

DIN EN ISO/IEC 27000

ICS 01.040.03; 01.040.35; 03.100.70; 35.030

Ersatz für
DIN ISO/IEC 27000:2011-07

**Informationstechnik –
Sicherheitsverfahren –
Informationssicherheits-Managementsysteme –
Überblick und Terminologie (ISO/IEC 27000:2016);
Deutsche Fassung EN ISO/IEC 27000:2017**

Information technology –
Security techniques –
Information security management systems –
Overview and vocabulary (ISO/IEC 27000:2016);
German version EN ISO/IEC 27000:2017

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information –
Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016);
Version allemande EN ISO/IEC 27000:2017

Gesamtumfang 49 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument wurde vom DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) in Zusammenarbeit mit der Schweizerischen Normenvereinigung (SNV) erarbeitet.

Die Internationale Norm ISO/IEC 27000:2016 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 DIN-Normenausschusses Informationstechnik und Anwendungen (NIA).

Die dieser Norm zugrunde liegende Internationale Norm ISO/IEC 27000 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.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des ISO/IEC DIS 27000 entsprechend der diesbezüglich durch ISO erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen ISO-Text.

Für die in diesem Dokument zitierte Internationale Norm wird im Folgenden auf die entsprechende Deutsche Norm hingewiesen:

ISO/IEC 27001 siehe DIN ISO/IEC 27001

Änderungen

Gegenüber DIN ISO/IEC 27000:2011-07 wurden folgende Änderungen vorgenommen:

- a) Beschreibung des PDCA-Zyklus gestrichen;
- b) neue Begriffsdefinitionen aufgenommen;
- c) Beschreibung neuer Normen der ISO/IEC 27000er Normenfamilie in Abschnitt 4 aufgenommen;
- d) Darstellung in Bild 1 überarbeitet und um neue Normen der ISO/IEC 27000er Normenfamilie ergänzt.

Frühere Ausgaben

DIN ISO/IEC 27000: 2011-07

Nationaler Anhang NA (informativ)

Literaturhinweise

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

— Leerseite —

Deutsche Fassung

Informationstechnik —
Sicherheitsverfahren —
Informationssicherheits-Managementsysteme —
Überblick und Terminologie
(ISO/IEC 27000:2016)

Information technology —
Security techniques —
Information security management systems —
Overview and vocabulary
(ISO/IEC 27000:2016)

Technologies de l'information —
Techniques de sécurité —
Systèmes de gestion de sécurité de l'information —
Vue d'ensemble et vocabulaire
(ISO/IEC 27000:2016)

Diese Europäische Norm wurde vom CEN am 26. Januar 2017 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 Management-Zentrum des CEN-CENELEC 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 und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
0 Einleitung	6
0.1 Überblick	6
0.2 ISMS-Normenfamilie	6
0.3 Zweck dieser Internationalen Norm	7
1 Anwendungsbereich	8
2 Begriffe	8
3 Managementsysteme für Informationssicherheit (ISMS)	21
3.1 Einleitung	21
3.2 Was ist ein ISMS?	22
3.2.1 Übersicht und Grundsätze	22
3.2.2 Informationen	23
3.2.3 Informationssicherheit	23
3.2.4 Management	23
3.2.5 Managementsystem	24
3.3 Prozessorientierter Ansatz	24
3.4 Warum ist ein ISMS wichtig?	24
3.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS	25
3.5.1 Übersicht	25
3.5.2 Identifizierung von Informationssicherheitsanforderungen	26
3.5.3 Beurteilung von Informationssicherheitsrisiken	26
3.5.4 Behandlung von Informationssicherheitsrisiken	26
3.5.5 Auswahl und Umsetzung von Maßnahmen	27
3.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS	28
3.5.7 Fortlaufende Verbesserung	28
3.6 Kritische Erfolgsfaktoren für das ISMS	29
3.7 Nutzen der ISMS-Normenfamilie	29
4 Die ISMS-Normenfamilie	30
4.1 Allgemeine Informationen	30
4.2 Normen, die einen Überblick geben und die Terminologie festlegen	31
4.2.1 ISO/IEC 27000 (dieses Dokument)	31
4.3 Normen, die Anforderungen festlegen	31
4.3.1 ISO/IEC 27001	31
4.3.2 ISO/IEC 27006	32
4.4 Normen, die allgemeine Leitfäden beschreiben	32
4.4.1 ISO/IEC 27002	32
4.4.2 ISO/IEC 27003	32
4.4.3 ISO/IEC 27004	32
4.4.4 ISO/IEC 27005	33
4.4.5 ISO/IEC 27007	33
4.4.6 ISO/IEC TR 27008	33
4.4.7 ISO/IEC 27013	33
4.4.8 ISO/IEC 27014	34
4.4.9 ISO/IEC TR 27016	34

4.5	Normen, die branchenspezifische Leitfäden beschreiben	34
4.5.1	ISO/IEC 27010.....	34
4.5.2	ISO/IEC 27011.....	35
4.5.3	ISO/IEC TR 27015.....	35
4.5.4	ISO/IEC 27017.....	35
4.5.5	ISO/IEC 27018.....	36
4.5.6	ISO/IEC TR 27019.....	36
4.5.7	ISO 27799	37
Anhang A (informativ) Verbformen zur Formulierung von Festlegungen.....		38
Anhang B (informativ) Begriffe und Zuständigkeit		39
B.1	Zuständigkeit für Begriffe	39
B.2	Begriffe, die in diesen Internationalen Standards verwendet werden	39
B.2.1	ISO/IEC 27001.....	39
B.2.2	ISO/IEC 27002.....	40
B.2.3	ISO/IEC 27003.....	40
B.2.4	ISO/IEC 27004.....	40
B.2.5	ISO/IEC 27005.....	40
B.2.6	ISO/IEC 27006.....	41
B.2.7	ISO/IEC 27007.....	41
B.2.8	ISO/IEC TR 27008.....	41
B.2.9	ISO/IEC 27010.....	41
B.2.10	ISO/IEC 27011.....	41
B.2.11	ISO/IEC 27014.....	42
B.2.12	ISO/IEC TR 27015.....	42
B.2.13	ISO/IEC TR 27016.....	42
B.2.14	ISO/IEC TR 27017.....	42
B.2.15	ISO/IEC TR 27018.....	42
B.2.16	ISO/IEC TR 27019.....	43
Literaturhinweise.....		44

Europäisches Vorwort

Der Text von ISO/IEC 27000:2016 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27000:2017 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2017, und etwaige entgegenstehende nationale Normen müssen bis August 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, 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 27000:2016 wurde von CEN als EN ISO/IEC 27000:2017 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der Grundsätze der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: www.iso.org/iso/foreword.html.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC/JTC 1 *Information Technology*, Unterkomitee SC 27 *IT Security Techniques*.

Diese vierte Ausgabe ersetzt die dritte Ausgabe (ISO/IEC 27000:2014), die technisch überarbeitet wurde.

0 Einleitung

0.1 Überblick

Internationale Normen für Managementsysteme stellen ein Vorgehensmodell zum Einrichten und Betreiben eines Managementsystems zur Verfügung. Dieses Modell berücksichtigt die Merkmale, zu denen unter Experten auf dem Gebiet Konsens herrscht, dass diese Merkmale den internationalen Stand der Technik widerspiegeln. ISO/IEC JTC 1/SC 27 unterhält ein Expertengremium, das sich der Entwicklung von Internationalen Managementsystemnormen für Informationssicherheit, auch bekannt als die Informationssicherheitsmanagementsystem (ISMS) Normenfamilie. Durch den Einsatz der ISMS-Normenfamilie können Organisationen ein Rahmenwerk zur Handhabung der Sicherheit ihrer Informationswerte einschließlich Finanzinformationen, geistige Eigentumsrechte und Details zu Beschäftigten, oder der ihnen von Kunden oder Dritten anvertrauten Informationen, entwickeln und umsetzen. Diese Standards können auch eingesetzt werden, um eine unabhängige Beurteilung ihres zum Schutz von Informationen eingesetzten ISMS vorzubereiten.

0.2 ISMS-Normenfamilie

Die ISMS-Normenfamilie (siehe Abschnitt 4) ist dafür vorgesehen Organisationen jedweder Art und Größe bei Umsetzung und Betrieb eines ISMS zu unterstützen und besteht aus den folgenden internationalen Standards, unter dem allgemeinen Titel *Information technology — Security techniques* (nachfolgend in numerischer Reihenfolge):

- ISO/IEC 27000, Information security management systems — Overview and vocabulary
- ISO/IEC 27001, Information security management systems — Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management — Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC DIS 27009, Sector-specific application of ISO/IEC 27001–Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014, Governance of information security

- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management — Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud Services
- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ANMERKUNG Der allgemeine Titel „Information technology — Security techniques“ zeigt an, dass diese Standards vom Joint Technical Committee ISO/IEC JTC 1, „Information technology“, Subcommittee SC 27, „IT Security techniques“ erarbeitet wurden.

Folgende Internationale Norm, die nicht unter diesem allgemeinen Titel veröffentlicht wurde gehört ebenfalls zur ISMS-Normenfamilie:

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

0.3 Zweck dieser Internationalen Norm

Diese Internationale Norm liefert einen Überblick über Informationssicherheitsmanagementsysteme und definiert zugehörige Begriffe.

ANMERKUNG Anhang A liefert eine Klarstellung wie Verbformen eingesetzt werden um Anforderungen und/oder Hilfestellungen innerhalb der ISMS-Normenfamilie auszudrücken.

Die ISMS-Normenfamilie beinhaltet Normen die:

- a) Anforderungen an ein ISMS und an diejenigen, die solche Systeme zertifizieren, festlegen;
- b) direkte Unterstützung, detaillierte Leitlinien und/oder Interpretationen für den Gesamtprozess zur Errichtung, Umsetzung, Aufrechterhaltung und Verbesserung eines ISMS anbieten;
- c) sektorspezifische Leitlinien für ISMS adressieren; und
- d) Konformitätsbewertung für ISMS adressieren.

Die Begriffe, die in dieser Internationalen Norm bereitgestellt werden:

- decken die allgemein gebräuchlichen Begriffe in der ISMS-Normenfamilie ab;
- decken nicht sämtliche Begriffe ab, die innerhalb der ISMS-Normenfamilie Anwendung finden und
- schränken die ISMS-Normenfamilie nicht darin ein, neue Begriffe zu definieren.

1 Anwendungsbereich

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

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1

Zugangssteuerung

(en: access control)

Mittel um sicherzustellen, dass der Zugang zu Werten aufgrund von Geschäfts- und Sicherheitsanforderungen (2.63) befugt und eingeschränkt ist

2.2

analytisches Modell

(en: analytical model)

Algorithmus oder Berechnung, der/die ein oder mehr *Elementarmessgrößen* (2.10) und/oder *abgeleitete Messgrößen* (2.22) mit Hilfe von zugehörigen *Entscheidungskriterien* (2.21) kombiniert

2.3

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

2.4

Attribut

(en: attribute)

Eigenschaft oder Merkmal eines *Objekts* (2.55), das mit menschlichen oder automatisierten Mitteln quantitativ oder qualitativ unterschieden werden kann

[ISO/IEC 15939:2007, 2.2 modifiziert – in der Definition wurde Entität durch Objekt ersetzt]

2.5

Audit

(en: audit)

systematischer, unabhängiger und dokumentierter *Prozess* (2.61) zum Erlangen von Auditnachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit die Auditkriterien erfüllt sind

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

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

2.6

Auditumfang

(en: audit scope)

Ausmaß und Grenzen eines *Audits* (2.5)

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

2.7

Authentisierung

(en: authentication)

Sicherstellung, dass die von einer Entität behaupteten Eigenschaften richtig sind

2.8

Authentizität

(en: authenticity)

Eigenschaft, dass eine Entität das ist, was sie angibt zu sein

2.9

Verfügbarkeit

(en: availability)

Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

2.10

Elementarmessgröße

(en: base measure)

Messgröße (2.47), die mittels eines *Attributs* (2.4) und der Methode ihrer Quantifizierung definiert ist

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

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

2.11

Kompetenz

(en: competence)

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

2.12

Vertraulichkeit

(en: confidentiality)

Eigenschaft, dass Information unbefugten Personen, Entitäten oder *Prozessen* (2.61) nicht verfügbar gemacht oder offengelegt wird

2.13

Konformität

(en: conformity)

Erfüllung einer *Anforderung* (2.63)

Anmerkung 1 zum Begriff: Der Begriff „Übereinstimmung“ ist gleichbedeutend aber veraltet.

2.14

Folge

(en: consequence)

Ergebnis eines *Ereignisses* (2.25), welches *Ziele* (2.56) beeinflusst

[ISO Guide 73:2009, 3.6.1.3, modifiziert]

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

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

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

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

2.15

fortlaufende Verbesserung

(en: continual improvement)

wiederkehrende Tätigkeit zum Steigern der *Leistung* (2.59)

2.16

Maßnahme

(en: control)

Mittel zur Veränderung von *Risiken* (2.68)

Anmerkung 1 zum Begriff: Maßnahmen umfassen Prozesse (2.61), Richtlinien, Geräte, Methoden oder anderweitige Handlungen, die Risiken (2.68) verändern.

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

[ISO Guide 73:2009 3.8.1.1]

2.17

Maßnahmenziel

(en: control objective)

Beschreibung dessen, was als Ergebnis umgesetzter *Maßnahmen* (2.16) erzielt werden soll

2.18

Korrektur

(en: correction)

Maßnahme zum Beseitigen einer erkannten *Nichtkonformität* (2.53)

2.19

Korrekturmaßnahme

(en: corrective action)

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (2.53) und zum Verhindern des erneuten Auftretens

2.20

Daten

(en: data)

Sammlung von Werten, die mit *Elementarmessgrößen* (2.10), *abgeleiteten Messgrößen* (2.22) und/oder *Indikatoren* (2.30) verknüpft sind

Anmerkung 1 zum Begriff: Die Definition findet nur im Kontext von ISO/IEC 27004 Anwendung.

[ISO/IEC 15939:2007, 2.4, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt]

2.21

Entscheidungskriterien

(en: decision criteria)

Schwellwerte, Sollvorgaben oder Schemata, die benutzt werden, um die Notwendigkeit einer Maßnahme oder weiteren Untersuchung zu ermitteln oder das Maß an Vertrauen in ein Ergebnis zu beschreiben

[ISO/IEC 15939:2007, 2.7]

2.22

abgeleitete Messgröße

(en: derived measure)

Messgröße (2.47), dies als Funktion von zwei oder mehr Werten von *Elementarmessgrößen* (2.10) definiert ist

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

2.23

dokumentierte Information

(en: documented information)

Information, die von einer *Organisation* (2.57) 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* (2.46), einschließlich damit verbundener *Prozesse* (2.61);
- Information, die für den Betrieb der *Organisation* (2.57) geschaffen wurden (Dokumentation);
- Nachweise erreichter Ergebnisse (Aufzeichnungen).

2.24

Wirksamkeit

(en: effectiveness)

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

2.25

Ereignis

(en: event)

Auftreten oder Veränderung einer bestimmten Menge von Umständen

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

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.

2.26

Geschäftsleitung

(en: executive management)

Person oder Personengruppe, die vom *Steuerungsgremium* (2.29) Verantwortung für die Umsetzung von Strategien und Richtlinien erhalten haben, um die Ziele der *Organisation* (2.57) zu erreichen

Anmerkung 1 zum Begriff: Die Geschäftsleitung wird manchmal *oberste Leitung* (2.84) genannt. Dazu können die Geschäftsführer, Finanzverantwortlichen, die Verantwortlichen für die Informationsverarbeitung und ähnliche Rollen gehören.

2.27

externer Kontext

(en: external context)

externes Umfeld, in dem die Organisation versucht ihre *Ziele* (2.56) zu erreichen

[ISO Guide 73:2009, 3.3.1.1]

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;