

DIN ISO/IEC 27001

ICS 35.040

**Informationstechnik –
IT-Sicherheitsverfahren –
Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC 27001:2005)**

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC 27001:2005)

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI 27001:2005)

Gesamtumfang 45 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 Prozessorientierter Ansatz	5
0.3 Verträglichkeit mit anderen Managementsystemen.....	7
1 Anwendungsbereich	7
1.1 Allgemeines.....	7
1.2 Anwendung	8
2 Normative Verweisungen.....	8
3 Begriffe	8
4 Informationssicherheits-Managementsystem	10
4.1 Allgemeine Anforderungen.....	10
4.2 Festlegung und Verwaltung des ISMS	10
4.2.1 Festlegen des ISMS	10
4.2.2 Umsetzen und Durchführen des ISMS.....	13
4.2.3 Überwachen und Überprüfen des ISMS	13
4.2.4 Instandhalten und Verbessern des ISMS	14
4.3 Dokumentationsanforderungen	14
4.3.1 Allgemeines.....	14
4.3.2 Lenkung von Dokumenten.....	15
4.3.3 Lenkung von Aufzeichnungen	16
5 Verantwortung des Managements	16
5.1 Verpflichtung des Managements	16
5.2 Management von Ressourcen.....	16
5.2.1 Bereitstellung von Ressourcen.....	16
5.2.2 Schulungen, Bewusstsein und Kompetenz	17
6 Interne ISMS-Audits.....	17
7 Managementbewertung des ISMS.....	18
7.1 Allgemeines.....	18
7.2 Eingaben für die Bewertung	18
7.3 Ergebnisse der Bewertung	18
8 Verbesserung des ISMS	19
8.1 Ständige Verbesserung.....	19
8.2 Korrekturmaßnahmen	19
8.3 Vorbeugungsmaßnahmen	19
Anhang A (normativ) Maßnahmenziele und Maßnahmen	21
Anhang B (informativ) OECD-Grundsätze und diese Internationale Norm	40
Anhang C (informativ) Übereinstimmung zwischen ISO 9001:2000, ISO 14001:2004 und dieser Internationalen Norm.....	42
Literaturhinweise	45

Nationales Vorwort

Die Internationale Norm ISO/IEC 27001:2005-10 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.

ISO/IEC 27001 ist aus dem britischen Standard BS 7799-2 hervorgegangen. Erklärtes Ziel dieser Norm ist es, die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) im Rahmen eines Prozess-Ansatzes darzustellen.

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. Aufbauend auf dieser Norm können nationale Zertifizierungsschemata definiert werden.

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

In ISO/IEC JTC 1/SC 27 wird zur Zeit eine Internationale Normenreihe von Informationssicherheits-Managementsystemen (ISM) entwickelt. Aufgrund der Bestrebungen, alle ISMS-Standards als ISO/IEC 27000er-Reihe zusammenzuführen, wurde ISO/IEC 17799:2005-06 (2. Ausgabe) in ISO/IEC 27002:2005-06 (1. Ausgabe) umbenannt. Demzufolge wird der Entwurf E DIN ISO/IEC 17799:2007-02 als Norm unter der Nummer DIN ISO/IEC 27002 veröffentlicht.

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

ISO 9001	siehe DIN EN ISO 9001
ISO 14001	siehe DIN EN ISO 14001
ISO 19011	siehe DIN EN ISO 19011
ISO/IEC 13335-1	siehe DIN ISO/IEC 13335-1
ISO/IEC 17799	siehe DIN ISO/IEC 27002

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 14001, *Umweltmanagementsysteme — Anforderungen mit Anleitung zur Anwendung*

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

DIN ISO/IEC 13335-1, *Informationstechnik — Sicherheitsverfahren — Management von Sicherheit in der Informations- und Kommunikationstechnik (IuK) — Teil 1: Konzepte und Modelle für IuK-Sicherheit*

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

Informationstechnik IT-Sicherheitsverfahren Informationssicherheits-Managementsysteme Anforderungen

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm wurde entwickelt, um ein Modell für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheits-Managementsystems (ISMS) bereitzustellen. Die Einführung eines ISMS sollte eine strategische Entscheidung für eine Organisation sein. Die Gestaltung und Umsetzung eines ISMS hängen von den Bedürfnissen und Zielen, Sicherheitsanforderungen, eingesetzten Verfahren und der Größe und Struktur der Organisation ab. Erwartungsgemäß ändern sich diese Faktoren und die sie unterstützenden Systeme im Laufe der Zeit. Es wird daher angenommen, dass die Umsetzung des ISMS den Bedürfnissen der Organisation angepasst wird, z. B. erfordert eine einfache Situation auch eine einfache ISMS-Lösung.

Diese Internationale Norm kann von interessierten Internen und Externen verwandt werden, um festzustellen, dass eine Organisation die Anforderungen erfüllt.

0.2 Prozessorientierter Ansatz

Diese Internationale Norm verwendet einen prozessorientierten Ansatz für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines organisationseigenen ISMS.

Um wirksam zu funktionieren, muss eine Organisation viele Aktivitäten identifizieren und verwalten. Jede Aktivität, die Ressourcen benutzt und verwaltet, um Eingaben in Ergebnisse zu verwandeln, kann als Prozess betrachtet werden. Das Ergebnis eines Prozesses bildet oft die direkte Eingabe für den nächsten Prozess.

Die Anwendung eines Systems von Prozessen in einer Organisation, verbunden mit der Identifizierung und dem Zusammenwirken dieser Prozesse und ihrer Verwaltung, kann als „prozessorientierter Ansatz“ verstanden werden.

Der in dieser Internationalen Norm präsentierte prozessorientierte Ansatz für das Management von Informationssicherheit betont die Wichtigkeit der folgenden Punkte für seine Anwender:

- a) Verständnis der Anforderungen der Organisation an Informationssicherheit, und die Notwendigkeit, eine Leitlinie und Ziele für Informationssicherheit festzulegen;
- b) Umsetzung und Betrieb von Maßnahmen, um die Informationssicherheitsrisiken einer Organisation in Zusammenhang mit den allgemeinen Geschäftsrisiken der Organisation zu verwalten;
- c) Überwachung und Überprüfung der Leistung und Wirksamkeit des ISMS und
- d) ständige Verbesserung auf der Basis von objektiven Messungen.

Diese Internationale Norm verwendet das „Plan-Do-Check-Act“ Modell (PDCA – „Planen, Durchführen, Prüfen, Handeln“) an, das benutzt wird, um die ISMS-Prozesse zu strukturieren. Bild 1 zeigt, wie ein ISMS die Informationssicherheitsanforderungen und -Erwartungen von Interessenten als Eingabe übernimmt und als Ergebnis durch die notwendigen Aktionen und Prozesse Informationssicherheit erzielt, die diese Anforderungen und Erwartungen erfüllt. Bild 1 zeigt ebenfalls die Verknüpfungen der in den Abschnitten 4, 5, 6, 7 und 8 beschriebenen Prozesse.

Die Anwendung des PDCA-Modells spiegelt auch die in den OECD Richtlinien (2002) ¹⁾ beschriebenen Grundsätze wider, die die Sicherheit von Informationssystem und -Netzen bestimmen. Diese Internationale Norm liefert ein stabiles Modell für die Umsetzung der Grundsätze in diesen Richtlinien, welche die Risikoeinschätzung, Sicherheitsgestaltung und Umsetzung, Sicherheitsmanagement und Neueinschätzung regeln.

BEISPIEL 1 Eine mögliche Anforderung ist, dass Informationssicherheitsverstöße keine ernsthaften Finanzschäden für eine Organisation und/oder Kompromittierung der Organisation verursachen dürfen.

BEISPIEL 2 Eine mögliche Erwartung ist, dass bei dem Auftreten eines ernsten Sicherheitsvorfalls – zum Beispiel dem Hacken der eBusiness-Webseite der Organisation – Personal mit ausreichender Schulung in den geeigneten Verfahren zur Verfügung steht, um die Auswirkungen so gering wie möglich zu halten.

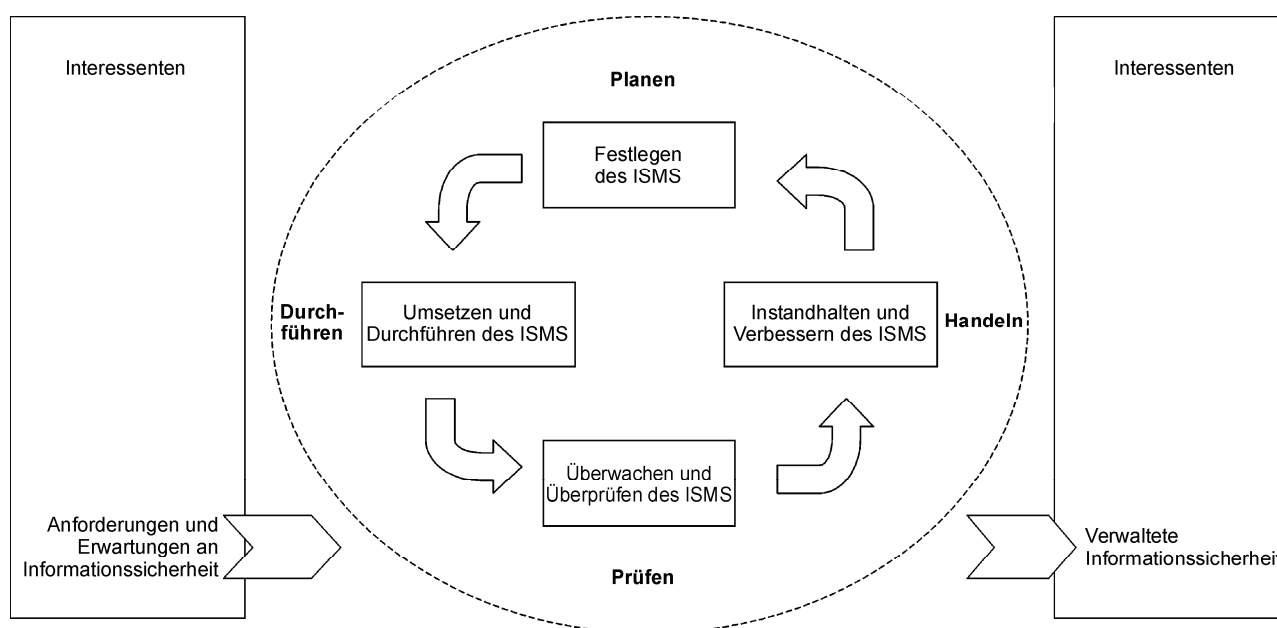


Bild 1 — Auf die ISMS-Prozesse angewandtes PDCA-Modell

¹⁾ OECD Richtlinien für die Sicherheit in Informationssystemen und -Netzen — Auf dem Weg zu einer Sicherheitskultur. Paris: OECD, Juli 2002. www.oecd.org

Planen (Festlegen des ISMS)	Festlegen der ISMS-Leitlinie, -Ziele, -Prozesse und -Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Rahmen aller Grundsätze und Ziele einer Organisation zu erreichen.
Durchführen (Umsetzen und Durchführen des ISMS)	Umsetzen und Durchführen der ISMS-Leitlinie, Maßnahmen, Prozesse und Verfahren.
Prüfen (Überwachen und Überprüfen des ISMS)	Einschätzen und ggf. Messen der Prozessleistung an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen, und Berichten der Ergebnisse an das Management zwecks Überprüfung.
Handeln (Instandhalten und Verbessern des ISMS)	Ergreifen von Korrekturmaßnahmen und Vorbeugungsmaßnahmen, basierend auf den Ergebnissen von internen ISMS-Audits und Überprüfungen des Managements und anderen wesentlichen Informationen, zur ständigen Verbesserung des ISMS.

0.3 Verträglichkeit mit anderen Managementsystemen

Diese Internationale Norm ist mit ISO 9001:2000 und ISO 14001:2004 abgestimmt worden, um die konsistente und integrierte Umsetzung und Durchführung mit verwandten Managementsystemen zu unterstützen. Ein entsprechend gestaltetes Managementsystem kann daher die Anforderungen all dieser Standards erfüllen. Tabelle C.1 zeigt die Beziehung zwischen den Abschnitten dieser Internationalen Norm, ISO 9001:2000 und ISO 14001:2004.

Die Gestaltung dieser Internationalen Norm ermöglicht es einer Organisation, ihr ISMS mit den Anforderungen verwandter Managementsysteme abzustimmen oder zu integrieren.

WICHTIG — Diese Veröffentlichung gibt nicht vor, alle notwendigen Bestimmungen eines Vertrages zu beinhalten. Anwender sind verantwortlich für ihre korrekte Anwendung. Einhaltung einer Internationalen Norm allein verleiht keine Immunität gegen gesetzliche Verpflichtungen.

1 Anwendungsbereich

1.1 Allgemeines

Diese Internationale Norm behandelt alle Arten von Organisationen (z. B. kommerzielle Unternehmen, Behörden, gemeinnützige Organisationen). Diese Internationale Norm legt die Anforderungen für das Festlegen, Umsetzen, Durchführen, Überwachen, Überprüfen, Instandhalten und Verbessern eines dokumentierten ISMS im Kontext der allgemeinen Geschäftsrisiken der Organisation fest. Sie legt außerdem Anforderungen für die Umsetzung von Sicherheitsmaßnahmen fest, die auf die Bedürfnisse der jeweiligen Organisation oder Teilen davon zugeschnitten sind.

Das ISMS soll sicherstellen, dass adäquate und angemessene Sicherheitsmassnahmen ausgewählt werden, die Informationswerte schützen und Vertrauen bei Interessenten erwecken.

ANMERKUNG 1 In dieser Internationalen Norm sollte der Begriff „Geschäft“ allgemein als diejenigen Aktivitäten interpretiert werden, die den wesentlichen Daseinszweck der Organisation ausmachen.

ANMERKUNG 2 ISO/IEC 17799 stellt Anleitungen zur Umsetzung bereit, die bei der Entwicklung von Maßnahmen verwendet werden können.

1.2 Anwendung

Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemeiner Natur und auf alle Organisationen anwendbar, unabhängig von Art, Größe und Beschaffenheit. Ein Ausschluss der in den Abschnitten 4, 5, 6, 7, und 8 festgelegten Anforderungen ist nicht zulässig, wenn eine Organisation Konformität mit dieser Internationalen Norm beansprucht.

Ausschlüsse von Maßnahmen, die zur Erfüllung der Kriterien für die Risikoakzeptanz als notwendig erachtet werden, müssen begründet werden. Außerdem muss nachgewiesen werden, dass die damit verbundenen Risiken von verantwortlichen Personen akzeptiert wurden. Wenn Maßnahmen ausgeschlossen werden, ist der Anspruch auf Konformität mit dieser Internationalen Norm nur zulässig, wenn diese Ausschlüsse nicht die Fähigkeit oder Verantwortung der Organisation beeinträchtigen, Informationssicherheit zu liefern, die die durch die Risikoeinschätzung und zutreffende gesetzliche oder behördlich Anforderungen bestimmten Sicherheitsanforderungen erfüllt.

ANMERKUNG Wenn eine Organisation bereits ein funktionsfähiges Managementsystem der Geschäftsprozesse hat (z. B. in Zusammenhang mit ISO 9001 oder ISO 14001), so sollte es in den meisten Fällen vorgezogen werden, die Anforderungen dieser Internationalen Norm innerhalb des existierenden Managementsystems zu erfüllen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. 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 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe:

3.1

Wert

alles, was für die Organisation von Wert ist

[ISO/IEC 13335-1:2004]

3.2

Verfügbarkeit

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

[ISO/IEC 13335-1:2004]

3.3

Vertraulichkeit

Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

[ISO/IEC 13335-1:2004]

3.4**Informationssicherheit**

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden

[ISO/IEC 17799:2005]

3.5**Informationssicherheitsereignis**

erkanntes Auftreten eines System-, Service- oder Netzwerkzustands, der einen möglichen Verstoß gegen die Informationssicherheitsleitlinie oder Fehler von Maßnahmen, oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt

[ISO/IEC TR 18044:2004]

3.6**Informationssicherheitsvorfall**

einzelnes oder Reihe von unerwünschten oder unerwarteten Informationssicherheitsereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird

[ISO/IEC TR 18044:2004]

3.7**Informationssicherheits-Managementsystem****ISMS**

Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt

ANMERKUNG Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.

3.8**Integrität**

Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten

[ISO/IEC 13335-1:2004]

3.9**Restrisiko**

nach der Risikobehandlung verbleibende Risiko

[ISO/IEC Guide 73:2002]

3.10**Risikoakzeptanz**

Entscheidung, ein Risiko zu akzeptieren

[ISO/IEC Guide 73:2002]

3.11**Risikoanalyse**

Systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des Risikos

[ISO/IEC Guide 73:2002]

3.12

Risikoeinschätzung

gesamter Prozess der Risikoanalyse und Risikobewertung

[ISO/IEC Guide 73:2002]

3.13

Risikobewertung

Prozess, in dem das eingeschätzte Risiko mit den festgelegten Kriterien verglichen wird, um die Bedeutung des Risikos zu bestimmen.

[ISO/IEC Guide 73:2002]

3.14

Risikomanagement

Koordinierte Aktivitäten zur Leitung und Kontrolle einer Organisation in Bezug auf Risiken

[ISO/IEC Guide 73:2002]

3.15

Risikobehandlung

Prozess für die Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos

[ISO/IEC Guide 73:2002]

ANMERKUNG In dieser Internationalen Norm wird der Begriff „Lenkung“ als Synonym zu „Maßnahme“ verwendet.

3.16

Erklärung zur Anwendbarkeit

Dokument, das die Maßnahmenziele und Maßnahmen beschreibt, die für das ISMS einer Organisation relevant und anwendbar sind

ANMERKUNG Maßnahmenziele und Maßnahmen basieren auf den Ergebnissen und Schlussfolgerungen der Risikoeinschätzungs- und Risikobehandlungsprozesse, gesetzlichen oder behördlichen Anforderungen, vertraglichen Verpflichtungen und den Geschäftsanforderungen der Organisation an Informationssicherheit.

4 Informationssicherheits-Managementsystem

4.1 Allgemeine Anforderungen

Die Organisation muss ein dokumentiertes ISMS im Kontext ihrer allgemeinen Geschäftsaktivitäten und der Risiken, der sie sich gegenüberstellt, festlegen, umsetzen, durchführen, überwachen, überprüfen, instandhalten und verbessern. Für diese Internationale Norm basiert der angewandte Prozess auf dem in Bild 1 gezeigten PDCA-Modell.

4.2 Festlegung und Verwaltung des ISMS

4.2.1 Festlegen des ISMS

Die Organisation muss die folgenden Schritte durchführen.

- a) Definition des Anwendungsbereiches und der Grenzen des ISMS, unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standortes, ihrer Werte (Assets) und ihrer Technologie, einschließlich der Details über und Rechtfertigung von jeglichen Ausschlüssen aus dem Anwendungsbereich (siehe 1.2).

- b) Definition der ISMS-Leitlinie unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standorts, ihrer Werte und ihrer Technologie, die:
- 1) einen Rahmen für Zielsetzungen vorgibt und eine generelle Richtung sowie Grundsätze für Aktionen hinsichtlich Informationssicherheit festlegt;
 - 2) geschäftliche, gesetzliche oder amtliche Anforderungen und vertragliche Sicherheitsverpflichtungen berücksichtigt;
 - 3) mit dem strategischen Risikomanagementkontext der Organisation abgestimmt ist, in dem die Einrichtung und Instandhaltung des ISMS erfolgen wird;
 - 4) Kriterien festlegt, nach denen Risiken bewertet werden (siehe 4.2.1 c)); und
 - 5) vom Management genehmigt wurde.

ANMERKUNG Im Rahmen dieser Internationalen Norm wird die ISMS-Leitlinie als Obermenge der Informationssicherheitsleitlinie betrachtet. Diese beiden Leitlinien können in einem Dokument beschrieben werden.

- c) Definition der Vorgehensweise der Organisation für Risikoeinschätzung.
- 1) Identifizierung einer Methode für die Risikoeinschätzung, die für das ISMS und die festgelegten Geschäftsanforderungen an Informationssicherheit sowie die gesetzlichen und amtlichen Anforderungen geeignet ist.
 - 2) Entwicklung von Kriterien für Risikoakzeptanz und Identifizierung von akzeptablen Risikoniveaus (siehe 5.1 f)).

Die ausgewählte Methode für die Risikoeinschätzung muss sicherstellen, dass die Risikoeinschätzung vergleichbare und reproduzierbare Resultate liefert.

ANMERKUNG Es gibt verschiedene Methoden für die Risikoeinschätzung. Beispiele für Methoden für Risikoeinschätzung werden in ISO/IEC TR 13335-3, *Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security* behandelt.

- d) Identifizierung der Risiken.
- 1) Identifizierung der organisationseigenen Werte (Assets) innerhalb des Anwendungsbereichs des ISMS, und die Eigentümer²⁾ dieser Werte.
 - 2) Identifizierung der Bedrohungen für diese organisationseigenen Werte (Assets).
 - 3) Identifizierung der Schwachstellen, die durch diese Bedrohungen ausgenutzt werden könnten.
 - 4) Identifizierung der Auswirkungen, die der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit auf die organisationseigenen Werte (Assets) haben darf.
- e) Analyse und Bewertung der Risiken.
- 1) Einschätzung des geschäftlichen Schadens für die Organisation, der durch Sicherheitsprobleme entstehen könnte; dies sollte die Folgen des Verlusts von Vertraulichkeit, Integrität oder Verfügbarkeit der organisationseigenen Werte (Assets) berücksichtigen.

²⁾ Der Begriff „Eigentümer“ bezeichnet eine natürliche oder juristische Person, die die vom Management zugewiesene Verantwortung für die Kontrolle von Produktion, Entwicklung, Pflege, Gebrauch und Sicherheit der Werte hat. Der Begriff „Eigentümer“ bedeutet nicht, dass diese Person irgendwelche Eigentumsrechte an dem Wert hat.

- 2) Einschätzung der realistischen Wahrscheinlichkeit, dass Sicherheitsprobleme auftreten, angesichts der existierenden Bedrohungen und Schwachstellen, der mit den organisationseigenen Werten (Assets) verbundenen Auswirkungen, und der momentan umgesetzten Maßnahmen.
 - 3) Einschätzung der Risikoniveaus.
 - 4) Bestimmung, ob die Risiken akzeptabel sind oder eine Behandlung im Rahmen der in 4.2.1 c) 2) festgelegten Kriterien erfordern.
- f) Identifizierung und Bewertung der Optionen für die Risikobehandlung.

Mögliche Aktionen sind:

- 1) Anwendung geeigneter Maßnahmen;
 - 2) bewusste und objektive Akzeptanz der Risiken, sofern diese eindeutig den Leitlinien und Kriterien der Organisation für Risikoakzeptanz genügen (siehe 4.2.1 c) 2));
 - 3) Vermeidung der Risiken; und
 - 4) Übertragung der zugehörigen Geschäftsrisiken an andere, z. B. Versicherer, Lieferanten.
- g) Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung.

Maßnahmenziele und Maßnahmen müssen ausgewählt und umgesetzt werden, um die in dem Risikoeinschätzungs- und Risikobehandlungsprozess identifizierten Anforderungen zu erfüllen. Diese Auswahl muss die Kriterien für Risikoakzeptanz (siehe 4.2.1 c) 2)) sowie die gesetzlichen, amtlichen und vertraglichen Anforderungen berücksichtigen.

Die Maßnahmenziele und Maßnahmen in Anhang A, die geeignet sind, die identifizierten Anforderungen abzudecken, müssen als Teil dieses Prozesses ausgewählt werden.

Die in Anhang A angegebenen Maßnahmenziele und Maßnahmen sind nicht erschöpfend, und zusätzliche Maßnahmenziele und Maßnahmen dürfen ebenfalls ausgewählt werden.

ANMERKUNG Anhang A enthält eine umfassende Liste von Maßnahmenzielen und Maßnahmen, die üblicherweise als geeignet für Organisationen angesehen werden. Anwender dieser Internationalen Norm werden auf Anhang A als Ausgangspunkt für die Maßnahmenauswahl verwiesen, um sicherzustellen, dass keine wichtigen Maßnahmenoptionen übersehen werden.

- h) Zustimmung des Managements zu den vorgeschlagenen Restrisiken.
- i) Genehmigung des Managements für die Umsetzung und Durchführung des ISMS.
- j) Erstellung einer Erklärung zur Anwendbarkeit.

Eine Erklärung zur Anwendbarkeit muss erstellt werden, die Folgendes beinhaltet:

- 1) die in 4.2.1 g) ausgewählten Maßnahmenziele und Maßnahmen, und die Gründe für ihre Auswahl;
- 2) die momentan umgesetzten Maßnahmenziele und Maßnahmen (siehe 4.2.1 e) 1)); und
- 3) den Ausschluss von Maßnahmenzielen und Maßnahmen in Anhang A, und die Gründe für ihren Ausschluss.

ANMERKUNG Die Erklärung zur Anwendbarkeit liefert eine Zusammenfassung der Entscheidungen zur Risikobehandlung. Die Begründung von Ausschlüssen sorgt für eine Gegenprobe, dass keine Maßnahmen versehentlich ausgelassen wurden.

4.2.2 Umsetzen und Durchführen des ISMS

Die Organisation muss die folgenden Schritte durchführen.

- a) Formulierung eines Risikobehandlungsplans, der die geeigneten Aktionen des Managements, Ressourcen, Verantwortlichkeiten und Prioritäten für das Management von Informationssicherheitsrisiken identifiziert (siehe Abschnitt 5).
- b) Umsetzung des Risikobehandlungsplans um die identifizierten Maßnahmenziele zu erreichen, einschließlich der Berücksichtigung der Finanzierung und der Zuweisung von Aufgaben und Verantwortlichkeiten.
- c) Umsetzung der in 4.2.1 g) ausgewählten Maßnahmen um die Maßnahmenziele zu erreichen.
- d) Definition eines Maßes für die Wirksamkeit der ausgewählten Maßnahmen oder Maßnahmengruppen; außerdem muss festgelegt werden, wie diese Maße benutzt werden können, um die Wirksamkeit der Maßnahmen einzuschätzen, und um dabei vergleichbare und reproduzierbare Resultate (siehe 4.2.3 c)) zu erhalten.

ANMERKUNG Das Messen der Wirksamkeit von Maßnahmen ermöglicht es Managern und Personal, zu bestimmen, wie gut die Maßnahmen die vorgesehenen Maßnahmenziele erreichen.

- e) Umsetzung von Programmen für Schulung und Bewusstseinsbildung (siehe 5.2.2).
- f) Verwaltung des Betriebs des ISMS.
- g) Verwaltung der Ressourcen für das ISMS (siehe 5.2).
- h) Umsetzung von Verfahren und anderen Maßnahmen, die eine sofortige Erkennung von Sicherheitsereignissen und Reaktion auf Sicherheitsvorfälle (siehe 4.2.3 a)) ermöglichen.

4.2.3 Überwachen und Überprüfen des ISMS

Die Organisation muss die folgenden Schritte durchführen.

- a) Ausführung von Verfahren zur Überwachung und Überprüfung und anderen Maßnahmen, um:
 - 1) Fehler in den Verarbeitungsergebnissen sofort zu erkennen;
 - 2) Versuchte und erfolgreiche Sicherheitsverstöße und Sicherheitsvorfälle sofort zu identifizieren;
 - 3) dem Management die Feststellung zu ermöglichen, ob die auf Personen übertragenen oder durch Informationstechnologie durchgeführten Sicherheitsaktivitäten erwartungsgemäß ausgeführt werden;
 - 4) die Entdeckung von Sicherheitsereignissen durch den Gebrauch von Indikatoren zu unterstützen, und dadurch Sicherheitsvorfälle zu verhindern; und
 - 5) zu bestimmen, ob die zum Beheben von Sicherheitsverstößen ergriffenen Aktivitäten wirksam waren.
- b) Regelmäßige Überprüfung der Wirksamkeit des ISMS (einschließlich der Einhaltung der ISMS-Leitlinie und -Ziele, sowie Überprüfung der Sicherheitsmaßnahmen) unter Berücksichtigung von Ergebnissen von Sicherheitsaudits, Sicherheitsvorfällen, Ergebnissen von Wirksamkeitsmaßen, sowie Vorschlägen und Feedback von allen Interessenten.
- c) Messung der Wirksamkeit von Maßnahmen, um zu bestätigen, dass Sicherheitsanforderungen erfüllt worden sind.

- d) Überprüfung der Risikoeinschätzungen in regelmäßigen Abständen und Überprüfung der Restrisiken und akzeptablen Risikoniveaus, unter Berücksichtigung von Änderungen:
- 1) der Organisation;
 - 2) der Technologie;
 - 3) von Geschäftsziele und -Prozesse;
 - 4) bei identifizierten Bedrohungen;
 - 5) der Wirksamkeit der umgesetzten Maßnahmen und
 - 6) in externen Ereignissen, wie Änderungen in der gesetzlichen oder amtlichen Umgebung, geänderte Verträge, und Änderungen im gesellschaftlichen Klima.
- e) Durchführung interner ISMS-Audits in geplanten Abständen (siehe Abschnitt 6).

ANMERKUNG Interne Audits, manchmal auch eigene Audits genannt, werden von der Organisation selbst oder in ihrem Auftrag für interne Zwecke durchgeführt.

- f) Ausführung einer regelmäßigen Managementbewertung des ISMS um sicherzustellen, dass der Anwendungsbereich adäquat bleibt und Verbesserungen im ISMS-Prozess erkannt werden (siehe 7.1).
- g) Aktualisierung von Sicherheitsplänen unter Berücksichtigung der Ergebnisse der Überwachungs- und Überprüfungsaktivitäten.
- h) Aufzeichnung von Aktivitäten und Ereignissen, die einen Einfluss auf die Wirksamkeit oder die Leistung des ISMS haben könnten (siehe 4.3.3).

4.2.4 Instandhalten und Verbessern des ISMS

Die Organisation muss die folgenden Schritte regelmäßig durchführen.

- a) Umsetzung der identifizierten Verbesserungen im ISMS.
- b) Ergreifung von geeigneten Korrekturmaßnahmen und Vorbeugungsmaßnahmen nach 8.2 und 8.3. Anwendung der Lektionen, die aus den Sicherheitserfahrungen anderer Organisationen und denen der eigenen Organisation gelernt wurden.
- c) Mitteilung der Maßnahmen und Verbesserungen an alle Interessenten, in einem den Umständen angemessenen Detaillierungsgrad, und ggf. Abstimmung des weiteren Vorgehens.
- d) Sicherstellung, dass die Verbesserungen die beabsichtigten Ziele erreichen.

4.3 Dokumentationsanforderungen

4.3.1 Allgemeines

Dokumentationen müssen Aufzeichnungen von Managemententscheidungen enthalten, sicherstellen, dass sich Aktivitäten auf Managemententscheidungen und Grundsätze zurückverfolgen lassen, und sicherstellen, dass die aufgezeichneten Ergebnisse reproduzierbar sind.

Es ist wichtig, dass es möglich ist, die Beziehung von den ausgewählten Maßnahmen zurück zu den Resultaten des Risikoeinschätzungs- und Risikobehandlungsprozesses nachzuweisen, und weiterhin zurück zu der ISMS-Leitlinie und den -Zielen.