



Leseprobe

Michael Brenner, Nils Gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser, Thomas Schaaf

Praxisbuch ISO/IEC 27001

Management der Informationssicherheit und Vorbereitung auf die
Zertifizierung

ISBN (Buch): 978-3-446-45139-1

ISBN (E-Book): 978-3-446-45260-2

Weitere Informationen oder Bestellungen unter

<http://www.hanser-fachbuch.de/978-3-446-45139-1>

sowie im Buchhandel.

2.4.2.3	ISO/IEC 27009: Anforderungen an die branchenspezifische Anwendung von ISO/IEC 27001	13
2.4.3	Allgemeine Leitfäden	13
2.4.3.1	ISO/IEC 27002: Leitfaden für das Informationssicherheitsmanagement	13
2.4.3.2	ISO/IEC 27003: Umsetzungsempfehlungen	13
2.4.3.3	ISO/IEC 27004: Messungen	14
2.4.3.4	ISO/IEC 27005: Risikomanagement.....	14
2.4.3.5	ISO/IEC 27007 und ISO/IEC TR 27008: Audit-Leitfäden	14
2.4.4	Sektor- und maßnahmenspezifische Leitfäden.....	14
2.5	Zusammenfassung	15
2.6	Beispiele für Prüfungsfragen zu diesem Kapitel.....	15
3	Grundlagen von Informationssicherheitsmanagementsystemen	17
3.1	Das ISMS und seine Bestandteile.....	17
3.1.1	(Informations-)Werte.....	18
3.1.2	Richtlinien, Prozesse und Verfahren	18
3.1.3	Dokumente und Aufzeichnungen	19
3.1.4	Zuweisung von Verantwortlichkeiten	20
3.1.5	Maßnahmenziele und Maßnahmen.....	21
3.2	Was bedeutet Prozessorientierung?	22
3.3	Die PDCA-Methodik: Plan-Do-Check-Act	23
3.3.1	Planung (Plan)	24
3.3.2	Umsetzung (Do).....	25
3.3.3	Überprüfung (Check).....	25
3.3.3.1	Konformität.....	25
3.3.3.2	Effektivität	26
3.3.3.3	Effizienz	26
3.3.4	Verbesserung (Act)	26
3.4	Zusammenfassung	26
3.5	Beispiele für Prüfungsfragen zu diesem Kapitel.....	27
4	ISO/IEC 27001 – Spezifikationen und Mindestanforderungen	29
4.0	Einleitung.....	31
4.0.1	Allgemeines	31
4.0.2	Kompatibilität mit anderen Normen für Managementsysteme	32
4.1	Anwendungsbereich	32
4.2	Normative Verweisungen.....	33
4.3	Begriffe	33
4.4	Kontext der Organisation	34
4.4.1	Verstehen der Organisation und ihres Kontextes	34
4.4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien....	35

4.4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	36
4.4.4	Informationssicherheitsmanagementsystem	36
4.5	Führung	37
4.5.1	Führung und Verpflichtung	37
4.5.2	Politik	38
4.5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	39
4.6	Planung	40
4.6.1	Maßnahmen zum Umgang mit Risiken und Chancen	40
4.6.2	Informationssicherheitsziele und Planung zu deren Erreichung	45
4.7	Unterstützung	46
4.7.1	Ressourcen	46
4.7.2	Kompetenz	46
4.7.3	Bewusstsein	47
4.7.4	Kommunikation	47
4.7.5	Dokumentierte Information	48
4.8	Betrieb	50
4.8.1	Betriebliche Planung und Steuerung	50
4.8.2	Informationssicherheitsrisikobeurteilung	51
4.8.3	Informationssicherheitsrisikobehandlung	52
4.9	Bewertung der Leistung	52
4.9.1	Überwachung, Messung, Analyse und Bewertung	52
4.9.2	Internes Audit	54
4.9.3	Managementbewertung	56
4.10	Verbesserung	57
4.10.1	Nichtkonformität und Korrekturmaßnahmen	57
4.10.2	Fortlaufende Verbesserung	58
4.11	Zusammenfassung	59
4.12	Beispiele für Prüfungsfragen zu diesem Kapitel	59
5	Maßnahmenziele und Maßnahmen im Rahmen des ISMS	63
5.1	A.5 Informationssicherheitsrichtlinien	65
5.1.1	A.5.1 Vorgaben der Leitung für Informationssicherheit	65
5.2	A.6 Organisation der Informationssicherheit	67
5.2.1	A.6.1 Interne Organisation	67
5.2.2	A.6.2 Mobilgeräte und Telearbeit	69
5.3	A.7 Personalsicherheit	70
5.3.1	A.7.1 Vor der Beschäftigung	71
5.3.2	A.7.2 Während der Beschäftigung	72
5.3.3	A.7.3 Beendigung und Änderung der Beschäftigung	73
5.4	A.8 Verwaltung der Werte	74
5.4.1	A.8.1 Verantwortlichkeit für Werte	74

5.4.2	A.8.2 Informationsklassifizierung.....	76
5.4.3	A.8.3 Handhabung von Datenträgern	77
5.5	A.9 Zugangssteuerung	80
5.5.1	A.9.1 Geschäftsanforderungen an die Zugangssteuerung.....	80
5.5.2	A.9.2 Benutzerzugangsverwaltung	81
5.5.3	A.9.3 Benutzerverantwortlichkeiten.....	83
5.5.4	A.9.4 Zugangssteuerung für Systeme und Anwendungen.....	83
5.6	A.10 Kryptographie	86
5.6.1	A.10.1 Kryptographische Maßnahmen.....	86
5.7	A.11 Physische und umgebungsbezogene Sicherheit	88
5.7.1	A.11.1 Sicherheitsbereiche.....	88
5.7.2	A.11.2 Geräte und Betriebsmittel	90
5.8	A.12 Betriebssicherheit	94
5.8.1	A.12.1 Betriebsabläufe und -verantwortlichkeiten	94
5.8.2	A.12.2 Schutz vor Schadsoftware.....	96
5.8.3	A.12.3 Datensicherung	97
5.8.4	A.12.4 Protokollierung und Überwachung	98
5.8.5	A.12.5 Steuerung von Software im Betrieb.....	99
5.8.6	A.12.6 Handhabung technischer Schwachstellen	100
5.8.7	A.12.7 Audit von Informationssystemen	101
5.9	A.13 Kommunikationssicherheit	103
5.9.1	A.13.1 Netzwerksicherheitsmanagement.....	103
5.9.2	A.13.2 Informationsübertragung.....	104
5.10	A.14 Anschaffung, Entwicklung und Instandhalten von Systemen	107
5.10.1	A.14.1 Sicherheitsanforderungen an Informationssysteme	107
5.10.2	A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen	108
5.10.3	A.14.3 Testdaten	111
5.11	A.15 Lieferantenbeziehungen.....	113
5.11.1	A.15.1 Informationssicherheit in Lieferantenbeziehungen	113
5.11.2	A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten.....	114
5.12	A.16 Handhabung von Informationssicherheitsvorfällen.....	116
5.12.1	A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen	116
5.13	A.17 Informationssicherheitsaspekte beim Business Continuity Management ...	119
5.13.1	A.17.1 Aufrechterhalten der Informationssicherheit	120
5.13.2	A.17.2 Redundanzen.....	121
5.14	A.18 Compliance.....	122
5.14.1	A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen	123
5.14.2	A.18.2 Überprüfungen der Informationssicherheit	124
5.15	Zusammenfassung	126
5.16	Beispiele für Prüfungsfragen zu diesem Kapitel.....	126

6	Verwandte Standards und Rahmenwerke	131
6.1	Standards und Rahmenwerke für IT- und Informationssicherheit	131
6.1.1	IT-Grundschutz-Kataloge	131
6.1.2	IT-Grundschutz-Standards	132
6.1.3	ISIS12	133
6.1.4	Cybersecurity Framework	133
6.1.5	ISO/IEC 15408	134
6.2	Standards und Rahmenwerke für Qualitätsmanagement, Auditierung und Zertifizierung	135
6.2.1	ISO 9000	135
6.2.2	ISO 19011	135
6.2.3	ISO/IEC 17020	136
6.3	Standards und Rahmenwerke für Risikomanagement	137
6.3.1	ISO 31000	137
6.3.2	COSO ERM	137
6.4	Standards und Rahmenwerke für Governance und Management in der IT	138
6.4.1	ITIL	138
6.4.2	ISO/IEC 20000	139
6.4.3	FitSM	140
6.4.4	COBIT	141
6.5	Beispiele für Prüfungsfragen zu diesem Kapitel	142
7	Zertifizierungsmöglichkeiten nach ISO/IEC 27000	145
7.1	ISMS-Zertifizierung nach ISO/IEC 27001	145
7.1.1	Grundlagen der Zertifizierung von Managementsystemen	145
7.1.1.1	Zertifizierung	145
7.1.1.2	Akkreditierung	146
7.1.2	Typischer Ablauf einer Zertifizierung	147
7.1.3	Auditumfang	149
7.1.4	Akzeptanz und Gültigkeit des Zertifikats	149
7.2	Personenqualifizierung auf Basis von ISO/IEC 27000	149
7.2.1	Programme zur Ausbildung und Zertifizierung von Personal	150
7.2.1.1	TÜV Süd: Qualifizierungsprogramm nach ISO/IEC 27000	150
7.2.1.2	APMG: ISO/IEC 27001 Certification	150
7.2.1.3	Peoplecert: ISO 27000 Information Security M.S.	151
7.2.1.4	ICO: Ausbildungsschema ISMS nach ISO/IEC 27000	151
7.2.2	Das Foundation-Zertifikat des TÜV Süd	152
7.2.2.1	Prüfungsspezifikation	152
7.2.2.2	Vorbereitung auf die Foundation-Prüfung	153
7.3	Zusammenfassung	154
7.4	Beispiele für Prüfungsfragen zu diesem Kapitel	155
A	Begriffsbildung nach ISO/IEC 27000	157

B	Abdruck der DIN ISO/IEC 27001	176
C	Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation	210
C.1	Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln	210
C.2	Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	217
	Literaturverzeichnis	236
	Index.....	239

Vorwort

Dieses Buch ist sowohl zur gezielten Vorbereitung auf die Prüfung zur ISO/IEC 27001 Foundation-Personenzertifizierung als auch als Nachschlagewerk für die Inhalte dieses Standards konzipiert, der 2015 als DIN ISO/IEC 27001:2015 erschien und die deutsche Version der englischsprachigen ISO/IEC 27001:2013 aus dem Jahr 2013 darstellt. Die DIN ISO/IEC 27001:2015 ist komplett als Faksimile in Anhang B dieses Buches enthalten.

Die ersten Kapitel führen Sie kompakt in die spannende, aber auch komplexe Welt der Informationssicherheit, Managementsysteme und Standards ein, die u. a. durch das IT-Sicherheitsgesetz kontinuierlich an Bedeutung gewinnt. 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 Mindestanforderungen und Maßnahmen aus ISO/IEC 27001. Sie werden in grau hinterlegten Boxen wörtlich wiedergegeben und zusätzlich erläutert.

Die Schwerpunkte der Erklärungen orientieren sich dabei an den Inhalten der Prüfung zum *Foundation Certificate in ISMS according to ISO/IEC 27001* nach dem Lehrgangskonzept der TÜV Süd Akademie. Dieses Buch ist aber natürlich auch für die Vorbereitung auf die Foundation-Prüfung aus einem der anderen Qualifizierungsprogramme zum Informationssicherheitsmanagement nach ISO/IEC 27001 verwendbar.

In diesem Buch finden Sie insgesamt 80 Beispiel-Prüfungsfragen. Ihr Format und Schwierigkeitsgrad entspricht wiederum dem der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie. Die Hälfte der Fragen finden Sie über die Kapitel 2–7 verteilt jeweils am Ende, wo auch die wichtigsten Inhalte nochmals kompakt zusammengefasst werden. Sie können sich damit schon beim ersten Durchlesen darauf vorbereiten, wie Prüfungsfragen zu den Inhalten typischerweise aussehen. Im Anhang finden Sie dann nochmals 40 Fragen am Stück. Dies entspricht genau dem Umfang der „richtigen“ Prüfung. Dadurch können Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln.

Noch ein abschließender Hinweis zum flüssigen Lesen: Verweise auf *Kapitel* beziehen sich ohne weitere Angabe immer auf dieses Buch. Verweise auf *Abschnitte* beziehen sich immer auf den entsprechenden Standard.

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

München, im Februar 2017

Die Autoren

1

Einführung und Basiswissen

In immer mehr Umfeldern gewinnt das Thema Informationssicherheit an Bedeutung, was nicht zuletzt mit einem steigenden öffentlichen Bewusstsein für Sicherheit und Schutz von Daten und Informationen zusammenhängt. 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 [Bun15] und entsprechenden Verordnungen kritische Infrastrukturen definiert, für diese höhere gesetzliche Anforderungen im Hinblick auf die IT-Sicherheit erlassen und verpflichtet die Betreiber, 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) standardisierte Dokumente handelt, erhöht dabei die Verbreitung, Bedeutung und Akzeptanz dieser Dokumente 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 Dingen:

1. **Begriffe:** Es werden die wichtigsten Fachbegriffe aus der Welt der Informationssicherheit definiert.
2. **Grundlegendes Managementsystem:** Es wird beschrieben, was eine Organisation tun und sicherstellen muss, um die eigenen Aktivitäten und Maßnahmen im Bereich Informationssicherheit wirksam steuern zu können.
3. **Maßnahmen:** Es werden 114 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 Aspekte. Während die beiden letzteren in späteren Kapiteln behandelt werden, beschäftigt sich dieses Kapitel zunächst mit dem ersten Aspekt, der Begriffsbildung.

■ 1.2 Begriffsbildung

Die Standardfamilie ISO/IEC 27000 dient also unter anderem 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 zunehmend vernetzten Welt sind Informationen Werte, die von entscheidender Wichtigkeit für den Geschäftsbetrieb einer Organisation sind. Durch den höheren Vernetzungsgrad sind diese Informationen einer stark zunehmenden Zahl von Bedrohungen ausgesetzt (vgl. auch [OEC15]). Informationssysteme, Netze und Organisationen sind gefährdet durch Cyber-Angriffe (böswärtiger Code, Denial-of-Service-Angriffe, Schadsoftware, Hacking, Spam etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer sowie Katastrophen und andere Gefahren. Gesetzliche Regelungen (wie z. B. das IT-Sicherheitsgesetz oder Datenschutzgesetze) fordern 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, elektronisch usw. Unabhängig vom Medium und dem Übertragungsmittel 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

Der Begriff Informationssicherheit wird in den Standards der Reihe ISO/IEC 27000 – und damit auch im Hauptdokument ISO/IEC 27001 – über die drei Aspekte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen definiert. Diese drei Aspekte können als die primären Schutzziele angesehen werden, deren Aufrechterhaltung in Kombination die Informationssicherheit ausmacht. Weitere Aspekte und damit Schutzziele wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit können ebenfalls betrachtet

werden (vgl. Anhang A). Die Schutzziele 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 Sicherheitsmechanismen, der Verletzung von Schutzzielen oder aber von Angriffen werden im Security-Engineering 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)

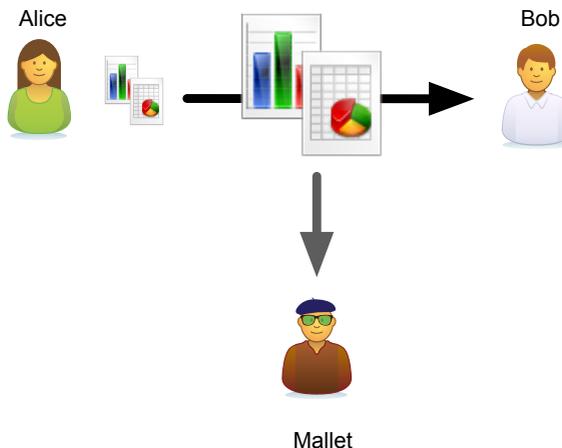


Abbildung 1.1 Verletzung der Vertraulichkeit durch Abhören

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

gelegt werden kann. Die Vertraulichkeit ist beispielsweise verletzt, wenn ein Angreifer eine Kommunikation abhören kann (vgl. Abbildung 1.1).

1.2.3.2 Integrität (Integrity)

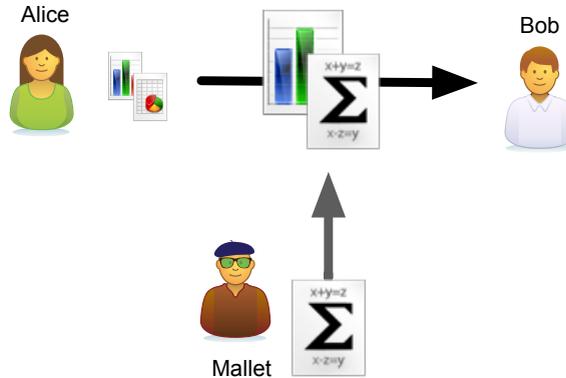


Abbildung 1.2 Verletzung der Integrität

Mit Integrität wird eine Eigenschaft bezeichnet, die Werte im Hinblick auf ihre Richtigkeit und Vollständigkeit schützt. Eine Integritätsprüfung einer digitalen Information oder Nachricht erkennt jede Veränderung an der Nachricht. Hierunter fallen alle denkbaren Manipulationen wie das Einfügen oder Löschen von Zeichen, das Wiedereinspielen einer Nachricht, das Umordnen von Daten oder Nachrichten sowie Duplikate.

Abbildung 1.2 stellt einen Angriff auf die Integrität der Kommunikation zwischen Alice und Bob dar. Mallet verändert die Nachricht, die Alice an Bob schickt.

1.2.3.3 Verfügbarkeit (Availability)

Die Verfügbarkeit bezeichnet die Eigenschaft einer Information oder eines Wertes, für einen berechtigten Nutzer verfügbar und nutzbar zu sein, sobald der Nutzer dies verlangt. Die Verfügbarkeit wird z. B. durch Elementarschäden oder Katastrophen bedroht. Die prominentesten Angriffe auf die Verfügbarkeit von Diensten oder Ressourcen sind Denial of Service (DoS) oder Distributed Denial of Service (DDoS) Angriffe.

1.2.3.4 Authentizität (Authenticity) und Authentisierung (Authentication)

Der Vorgang der zweifelsfreien Ermittlung und Prüfung einer Entität bzw. einer geforderten Charakteristik einer Entität wird als Authentisierung bezeichnet. Dementsprechend bezeichnet Authentizität die Eigenschaft einer Entität, das zu sein, was sie vorgibt zu sein. In der Benutzerverwaltung wird über verschiedenste Mechanismen ein Nutzer zweifelsfrei mit einer digitalen ID (z. B. einer eindeutigen Benutzerkennung) verbunden. Bei der Authentisierung wird diese Verbindung zwischen digitaler ID und Nutzer geprüft (z. B. durch Eingabe eines Passwortes, das nur der Nutzer kennt). Nach dieser Prüfung kann man davon ausgehen, dass die digitale ID authentisch ist.

In Abbildung 1.3 wird ein Man-in-the-Middle-Angriff dargestellt. Mallet unterbricht die Kommunikationsbeziehung zwischen Alice und Bob und gibt sich gegenüber Bob als Alice

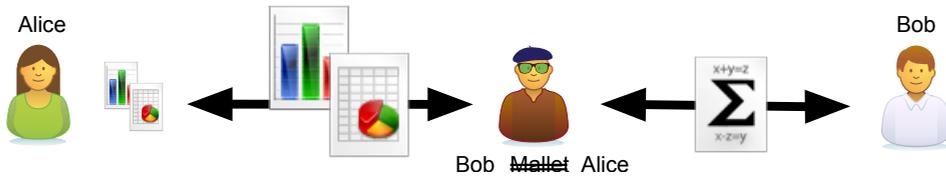


Abbildung 1.3 Verletzung der Authentizität durch einen Man-in-the-Middle-Angriff

und gegenüber Alice als Bob aus. Er fälscht gewissermaßen seine Identität. Damit ist die Authentizität nicht mehr gewährleistet. Steht Alice und Bob nur der verwendete Kommunikationskanal zur Verfügung, so ist dieser Angriff nur sehr schwer zu erkennen.

1.2.3.5 Nichtabstreitbarkeit/Verbindlichkeit (Non-repudiation)

Mit Verbindlichkeit bezeichnet man den Vorgang, mit dem der Eintritt eines Ereignisses oder einer Aktion sowie die verursachende Entität zweifelsfrei belegt werden können. Damit können Kontroversen geklärt werden über das Eintreten oder Nichteintreten eines Events oder einer Aktion und die Beteiligung von Entitäten daran. Beispielsweise kann ein Nutzer die Auslösung einer Aktion später nicht leugnen.

1.2.3.6 Verlässlichkeit (Reliability)

Die Eigenschaft, ein konsistentes und bestimmungsgemäßes Verhalten zu zeigen und konsistente Ergebnisse zu liefern, wird als Verlässlichkeit bezeichnet. Beispielsweise würde eine Verschlüsselungssoftware für E-Mails, die jede dritte Nachricht unverschlüsselt überträgt, die Sicherheitsanforderung nach Verlässlichkeit nicht erfüllen.

1.2.3.7 Zugriffssteuerung (Access Control)

Nach ISO/IEC 27001 stellt die Zugriffssteuerung sicher, dass der Zugang zu Werten (Assets) nur autorisiert erfolgen kann und Einschränkungen auf Basis von Geschäfts- oder Sicherheitsanforderungen möglich sind. Die Zugriffssteuerung setzt ein Berechtigungskonzept technisch um; nur Berechtigte dürfen auf IT-Systeme und Informationen zugreifen.

1.2.3.8 Zurechenbarkeit (Accountability)

Die Zurechenbarkeit realisiert die Verantwortlichkeit einer Entität für ihre Aktionen und Entscheidungen. So müssen z. B. sicherheitsrelevante Aktionen demjenigen, der die entsprechende Aktion ausgeführt hat, zurechenbar sein. Die Zuweisung von Verantwortlichkeiten und die Übernahme von Verantwortung für Assets sind Grundsätze des Standards (vgl. Kapitel 3.1.4), die sich aber nur umsetzen lassen, wenn es Mechanismen gibt, um eine Zurechenbarkeit technisch umzusetzen.

■ 1.3 IT-Sicherheitsgesetz & Co.

Am 12. Juni 2015 wurde durch den Deutschen Bundestag das IT-Sicherheitsgesetz (IT-SiG) [Bun15] beschlossen, das in erster Linie Änderungen an bestehenden Gesetzen, darunter das BSI-Gesetz (BSiG), umfasst. Im Kern bedeuten diese Änderungen die Abkehr vom Prinzip der Freiwilligkeit für den Bereich sogenannter kritischer Infrastrukturen. Deren Betreiber werden nach dem Gesetz verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Den Nachweis darüber haben die Betreiber durch Sicherheitsaudits, Prüfungen und/oder Zertifizierungen zu erbringen, indem sie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Aufstellung der durchgeführten Audits oder Zertifizierungen übermitteln.

Darüber hinaus müssen Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen erhebliche IT-Sicherheitsvorfälle melden. Das BSI wird zur Zentralstelle für IT-Sicherheit und wertet Meldungen der Betreiber kritischer Infrastrukturen aus.

■ 1.4 Überblick über die folgenden Kapitel

In Kapitel 2 wird ein grundlegender Überblick über die Standardfamilie ISO/IEC 27000 und ihre Struktur gegeben, bevor im darauffolgenden Kapitel die Grundlagen eines Informationssicherheitsmanagementsystems dargestellt werden. Der Standard ISO/IEC 27001 wird in den Kapiteln 4 und 5 ausführlich erläutert und kommentiert. Die Mindestanforderungen, d. h. die Abschnitte 1 bis 10 des Standards, finden sich in den Kapiteln 4.1 bis 4.10. Die Anhangteile A.5 bis A.18 von ISO/IEC 27001, die Maßnahmen und Maßnahmenziele enthalten, werden in Kapitel 5 ausführlich erklärt. Die folgenden Kapitel erläutern verwandte Standards und Rahmenwerke sowie die verschiedenen Zertifizierungsmöglichkeiten nach ISO/IEC 27000. Im Anhang des Buches finden Sie 40 Prüfungsfragen mit entsprechenden Musterlösungen, die vom Schwierigkeitsgrad her der ISO/IEC 27001 Foundation-Prüfung entsprechen.

■ 1.5 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 210.



Prüfungsfrage 1.1:

Was versteht ISO/IEC 27000 unter dem Begriff Vertraulichkeit (engl. *Confidentiality*)?

- A) Den Abschluss einer Vertraulichkeitsvereinbarung (Non-disclosure agreement).
- B) Die Geheimhaltungsverpflichtung aller Mitarbeiter, die Zugriff auf das ISMS haben.
- C) Die Vertraulichkeit schützt die Werte im Hinblick auf ihre Richtigkeit und Vollständigkeit.
- D) Eine Information ist für unautorisierte Personen, Entitäten oder Prozesse nicht zugänglich.



Prüfungsfrage 1.2:

Was versteht ISO/IEC 27000 unter dem Begriff Verfügbarkeit (engl. *Availability*)?

- A) Die Eigenschaft einer Information oder eines Wertes, für eine berechnigte Person oder Entität zugreifbar und nutzbar zu sein.
- B) Die Eigenschaft einer informationsverarbeitenden Einrichtung, genügend Ressourcen für eine Aufgabe zur Verfügung zu haben.
- C) Die Eigenschaft einer Information oder eines Wertes, vor Manipulation geschützt zu sein.
- D) Die Eigenschaft einer Information oder eines Wertes, vor Offenlegung geschützt zu sein.



Prüfungsfrage 1.3:

Was versteht ISO/IEC 27000 unter dem Begriff Nichtabstreitbarkeit (engl. *Non-repudiation*)?

- A) Die verbindliche Regelung interner Sicherheitsaudits.
- B) Nichtabstreitbarkeit bezeichnet die Eigenschaft eines Wertes, für einen berechtigten Nutzer verfügbar und nutzbar zu sein.
- C) Als Nichtabstreitbarkeit bezeichnet man den Vorgang, mit dem der Eintritt eines geforderten Ereignisses oder einer Aktion zweifelsfrei einem Verursacher zugerechnet werden kann. Dieser kann den Vorgang nicht leugnen.
- D) Die Eigenschaft, ein konsistentes und bestimmungsgemäßes Verhalten zu zeigen und konsistente Ergebnisse zu liefern.

Index

A

Abhören 91
Access Control 5
Accountability 5
Act-Phase 26, 29, 57
Änderungssteuerung 95
Akkreditierung 12, **146**
analytisches Modell 157
Anforderung 169
Angriff 157
Anschaffung von Systemen 107
Anwendungsbereich 10, 32, 36, 44, 145, 149
APMG 150
Asset 18
Attribut 157
Audit 14, 57, 115, 145, 147, 158
– Bericht 56
– externes 54
– Informationssysteme 101
– internes 54
– Nachweise 55
– Programm 55
– Protokoll 56
– Umfang 149, 158
Auditor 55
Aufgabe des Managements 20
Aufgabentrennung 68
Aufzeichnung **19**
ausgliedern 168
Authentication 4
Authenticity 4
Authentisierung **4**, 158
Authentizität **4**, 158
Availability 4
AXELOS 138

B

Bayerischer IT-Sicherheitscluster e.V. 133
Bedrohung 174

Befugnisse 39
Benutzerverantwortlichkeiten 83
Benutzerzugangsverwaltung 81
Beschäftigung 71
Best Practices 13
Betrieb 50
Betriebs- und Kommunikationsmanagement
– Netzsicherheit 103
Betriebsablauf-Verantwortung 94
Betriebsmanagement
– Überwachung 98
Betriebsmittel 90
Betriebssicherheit 94
Beweismaterial 119
Bewusstsein 47
BSI *siehe* Bundesamt für Sicherheit in der
Informationstechnik
BS 7799 13
Bundesamt für Sicherheit in der
Informationstechnik 131
– IT-Grundschutz-Kataloge 131
– IT-Grundschutz-Standards 132
Business Continuity Management 119

C

Chancen 40
Check-Phase 25, 29, 52
Chief Information Security Officer 21
CISO *siehe* Chief Information Security Officer
COBIT 141
Committee of Sponsoring Organizations of the
Treadway Commission
– ERM 137
Compliance 122
Computer Security Incident Response Team
116
Confidentiality *siehe* Vertraulichkeit
Control Objectives 29
Controls 29

COSO

- see Committee of Sponsoring Organizations of the Treadway Commission 137

COSO ERM 137

CSIRT *siehe* Computer Security Incident Response Team

Cybersecurity Framework 133

D

DAkkS *siehe* Deutsche Akkreditierungsstelle

Daten 160

Datenschutzbeauftragter 20

Datensicherung 97

Datenträger 77

Definitionsebene 19

Deming-Kreislauf 24, 29

Deutsche Akkreditierungsstelle 146

Dienstleistungserbringung 114

Do-Phase 25, 29, 46, 50

Dokument 19

Dokumentation 19, 48

Dokumentenaudit 55, 147

Dokumentenlenkung 20, 49, 49

Dokumentenvorlage 50

DoS-Angriff 4

Durchführungsebene 19

E

Effektivität 26, 56

Effizienz 26, 56

Elementarmaß 158

Entscheidungskriterien 161

Entsorgung von Datenträgern 78

Entwicklung 107

– Ausgliederte 110

Entwicklungsprozess 108

Entwicklungsumgebung 110

Ereignis 161

Ereignismeldung 117

Ereignisprotokollierung 98

Examination Institute 150

Externes Audit 54, 145

Externe Mitarbeiter 20

F

FitSM 140

Folge 159

Fortbildungsprogramme 20

Foundation-Zertifikat 150, 152

– Prüfungsspezifikation 152

– Prüfungsvorbereitung 153

Führung 37

G

Gesamtverantwortung 20

Geschäftsleitung 162

H

Hilfsprogramme mit privilegierten Rechten 85

I

ICO 151

Indikator 19, 163

Information 2, 161

– Übertragung von 104

– Handhabung 77

– Kennzeichnung 76

– Klassifizierung 76

Information Security Officer 21

Information Systems Audit and Control

Association 141

informationsaustauschende Gemeinschaft 164

Informationsbedarf 163

Informationsklassifizierung 76

Informationssicherheit 2, 163

– Aufrechterhaltung 163

– Organisation 67

– Steuerung 162

Informationssicherheitsereignis 117, 163

Informationssicherheitsmanagementsystem
17, 36

– Audit 14

– Dokumentation 19

– Kernbestandteile 17

Informationssicherheitsrichtlinie 65

Informationssicherheitsvorfall 116, 164

– Handhabung 164

Informationssysteme 164

– Audit 101

– Schwachstellenmanagement 100

– Sicherheitsanforderungen 107

Informationsveranstaltungen 20

informationsverarbeitende Einrichtungen 163

Informationszugangsbeschränkung 84

Informativer Standard 10

Installation 99

Instandhaltung 107

Integrität 4, 164

Integrity *siehe* Integrität

Interessierte Partei 165

International Organization for Standardization

1

Internes Audit 54

Interne Organisation 67

Inventar 74

- Inventarisierung der Werte 75
 ISACA *siehe* Information Systems Audit and Control Association
 ISIS12 133
 ISMS *siehe*
 Informationssicherheitsmanagementsystem
 ISMS-Projekt 165
 ISO *siehe* International Organization for Standardization, *siehe* Information Security Officer
 ISO/IEC 15408 134
 ISO/IEC 17020 136
 ISO/IEC 17021 12, 13, 136, 146, 148
 ISO/IEC 17024 136
 ISO/IEC 17025 137
 ISO/IEC 17799 13, 63, 145
 ISO/IEC 20000 22, 139
 ISO/IEC 27000 10
 ISO/IEC 27001 12
 ISO/IEC 27002 13
 ISO/IEC 27003 13
 ISO/IEC 27004 14
 ISO/IEC 27005 14
 ISO/IEC 27006 12, 137, 148
 ISO/IEC 27007 14
 ISO/IEC 27008 14
 ISO/IEC 27009 12, 13
 ISO 19011 135, 148
 ISO 31000 137
 ISO 9000 10, 22, 135
 ISO 9001 135
 ISO 9004 135
 IT Service Management 95
 IT-Grundschutz-Kataloge 131
 IT-Grundschutz-Standards 132
 IT-Sicherheitsgesetz 6
 ITEMO e.V. 140
 ITIL *siehe* IT Infrastructure Library, 138
 ITSM *siehe* IT Service Management
- K**
 Kapazitätssteuerung 95
 Kategorien von Werten 18
 Kennzeichnung von Information 76
 Kernbestandteile eines ISMS 17
 Klassifizierung von Information 76
 Kommunikation 47
 Kompetenz 46, 159
 Konformität 12, 25, 56, 57, 146, 159
 Kontext 162
 – der Organisation 34
 – interner 165
- Kontinuierliche Verbesserung 23
 Korrektur 160
 Korrekturmaßnahme 160
 Kryptographie 86
- L**
 Leistung 168
 Leitfaden 13
 Leitung 37, 174
 Lieferantenbeziehungen 113
 Lizenzmanagement 124
- M**
 Management der Netzsicherheit 103
 Management Review 56
 Managementbewertung 56
 Managementsystem 17, 166
 Maß 161, 166
 Maßeinheit 174
 Maßnahme 21, 63–126, 160
 – Betriebsmanagement 99
 – Organisation der Informationssicherheit 67
 – Personalsicherheit 70
 – Physische und umgebungsbezogene Sicherheit 88
 – Sicherheitsrichtlinie 65
 – Verwaltung der Werte 74
 – Zugangssteuerung 80
 Maßnahmenziele 21, 63–126, 160
 Measurement 14
 Messergebnisse 167
 Messfunktion 166
 Messmethode 167
 Messung 14, 52, 166
 Mobilgeräte 69
- N**
 NAC *siehe* Network Access Control
 Nachvollziehbarkeit 19
 National Institute of Standards and Technology
 – Cybersecurity Framework 133
 Network Access Control 103
 Network Time Protocol 99
 Netzsicherheit 103
 Netzsicherheitsmanagement 103
 Netztrennung 104
 Netzzugang 81
 Nichtabstreitbarkeit 5, 167
 Nichtkonformität 167
 NIM *siehe* Netzwerk für Informationssicherheit im Mittelstand

- NIST *siehe* National Institute of Standards and Technology
- Non-repudiation 5
- Norm 10
- Normative Verweisungen 33
- Normativer Standard 10
- Notfallmanagement 120
- NTP *siehe* Network Time Protocol
- O**
- Objekt 167
- Organisation 168
- Organisation der Informationssicherheit 67
- Interne Organisation 67
 - Mobilgeräte 69
 - Telearbeit 69
- Organisationszertifizierung 145
- P**
- PDCA 24, 29
- PDCA-Methodik 17, 23
- Peoplecert 151
- Personalsicherheit 70
- Änderung der Beschäftigung 73
 - Beendigung der Beschäftigung 73
 - Vor der Beschäftigung 71
 - Während der Beschäftigung 72
- Personenzertifizierung 145, 149
- Physische Sicherheit 88
- Sicherheit von Betriebsmitteln 90
 - Sicherheitsbereiche 88
- PKI *siehe* Public-Key-Infrastructure
- Plan 40
- Plan-Phase 24, 29, 40
- Planung 24, 40
- Politik 38, 169
- Privilegierte Rechte 85
- Privilegierte Zugangsrechte 82
- Protokollierung 98
- Prozess 18, 22, 169
- Prozessmanagement 23
- Prozessorientierung 22
- Public-Key-Infrastructure 87
- Q**
- Qualifizierungsprogramm 150
- Qualitätsmanagement 23
- R**
- Rahmenwerk 131
- Rechtsprechung 20
- Redundanz 121
- Registrierung und Deregistrierung von Benutzern 81
- Reliability 5
- RESILIA 139
- Ressourcen 24, 46
- Restrisiko 169
- Rezertifizierung 149
- Richtlinie 18, 65
- themenspezifisch 66
- Risiko 170
- Absprachen 171
 - Akzeptanz 43, 170
 - Analyse 43, 171
 - Behandlung 43, 173
 - Beurteilung 42, 43, 51, 171
 - Bewertung 43, 172
 - Eigentümer 172
 - Identifizierung 172
 - Kommunikation 171
 - Kriterien 171
 - Management 14, 75
- Risikomanagement 42, 74, 137, 172
- Prozess 172
- Risikoniveau 165
- Rollen 20, 21
- Rückgabe von organisationseigenen Werten 75
- Rückverfolgbarkeit 19
- S**
- Schadsoftware 96
- Schulung 153
- Schutzniveau 21
- Schutzziel 3
- Schwachstellen 100, 117, 175
- Schwachstellenmanagement 100
- Scope *siehe* Anwendungsbereich
- Scoping 10, 145
- Scoping statement 145
- Security Information & Event Management 98
- Sichere Anmeldeverfahren 84
- Sicherheit
- Betriebsmittel 90
 - Physische und umgebungsbezogene 88
 - Umgebungsbezogene 88
- Sicherheitsanforderung 3
- Sicherheitsbereiche 88
- Sicherheitsrichtlinie *siehe* Informationssicherheitsrichtlinie
- Sicherheitsvorfälle 116
- Sicherheitsziele 45
- Sicherung 97

SIEM *siehe* Security Information & Event Management
 Skala 173
 Software 99
 Stakeholder 174
 Standard 10
 – Informativer 10
 – Normativer 10
 Standardfamilie 9
 Standardisierung 9
 Statement of applicability 145
 Steuerung 162
 Steuerungsebene 19
 Steuerungsgremium 162
 Support 46
 System zur Verwaltung von Kennwörtern 84
 Systemabnahmetest 111

T

TÜV Süd 150
 Telearbeit 69
 Terminologie 10
 Testdaten 111
 Testen 110

U

Überblicksdokument 10
 Überprüfung 25, 52, 115, 169
 – Ziel der 170
 Überprüfung von Benutzerzugangsrechten 82
 Übertragung von Informationen 104
 Überwachung 52, 98, 115, 167
 Überwachungsaudit 149
 Uhrensynchronisation 99
 Umgebungsbezogene Sicherheit *siehe*
 Physische Sicherheit
 Umsetzung 25, 46, 50
 Unterstützungsprozess 108
 Urheberrecht 123

V

Validierung 174
 Verantwortlichkeit 20, 39, 66
 Verantwortung 67, 72, 74
 – von Benutzern 83
 Verbesserung 26, 57, 159
 Verbesserungsmaßnahmen 26
 Verbindlichkeit 5
 Verfahren 18
 Verfahrensanweisung 19
 Verfügbarkeit 4, 158
 Verifizierung 175

Verlässlichkeit 5, 169
 Verschlüsselung 92
 Vertrauenswürdige Einheit 174
 Vertraulichkeit 3, 159
 Verwaltung
 – geheimer Authentisierungsinformation von Benutzern 82
 – privilegierter Zugangsrechte 82
 – von Kennwörtern 84
 Verwaltung der Werte 74
 – Datenträger 77
 – Entsorgung von Datenträgern 78
 – Handhabung von Werten 77
 – Informationsklassifizierung 76
 – Inventar 75
 – Kennzeichnung von Information 76
 – Klassifizierung von Information 76
 – Rückgabe von Werten 75
 – Verantwortung 74
 – Wechseldatenträger 77
 – Zulässiger Gebrauch 75
 – Zuständigkeit 75
 Verwaltung geheimer Authentisierungsinformation von Benutzern 82
 Verwaltung privilegierter Zugangsrechte 82
 Verwandte Standards 131
 – Auditierung 135
 – Governance 138
 – IT- und Informationssicherheit 131
 – Management der IT 138
 – Qualitätsmanagement 137
 – Risikomanagement 137
 – Zertifizierung 135
 Verwertungsrecht 123
 Vorgaben 65
 Vorstand 20

W

Wahrscheinlichkeit 166
 Wechseldatenträger 77
 Wert 18, 74
 – Handhabung 77
 – Inventar 75
 – Kennzeichnung 76
 – Klassifizierung 76
 – Management 74
 – Rückgabe 75
 – Verantwortung 74
 – Zulässiger Gebrauch 75
 – Zuständigkeit 75
 Wiederholungsaudit 149

Wirksamkeit 161
Wirkungsgrad 26

Z

Zeitpunkte 24
Zertifikat 149
Zertifizierung 145
– Ablauf 147
– Akkreditierung 146
– Organisationszertifizierung 145
– Personenzertifizierung 145, 149
– Rezertifizierung 149
Zertifizierungsaudit 12, 147
Zertifizierungsprüfung 210
Zertifizierungsstelle 12, 147
Ziel 168
Zugang 80
Zugang zu Netzwerken und Netzwerkdiensten 81
Zugangssteuerung 80, 157
– Überprüfung von Benutzerzugangsrechten 82
– Benutzerverantwortlichkeiten 83
– Benutzerzugangsverwaltung 81
– Gebrauch von Hilfsprogrammen mit privilegierten Rechten 85
– Geschäftsanforderungen 80
– Informationszugangsbeschränkung 84
– Quellcode von Programmen 85
– Registrierung und Deregistrierung von Benutzern 81
– Sichere Anmeldeverfahren 84
– System zur Verwaltung von Kennwörtern 84
– Systeme und Anwendungen 83
– Verwaltung geheimer Authentisierungsinformation von Benutzern 82
– Verwaltung privilegierter Zugangsrechte 82
– Zugang zu Informationen 80
– Zugang zu Netzwerken und Netzwerkdiensten 81
– Zugangssteuerungsrichtlinie 80
– Zuteilung von Benutzerzugängen 82
Zugangssteuerungsrichtlinie 80
Zugriff 80
Zugriffskontrolle 5
Zugriffssteuerung 5
Zulässiger Gebrauch von Werten 75
Zurechenbarkeit 5
Zuständigkeit
– organisationseigener Werte 75
Zuteilung von Benutzerzugängen 82
Zutritt 80
Zuweisung
– Rollen 20