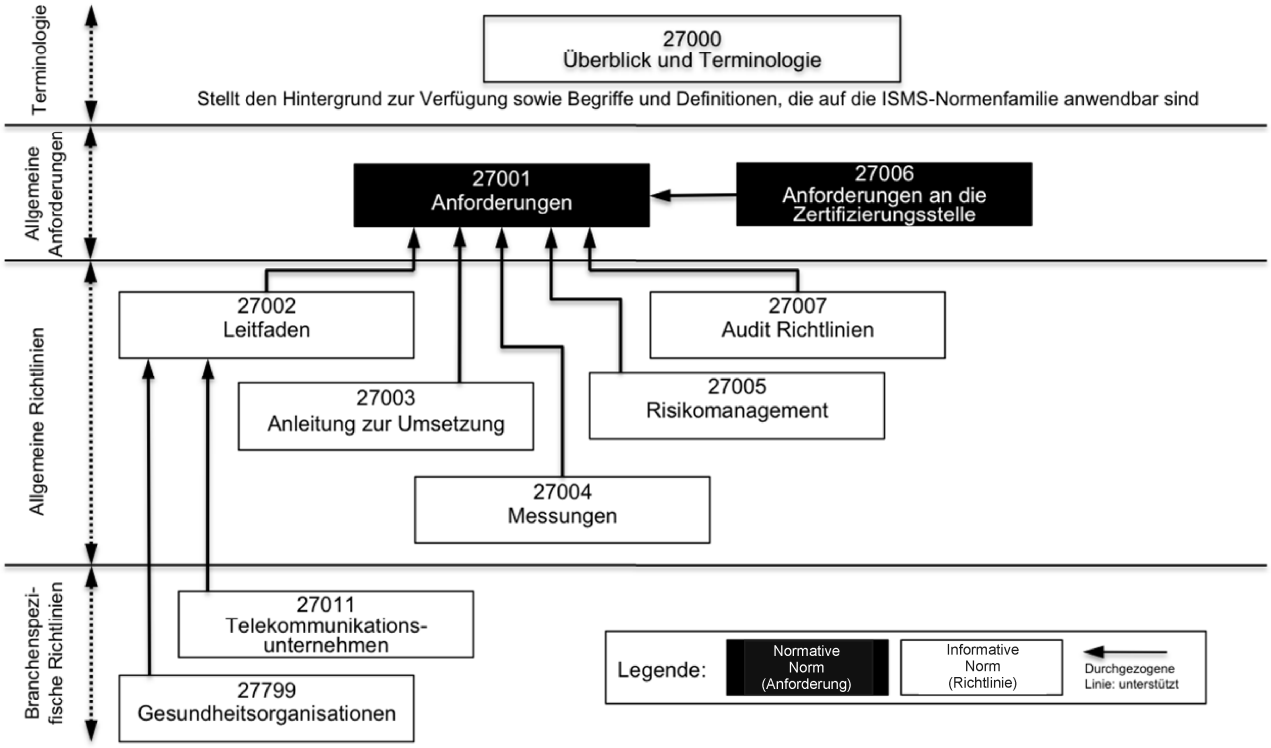

Bild 1 — Beziehungen der ISMS-Normenfamilie

Die folgenden Normen bieten direkte Unterstützung, detaillierte Anleitung und/oder die Auslegung der übergeordneten PDCA-Prozesse und -Anforderungen nach ISO/IEC 27001 (siehe 4.3.1): ISO/IEC 27000 (siehe 4.2.1), ISO/IEC 27002 (siehe 4.4.1), ISO/IEC 27003 (siehe 4.4.2), ISO/IEC 27004 (siehe 4.4.3), ISO/IEC 27005 (siehe 4.4.4) und ISO/IEC 27007 (siehe 4.4.5).

ISO/IEC 27006 (siehe 4.3.2) befasst sich mit den Anforderungen von Stellen, die ISMS-Zertifizierungen anbieten. ISO/IEC 27011 (siehe 4.5.1) und ISO 27799 (siehe 4.5.2) befassen sich mit branchenspezifischen Richtlinien für ISMS[3)].

---

2) Die Internationalen Normen ISO/IEC 27003, ISO/IEC 27004 und ISO/IEC 27007 sind derzeit in Arbeit.

3) ISO/IEC 27008, ISO/IEC 27009 und ISO/IEC 27010 sind für zukünftige Normen reserviert, die zur ISMS-Normenfamilie gehören und die noch nicht definiert waren, als diese Internationale Norm veröffentlicht wurde.

Die Normen der ISMS-Normenfamilie stehen in Beziehung zu vielen anderen ISO- und ISO/IEC-Normen und werden klassifiziert und genauer bezeichnet als:

a) Normen, die einen Überblick geben und die Terminologie beschreiben (siehe 4.2);

b) Normen, die Anforderungen festlegen (siehe 4.3);

c) Normen, die allgemeine Richtlinien beschreiben (siehe 4.4); oder

d) Normen, die branchenspezifische Richtlinien beschreiben (siehe 4.5).

4.2 Normen, die einen Überblick geben und die Terminologie beschreiben

4.2.1 ISO/IEC 27000 (dieses Dokument)

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Anwendungsbereich: Diese Internationale Norm liefert Institutionen und Einzelpersonen:

a) einen Überblick über die ISMS-Normenfamilie;

b) eine Einführung in den Bereich der Informationssicherheitsmanagementsysteme (ISMS);

c) eine Kurzbeschreibung des PDCA-Prozesses; und

d) die Terminologie und Definitionen, die durchgehend in der ISMS-Normenfamilie verwendet werden.

Zielsetzung: ISO/IEC 27000 beschreibt die Grundlagen von Managementsystemen für die Informationssicherheit, die Gegenstand der ISMS-Normenfamilie sind, und definiert die zugehörigen Begriffe.

4.3 Normen, die Anforderungen festlegen

4.3.1 ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements

Anwendungsbereich: Diese Internationale Norm legt die Anforderungen an die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und Verbesserung von formalisierten Informationssicherheitsmanagementsystemen (ISMS) im Rahmen der übergreifenden Unternehmensrisiken einer Institution fest. Sie legt Anforderungen an die Implementierung von Sicherheitsmaßnahmen fest, die speziell an die jeweiligen individuellen Bedürfnisse der Institution oder Teilbereiche der Institution angepasst sind. Diese Internationale Norm gilt allgemein für alle Arten von Institutionen (z. B. Wirtschaftsunternehmen, Behörden, gemeinnützige Institutionen).

Zielsetzung: ISO/IEC 27001 gibt normative Anforderungen an die Entwicklung und den Betrieb eines ISMS vor, einschließlich eines Maßnahmenkatalogs für die Kontrolle und Verringerung der Risiken, denen die Informationswerte unterliegen, die die Institution durch den Betrieb ihres ISMS zu schützen sucht. Institutionen, die ein ISMS betreiben, können Konformität auditieren und zertifizieren lassen. Die Maßnahmenziele und Maßnahmen aus Anhang A (ISO/IEC 27001) müssen als Teil dieses ISMS-Prozesses so ausgewählt werden, dass die identifizierten Anforderungen abgedeckt werden. Die Maßnahmenziele und Maßnahmen, die in Tabelle A.1 aufgelistet sind (ISO/IEC 27001), sind direkt abgeleitet von und abgestimmt mit den Maßnahmenzielen und Maßnahmen nach ISO/IEC 27002, Abschnitte 5 bis 15.

4.3.2 ISO/IEC 27006

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Anwendungsbereich: Diese Internationale Norm legt zusätzlich zu den Anforderungen, die in ISO/IEC 17021 enthalten sind, weitere Anforderungen fest und liefert Leitlinien für Institutionen, die Audit- und Zertifizierungsleistungen für ISMS nach ISO/IEC 27001 anbieten. Sie verfolgt in erster Linie den Zweck, die Akkreditierung von Zertifizierungsstellen zu unterstützen, die die Zertifizierung von ISMS nach ISO/IEC 27001 durchführen.

Zielsetzung: ISO/IEC 27006 ergänzt ISO/IEC 17021 hinsichtlich der Beschreibung der Anforderungen für die Akkreditierung von Zertifizierungsstellen und ermöglicht es damit diesen Institutionen, Zertifizierungen nach den in ISO/IEC 27001 dargelegten Anforderungen durchzuführen.

4.4 Normen, die allgemeine Richtlinien beschreiben

4.4.1 ISO/IEC 27002

Information technology — Security techniques — Code of practice for information security management

Anwendungsbereich: Diese Internationale Norm stellt eine Liste von allgemein anerkannten Maßnahmenzielen und empfohlenen Maßnahmen zur Verfügung, die als Anleitung zur Umsetzung für die Auswahl und Etablierung von Maßnahmen zur Erreichung von Informationssicherheit dienen soll.

Zielsetzung: ISO/IEC 27002 ist eine Anleitung für die Umsetzung von Informationssicherheits-Maßnahmen. Insbesondere werden in den Abschnitten 5 bis 15 zur Unterstützung der Maßnahmen, die in den Abschnitten A.5 bis A.15 von ISO/IEC 27001 festgelegt sind, spezifische Ratschläge zur Implementierung und empfohlene Methoden dargestellt.

4.4.2 ISO/IEC 27003

Information technology — Security techniques — Information security management system implementation guidance

Anwendungsbereich: Diese Internationale Norm wird eine Anleitung für die praktische Umsetzung von ISMS nach ISO/IEC 27001 zur Verfügung stellen sowie weitere Informationen für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung von ISMS nach ISO/IEC 27001.

Zielsetzung: ISO/IEC 27003 wird einen prozessorientierten Ansatz zur erfolgreichen Implementierung eines ISMS nach ISO/IEC 27001 zur Verfügung stellen.

4.4.3 ISO/IEC 27004

Information technology — Security techniques — Information security management — Measurement

Anwendungsbereich: Diese Internationale Norm wird Leitlinien und Hinweise zur Entwicklung und Anwendung von Messwerten zur Verfügung stellen, um die Wirksamkeit von ISMS, Maßnahmenzielen und Maßnahmen zur Implementierung und zum Management von Informationssicherheit nach ISO/IEC 27001 zu bewerten.

Zielsetzung: ISO/IEC 27004 wird ein Rahmenwerk für Messungen liefern, das es ermöglicht, die Wirksamkeit von ISMS nach ISO/IEC 27001 zu bewerten.

4.4.4 ISO/IEC 27005

Information technology — Security techniques — Information security risk management

Anwendungsbereich: Diese Internationale Norm liefert Richtlinien für das Informationssicherheits-Risikomanagement. Der in dieser Internationalen Norm beschriebene Ansatz unterstützt die allgemeinen Konzepte, die in ISO/IEC 27001 festgelegt sind.

Zielsetzung: ISO/IEC 27005 liefert Leitlinien für die Umsetzung eines prozessorientierten Risikomanagement-Ansatzes, der die erfolgreiche Implementierung und die Einhaltung der Anforderungen des Informationssicherheits-Risikomanagements nach ISO/IEC 27001 unterstützt.

4.4.5 ISO/IEC 27007

Information technology — Security techniques — Guidelines for information security management systems auditing

Anwendungsbereich: Diese Internationale Norm wird Leitlinien für die Durchführung von ISMS-Audits bereitstellen sowie Leitlinien hinsichtlich der Befähigung von ISMS-Auditoren zusätzlich zu den Leitlinien, die in ISO 19011 enthalten sind, die für Managementsysteme im Allgemeinen gelten.

Zielsetzung: ISO/IEC 27007 wird Leitlinien für Institutionen zur Verfügung stellen, die interne oder externe Audits eines ISMS durchführen oder ein ISMS-Auditprogramm nach den in ISO/IEC 27001 festgelegten Anforderungen managen müssen.

4.5 Normen, die branchenspezifische Richtlinien beschreiben

4.5.1 ISO/IEC 27011

Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Anwendungsbereich: Diese Internationale Norm stellt Richtlinien zur Unterstützung bei der Umsetzung von Informationssicherheitsmanagement (ISM) in Telekommunikationsunternehmen zur Verfügung.

Zielsetzung: ISO/IEC 27011 stellt Telekommunikationsunternehmen eine Anpassung der ISO/IEC 27002 Richtlinien speziell für ihre Branche zur Verfügung, die die Anleitung zur Erfüllung der Anforderungen von ISO/IEC 27001, Anhang A, ergänzen.

4.5.2 ISO 27799

Health informatics — Information security management in health using ISO/IEC 27002

Anwendungsbereich: Diese Internationale Norm stellt Richtlinien zur Verfügung, die die Umsetzung von Informationssicherheitsmanagement (ISM) in Institutionen des Gesundheitswesens unterstützen.

Zielsetzung: ISO 27799 stellt Gesundheitsorganisationen eine Anpassung der ISO/IEC 27002 Richtlinien speziell für ihre Branche zur Verfügung, die die Anleitung zur Erfüllung der Anforderungen von ISO/IEC 27001, Anhang A, ergänzen.

Anhang A
(informativ)

Formen des sprachlichen Ausdrucks von Regelungen

Die Dokumente der ISMS-Normenfamilie stellen für niemanden eine Verpflichtung dar, sie zu befolgen. Eine solche Verpflichtung kann jedoch, z. B. durch die Gesetzgebung oder durch einen Vertrag, auferlegt werden. Um in der Lage zu sein, Übereinstimmung mit einem Dokument geltend zu machen, muss der Nutzer die Anforderungen, die es zu erfüllen gilt, identifizieren können. Er muss weiterhin in der Lage sein, diese Anforderungen von anderen Empfehlungen, die eine gewisse Entscheidungsfreiheit lassen, unterscheiden zu können.

Die folgende Tabelle stellt klar, wie ein Dokument der ISMS-Normenfamilie hinsichtlich des sprachlichen Ausdrucks als Anforderung oder Empfehlung interpretiert werden muss.

INDIKATION	ERKLÄRUNG
Anforderung	Die Formulierungen „muss“ und „darf nicht“ zeigen an, dass es sich um Anforderungen handelt, die strikt zu befolgen sind, um dem Dokument zu entsprechen, und von denen keine Abweichung zulässig ist.
Empfehlung	Die Ausdrücke „sollte“ und „sollte nicht“ zeigen an, dass eine von mehreren Möglichkeiten als besonders angemessen empfohlen wird, ohne andere Möglichkeiten zu erwähnen oder auszuschließen, oder dass eine bestimmte Vorgehensweise bevorzugt wird, aber nicht notwendigerweise erforderlich ist, oder dass (in der verneinten Form) eine bestimmte Möglichkeit oder Vorgehensweise missbilligt, aber nicht verboten wird.
Zulässigkeit	Die Ausdrücke „darf“ und „braucht nicht“ zeigen eine Vorgehensweise an, die im Rahmen des Dokuments zulässig ist.
Möglichkeit	Die Ausdrücke „kann“ und „kann nicht“ zeigen die Möglichkeit an, dass sich etwas ereignet.

Anhang B
(informativ)

Kategorisierte Begriffe

B.1 Begriffe mit Bezug auf Informationssicherheit

2.2 Zurechenbarkeit (en: *accountability*)

2.5 Authentisierung (en: *authentication*)

2.6 Authentizität (en: *authenticity*)

2.7 Verfügbarkeit (en: *availability*)

2.9 Vertraulichkeit (en: *confidentiality*)

2.19 Informationssicherheit (en: *information security*)

2.25 Integrität (en: *integrity*)

2.27 Nicht-Abstreitbarkeit (en: *non-repudiation*)

2.33 Verlässlichkeit (en: *reliability*)

B.2 Begriffe mit Bezug zum Management

2.8 Business Continuity (en: *business continuity*)

2.12 Korrekturmaßnahme (en: *corrective action*)

2.13 Wirksamkeit (en: *effectiveness*)

2.14 Effizienz (en: *efficiency*)

2.16 Richtlinie (en: *guideline*)

2.23 Informationssicherheitsmanagementsystem (ISMS) (en: *information security management system*)

2.26 Managementsystem (en: *management system*)

2.28 Leitlinie (en: *policy*)

2.29 Vorbeugungsmaßnahmen (en: *preventive action*)

2.31 Prozess (en: *process*)

B.3 Begriffe mit Bezug zu Informationssicherheits-Risiken

2.1 Zugriffskontrolle (en: *access control*)

2.3 Wert (en: *asset*)

2.4 Angriff (en: *attack*)

2.10 Maßnahme (en: *control*)

2.11 Maßnahmenziel (en: *control objective*)

2.15 Ereignis (en: *event*)

2.17 Auswirkung (en: *impact*)

2.18 Informationswert (en: *information asset*)

2.20 Informationssicherheits-Ereignis (en: *information security event*)

2.21 Informationssicherheits-Vorfall (en: *information security incident*)

2.22 Management von Informationssicherheits-Vorfällen (en: *information security incident management*)

2.24 Informationssicherheits-Risiko (en: *information security risk*)

2.34 Risiko (en: *risk*)

2.35 Risikoakzeptanz (en: *risk acceptance*)

2.36 Risikoanalyse (en: *risk analysis*)

2.37 Risikoeinschätzung (en: *risk assessment*)

2.38 Risikokommunikation (en: *risk communication*)

2.39 Risikokriterien (en: *risk criteria*)

2.40 Risikobestimmung (en: *risk estimation*)

2.41 Risikobewertung (en: *risk evaluation*)

2.42 Risikomanagement (en: *risk management*)

2.43 Risikobehandlung (en: *risk treatment*)

2.45 Bedrohung (en: *threat*)

2.46 Schwachstelle (en: *vulnerability*)

B.4 Begriffe mit Bezug auf die Dokumentation

2.30 Verfahren (en: *procedure*)

2.32 Aufzeichnung (en: *record*)

2.44 Erklärung zur Anwendbarkeit (en: *statement of applicability*)

Literaturhinweise

[1] ISO/IEC 17021:2006, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[4] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[6] ISO/IEC 27003[4)], *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 27004[5)], *Information technology — Security techniques — Information security management — Measurement*

[8] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27006:2007*, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[10] ISO/IEC 27007[6)]*, Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC 27011[7)], *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[12] ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

[13] ISO/IEC Guide 73:2002*, Risk Management — Vocabulary — Guidelines for use in standards*

4) In Arbeit.

5) In Arbeit.

6) In Arbeit.

7) In Arbeit.