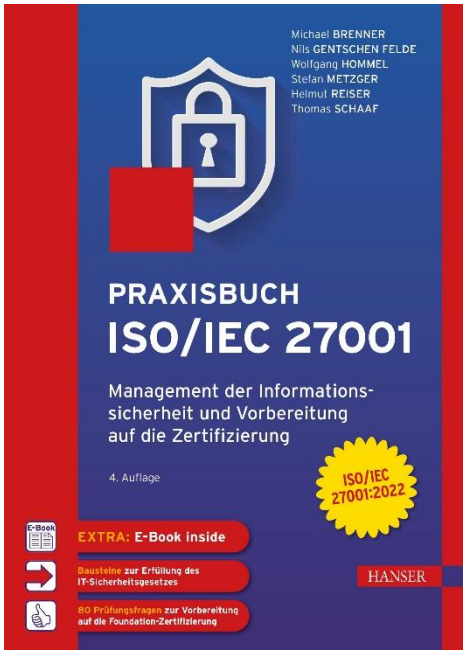
HANSER



Leseprobe

zu

Praxisbuch ISO/IEC 27001

von Michael Brenner, Nils gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser und Thomas Schaaf

Print-ISBN: 978-3-446-47395-9
E-Book-ISBN: 978-3-446-47458-1
E-Pub-ISBN: 978-3-446-47615-8

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446473959
sowie im Buchhandel

Inhaltsverzeichnis

Vorwort

Liebe Leserinnen und Leser,

dieses Buch ist dafür konzipiert, Sie auf Basis des Wortlauts der internationalen Norm ISO/IEC 27001 in das Thema Informationssicherheitsmanagementsysteme einzuführen, auf eine Personenzertifizierung vorzubereiten und als Nachschlagewerk zu dienen.

Im Jahr 2022 haben sich im wichtigen Anhang A der internationalen ISO/IEC 27001 größere Veränderungen ergeben, deren Überführung in die deutsche DIN ISO/IEC 27001 zum Zeitpunkt der Drucklegung der vorliegenden vierten Auflage dieses Buchs noch in Arbeit sind. Kapitel 4 des Buchs enthält den deutschen Wortlaut der DIN ISO/IEC 27001:2017, da die entsprechenden Teile in der englischen Norm bis auf kleine textuelle Ergänzungen, die wir berücksichtigt haben, nicht verändert wurden. Anhang B.1 enthält die deutsche Fassung der Norm ISO/IEC 27001 vollständig und im Original-Wortlaut und -Layout. Für die noch nicht offiziell übersetzten veränderten Teile der Norm, also den Anhang A, liefern wir in Kapitel 5 des Buchs zusätzlich eigene deutsche Fachübersetzungen, sowie in Anhang B.3 einen tabellarischen Überblick über alle aktuellen Maßnahmen (Controls), damit Sie sowohl mit dem englischen Original als auch einem deutschen Text arbeiten können.

Das erste Kapitel führt Sie kompakt in die spannende, aber auch komplexe Welt der Informationssicherheit, Managementsysteme und Standards ein. Nach einem Überblick über die Reihe der ISO/IEC 27000-Standards und die Grundlagen von Informationssicherheitsmanagementsystemen finden Sie in den Kapiteln 4 und 5 alle Anforderungen und Maßnahmen aus ISO/IEC 27001. Sie werden in grau hinterlegten Boxen wörtlich wiedergegeben und zusätzlich erläutert. Die Schwerpunkte der Erklärungen orientieren sich an den Inhalten der Prüfungen zu den Foundation-Lehrgangskonzepten u. a. von APMG, ICO und TÜV Süd Akademie; das Buch ist aber auch für die Vorbereitung auf die Prüfung in einem der anderen Qualifizierungsprogramme nach ISO/IEC 27001 verwendbar. Ferner finden Sie in diesem Buch insgesamt 80 Beispiel-Prüfungsfragen. Ihr Format und Schwierigkeitsgrad entspricht dem der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie mit genau einer richtigen Antwort pro Frage. Die Hälfte der Fragen finden Sie über die Kapitel 2–7 verteilt jeweils am Ende, wo auch die wichtigsten Inhalte nochmals kompakt zusammengefasst werden. Im Anhang finden Sie dann nochmals 40 Fragen am Stück. Dies entspricht dem Umfang der „richtigen“ Prüfung. Dadurch können Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln.

Wir wünschen Ihnen viel Erfolg bei der Prüfung und bei der praktischen Anwendung!

München, im September 2022 *Die Autoren*

1 Einführung und Basiswissen

Nachdem das Thema Informationssicherheit einige Jahrzehnte lang ein gewisses Nischendasein gefristet hat, gewinnt es in den letzten Jahren massiv an Bedeutung. Das hängt nicht zuletzt mit einem steigenden öffentlichen Bewusstsein für die Sicherheit und den Schutz von Daten und Informationen zusammen. Auch die mediale Aufmerksamkeit ist einem Unternehmen sicher, wenn sich beispielsweise herausstellt, dass es nachlässig mit seinen Kundendaten umgeht, oder wenn sicherheitsrelevante Vorfälle zu Ausfällen mit großer geschäftlicher Auswirkung führen.

Der Gesetzgeber hat mit dem IT-Sicherheitsgesetz und entsprechenden Verordnungen kritische Infrastrukturen definiert. Für diese wurden höhere rechtliche Anforderungen im Hinblick auf die IT-Sicherheit erlassen und die Betreiber verpflichtet, angemessene organisatorische und technische Vorkehrungen für die IT-Sicherheit zu treffen und dabei den Stand der Technik einzuhalten.

Wenn sich eine Organisation heute vornimmt, einen strukturierten Ansatz zum wirksamen Management der Informationssicherheit einzuführen, kommt sie an der Standard-Reihe ISO/IEC 27000 praktisch nicht vorbei. Bei ISO/IEC 27000 handelt es sich um eine Reihe von Dokumenten, in denen verschiedene Aspekte des Informationssicherheitsmanagements betrachtet werden. Dass es sich um von der ISO (International Organization for Standardization) und der IEC (International Electrotechnical Commission) standardisierte Dokumente handelt, erhöht dabei die Verbreitung, Bedeutung und Akzeptanz dieser Standards ganz maßgeblich. Das zentrale und wichtigste Dokument der Reihe ist dabei ISO/IEC 27001.

1.1 Worum geht es in ISO/IEC 27001?

Die Standardfamilie ISO/IEC 27000 befasst sich hauptsächlich mit drei Kernbereichen:

1. **Begriffe:** Es werden die wichtigsten Fachbegriffe aus der Welt der Informationssicherheit definiert.
2. **Grundlegendes Managementsystem:** Es wird beschrieben, was eine Organisation umzusetzen hat und sicherstellen muss, um die eigenen Aktivitäten und Maßnahmen im Bereich Informationssicherheit wirksam steuern zu können.

3. **Maßnahmen:** Es werden Maßnahmen beschrieben, die eine Organisation grundsätzlich umzusetzen hat, um ein hohes Maß an Informationssicherheit gewährleisten zu können.

Dieses Buch bietet einen Überblick über alle drei Bereiche. Während die beiden letzteren in späteren Kapiteln behandelt werden, beschäftigt sich dieses Kapitel zunächst mit der Begriffsbildung.

1.2 Begriffsbildung

Die Standardfamilie ISO/IEC 27000 dient ganz wesentlich dazu, die Verwendung von Fachbegriffen zu vereinheitlichen. Nur so kann erreicht werden, dass diejenigen, die sich mit Informationssicherheitsmanagement beschäftigen, nicht aneinander vorbeireden, obwohl sie eigentlich inhaltlich dasselbe meinen.

Im Folgenden werden die wichtigsten Begriffe und Grundlagen rund um das Thema Informationssicherheit vorgestellt, die zum Verständnis der ISO/IEC 27000 Standards erforderlich sind.

1.2.1 Informationen

In unserer inzwischen hochgradig vernetzten Welt sind Informationen Werte, die von entscheidender Wichtigkeit für den Geschäftsbetrieb einer Organisation sind. Dabei sind diese Informationen einer stark zunehmenden Zahl von Bedrohungen ausgesetzt. Informationssysteme, Netze und Organisationen sind dabei beispielsweise durch Cyber-Angriffe (Ransomware, Denial-of-Service-Angriffe, Hacking, Spam etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer sowie Katastrophen und andere Gefahren gefährdet. Gesetzliche Regelungen (wie z. B. das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung) fordern entsprechend Schutzmaßnahmen für sensible Informationen.

Der Begriff „Informationen“ wird hierbei sehr weit gefasst. Sie können in Form verschiedener Medien vorliegen: geschrieben, gedruckt, elektronisch, als Film etc., und auf unterschiedlichen Wegen übermittelt werden, z. B. per Post, per Funk, über das Internet usw. Unabhängig vom Medium und vom Übertragungsweg ist die Aufgabe der Informationssicherheit, diese Informationen angemessen vor der zunehmenden Zahl von Bedrohungen zu schützen. Nur so können die Risiken minimiert, der Geschäftsbetrieb gesichert und die Wettbewerbsfähigkeit, Rentabilität sowie die Chancen einer Organisation maximiert werden.

1.2.2 Informationssicherheit

Für die Informationssicherheit existiert, anders als beispielsweise für Gewichte, Längen oder Temperaturen, keine physikalische Maßeinheit, um sie einfach in Zahlen – also *quantitativ* – auszudrücken. Deshalb wählen die Standards der Reihe ISO/IEC 27000 – und damit auch das Hauptdokument ISO/IEC 27001 – einen praxisbewährten *qualitativen* Ansatz

über Schutzziele. Diese werden nachfolgend im Einzelnen vorgestellt und genauer erläutert.

1.2.3 Sicherheitsanforderungen und Schutzziele

Die Gefährdung wichtiger Informationen lässt sich alleine mit Beispielen natürlich nur ungenau und unvollständig fassen. In der ISO/IEC 27000 und im Security Engineering werden deshalb abstrakte Schutzziele bzw. Sicherheitsanforderungen für Informationswerte (zum Begriff der „(Informations-)Werte“ vgl. Kapitel 3.1.1) definiert. Die zentralen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit (engl. *Confidentiality, Integrity and Availability*, als Eselsbrücke gerne mit „CIA“ abgekürzt) von Informationen. Andere wünschenswerte Eigenschaften, deren Aufrechterhaltung nach ISO/IEC 27000 ebenfalls Gegenstand der Informationssicherheit sein können, sind Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit (engl. *Authenticity, Accountability, Non-repudiation and Reliability*). Diese Schutzziele, auf denen der Informationssicherheitsbegriff der Standardfamilie ISO/IEC 27000 basiert, werden im Folgenden erläutert.

Zur Beschreibung von Angriffsszenarien und Sicherheitsmaßnahmen werden oft fiktive Personen verwendet. Diese Personen haben definierte Rollen und Namen. Die „Guten“ heißen immer Alice und Bob und versuchen in der Regel, miteinander zu kommunizieren. Der „Böse” (engl. *malicious*) heißt Mallet; er versucht, Alice, Bob oder deren Interaktionen oder Kommunikation anzugreifen, abzuhören oder zu stören. Im Folgenden werden Alice, Bob und Mallet in diesem Sinn verwendet, um die Verletzung von Schutzzielen zu verdeutlichen.

1.2.3.1 Vertraulichkeit (Confidentiality)

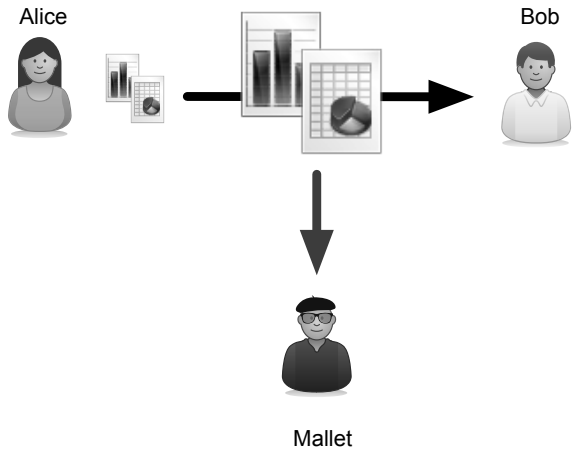


Abbildung 1.1 Verletzung der Vertraulichkeit durch Abhören

Die Vertraulichkeit bezeichnet die Eigenschaft, dass eine Information für unautorisierte Personen, Entitäten oder Prozesse nicht zugänglich ist und von diesen auch nicht offen-

5 Maßnahmen im Rahmen des ISMS

Im normativen Anhang A *Referenzmaßnahmen* (vgl. S. 209) beschreibt ISO/IEC 27001 eine sehr umfangreiche Reihe von Maßnahmen, deren Umsetzung zur Reduzierung der Risiken für die Informationssicherheit beiträgt. Trotz des Umfangs ist diese Maßnahmenliste nicht vollständig; jede Organisation muss sich deshalb auch überlegen, welche weiteren Maßnahmen in ihrem konkreten Fall benötigt werden. Die Maßnahmen wurden ursprünglich aus den Abschnitten 5 bis 15 der Norm ISO/IEC 17799 abgeleitet, woraus sich auch die Nummerierung des Anhangs A von ISO/IEC 27001 beginnend mit A.5 ergibt. In der aktuellen Version der Norm wurde die Anzahl der Abschnitte drastisch auf nur noch vier reduziert. In der ersten Version von ISO/IEC 27001 waren es elf und dann 14. Die Kapitel von ISO/IEC 27002 orientieren sich auch an dieser Struktur und Reihenfolge. Auch die Anzahl der Maßnahmen wurde von 114 auf 93 konsolidiert.

In diesem Kapitel gehen wir auf alle in Anhang A von ISO/IEC 27001 aufgeführten Maßnahmen ein. Einige Maßnahmen sind dabei ausführlicher beschrieben als andere. Das bedeutet **nicht**, dass sie theoretisch oder in der Praxis wichtiger sind als die anderen, sondern spiegelt vielmehr die Schwerpunkte des ISO/IEC 27001 Foundation-Kurses wider. Zu ausgewählten Maßnahmen werden in Anlehnung an ISO/IEC 27002 jeweils auch praktische Beispiele zur Umsetzung gegeben.

Die ISO/IEC 27000-Normenreihe fasst die Maßnahmen in vier Kategorien zusammen (vgl. Abbildung 5.1). Nachfolgend werden die einzelnen Kategorien in der Reihenfolge, wie sie auch in ISO/IEC 27001 genannt sind, besprochen:

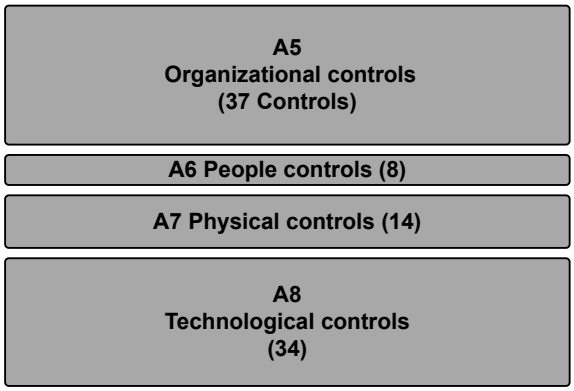


Abbildung 5.1 Struktur der Maßnahmen aus Anhang A von ISO/IEC 27001

5.1 A.5 Organizational Controls – Organisatorisches Maßnahmen

5.1.1 A.5.1 Informationssicherheitsrichtlinien

Anforderungen: Eine Informationssicherheitsrichtlinie und themenspezifische Richtlinien müssen definiert, vom Topmanagement genehmigt, veröffentlicht, an relevante Mitarbeitende und andere interessierte Parteien kommuniziert und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

Control **Policies for information security** according to ISO/IEC 27001:2022:
Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**
A.5.1.1 Informationssicherheitsrichtlinien
A.5.1.2 Überprüfung der Informationssicherheitsrichtlinien

Wie bereits in Kapitel 3.1.2 und Kapitel 4.5.2 erläutert, sind die mit dem ISMS verbundenen Zielsetzungen – die Informationssicherheitspolitik der Organisation – von der höchsten Ebene des Managements der Organisation zu definieren. Dokumentiert wird dies in einer übergeordneten Informationssicherheitsrichtlinie, die eine organisationsweit kommunizierte Absichtserklärung des Topmanagements darstellt.

Berücksichtigt werden sollten in der übergeordneten Richtlinie allgemeine ISMS-Ziele und -Prinzipien (z. B. risikobasierter Ansatz, Schutz von Werten, kontinuierliche Verbesserung), aber auch vertragliche und gesetzliche Rahmenbedingungen sowie Strategien und allge-

meine Ziele der Organisation. Die Richtlinie ist auch eine gute Stelle, um übergreifende Verantwortlichkeiten für die Informationssicherheit und deren Management zu definieren.

Die übergeordnete Informationssicherheitsrichtlinie (oder auch: ISMS-Richtlinie) wird durch themenspezifische Richtlinien ergänzt.

Themen für spezifische Richtlinien können beispielsweise sein:

- Umgang mit Informationen und Werten bzw. Assets (siehe Kapitel 5.1.10)
- Informationsklassifizierung (siehe Kapitel 5.1.12)
- Übertragung von Informationen (siehe Kapitel 5.1.14)
- Zugangssteuerung und Zugangsberechtigungen (siehe Kapitel 5.1.15 und 5.1.18)
- Lieferantenbeziehungen (siehe Kapitel 5.1.19)
- Verwendung von Clouddiensten (siehe Kapitel 5.1.23)
- Schutz der Rechte an geistigem Eigentum (siehe Kapitel 5.1.32)
- Umgang mit Aufzeichnungen (siehe Kapitel 5.1.33)
- Privatsphäre und Schutz personenbezogener Daten (siehe Kapitel 5.1.34)
- Home Office und Remote-Arbeiten (siehe Kapitel 5.2.7)
- Aufgeräumte Schreibtische und Gerätesperren (clear desk and clear screen) (siehe Kapitel 5.3.7)
- Mobile Speichermedien (siehe Kapitel 5.3.10)
- Anwender-Endgeräte (siehe Kapitel 5.4.1)
- Management technischer Schwachstellen und Kommunikation dieser (siehe Kapitel 5.4.8)
- Aufbewahrung und Löschung von Informationen (siehe Kapitel 5.4.10)
- Datensicherung und Backups (siehe Kapitel 5.4.13)
- Protokollierung und Umgang mit Log-Files (siehe Kapitel 5.4.15)
- Einsatz von Kryptographie (siehe Kapitel 5.4.24)

Die themenspezifischen Richtlinien müssen nicht notwendigerweise von der obersten Leitung erlassen und freigegeben werden; dies kann auf einer niedrigeren, der Regelung des jeweiligen Themas angemessenen Ebene geschehen.

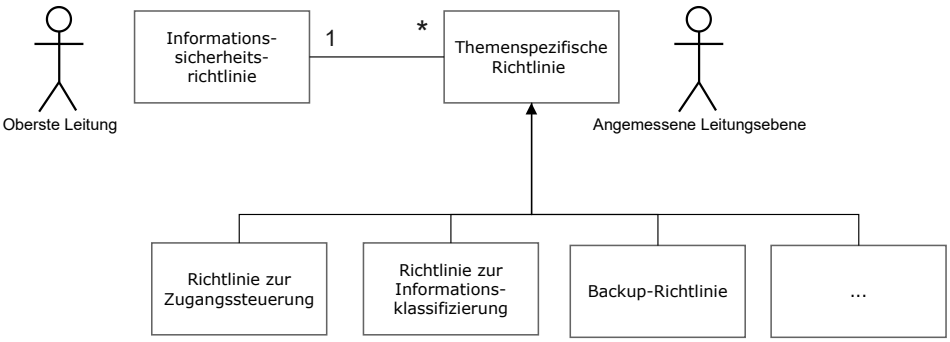


Abbildung 5.2 Informationssicherheitsrichtlinie und themenspezifische Richtlinien

Richtlinien adressieren meist nicht nur einen kleinen Kreis von Spezialisten, sondern ein relativ breites Publikum innerhalb (und teilweise auch außerhalb) der Organisation. Sie

sollten immer relativ kurz gehalten werden sowie prägnant und verständlich formuliert sein. Regelungen zu Details finden gegebenenfalls ihren Platz besser in anderen Vorgabedokumenten wie Prozess- und Verfahrensdefinitionen, Arbeitsanweisungen und Ähnlichem.

Richtlinien sind allen maßgeblichen Parteien zu kommunizieren. Dabei ist natürlich darauf zu achten, dass es hierbei nicht zu einer unnötigen Verbreitung vertraulicher Informationen außerhalb der Organisation kommt.

Richtlinien als übergeordnete Zielvorgaben ändern sich in der Regel seltener als Prozess- und Verfahrensdefinitionen und andere konkretere Vorgabedokumente. Dennoch müssen auch sie einer regelmäßigen Überprüfung unterzogen und kontinuierlich weiter entwickelt werden. Für die Überprüfung, Weiterentwicklung und Freigabe der verschiedenen Richtlinien sollten jeweils geeignete Verantwortlichkeiten definiert und zugewiesen werden. Eine Überprüfung einer Richtlinie sollte spätestens in einem festgelegten Abstand (z. B. jährlich) erfolgen. Auch wenn sich neue Erkenntnisse oder Erfordernisse – z. B. aus Managementbewertungen, Audits, Änderungen im Geschäftsumfeld, neuen Gefahrenlagen oder der Analyse von Informationssicherheitsvorfällen – ergeben, kann eine Überprüfung angezeigt sein.

5.1.2 A.5.2 Rollen und Verantwortlichkeiten für die Informationssicherheit

Anforderungen: Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen der Organisation definiert und zugewiesen werden.

Control **Information security roles and responsibilities** according to ISO/IEC 27001:2022:
Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**
A.6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Die wirksame Wahrnehmung von Verantwortlichkeiten im Kontext der Informationssicherheit ist die Basis für deren Erhalt und Management. Wichtig ist also, dass eine angemessene Struktur von Rollen und Funktionen mit zugewiesenen Verantwortlichkeiten (man sagt manchmal auch: eine Informationssicherheitsorganisation) definiert und innerhalb der Gesamtorganisation bekannt ist.

Die Rollen sollten so definiert sein, dass die Verantwortlichkeiten beim Schutz von Werten, bei der Ausführung der Informationssicherheitsprozesse sowie im Risikomanagement eindeutig festgelegt sind – bei Letzterem speziell auch die Rolle des Risikoeigentümers (vgl. Kapitel 4.6.1.2 und 4.6.1.3).

Für alle Rollen ist ihre jeweilige Verantwortung sowie ihre Zuweisung an eine konkrete Person, Funktion oder Stelle in der Organisation zu dokumentieren. Es empfiehlt sich, die Verantwortung für die übergreifende Koordination des Managements der Informations-

sicherheit einer Person bzw. Stelle zuzuweisen, welche diese Rolle als ihre Hauptfunktion erfüllt. Diese Rolle bzw. Funktion wird in der Praxis unterschiedlich benannt – gängige Bezeichnungen sind z. B. Chief Information Security Officer (CISO), Informationssicherheits-Beauftragte(r), Information Security Officer oder ISMS-Beauftragte(r).

5.1.3 A.5.3 Aufgabentrennung

Anforderungen: Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen der Organisation definiert und zugewiesen werden.

Control **Segregation of duties** according to ISO/IEC 27001:2022:
Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**
A.6.1.2 Aufgabentrennung

Bei der Zuweisung von Verantwortlichkeiten und Pflichten – im ISMS selbst, aber auch in anderen relevanten Bereichen wie z. B. der IT-Administration – sollte auf eine angemessene Trennung von Aufgaben geachtet werden.

Mit der Aufgabentrennung wird das Risiko eines Missbrauchs, sei er irrtümlich oder vorsätzlich, minimiert. Ein Ziel kann hierbei beispielsweise sein, dass Werte mit hohem Schutzbedarf nur unter Einhaltung eines Vieraugenprinzips verwendet und modifiziert werden dürfen.

Für kleine Organisationen, in denen eine Aufgabentrennung in allen Bereichen nur schwer umsetzbar ist, können andere Maßnahmen wie Überwachung der Tätigkeiten, Prüfpfade und Leitungsaufsicht etabliert werden.

5.1.4 A.5.4 Verantwortung des Topmanagements

Anforderungen: Das Topmanagement muss alle Mitarbeitenden verpflichten, die Informationssicherheit in Übereinstimmung mit der Informationssicherheitsrichtlinie, themenspezifischen Richtlinien und Verfahren der Organisation aufrechtzuerhalten.

Control **Management responsibilities** according to ISO/IEC 27001:2022:
Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**
A.7.2.1 Verantwortlichkeiten der Leitung

Das Engagement der obersten Leitung ist ein kritischer Erfolgsfaktor für ein wirksames ISMS. Insbesondere sollte die Leitung bei der Informationssicherheit innerhalb der Or-

ganisation eine Vorbildfunktion erfüllen. Sie muss die Informationssicherheit aktiv fördern sowie unterstützen und dafür sorgen, dass die Beschäftigten über ihre Rollen, Verantwortlichkeiten und über die Richtlinien, Regeln, Maßnahmen und Verfahren Bescheid wissen. Das Bewusstsein für Informationssicherheit sollte gestärkt und die Beschäftigten dafür auch motiviert und kontinuierlich weitergebildet werden (siehe auch Kapitel 5.2.3).

5.1.5 A.5.5 Kontakt zu Behörden

Anforderungen: Die Organisation muss den Kontakt zu den zuständigen Behörden herstellen und aufrechterhalten.

Control **Contact with authorities** according to ISO/IEC 27001:2022:
The organization shall establish and maintain contact with relevant authorities.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**
A.6.1.3 Kontakt mit Behörden

Oft auch auf regelmäßiger Basis, insbesondere aber in besonderen Situationen wie beim Umgang mit schweren Informationssicherheitsvorfällen (vgl. Kapitel 5.1.24), ist eine angemessene Kommunikation mit Behörden notwendig.

Bereits vor einem solchen Kontakt werden Verfahren und Verantwortlichkeiten bestimmt und dokumentiert, die festlegen, wer wann mit welchen Behörden kommuniziert. Dies betrifft z. B. Strafverfolgungsbehörden oder auch Aufsichtsbehörden. Dabei ist auch festzulegen, wer berechtigt ist, Informationen über Sicherheitsvorfälle an Externe weiterzugeben und in welcher Art die Weitergabe solcher Informationen erfolgt. Gegebenenfalls besteht durch gesetzliche und behördliche Auflagen (vgl. Kapitel 1.3) sogar eine gesetzliche Verpflichtung zur Meldung.

5.1.6 A.5.6 Kontakt zu speziellen Interessengruppen

Anforderungen: Die Organisation muss Kontakte zu speziellen Interessengruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden herstellen und pflegen.

Control **Contact with special interest groups** according to ISO/IEC 27001:2022:
The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**
A.6.1.4 Kontakt mit speziellen Interessensgruppen

Ein Austausch mit anderen Organisationen zum Thema Informationssicherheit kann vielfältige Vorteile haben. Mitgliedschaften in Interessengruppen können dazu dienen, besser über den aktuellen Stand allgemeiner und sektorspezifischer Gefährdungen sowie Good Practices informiert zu sein. Es können auch Vereinbarungen zur Kooperation und Koor-

eines Lesezugriffs, der mitunter auch auf zuvor erstellte Kopien von Systemdateien erfolgt, die im Anschluss an die Tests wieder gelöscht werden.

5.5 Beispiele für Prüfungsfragen zu diesem Kapitel

Nachfolgend finden Sie Beispiele für Prüfungsfragen, die sich thematisch mit den in diesem Kapitel erlernten Inhalten auseinandersetzen. Die richtigen Antworten inklusive Erläuterungen und Verweisen befinden sich in Anhang C.1 ab Seite 240.

Prüfungsfrage 5.22:
Durch welche Maßnahme gemäß Anhang A aus ISO/IEC 27001 wird am ehesten vermieden, dass beispielsweise Entwickler von Software versehentlich oder absichtlich produktive Systeme kompromittieren?

A) Sichere Authentifizierung

B) Redundanz informationsverarbeitender Systeme

C) Trennung von Netzen

D) Trennung von Entwicklungs-, Test- und Produktivumgebungen

Prüfungsfrage 5.23:
Welche der folgenden Aspekte und Anforderungen sind im Zusammenhang mit Betriebsmitteln und unterstützenden Versorgungseinrichtungen *nicht* Teil der Maßnahmen zur physischen Sicherheit gemäß Abschnitt A.7 in ISO/IEC 27001?

A) Betriebsmittel müssen sicher und geschützt platziert werden.

B) Die Konfigurationen, einschließlich der Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.

C) Kabel zur Stromversorgung, Datenübertragung oder Anbindung an Informationsdienste müssen vor Abhören, Manipulation oder Beschädigung geschützt werden.

D) Betriebsmittel müssen sachgerecht gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen zu gewährleisten.

Prüfungsfrage 5.24:
Was muss gemäß Maßnahme A.6.5 aus ISO/IEC 27001 im Zusammenhang mit Beendigung oder Wechsel des Beschäftigungsverhältnisses festgelegt werden?

A) Kennungen der Nutzerendgeräte, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses zurückgegeben werden müssen

B) Verantwortlichkeiten und Pflichten im Zusammenhang mit der Informationssicherheit, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses fortbestehen

C) Verträge, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses neu ausgehandelt werden müssen

D) Gültigkeitsdauer von digitalen Identitäten, Benutzerkennungen und Zertifikaten, die auch nach Beendigung oder Wechsel des Beschäftigungsverhältnisses noch verwendet werden

Prüfungsfrage 5.25:
Wobei handelt es sich um eine technische Maßnahme gemäß ISO/IEC 27001, Anhang A.8?

A) Aufgabentrennung

B) Screening

C) Datensicherung

D) Remote-Arbeiten

Prüfungsfrage 5.26:
Was ist Gegenstand der Maßnahme *Überwachungsaktivitäten (A.8.16)* gemäß Anhang A in ISO/IEC 27001?

A) Überwachung des Personals im Hinblick auf vorsätzliche Verletzungen der Informationssicherheit

B) Überwachung des Umsetzungsstands von Maßnahmen zur Risikobehandlung

C) Überwachung von Netzen, Systemen und Anwendungen im Hinblick auf Anomalien

D) Überwachung von Sicherheitsbereichen mithilfe von Videokameras

Prüfungsfrage 5.27:
Wobei handelt es sich um eine organisatorische Maßnahme gemäß ISO/IEC 27001, Anhang A.5?

A) Aufgeräumter Schreibtisch und Gerätesperre

B) Schutz vor Schadsoftware

C) Reaktion auf Informationssicherheitsvorfälle

D) Einsatz von Kryptographie

7 Zertifizierungsmöglichkeiten nach ISO/IEC 27000

Im Kontext von ISO/IEC 27000 gibt es zwei grundsätzlich verschiedene Arten der Zertifizierung. Zunächst kann natürlich das ISMS einer Organisation nach ISO/IEC 27001 zertifiziert werden – diese Möglichkeit zu schaffen, war ja in der Entstehungsgeschichte der ISO/IEC 27000 der wesentliche Grund für die Ergänzung des Leitfadens für Informationssicherheitsmanagement (ISO/IEC 17799 bzw. ISO/IEC 27002) um die normativen Anforderungen in ISO/IEC 27001.

Daneben gibt es die Personenzertifizierungen, die keine Zertifizierungen nach der Norm ISO/IEC 27001 darstellen, sondern Personen ermöglichen, ihr Wissen und ihre Qualifikationen hinsichtlich der Inhalte und der Anwendung der ISO/IEC 27000-Standardfamilie nachzuweisen.

7.1 ISMS-Zertifizierung nach ISO/IEC 27001

Die Zertifizierung des ISMS ermöglicht es einer Organisation, ihre Fähigkeit, ein effektives Informationssicherheitsmanagement zu betreiben, gegenüber bestehenden und zukünftigen Kunden, Aufsichtsbehörden oder anderen interessierten Parteien nachzuweisen.

7.1.1 Grundlagen der Zertifizierung von Managementsystemen

Nachfolgend werden die Begriffe Zertifizierung und Akkreditierung erläutert, die im Zusammenhang mit Konformitätsbewertungen von Managementsystemen wichtig sind.

7.1.1.1 Zertifizierung

Zum Erreichen einer *Zertifizierung* eines Managementsystems ist ein externes, von einer akkreditierten Zertifizierungsstelle beauftragtes Audit (vgl. Kapitel 4.9.2 ab Seite 63) zwingend notwendig. Im Rahmen dieses sogenannten Zertifizierungsaudits wird die Einhaltung der Anforderungen des Standards, d. h. die Konformität des Managementsystems zum Standard, überprüft und bewertet.

Welche Bereiche der Organisation dabei auditiert werden, ergibt sich auf Basis des erklärten Anwendungsbereichs des Managementsystems (*Scoping Statement*). Welche Maßnahmen auditiert werden, leitet sich aus der Erklärung zur Anwendbarkeit des Standards (*Statement of Applicability*), s. a. Kapitel 4.4.3 und 4.6.1.3, ab. Die Angemessenheit dieser Erklärung und der dort festgelegten Ausschlüsse wird selbstverständlich überprüft. Die Anforderungen aus den Kapiteln 4 bis 10 der Norm sind in einem Zertifizierungsaudit immer Teil der Auditkriterien.

Im Nachgang eines Audits wird ein Auditbericht erstellt. Dieser enthält die im Audit getroffenen Feststellungen, welche in verschiedene Kategorien – z. B. positiver Aspekt, Verbesserungspotenzial, Nebenabweichung, (Haupt-)Abweichung – eingeteilt sind. Sind während des Audits keine (Haupt-)Abweichungen festgestellt worden, d. h. keine Defizite, welche die Wirksamkeit des ISMS infrage stellen, wird als Auditschlussfolgerung vom Audit-Team die Ausstellung des Zertifikats empfohlen werden. In diesem Fall wird die Zertifizierungsstelle das Zertifikat nach einer Überprüfung der vom Audit-Team eingereichten Unterlagen ausstellen.

7.1.1.2 Akkreditierung

Auch an die Organisationen, die Managementsysteme zertifizieren, werden Anforderungen gestellt. Die Erfüllung dieser Anforderungen wird von einer Akkreditierungsstelle überprüft.

Vereinfacht ausgedrückt ist eine Akkreditierung eine Art Zertifizierung der Zertifizierer. Obwohl die Worte Akkreditierung und Zertifizierung häufig synonym verwendet werden, sind es genau genommen unterschiedliche Dinge: Eine Zertifizierung bestätigt die Konformität zu einem Standard, eine Akkreditierung ist die formale Anerkennung einer Kompetenz (hier: die Kompetenz einer Stelle, Konformitätsbewertungen von ISMS durchzuführen).

Die Europäische Union sieht Akkreditierung als eine hoheitliche Aufgabe. Entsprechend lassen sich in Europa Zertifizierungsstellen für Managementsysteme die Kompetenz, bestimmte Konformitätsbewertungsaufgaben durchzuführen, bei einem zentralen, nationalen Akkreditierer bestätigen. Dies ist beispielsweise in Deutschland die DAkkS (Deutsche Akkreditierungsstelle GmbH), in Österreich die vom Bundesministerium für Wissenschaft, Forschung und Wirtschaft betriebene „Akkreditierung Austria“, in der Schweiz die SAS (Schweizerische Akkreditierungsstelle, Teil des Staatssekretariats für Wirtschaft). Die Harmonisierung und wechselseitige Anerkennung von Akkreditierungen wird durch die *European co-operation for Accreditation*[1] geregelt.

Allgemeine Anforderungen an Zertifizierungsstellen, nach denen alle in der *European co-operation for Accreditation* organisierten Akkreditierer prüfen, sind in ISO/IEC 17021 (*Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren*) [DIN15] festgelegt. ISO/IEC 27006 (*Requirements for bodies providing audit and certification of information security management systems*) [DIN15] konkretisiert und ergänzt die Anforderungen aus ISO/IEC 17021 für Stellen, die Managementsysteme für Informationssicherheit auditieren und zertifizieren.

Abbildung 7.1 verdeutlicht die Zusammenhänge noch einmal an einem Beispiel. Will die spanische Firma Colmo S. A. beispielsweise die Archivierung ihrer Dokumente an die deut-

[1] http://www.european-accreditation.org/

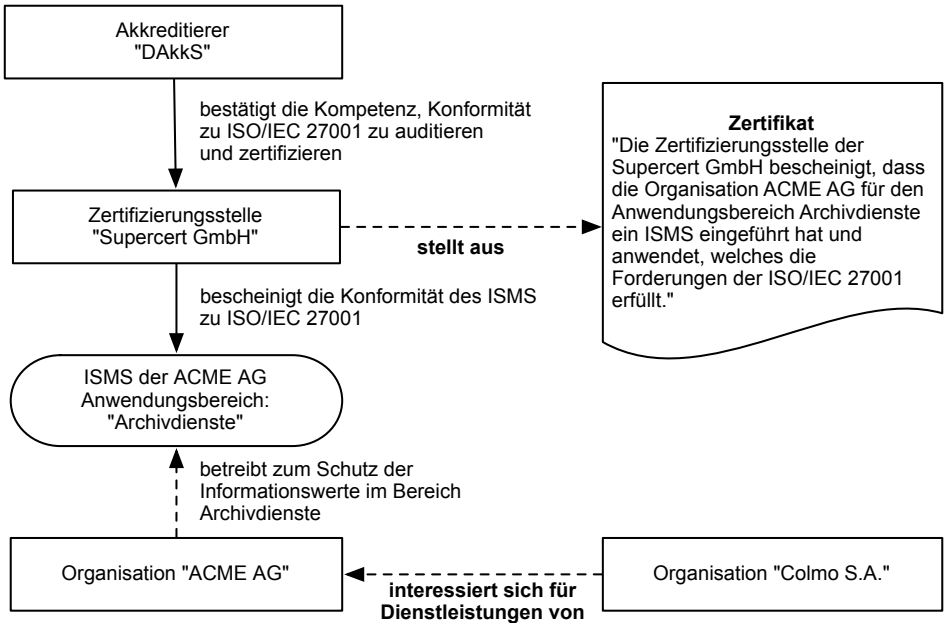


Abbildung 7.1 Zertifizierung und Akkreditierung

sche ACME AG auslagern, so wird es sie sicherlich interessieren, ob die ACME AG in diesem Bereich ein vernünftiges Informationssicherheitsmanagement betreibt. Hier kann die ACME AG darauf verweisen, dass es die Anforderungen der ISO/IEC 27001 erfüllt und dass dies von der Supercert GmbH bestätigt worden ist. Nun hat vielleicht bei der Colmo S. A. noch nie jemand etwas von der Supercert GmbH gehört. Die Kompetenz der Supercert GmbH, solche Bewertungen vorzunehmen, ist aber von einem nationalen Akkreditierer bestätigt worden, der nach denselben Prinzipien vorgeht und prüft wie die nationale Akkreditierungsstelle in Spanien. Daher kann die Colmo S. A. die von der ACME AG vorgelegte Zertifizierung als seriös ansehen.

Natürlich erlaubt auch die Vorlage einer ISO/IEC 27001-Zertifizierung nicht das bedenkenlose Vertrauen in die Informationssicherheit bei einer Organisation. Aber sie zeigt immerhin, dass – zumindest im zertifizierten Geltungsbereich – die notwendigen Grundlagen für ein effektives Management der Informationssicherheit vorhanden sind.

7.1.2 Typischer Ablauf einer Zertifizierung

Eine Zertifizierung erfolgt durch eine entsprechend akkreditierte Zertifizierungsstelle. Die Abbildung 7.2 zeigt exemplarisch einen typischen Ablauf.

Ein Zertifizierungsaudit sollte gründlich vorbereitet werden. Die Ergebnisse interner Audits (siehe Kapitel 4.9.2) bzw. Self-Assessments helfen bei der Erkennung von Lücken bis zur Erfüllung aller in ISO/IEC 27001 enthaltenen Anforderungen. Es lohnt sich aber oft, bereits frühzeitig mit der gewünschten Zertifizierungsstelle Kontakt aufzunehmen, um z. B. in Vorgesprächen zu klären, welche Unterlagen die Auditoren erwarten oder wie die wichtigs-

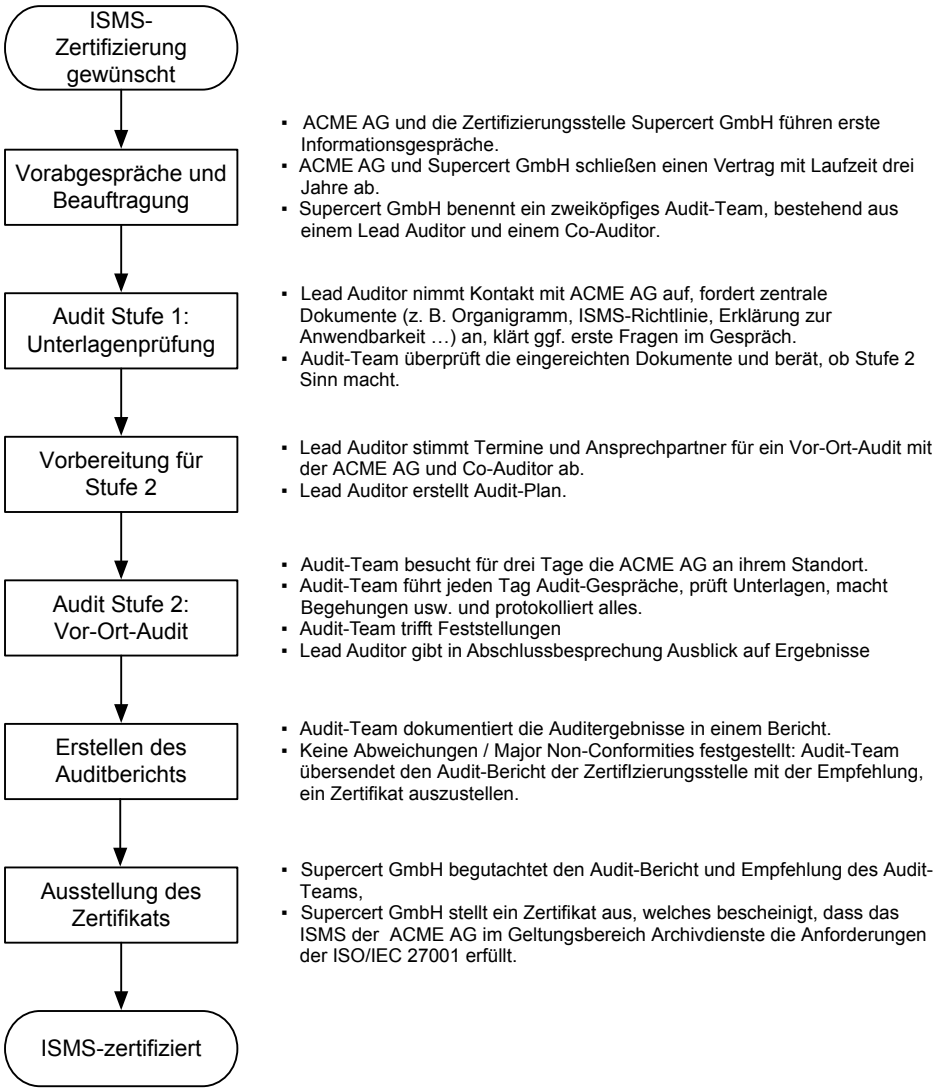


Abbildung 7.2 Beispielhafter Ablauf einer Zertifizierung

ten Verbesserungsmaßnahmen grob zu priorisieren sind. Viele Zertifizierungsstellen bieten auch ein sogenanntes Vor-Audit als Dienstleistung an, welches eine Art vereinfachten Probelauf für das Zertifizierungsaudit bietet und hilft, unangenehme Überraschungen zu vermeiden.

Das eigentliche Zertifizierungsaudit läuft meist in zwei Phasen ab. In der ersten Phase (Stufe 1) werden von den Auditoren primär Dokumente und Aufzeichnungen überprüft. Basierend auf den Ergebnissen dieses Dokumentenaudits geben die Auditoren eine Empfehlung ab, ob es sinnvoll ist, mit dem Audit zu diesem Zeitpunkt weiter zu verfahren. Wenn ja, wird ein Auditplan für die zweite Phase erstellt. In der zweiten Phase (Stufe 2) führt ein Team von

Index