

DIN ISO/IEC 27001

ICS 35.040

Einsprüche bis 2014-03-10
Vorgesehen als Ersatz für
DIN ISO/IEC 27001:2008-09

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC DIS 27001:2013)**

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC DIS 27001:2013)
Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI DIS 27001:2013)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-01-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 32 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Inhalt

	Seite
Nationales Vorwort	3
Nationaler Anhang NA (informativ) Literaturhinweise.....	4
0 Einleitung.....	5
0.1 Allgemeines	5
0.2 Kompatibilität mit anderen Normen für Managementsysteme	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Kontext der Organisation.....	6
4.1 Verständnis der Organisation und ihres Kontexts.....	6
4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien.....	6
4.3 Festlegung des Geltungsbereichs des Informationssicherheitsmanagementsystems	7
4.4 Informationssicherheitsmanagementsystem	7
5 Führung	7
5.1 Führung und Engagement	7
5.2 Leitlinie	8
5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse.....	8
6 Planung	8
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	8
6.2 Informationssicherheitsziele und Pläne für deren Erreichung	10
7 Unterstützung.....	11
7.1 Ressourcen	11
7.2 Kompetenz.....	11
7.3 Bewusstsein	11
7.4 Kommunikation.....	12
7.5 Dokumentierte Informationen.....	12
8 Einsatz	13
8.1 Einsatzplanung und -kontrolle	13
8.2 Informationssicherheitsrisikoeinschätzung	13
8.3 Informationssicherheitsrisikobehandlung	13
9 Leistungsauswertung.....	14
9.1 Überwachung, Messung, Analyse und Auswertung	14
9.2 Internes Audit.....	14
9.3 Prüfung durch die Leitung	15
10 Verbesserung	15
10.1 Fehler und Korrekturmaßnahmen	15
10.2 Laufende Verbesserung	16
Anhang A (normativ) Referenz-Maßnahmenziele und Maßnahmen	17
Literaturhinweise	32

Nationales Vorwort

Die Internationale Norm ISO/IEC DIS 27001:2013 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 27001 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.

DIN ISO/IEC 27001 beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind.

Für die in diesem Dokument zitierte internationale Norm wird im Folgenden auf die entsprechende deutsche Norm hingewiesen:

ISO/IEC 27000 siehe DIN ISO/IEC 27000

Änderungen

Gegenüber DIN ISO/IEC 27001:2008-09 wurden folgende Änderungen vorgenommen:

- a) Anpassung an die neue Struktur für ISO Management System Standards, vorgegeben im Anhang SL der ISO/IEC Direktiven.
- b) Folgende Abschnitte wurden neu aufgenommen:
4.2(a), 4.3(c), 5.1(b), 6.1.1(a), 6.1.1(b), 6.1.1(c), 6.1.2(a), 6.2, 7.3(a), 7.4(a), 7.4(b), 7.4(c), 7.4(d), 7.4(e), 7.5.1(b), 8.1, 9.1(c), 9.1(d), 9.1(f), 9.3(4), 10.1(a), 10.1(1), 10.1(2), 10.1(e), 10.1(f)
- c) Folgende Abschnitte wurden gestrichen:
4.2.1, 4.2.1(i), 4.2.3(1), 4.2.3(2), 4.2.3(4), 4.2.3(5), 4.2.3(h), 4.3.1, 4.3.1(c), 4.3.2, 4.3.3, 5.2.1(b), 5.2.1(d), 8.3(d), 8.3(e), 8.3

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 27000, *Informationstechnik* — *IT-Sicherheitsverfahren* — *Informationssicherheits-*
Managementsysteme — *Überblick und Terminologie*

Informationstechnologie — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm wurde erarbeitet, um Anforderung für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Implementierung eines Informationssicherheitsmanagementsystems innerhalb einer Organisation richten sich nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern werden.

Das Informationssicherheitsmanagementsystem schützt die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen durch Anwendung eines Risikomanagement-Prozesses und verleiht dadurch interessierten Parteien das Vertrauen darauf, dass mit Risiken angemessen umgegangen wird.

Hierfür ist es wichtig, dass das Informationssicherheitsmanagementsystem in die Abläufe und die gesamte Verwaltungsstruktur der Organisation integriert ist und einen untrennbaren Bestandteil davon darstellt. Außerdem muss die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt werden. Es ist davon auszugehen, dass die Implementierung eines Informationssicherheitsmanagementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Diese Internationale Norm kann von internen und externen Parteien – darunter Zertifizierungsstellen – dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu bewerten.

Die Anforderungen werden in dieser Internationalen Norm weder in der Reihenfolge ihrer Wichtigkeit aufgeführt noch in der zeitlichen Abfolge, in der sie umgesetzt werden sollten. Die Listeneinträge werden lediglich zu Referenzzwecken aufgeführt.

Mit ISO/IEC 27000 wird ein Überblick über Informationssicherheitsmanagementsysteme gegeben und das entsprechende Vokabular für Systeme vorgegeben, auf welche die ISMS-Normenfamilie (einschließlich ISO/IEC 27003, ISO/IEC 27004 und ISO/IEC 27005) anwendbar ist. Außerdem beinhaltet die Norm Festlegungen zu den dazugehörigen Begriffen und Definitionen.

0.2 Kompatibilität mit anderen Normen für Managementsysteme

In dieser Internationalen Norm werden die grobe Struktur, die gleichen Titel von Unterabschnitten, identischer Text, häufige Begriffe und wichtige Definitionen angewandt wie in Anhang SL von ISO/IEC-Richtlinien, Teil 1. Dadurch wird die Kompatibilität mit anderen Normen für Managementsysteme gewahrt, die ebenfalls Anhang SL übernommen haben.

Diese gemeinsame Herangehensweise nach den Definitionen in Anhang SL ist für diejenigen Organisationen nützlich, die sich für den Einsatz eines einzelnen Managementsystems zur Erfüllung der Anforderungen von zwei oder mehr Normen für Managementsysteme entscheiden.

1 Anwendungsbereich

Diese Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und laufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet diese Internationale Norm Anforderungen für die Einschätzung und Handhabung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen ungeachtet ihrer Art und Größe anwendbar sein. Wenn eine Organisation Konformität mit dieser Internationalen Norm für sich beansprucht, darf sie keine der Anforderungen in den Abschnitten 4 bis 10 ausschließen.

2 Normative Verweisungen

Das folgende zitierte Dokument ist für die Anwendung dieses Dokuments unverzichtbar. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die in ISO/IEC 27000 angegebenen Begriffe.

4 Kontext der Organisation

4.1 Verständnis der Organisation und ihres Kontexts

Die Organisation muss festlegen, welche externen und internen Angelegenheiten für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagementsystems zu erreichen.

ANMERKUNG Die Ermittlung dieser Angelegenheiten bezieht sich auf die Festlegung des externen und internen Kontexts des Unternehmens, wie in ISO 31000:2009, 5.3.1 geschildert.

4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien

Die Organisation muss Folgendes festlegen:

- a) interessierte Parteien, die im Hinblick auf das Informationssicherheitsmanagementsystem relevant sind; und
- b) die Anforderungen dieser interessierten Parteien in Bezug auf die Informationssicherheit.

ANMERKUNG Die Anforderungen interessierter Parteien können gesetzliche und amtliche Vorgaben sowie vertragliche Verpflichtungen beinhalten.

4.3 Festlegung des Geltungsbereichs des Informationssicherheitsmanagementsystems

Die Organisation muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems festlegen und damit seinen Geltungsbereich festlegen.

Bei der Festlegung des Geltungsbereichs muss die Organisation Folgendes berücksichtigen:

- a) die in 4.1 genannten externen und internen Angelegenheiten;
- b) die in 4.2 genannten Anforderungen; und
- c) Schnittstellen und Abhängigkeitsverhältnisse zwischen Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten anderer Organisationen.

Der Geltungsbereich muss als dokumentierte Information verfügbar sein.

4.4 Informationssicherheitsmanagementsystem

Die Organisation muss ein Informationssicherheitsmanagementsystem nach den Anforderungen dieser Internationalen Norm einrichten, implementieren, aufrechterhalten und laufend verbessern.

5 Führung

5.1 Führung und Engagement

Die Leitung muss durch folgende Maßnahmen ihre Führung und ihr Engagement in Bezug auf das Informationssicherheitsmanagementsystem demonstrieren:

- a) Sicherstellen, dass eine Informationssicherheitsleitlinie und Informationssicherheitsziele vorgegeben werden und mit der strategischen Ausrichtung der Organisation vereinbar sind;
- b) Sicherstellen, dass die Anforderungen im Rahmen des Informationssicherheitsmanagementsystem in die Prozesse der Organisation integriert werden;
- c) Sicherstellung, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen bereitstehen;
- d) Kommunikation der Bedeutung eines effektiven Informationssicherheitsmanagements sowie der Einhaltung der Anforderungen im Rahmen des Informationssicherheitsmanagementsystems;
- e) Sicherstellen, dass mit dem Informationssicherheitsmanagementsystem die beabsichtigten Ergebnisse erzielt werden;
- f) Führen und Unterstützen von Personen, damit diese einen Beitrag zur Wirksamkeit des Informationssicherheitsmanagementsystems leisten;
- g) Fördern der laufenden Verbesserung; und
- h) Unterstützen anderer relevanter Führungskräfte bei der Demonstration ihrer Führung im jeweiligen Zuständigkeitsbereich.

5.2 Leitlinie

Die Leitung muss eine Informationssicherheitsleitlinie vorgeben, die folgende Eigenschaften aufweist:

- a) Eignung für den Zweck der Organisation;
- b) Einbeziehung von Informationssicherheitszielen (siehe 6.2) oder Bereitstellung eines Frameworks zur Vorgabe von Sicherheitszielen;
- c) Einbeziehung einer Verpflichtung zur Einhaltung der Anforderungen in Bezug auf die Informationssicherheit; und
- d) Einbeziehung einer Verpflichtung zur laufenden Verbesserung des Informationssicherheitsmanagementsystems.

Die Informationssicherheitsleitlinie muss:

- e) als dokumentierte Information verfügbar sein;
- f) innerhalb der Organisation bekannt gemacht werden; und
- g) ggf. interessierten Parteien zur Verfügung stehen.

5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse

Die Leitung muss sicherstellen, dass die Zuständigkeiten und Befugnisse von Aufgaben, die für die Informationssicherheit relevant sind, zugewiesen und kommuniziert werden.

Die Leitung muss Zuständigkeiten und Befugnisse für folgende Aspekte zuweisen:

- a) Sicherstellen, dass das Informationssicherheitsmanagementsystem den Anforderungen dieser Internationalen Norm entspricht; und
- b) Berichterstaten zur Leistung des Informationssicherheitsmanagementsystems gegenüber der Leitung.

ANMERKUNG Die Leitung weist u. U. auch Zuständigkeiten und Befugnisse für die Berichterstattung zur Leistung des Informationssicherheitsmanagementsystems innerhalb der Organisation zu.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Chancen

6.1.1 Allgemeines

Beim Planen des Informationssicherheitsmanagementsystems muss die Organisation die unter 4.1 genannten Angelegenheiten sowie die unter 4.2 genannten Anforderungen berücksichtigen und ermitteln, auf welche Risiken und Chancen zu achten sein wird, um Folgendes zu erreichen:

- a) Sicherstellen, dass mit dem Informationssicherheitsmanagementsystem die beabsichtigten Ergebnisse erzielt werden können;
- b) Vorbeugen oder Abschwächen unerwünschter Auswirkungen; und
- c) laufende Verbesserung.

Die Organisation muss Folgendes planen:

- d) Maßnahmen zum Umgang mit Risiken und Chancen; und
- e) Möglichkeiten zur
 - 1) Integration und Einbeziehung dieser Maßnahmen in die eigenen Informationssicherheitsmanagementprozesse; und
 - 2) Auswertung der Wirksamkeit dieser Maßnahmen.

6.1.2 Informationssicherheitsrisikoeinschätzung

Die Organisation muss einen Prozess zur Informationssicherheitsrisikoeinschätzung festlegen, der Folgendes bewirkt:

- a) Einrichten und Aufrechterhalten von Informationssicherheitsrisikokriterien einschließlich Risikoakzeptanzkriterien;
- b) Festlegen der Kriterien für eine Durchführung von Informationssicherheitrisikoeinschätzungen; und
- c) Sicherstellen, dass wiederholte Informationssicherheitsrisikoeinschätzungen zu konsistenten, aussagekräftigen und vergleichbaren Ergebnissen führen.

Die Organisation muss Folgendes leisten:

- d) Ermitteln der Informationssicherheitsrisiken.
 - 1) Anwenden des Informationssicherheitsrisikoeinschätzungsprozesses zur Ermittlung von Risiken im Zusammenhang mit Mängeln bei Vertraulichkeit, Integrität und Verfügbarkeit von Informationen innerhalb des Geltungsbereichs des ISMS.
 - 2) Ermitteln der Risikoeigentümer.
- e) Analyse der Informationssicherheitsrisiken.
 - 1) Bewerten der potenziellen Auswirkungen bei Eintritt der nach 6.1.1 e) 1) ermittelten Risiken.
 - 2) Bewerten der realistischen Eintretenswahrscheinlichkeiten der nach 6.1.1 e) 1) ermittelten Risiken.
 - 3) Festlegen der Risikostufen.
- f) Auswertung der Informationssicherheitsrisiken.
 - 1) Vergleich der analysierten Risiken mit den nach 6.1.2 a) festgelegten Risikokriterien und Festlegen von Prioritäten bezüglich des Umgangs mit diesen Risiken.

Die Organisation muss dokumentierte Informationen über den Informationssicherheitsrisikoeinschätzungsprozess aufbewahren.

6.1.3 Informationssicherheitsrisikobehandlung

Die Organisation muss einen Prozess für die Informationssicherheitsrisikobehandlung festlegen, der Folgendes bewirkt:

- a) Auswahl angemessener Optionen für die Sicherheitsrisikobehandlung unter Berücksichtigung der Ergebnisse der Risikoeinschätzung;
- b) Festlegen aller Maßnahmen, die zur Implementierung der gewählten Optionen für die Sicherheitsrisikobehandlung erforderlich sind;

ANMERKUNG Organisationen können Maßnahmen nach Bedarf gestalten oder vorgefertigte Maßnahmen aus einer beliebigen Quelle wählen.

- c) Vergleich der nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in Anhang A und Vergewisserung, dass keine erforderlichen Kontrollmaßnahmen ausgelassen wurden;

ANMERKUNG 1 Anhang A enthält eine umfassende Liste von Maßnahmenzielen und Maßnahmen. Anwender dieser Internationalen Norm werden für die Sicherstellung, dass keine wichtigen Maßnahmen übersehen wurden, auf Anhang A verwiesen.

ANMERKUNG 2 Maßnahmenziele sind implizit in den gewählten Maßnahmen enthalten. Die Liste der Maßnahmenziele und Maßnahmen in Anhang A ist nicht erschöpfend; u. U. sind weitere Maßnahmenziele und Maßnahmen erforderlich.

- d) Erstellen einer Erklärung zur Anwendung, die die erforderlichen Maßnahmen (siehe 6.1.3 a), b) und c)) und Gründe für deren Einbeziehung enthält (egal, ob sie implementiert werden oder nicht) sowie Gründe für die Nichteinbeziehung von Maßnahmen in Anhang A.
- e) Formulieren eines Plans für die Informationssicherheitsrisikobehandlung;
- f) Einholen einer Genehmigung des Plans für die Informationssicherheitsrisikobehandlung seitens der Risikoeigentümer sowie deren Akzeptanz der verbleibenden Informationssicherheitsrisiken.

Die Organisation muss dokumentierte Informationen über den Prozess zur Informationssicherheitsrisikobehandlung aufbewahren.

ANMERKUNG Die in dieser Internationalen Norm genannten Prozesse für die Informationssicherheitsrisikoeinschätzung und den Umgang damit entsprechen den Grundsätzen und allgemeinen Richtlinien in ISO 31000.

6.2 Informationssicherheitsziele und Pläne für deren Erreichung

Die Organisation muss in relevanten Funktionen und auf relevanten Ebenen Informationssicherheitsziele festlegen.

Diese Informationssicherheitsziele müssen:

- a) mit der Informationssicherheitsleitlinie konsistent sein;
- b) messbar sein (falls praktikabel);
- c) unter Berücksichtigung der anwendbaren Informationssicherheitsanforderungen, der Risikoeinschätzung und der Ergebnisse des Umgangs mit diesen Risiken festgelegt werden;
- d) kommuniziert werden, und
- e) ggf. aktualisiert werden.

Die Organisation muss dokumentierte Informationen über die Informationssicherheitsziele aufbewahren.