

DIN ISO/IEC 27000

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

Inhalt

	Seite
Nationales Vorwort	3
Nationaler Anhang NA (informativ) Literaturhinweise.....	4
0 Einleitung.....	5
0.1 Überblick.....	5
0.2 ISMS-Normenfamilie	5
0.3 Ziel dieser Internationalen Norm	6
1 Anwendungsbereich	7
2 Begriffe	7
3 Managementsysteme für die Informationssicherheit	12
3.1 Einleitung.....	12
3.2 Was ist ein ISMS?	13
3.3 Prozessorientierter Ansatz	15
3.4 Warum ist ein ISMS wichtig?	15
3.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS	16
3.6 Kritische Erfolgsfaktoren für ein ISMS.....	18
3.7 Vorteile der ISMS-Normenfamilie	18
4 Aufbau der ISMS-Normenfamilie	19
4.1 Allgemeines	19
4.2 Normen, die einen Überblick geben und die Terminologie beschreiben	20
4.3 Normen, die Anforderungen festlegen	20
4.4 Normen, die allgemeine Richtlinien beschreiben.....	21
4.5 Normen, die branchenspezifische Richtlinien beschreiben	22
Anhang A (informativ) Formen des sprachlichen Ausdrucks von Regelungen	23
Anhang B (informativ) Kategorisierte Begriffe	24
Literaturhinweise	26

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-Normenfamilie¹⁾ 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-Normenfamilie 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