

Edition <kes>

Heinrich Kersten
Gerhard Klett
Jürgen Reuter
Klaus-Werner Schröder

IT-Sicherheits- management nach der neuen ISO 27001

ISMS · Risiken · Kennziffern · Controls

2. Auflage

<kes>

 Springer Vieweg

Edition <kes>

Mit der allgegenwärtigen IT ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Die <kes> – Zeitschrift für Informations-Sicherheit – wird von der DATAKONTEXT GmbH im zweimonatigen Rhythmus veröffentlicht und behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz. Nähere Informationen rund um die Fachzeitschrift finden Sie unter www.kes.info.

Die Autoren der Zeitschrift und der Buchreihe Edition <kes> helfen den Anwendern in Basic- und Expert-Seminaren bei einer praxisnahen Umsetzung der Informations-Sicherheit: www.itsecuritycircles.de

Weitere Bände in dieser Reihe <http://www.springer.com/series/12374>

Heinrich Kersten • Gerhard Klett
Jürgen Reuter • Klaus-Werner Schröder

IT-Sicherheitsmanagement nach der neuen ISO 27001

ISMS • Risiken • Kennziffern • Controls

2., Aktualisierte Auflage

Heinrich Kersten
CE-Consulting
Meckenheim, Deutschland

Gerhard Klett
GK IT-Security Consulting
Battenberg, Deutschland

Jürgen Reuter
Technologiezentrum Rhein-Main
Darmstadt, Deutschland

Klaus-Werner Schröder
IT-Sicherheitsberatung
Remagen, Deutschland

DIN-Normen wiedergegeben mit Erlaubnis von DIN Deutsches Institut für Normung e. V. Maßgebend für das Anwenden der DIN-Norm ist deren Fassung mit dem neuesten Ausgabedatum, die bei der Beuth Verlag GmbH, Am DIN Platz, Burggrafenstraße 6, 10787 Berlin, erhältlich ist.

ISSN 2522-0551

ISSN 2522-056X (electronic)

Edition <kes>

ISBN 978-3-658-27691-1

ISBN 978-3-658-27692-8 (eBook)

<https://doi.org/10.1007/978-3-658-27692-8>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2016, 2020

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Dieses Buch behandelt das Management der Informationssicherheit auf der Basis der aktuellen Fassung¹ der Norm ISO/IEC 27001. Alle seit der ersten Auflage erfolgten Änderungen an dieser Norm und anderen Vorgabewerken wurden in dieser zweiten Auflage des Buches berücksichtigt.

Auch wenn der Titel nur die ISO 27001 nennt, muss zunächst festgestellt werden, dass es im Grunde um eine ganze Normenreihe geht, die als ISO/IEC 27000 bekannt und deren durchgängiges Thema die Informationssicherheit ist: die Sicherheit (bei) der Informationsverarbeitung in Organisationen.

Die ISO 27001 ist der zentrale Part dieser Reihe, weil hierin die Vorgaben für ein ISMS² dargestellt sind. Sie ist somit allen weiteren Normen dieser Reihe quasi übergeordnet. Die Reihe selbst beinhaltet eine Sammlung themenspezifischer bzw. branchenspezifischer Normen und ist sehr umfassend angelegt, allerdings erst zum Teil realisiert und publiziert.

Die ISO 27001 geht auf einen älteren britischen Standard (BS7799:1995) zurück und erschien erstmalig 2005 in englischer Sprache (deutsche Fassung 2008), sodann 2013 in neuer, überarbeiteter Fassung. Im März 2015 wurde diese Fassung auch in deutscher Sprache herausgegeben. Im Oktober 2014 und im Dezember 2015 erschienen zwei technische Korrekturen,³ die Anlass für eine Neufassung 2017-06 der ISO 27001 und ISO 27002 in deutscher Sprache waren.

In die jeweiligen Überarbeitungen gingen vor allem Erfahrungen aus der Anwendungspraxis sowie mit vielen zwischenzeitlich stattgefundenen Audits ein. Manches wurde vereinfacht – andere sagen verwässert – vieles neu geordnet, einige Dinge erschienen erstmalig oder wurden stärker herausgestellt.

Vor diesem Hintergrund kann die Community inzwischen auf eine fast 25-jährige Erfahrung mit standardisierten Sicherheitsmanagement-Systemen zurückblicken.

Zwar kann sich die ISO 27001 nicht mit der weltweit erfolgreichsten Management-Norm ISO 9001 messen, jedoch hat sie ebenfalls eine hohe internationale Akzeptanz

¹ Stand: September 2019.

² Informationssicherheits-Managementsystem.

³ In Kap. 1 sind weitere Daten zum Versionsverlauf des Standards angegeben.

erreicht. Dies lässt sich daran erkennen, dass sie national und international in Ausschreibungsunterlagen und Sicherheitskatalogen Eingang gefunden hat und inzwischen ca. 40.000 Organisationen weltweit nach dieser Norm zertifiziert sind – mit stetig steigender Tendenz.⁴

So positiv eine Norm zu bewerten ist, die sich an neue Erkenntnisse und dem Fortschreiten der Informationstechnologie (IT) anpasst: Die Anwender bzw. Nutzer sehen Neufassungen immer skeptisch, weil dies in den allermeisten Fällen mit neuem Aufwand verbunden ist – sei es, dass neue Sicherheitsmaßnahmen gefordert, methodische Ansätze stärker reglementiert, oder auch „nur“ dokumentative Anpassungen des eigenen Management-Systems erforderlich werden.

Um es vorwegzunehmen: Wer sich bisher nach der Normfassung von 2005/2008 gerichtet hat, wird an seiner Dokumentation zahlreiche Anpassungen vornehmen, einige neue Controls (Sicherheitsanforderungen) umsetzen und einige Management-Aspekte stärker als bisher berücksichtigen müssen. Die letzte Normanpassung (deutsch 2017-06) erfordert dagegen nur geringen Aufwand bei der Umsetzung.

Im vorliegenden Buch wird der Hauptteil der ISO 27001 – die Beschreibung des ISMS – in Kap. 2 eingehend kommentiert und an Beispielen erläutert. Daran schließt sich die Darstellung besonderer Management-Verfahren an: Risikobeurteilung und -behandlung (Kap. 3), das Messen von Sicherheitskennzahlen (Kap. 4) und das Management interner und externer Audits (Kap. 5).

Das umfangreiche Kap. 6 kommentiert detailliert alle 114 Controls aus dem Anhang A der Norm und gibt Hinweise und Beispiele für die Umsetzung.

Eine Herausforderung stellt für viele Organisationen die Einbeziehung von mobilen IT-Systemen in ihre IT-Infrastruktur dar. In Kap. 7 erläutern wir deshalb, welche Anpassungen diesbezüglich an einem ISMS vorzunehmen sind und wie sich das auf Leit- und Richtlinien sowie Sicherheits- und Notfallkonzepte auswirken kann. Dieser „Abstieg“ zur Praxis macht viele der abstrakten Norminhalte verständlicher.

Im Kap. 8 erläutern wir eine Art Fahrplan für Organisationen, die sich an älteren Normfassungen orientiert haben und sich nun nach der aktuellen Fassung ausrichten wollen oder sogar müssen: Wie kann man die notwendigen Anpassungen des ISMS effektiv angehen?

Da in Organisationen nicht nur das Sicherheitsthema, sondern viele andere Themen (z. B. IT-Prozesse, Qualität, Umweltschutz, Compliance) zu managen sind, behandeln wir in Kap. 9, wie die Integration der Informationssicherheit bzw. eines ISMS in ein übergeordnetes internes Kontrollsystem (IKS) zu bewerkstelligen ist.

Ein weiteres aktuelles – wenn auch nicht für alle Organisationen relevantes – Thema ist in Deutschland das IT-Sicherheitsgesetz (2015). Es fordert für den Bereich kritischer Infrastrukturen, dass dort nachweislich eine der Bedeutung dieses Bereichs angemessene Informationssicherheit realisiert werden muss. Dabei sind regelmäßige Audits, z. B. auf der Basis der ISO 27001 bzw. des BSI-Grundschutzes, vom Gesetz vorgeschrieben. Je nach Branche bzw. Sektor kann auch eine Zertifizierung nach den genannten Standards

⁴Zahlen gemäß der offiziellen Statistik der ISO, letzter verfügbarer Stand 31.12.2017.

verpflichtend sein. Vor diesem Hintergrund erläutern wir in Abschn. 10.1 die Auswirkungen des Gesetzes auf die Anwendung der ISO 27001.

Mit Inkrafttreten der Datenschutz-Grundverordnung in der EU am 25. Mai 2018 sind auch bei der Verarbeitung personenbezogener Daten Anforderungen an die Informationssicherheit gestellt worden, die es bei der Umsetzung der ISO 27001 zu berücksichtigen gilt. Hierzu geben wir einige Informationen im Abschn. 10.2.

Das vorliegende Buch in der 2. Auflage soll zum Verständnis der aktuellen ISO 27001 beitragen und bei deren Umsetzung in der betrieblichen Praxis unterstützen. Es ist gleichzeitig eine Fortschreibung des älteren, bisher in vier Auflagen erschienenen Werkes „IT-Sicherheitsmanagement nach ISO 27001 und IT-Grundschutz“ im gleichen Verlag.

Die Autoren bedanken sich herzlich für die Unterstützung durch Frau Dr. Kathke und das Lektorat bei Springer Vieweg.

Meckenheim, Deutschland
Battenberg, Deutschland
Darmstadt, Deutschland
Remagen, Deutschland
September 2019

Heinrich Kersten
Gerhard Klett
Jürgen Reuter
Klaus-Werner Schröder

Inhaltsverzeichnis

1 Einführung	1
1.1 Historie und Informationen	1
1.2 Die Normenreihe	3
1.3 Das ISMS	5
1.4 Der Anhang A	12
1.5 ISMS und Auslagerung	14
1.6 Checkliste	15
Literatur	16
2 Die Anforderungen an ein ISMS	17
2.1 Kontext der Organisation (NK 4)	17
2.2 Führung (NK 5)	20
2.3 Planung (NK 6)	22
2.4 Unterstützung (NK 7)	27
2.5 Betrieb (NK 8)	31
2.6 Bewertung der Leistung (NK 9)	32
2.7 Verbesserung (NK 10)	36
2.8 Checkliste	37
Literatur	38
3 Risikomanagement	39
3.1 Risikomanagement als Aufgabe	39
3.2 Verfahren der Risikobeurteilung	47
3.2.1 IT-Grundschutz und Erweiterung	48
3.2.2 Ein Beispiel aus ISO 27005	51
3.2.3 Die Scorecard-Methode	52
3.2.4 Angriffspotenzial nach ISO 15408	60
Literatur	62

4	Sicherheit messen	63
4.1	Ziele	63
4.2	Überwachen und Messen	64
4.3	Messungen bewerten	73
	Literatur	74
5	Interne und externe Audits	75
5.1	Ziele und Nutzen	76
5.2	Die Rahmenbedingungen	80
5.3	Vorbereiten eines Audits	90
5.4	Durchführung eines Audits	93
5.5	Typische Defizite	96
5.6	Auditbericht und Auswertung	100
	Literatur	101
6	Die Controls im Anhang A	103
6.1	Überblick	103
6.2	Die einzelnen Controls	105
6.2.1	Informationssicherheitsrichtlinien (A.5)	105
6.2.2	Organisation der Informationssicherheit (A.6)	108
6.2.3	Personalsicherheit (A.7)	115
6.2.4	Verwaltung der Werte (A.8)	120
6.2.5	Zugangsteuerung (A.9)	128
6.2.6	Kryptografie (A.10)	141
6.2.7	Physische und umgebungsbezogene Sicherheit (A.11)	144
6.2.8	Betriebssicherheit (A.12)	156
6.2.9	Kommunikationssicherheit (A.13)	169
6.2.10	Anschaffung, Entwicklung und Instandhalten von Systemen (A.14)	177
6.2.11	Lieferantenbeziehungen (A.15)	191
6.2.12	Handhabung von Informationssicherheitsvorfällen (A.16)	196
6.2.13	Informationssicherheitsaspekte beim Business Continuity Management (A.17)	201
6.2.14	Compliance (A.18)	208
	Literatur	216
7	ISMS und mobile Infrastrukturen	217
7.1	Übersicht	217
7.2	Mobile Infrastrukturen in Unternehmen	218
7.3	ISMS und Mobile Device Management	219
7.4	Sicherheitsleitlinie	221

7.5	Sicherheitsrichtlinie	222
7.6	BCM und Notfallmanagement	228
	Literatur	229
8	Umsteigen von älteren Normfassungen auf die aktuelle Norm	231
8.1	Von 2008 nach 2015	231
8.1.1	Vorüberlegungen	231
8.1.2	Hauptteil der ISO 27001	234
8.1.3	Anhang A der Norm	237
8.1.4	Weitere Dokumente und Pläne	239
8.1.5	Checkliste	240
8.2	Von 2015 nach 2017	241
8.3	Neue Entwicklungen	242
	Literatur	242
9	Interne Kontrollsysteme	245
9.1	Problemstellung	245
9.2	Beispiele	250
9.3	Handlungsempfehlung	252
	Literatur	253
10	ISMS: Auswirkungen aktueller gesetzlicher Vorgaben	255
10.1	Das IT-Sicherheitsgesetz	255
10.2	Die Datenschutz-Grundverordnung	259
10.2.1	Einbeziehung des Datenschutzes in ein ISMS	259
10.2.2	Datenschutz-Folgenabschätzung	262
	Literatur	262
	Fachbegriffe englisch/deutsch	265
	Stichwortverzeichnis	267

Verwendete Abkürzungen

ACL	Access Control List
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analysis (Geschäftsauswirkungsanalyse)
BS	British Standard
bsi	British Standards Institution
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device (Policy für das MDM)
CBT	Computer Based Training
CC	Common Criteria
CERT	Computer Emergency Response Team
CI	Configuration Item
CMDB	Configuration Management Data Base
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DAC	Discretionary Access Control
DIN	Deutsche Institut für Normung e.V.
DLP	Data Leakage/Loss Prevention/Protection
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung der EU
EDI	Electronic Data Interchange
EN	European Norm
EnWG	Energiewirtschaftsgesetz
EVU	Energieversorgungs-Unternehmen
ID	Identifikation(sname)
IDS	Intrusion Detection System
IKS	internes Kontrollsystem
IPS	Intrusion Prevention System
ISAE	International Standard on Assurance Engagements
ISF	Information Security Forum
ISM	Information Security Management
ISMS	Information Security Management System

ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches ...
IT-SG	IT-Sicherheitsgesetz
KMU	kleines, mittelständisches Unternehmen
LAN	Local Area Network
MAC	Mandatory Access Control
MDM	Mobile Device Management
MTPD	Maximum Tolerable Period of Disruption
NA	Normabschnitt
NDA	Non Disclosure Agreement
NK	Normkapitel
NSTAC	National Security Telecommunications Advisory Committee
NTP	Network Time Protocol
PAN	Payment Account Number
PCI-DSS	Payment Card Industry Data Security Standard
PCMCIA	PC Memory Card International Association
PDCA	Plan-Do-Check-Act
PIN	Personal Identification Number
PTB	Physikalisch-Technische Bundesanstalt
QM	Quality Management
RBAC	Role Based Access Control
RZ	Rechenzentrum
SDM	Standard-Datenschutzmodell
SLA	Service Level Agreement
SoA	Statement of Applicability
SOX	Sarbanes-Oxley Act
SSL	Secure Socket Layer
TK	Telekommunikation(s-)
USB	Universal Serial Bus
USV	unterbrechungsfreie Stromversorgung
WBT	Web-based Training
WLAN	Wireless LAN (Local Area Network)
ZDA	Zertifizierungsdiensteanbieter



- ▶ **Zusammenfassung** In diesem einführenden Kapitel wollen wir einen ersten Überblick über die ISO 27001 geben, einige Begriffe erläutern und mit einer ersten Checkliste für vorbereitende Aktivitäten schließen.

Zunächst ein wichtiger Hinweis: Im Folgenden werden wir häufig von *Sicherheit* sprechen und meinen damit die Informationssicherheit oder nach älterem Sprachgebrauch die IT-Sicherheit. Wenn keine Missverständnisse zu befürchten sind, lassen wir die Vorsilben „Informations-“ oder „IT-“ weg, um die Lesbarkeit zu verbessern.

Weiterhin: Mit *Organisation* bezeichnen wir Behörden, Unternehmen, Vereine, NGOs etc. Wenn wir den internen Aufbau einer Organisation und die internen Abläufe meinen, sprechen wir von *Aufbau- und Ablauforganisation*.

1.1 Historie und Informationen

Auch heute noch kann man in der ISO 27001 [1] und der ISO 27002 [2] vieles erkennen, das auf den älteren, zweiteiligen British Standard BS 7799 [3, 4] zurückgeht. Dieser nationale Standard wurde von der British Standards Institution (bsi)¹ herausgegeben und durch viele Guidelines ergänzt. Diese britische Fachbehörde – ein Key Player in diesem Kontext – ist auch in Deutschland vertreten und bietet unter www.bsigroup.com/de-DE/ deutschsprachige Seiten an, z. B. mit Informationen zur ISO 27001.

¹Nicht zu verwechseln mit dem deutschen BSI = Bundesamt für Sicherheit in der Informationstechnik.

Abb. 1.1 Normenreihe ISO/
IEC 27000: Basisnormen



Das britische bsi ist gleichzeitig eine international anerkannte Zertifizierungsstelle für ISO 27001 und damit eine der Stellen, die befugt sind, Auditoren zu qualifizieren und einzusetzen, um die Übereinstimmung einer Organisation mit der ISO 27001 im Rahmen einer Zertifizierung zu überprüfen.

Es sei an dieser Stelle schon erwähnt, dass in vielen Ländern nationale Strukturen mit Zertifizierungsstellen und lizenzierten Auditoren aufgebaut worden sind;² weiterhin existieren internationale Anerkennungsverträge, durch die in einem Land erteilte Zertifikate auch in anderen Vertragsländern anzuerkennen sind.³ Genauere Informationen hierzu erhält man unter www.iso.org und www.iaf.nu.

Wer nähere Informationen, Interpretationen, Whitepapers und andere Hilfsmittel zur ISO 27000-Reihe sucht, ist bei www.iso27001security.com gut aufgehoben – allerdings liegen die Informationen überwiegend nur in englischer Sprache vor.

²Siehe für Deutschland: www.dakks.de, Services/Datenbank, Suchmaske „Managementsysteme 2“.

³Nicht hierunter fallen Zertifizierungen durch das deutsche BSI nach dem Grundschatz-Standard. Auch wenn die Zertifikate als „ISO 27001-Zertifikat auf der Basis von IT-Grundschatz“ bezeichnet werden, sind sie in dem zuvor geschilderten Sinne nicht international anerkannt und werden auch nicht in der ISO-Statistik berücksichtigt.

27010 Inter-Sektor-/ Inter- Org-Kommunikation	27011 Telekommunikation	27013 ISMS & ITIL	27017 Cloud Security
27018 Datenschutz in Clouds	27019 Prozesssteuerung Energiesektor	27021 Kompetenzen ISMS- Personal	27031 Business Continuity
27032 Cybersecurity	27033 Network Security	27034 Application Security	27035 Incident Management
27036 Supplier Security	27039 Intrusion Prevention	27040 Storage Security	27799 Gesundheitswesen

Abb. 1.2 Normenreihe ISO/IEC 27000: Sektor-/branchenspezifische Normen

1.2 Die Normenreihe

Die Normenreihe ISO 27000 ist sehr umfangreich und wird ständig weiter ausgebaut. In der Abb. 1.1 sieht man die Hauptnorm 27001 und die unterstützenden Normen 27002 bis 27008, die bestimmte Aspekte der Hauptnorm vertiefen. Die in der Abb. 1.1 fehlende Norm 27006 richtet sich (nur) an Zertifizierungsstellen.

Daneben gibt es eine umfangreiche Sammlung von Normen zu branchen- bzw. sektorspezifischen Aspekten sowie zu anderen Sicherheitsthemen. Die Abb. 1.2 gibt dazu einige Beispiele (Titel der Normen nur verkürzt wiedergegeben).

Die ISO 27001

Die zentrale Norm ISO 27001 besteht aus einem Hauptteil und einem umfangreichen Anhang A. Werfen wir zunächst einen Blick auf das Inhaltsverzeichnis des Hauptteils der (deutschen) ISO 27001 (vgl. Tab. 1.1).

Nach der thematischen Einführung (Kap. 0) und der Beschreibung des Einsatzgebietes der Norm (Kap. 1) wird auf die Basisnorm ISO 27000 dieser Reihe verwiesen (Kap. 2, 3), die das gesammelte Begriffskompodium für die Normenreihe enthält – übrigens die einzige Norm dieser Reihe, die kostenfrei⁴ zum Download zur Verfügung steht.

⁴In englischer Sprache.

Tab. 1.1 Kapitelübersicht der ISO 27001

Kap. 0	Einführung
Kap. 1	Anwendungsbereich
Kap. 2	Normative Verweise
Kap. 3	Begriffe
Kap. 4	Kontext der Organisation
Kap. 5	Führung
Kap. 6	Planung
Kap. 7	Unterstützung
Kap. 8	Betrieb
Kap. 9	Bewertung der Leistung
Kap. 10	Verbesserung

- **Tipp** Besorgen Sie sich die ISO 27000 und gehen Sie die dort verzeichneten Begriffe durch: Testen Sie, ob Ihr Begriffsverständnis zumindest grob mit der Norm übereinstimmt!

In den Kap. 4 bis 10 der ISO 27001 werden die Anforderungen an das Management der Informationssicherheit festgelegt. Diese Anforderungen sind jedoch so allgemein gehalten, dass man eher von einer Meta-Methode sprechen sollte, d. h. es handelt sich weder um ein direkt umsetzbares Arbeitsprogramm mit dem Ziel, Informationssicherheit herzustellen, noch sind die Methoden dafür festgeschrieben – sie sind vielmehr weitgehend durch den Anwender wählbar.

Dann überrascht auch nicht mehr die Tatsache, dass im Hauptteil der Norm weder konkrete technische noch andere Sicherheitsmaßnahmen im engeren Sinne aufgeführt sind.

Dieses abstrakte Vorgehen in der ISO 27001 lässt den Inhalt zunächst etwas spröde und sperrig erscheinen, jedenfalls hat man sich so weit von der Praxis gelöst, dass man mit Fug und Recht behaupten kann, die ISO 27001 sei

- anwendbar auf jede Art von Organisation (Behörden, Unternehmen, Vereine, NGOs etc.),
- beliebig skalierbar, d. h. auf kleinste bis auf allergrößte Organisationen (was erfahrungsgemäß auch stimmt!) und
- in jedem Land und länderübergreifend anwendbar.

Der letzte Punkt wird dadurch unterstützt, dass die Norm auf keine spezifischen nationalen Eigenheiten – etwa bestimmte Gesetze oder Mentalitäten – eingeht, sondern lediglich Aspekte behandelt, die in jedem Land eine gewisse Entsprechung finden, z. B. den Schutz des intellektuellen Eigentums oder personenbezogener Daten. Hierbei darf man keine Tiefe erwarten, vielmehr läuft es meist auf die Forderung nach der Erfüllung der jeweiligen nationalen Gesetze hinaus.

Diesen Punkt muss man in Betracht ziehen, wenn es z. B. darum geht, eine nach ISO 27001 zertifizierte Organisation aus einem anderen Land als Dienstleister einzusetzen. Ob ein solcher Dienstleister beispielsweise die deutschen Datenschutzbestimmungen (BDSG [6]) bzw. die Datenschutz-Grundverordnung der EU [7] erfüllt, erschließt sich **nicht** aus der Tatsache, dass der Dienstleister nach ISO 27001 zertifiziert ist und somit das entsprechende Datenschutz-Control⁵ A.18.1.4 umgesetzt haben müsste. Letzteres besagt bestenfalls, dass die Organisation in *ihrem* Land die dort geltenden Bestimmungen erfüllt.

1.3 Das ISMS

Die Kap. 4 bis 10 der ISO 27001 beschreiben Anforderungen an ein System zum Management der Informationssicherheit, kurz: ISMS = Informations-Sicherheits-Management-System. Was ist mit *System* gemeint? Ist das gleichbedeutend mit dem Prozess des Sicherheitsmanagements?

Als Management-System für ein Thema X bezeichnet man allgemein alles, was eingesetzt wird, um die wesentlichen Ziele für das Thema X zu ermitteln, diese Ziele zu erreichen und ihre Aufrechterhaltung zu überwachen. Was setzt man dazu alles ein? Typisch ist,

- Ziele in Form von Leitlinien zu formulieren,
- Risiken und Chancen für diese Ziele zu analysieren,
- Rollen bzw. Verantwortlichkeiten für bestimmte (Teil-)Ziele zu definieren,
- Methoden oder Verfahren zu deren Erreichung zu vermitteln,
- den vom Thema X Betroffenen besondere Regelwerke oder Richtlinien aufzugeben,
- Prozesse bzw. Abläufe und dafür erforderliche Maßnahmen zu planen und umzusetzen,
- Überprüfungen der Zielerreichung zu planen, durchzuführen und auszuwerten.

Für eine Organisation ist das Thema „X = Informationssicherheit“ Teil ihres gesamten Management-Systems, das sich möglicherweise auch um andere Themen wie Qualität, Umweltschutz, Compliance kümmern muss (vgl. Kap. 9). Dies wird natürlich erleichtert, wenn für alle Themen gleichartige Management-Systeme zum Einsatz kommen. Genau das ist das Ziel der aktuellen Management-Normen der ISO. Diese Vereinheitlichung führt zu Aufwands- und Kosteneinsparung und erhöht die Akzeptanz bei allen Betroffenen.

- ▶ **Tip** Ist in Ihrer Organisation bereits ein anderes Management-System vorhanden – z. B. gemäß ISO 9001 [5] –, dann können Sie dessen „Architektur“ auch für die ISO 27001 übernehmen.

⁵Aus dem Anhang A der Norm.

Vor diesem Hintergrund können wir schon an dieser Stelle ein typisches Missverständnis ausräumen und unsere Eingangsfragen beantworten: ISMS ist nicht eine Abkürzung für die Rolle *IT-Sicherheitsbeauftragte(r)* oder die Organisationseinheit *IT-Sicherheitsmanagement* oder den entsprechenden Prozess des IT-Sicherheitsmanagements! Diese Rolle bzw. Funktion und auch der Prozess sind lediglich Teile des ISMS, wie ein Blick auf die zuvor aufgezählten Punkte zeigt.

Der Anwendungsbereich⁶ eines ISMS ist meist die gesamte Organisation. Es kommt aber auch vor, dass das ISMS beschränkt wird auf bestimmte Standorte, Geschäftsprozesse, Abteilungen etc. – was durchaus zulässig ist. Die Idee, hierdurch Aufwand einzusparen, hat sich aber in der Praxis als nicht sehr effektiv herausgestellt.

Wichtige Aufgaben eines ISMS sind:

- die Formulierung von (Sicherheits-)Zielen
- die Bestimmung der Assets
- die Risikobeurteilung
- die Risikobehandlung
- die kontinuierliche Verbesserung

Wir erläutern diese Aufgaben in den folgenden Abschnitten.

Sicherheitsziele

Sicherheitsziele werden in der Norm nur beispielhaft aufgezählt und sind meist mit den Begriffen Vertraulichkeit, Integrität und Verfügbarkeit verbunden.

- Die Vertraulichkeit von Informationen zu wahren meint, dass diese nur einem entsprechend autorisierten Personenkreis zur Kenntnis gelangen.
- Ähnlich meint die Wahrung der Integrität von Daten, dass nur autorisierte Änderungen vorgenommen werden dürfen.
- Bei der Verfügbarkeit geht es darum, dass Daten für autorisierte Zwecke ausreichend schnell zur Verfügung stehen müssen – genauer: Verzögerungen sind nur in akzeptablen Umfang zulässig.

Die Ziele der Integrität und Verfügbarkeit werden nicht nur für Daten, sondern analog auch für Systeme, IT-Anwendungen und Prozesse definiert.

Wer zur Kenntnisnahme oder Änderung autorisiert ist bzw. welche Verzögerung noch als akzeptabel angesehen wird, ist durch die jeweilige Organisation für ihre geschäftlichen Zwecke festzulegen. Möglicherweise existieren dazu auch Vorgaben in relevanten Gesetzen, Verträgen und anderen Standards.

Neben diesen drei klassischen Sicherheitszielen wird es bei Organisationen im Detail viele weitere Ziele geben. Im Zusammenhang mit dem Datenaustausch über Netzwerke

⁶Auch *Geltungsbereich* genannt, im Englischen: Scope.

werden beispielsweise die Authentizität von Absendern und des Datenursprungs, auch der Nachweis des Empfangs bzw. des Absendens von Daten gefordert.

Eine weitere Gruppe von Zielen stellen die Compliance-Ziele dar, bei denen es um die Einhaltung von Vorgaben gesetzlicher (z. B. BDSG) oder vertraglicher (z. B. SLAs) Art geht.

Jede Organisation ist frei, die für ihren geschäftlichen Kontext als relevant erachteten Ziele individuell festzulegen. Diese Ziele sind zu dokumentieren, was meist im Überblick in einer *Security Policy* erfolgt – im Deutschen meist als *Sicherheitsleitlinie* bezeichnet.⁷

Davon zu unterscheiden sind *Sicherheitsrichtlinien*, die ein spezielles Thema aus Sicht einer Zielgruppe behandeln: Als Beispiel sei eine Richtlinie für mobiles Arbeiten genannt, in der alle Grundsätze und Regeln für das Arbeiten mit Smartphone, Tablets & Co. für die Zielgruppe der Nutzer dargestellt werden.

Leitlinie

Wie sieht eine Leitlinie aus? Der Mindestumfang lässt sich durch die Übersicht in der Abb. 1.3 charakterisieren.

Im ersten Teil *Definition* wird die Organisation genannt, dann werden ihr organisatorischer Aufbau und ihre Standorte beschrieben.

Beim Geschäftszweck sollte die Geschäftstätigkeit der Organisation dargestellt werden; das könnte z. B. durch die Beschreibung der vorhandenen Geschäftsprozesse geschehen. Der Geschäftszweck kann dabei die gesamte Geschäftstätigkeit der Organisation umfassen, sich aber auch nur auf einzelne Teilbereiche beziehen. Im Ergebnis wird der

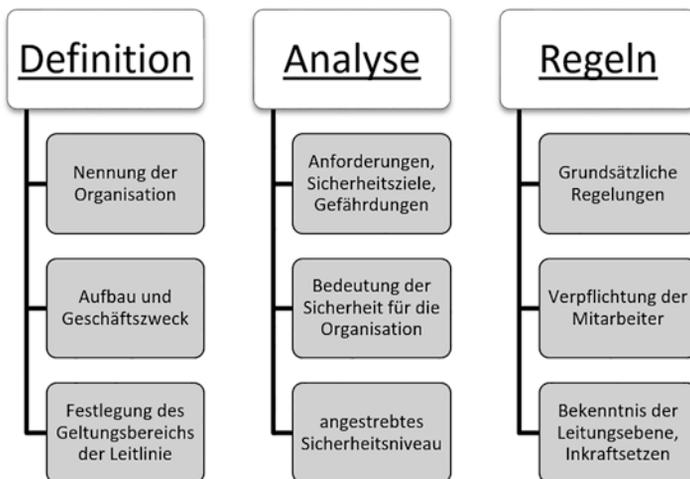


Abb. 1.3 Aufbau einer Sicherheitsleitlinie

⁷In der aktuellen deutschen Normfassung etwas unglücklich mit *Sicherheitspolitik* übersetzt.

Geltungsbereich der Leitlinie festgelegt. Im Grunde wird hier bereits die Entscheidung über den Anwendungsbereich des ISMS (den Scope) getroffen.

Unter *Analyse* werden die regulativen Anforderungen (Gesetze, Richtlinien, Konzernvorgaben, besondere Verträge) im Überblick dargestellt. Was die Sicherheitsziele anbetrifft, wird man in der Leitlinie keine detaillierte Darstellung wie in einem Sicherheitskonzept vorsehen – vielmehr geht es darum, Orientierung zu vermitteln. Hier können die Ziele der Vertraulichkeit, Integrität und Verfügbarkeit in Relation zu Kundendaten, personenbezogenen Daten, Projektdaten, Daten bestimmter Organisationsbereiche oder Anwendungen gesetzt werden. Hinzu kommen meist Anforderungen an die Verfügbarkeit von Systemen, Anwendungen und unterstützenden Einrichtungen. Daraus lassen sich sofort die relevanten Gefährdungen formulieren, indem man die Ziele sozusagen „negiert“: Aus dem Ziel der Vertraulichkeit von Kundendaten wird dann die Gefährdung *Verlust der Vertraulichkeit von Kundendaten*.

Bei den grundsätzlichen Regelungen geht es im Abschnitt *Regeln* um

- die Erläuterung der Sicherheitsorganisation (Rollen, Aufgaben, Ansprechpartner, auch eingerichtete Gremien) und
- zentrale Grundsätze und Verfahren der Sicherheit wie etwa das Eigentümer-Prinzip für Assets, mögliche Klassifikationsschemata für Daten,
- wichtige Richtlinien (z. B. für mobiles Arbeiten mit oder ohne BYOD), die Lenkung dokumentierter Informationen (insbesondere von Aufzeichnungen).

Das gilt natürlich nur insoweit, als die genannten Sachverhalte in der Organisation zur Anwendung kommen.

Die Leitlinie schließt meist mit der Verpflichtung der Mitarbeiter zur Einhaltung der Regeln sowie einem Bekenntnis der Leitung, die Sicherheit bzw. das ISMS aktiv zu unterstützen.

Assets

Unter *Assets* wird alles verstanden, was für eine Organisation einen Wert darstellt. Dies können zunächst Grundstücke, Gebäude, Maschinen und Anlagen, Geschäftsprozesse sein – aber natürlich auch die sogenannten *Information Assets* (Informationswerte) wie Informationen/Daten, Systeme, Anwendungen, IT Services. Ergänzend kann man auch Soft Assets betrachten wie das Image oder die Kreditwürdigkeit einer Organisation.

Eine Anforderung der Norm ist, dass alle für die Organisation relevanten Information Assets erfasst bzw. inventarisiert werden müssen – etwa in Form einer Tabelle oder einer Datenbank. Dabei werden üblicherweise neben der Bezeichnung eines Assets weitere Daten erfasst, z. B. Angaben zum (Speicher-, Lager- oder Stand-)Ort eines Assets, eine Klassifizierung des Wertes sowie der Asset Owner. Diese Person, Rolle oder Organisationseinheit ist für das jeweilige Asset verantwortlich und auch primärer Ansprechpartner für alle Sicherheitsaspekte, die mit diesem Asset verbunden sind. Meist obliegt dieser

Funktion auch die Kontrolle über die Risiken, denen ein Asset ausgesetzt ist. Gelegentlich findet man aber auch eine Aufteilung in *Asset Owner* und *Risk Owner*.

Bei der Vielzahl von Assets in der Praxis ist die Inventarisierung durchaus aufwendig. Eine Methode zur Begrenzung des Aufwands besteht darin, gleichartige Assets (z. B. bestimmte Server) gemeinsam als *ein* Asset zu betrachten. Diese Gruppe wird dann als *ein* Element in die Inventarliste aufgenommen. Diese Gruppierung ist immer dann möglich, wenn gleichartige Assets (vergleichbarer Wert, vergleichbare Risiken) vorliegen.

Eine andere Idee ist die Einführung einer Hierarchie: Betrachtet eine Organisation ihre Geschäftstätigkeit als eine Gruppe von Geschäftsprozessen, könnten diese als Top Level Assets gesehen werden. Alles, was für den Betrieb eines Geschäftsprozesses erforderlich ist (Personal, IT, Anlagen, Standorte etc.), wird diesem Geschäftsprozess als Ressourcen zugeordnet. Damit hat man ein Ordnungssystem – eine Hierarchie mit den Stufen „Top Level“ und „Ressourcen“ – eingeführt. Dies macht die Inventarisierung nicht nur übersichtlicher, es beinhaltet auch ein Vorgehensmodell, nämlich die einzelnen Geschäftsprozesse sequenziell oder parallel abzarbeiten, möglicherweise mit einer gewissen Priorisierung.

Die zuvor skizzierte Gruppierung kann sowohl bei den Top Level Assets wie auch bei den Ressourcen als zusätzliches Element genutzt werden.

Ein weiterer Punkt: An verschiedenen Stellen in der Organisation könnte es bereits Listen von Assets geben, auf die man zurückgreifen kann. Diese Situation liegt oft beim Asset Management (wenn existent), der Anlagenbuchhaltung oder bei der Einkaufsabteilung vor. Solche Listen zu nutzen hieße, nicht bei Null beginnen zu müssen ...

- Bevor Sie mit der Erfassung der Information Assets (nach der ISO-Norm) beginnen, sollten die Prozesse des Change Managements und des Configuration Managements aktiviert werden, d. h. jede Art von Änderungen im Detail bzw. an der Konfiguration komplexer Objekte muss formal beantragt und darf erst nach schriftlicher Genehmigung durchgeführt werden. Andernfalls werden die Daten über die Assets schnell „veralten“.

Risikobeurteilung

Jede Änderung des Zustands einer Informationsverarbeitung wird als *Ereignis* (Event) bezeichnet. Handelt es sich um ein Ereignis, das zumindest theoretisch Auswirkungen auf die Sicherheit haben könnte, spricht man von einem *Sicherheitsereignis* (Security Event). Auswirkungen auf die Sicherheit liegen immer dann vor, wenn Sicherheitsziele einer Organisation beeinträchtigt werden können.

Ein *Sicherheitsvorfall* (Security Incident) ist ein Ereignis, bei dem eine hohe Wahrscheinlichkeit für Auswirkungen auf die Sicherheit besteht. In der Norm wird sehr genau zwischen Events und Incidents unterschieden.

Ein (Sicherheits-)*Notfall* ist ein Sicherheitsvorfall mit gravierenden oder sogar katastrophalen Auswirkungen auf die Sicherheit.

In der Informationssicherheit wird der mögliche Eintritt von Sicherheitsereignissen als Risiko angesehen. Ein Risiko wird in aller Regel als eine Kombination aus Eintrittswahrscheinlichkeit und Schadenhöhe definiert. Sind Eintrittswahrscheinlichkeit und Schadenhöhe zahlenmäßig bestimmbar, wäre das Produkt beider Zahlen ein solche Kombination.

In der Praxis lassen sich Risiken meist *nicht* auf diese Weise berechnen, weil hinreichend genaue Zahlen fehlen: Man legt deshalb für Eintrittswahrscheinlichkeit und Schadenhöhe jeweils Stufen fest, und betrachtet Risikoklassen als Kombination solcher Stufen. Im Kap. 3 geben wir einige Beispiele für solche Methoden.

Ein Risiko kann immer dann eintreten, wenn Schwachstellen vorhanden sind, d. h. wenn Sicherheitsmaßnahmen fehlen, ungeeignet konstruiert oder fehlerhaft angewendet werden. Bei den letzten beiden Fällen spricht man von konstruktiven bzw. operativen Schwachstellen.

Bei der *Risikoidentifizierung* geht es um die Ermittlung (Erfassung und Benennung) von einzelnen Risiken für die Informationswerte der Organisation, soweit sie im Anwendungsbereich des ISMS liegen. Diese Ermittlung muss im Zusammenspiel mit den Verantwortlichen (Asset Owner bzw. Risk Owner) für die einzelnen Informationswerte geschehen.

In der *Risikoanalyse* werden für jedes Risiko Schadenhöhe und die Eintrittshäufigkeit abgeschätzt bzw. klassifiziert, das Risiko wird dementsprechend festgelegt – z. B. in eine Risikoklasse eingeordnet.

Bei der *Risikobewertung* geht es um die Feststellung, welche Auswirkungen ein Risiko auf die Organisation hat: Meist geschieht dies durch eine Bewertung der Risiken mit Stufen wie TOLERABEL, MITTEL, GRAVIEREND, KATASTROPHAL.

In der Norm wird *Risikobeurteilung* als Zusammenfassung der Teilaktivitäten Risikoidentifizierung, Risikoanalyse und Risikobewertung betrachtet.

Gelegentlich taucht in der Norm auch das Wort *Chancen* auf: Eine Chance besteht immer dann, wenn ein Ereignis mit einer gewissen Wahrscheinlichkeit einen Nutzen zur Folge haben kann.

Risikobehandlung

Zur Behandlung ermittelter Risiken dienen nach Vorgaben der Norm *Optionen* und *Sicherheitsmaßnahmen*.

Typische Optionen zur Risikobehandlung sind

- die Risikoakzeptanz – man übernimmt einfach das Risiko ohne weitere Maßnahmen,
- die Risikoverlagerung – z. B. durch Verlagerung der betroffenen Informationsverarbeitung an einen sichereren Ort, an einen qualifizierten Dienstleister, oder durch Versicherung der möglichen Schäden,
- die Risikoreduktion – durch Einsatz geeigneter Sicherheitsmaßnahmen,
- die Risikovermeidung – z. B. durch Änderung des fraglichen Geschäftsprozesses und der unterstützenden IT, oder durch Einstellung des risikoreichen Geschäftsprozesses.

Sicherheitsmaßnahmen können aus sehr unterschiedlichen Bereichen kommen: rechtliche, organisatorische, personelle, infrastrukturelle und IT-Maßnahmen.

Bevor man solche Maßnahmen festlegt, sollten zunächst die Risiken priorisiert werden: Die vernünftige Vorgehensweise besteht darin, zunächst die am höchsten bewerteten Risiken zu behandeln, dann die Risiken der zweithöchsten Bewertungsstufe usw. Die unterste Bewertungsstufe bedarf möglicherweise keiner besonderen Maßnahmen, weil man die entsprechenden Risiken einfach toleriert.

Eine weitere wichtige Aktivität besteht darin, bereits *vorhandene* Sicherheitsmaßnahmen zu ermitteln: Viele Organisationen fangen nicht bei Null an, sondern haben in der Vergangenheit schon Sicherheitsmaßnahmen eingerichtet, diese aber nicht systematisch erfasst und dokumentiert.

Somit steht die Aufgabe an, alle vorhandenen Maßnahmen zu erfassen, dann zu überprüfen, ob die betrachteten Risiken damit bereits ausreichend reduziert werden oder ob neue bzw. stärkere Maßnahmen erforderlich werden – ggf. auch, ob eine andere Option zur Risikobehandlung gewählt wird. Diese Vorgehensweise wird seitens der Norm durch den Anhang A und das damit zusammenhängende *Statement of Applicability* (SoA) unterstützt. Wir behandeln es beim Überblick über den Anhang A.

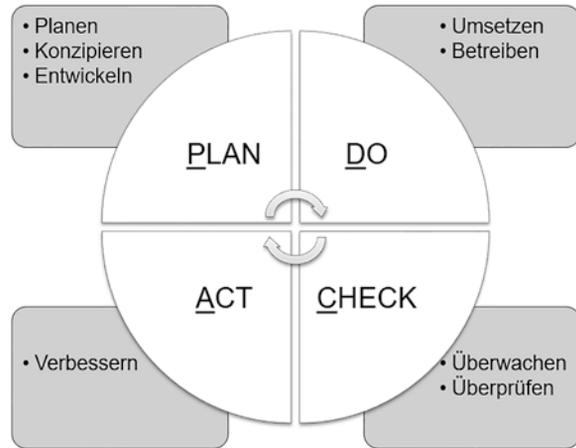
Wie schon zum Ausdruck kam, muss nach der Festlegung der Sicherheitsmaßnahmen der Prozess der Risikobeurteilung erneut durchlaufen werden: Es werden auf diese Weise die verbleibenden Risiken⁸ ermittelt und bewertet. Erst wenn eine ausreichende Reduktion vorliegt, wird man mit den vorhandenen und geplanten Maßnahmen „zufrieden“ sein. Man kann dies von Risiko zu Risiko einzeln entscheiden – oder einen allgemeinen Schwellenwert für die Akzeptanz verbleibender Risiken festlegen. Der Schwellenwert wird in unserem Kontext meist eine der festgelegten Bewertungsstufen sein: Risiken einer bestimmten Stufe (und aller Stufen darunter) werden als akzeptabel angesehen.

Kontinuierliche Verbesserung

Einen Prozess der kontinuierlichen Verbesserung in das ISMS einzubauen, hat vor allem drei Gründe:

- Ein funktionierendes ISMS ist ein komplexes System, das meist nur schrittweise realisiert wird. Erst nach einiger Zeit – durchaus manchmal erst nach einigen Jahren – wird das ISMS die „volle Leistung“ bringen. Bei jedem Schritt muss sich das ISMS verbessern.
- Im Laufe des Betriebs des ISMS, auch im Rahmen von Überwachungen und Audits, werden Unzulänglichkeiten, Fehler und Schwachstellen offenbar, so dass Änderungen, Reparaturen und Verbesserungen am ISMS erforderlich werden.

⁸ Statt von *verbleibenden Risiken* sprechen wir im Deutschen oft von *Restrisiken*, was nicht ganz übereinstimmt. Wir ignorieren hier jedoch die Unterschiede.

Abb. 1.4 PDCA-Modell

- Änderungen der Geschäftstätigkeit der Organisation oder des regulativen Umfelds haben fast immer Anpassungen und Ergänzungen beim ISMS zur Folge. Die Anpassung an neue Gegebenheiten ist ebenfalls als Verbesserung zu werten.

Die klassische Methode zur kontinuierlichen Verbesserung ist das *Plan-Do-Check-Act* (PDCA) (vgl. Abb. 1.4). Etwas verkürzt könnte man sagen: In der Phase P konzipiert man das ISMS und die gewünschte Sicherheit, in D setzt man das Konzept um, in C findet eine Überprüfung statt, in A werden die Prüfergebnisse sowie ggf. neue Anforderungen ausgewertet und führen möglicherweise zu Änderungsbedarf. Mit diesem steigt man wieder in P ein usw.

PDCA ist als *Regelkreis* zu verstehen, d. h. nach Durchlaufen der vier Phasen startet man wieder bei PLAN. Eine allseits akzeptierte Vorgehensweise ist, den Regelkreis mindestens einmal jährlich zu durchlaufen. Der Sollwert des Regelkreises ist die gewünschte Sicherheit, der man bei jedem Durchlaufen des PDCA wieder ein Stück näherkommt. Seine Wirkung entfaltet PDCA meist erst nach mehreren Jahren der Anwendung.

Die Anwendung der PDCA-Methode ist in der Neufassung der Norm nicht (mehr) vorgeschrieben. Die Forderung nach kontinuierlicher Verbesserung bleibt allerdings bestehen – sie kann ggf. auch mit anderen methodischen Ansätzen realisiert werden.

1.4 Der Anhang A

Der bekannte, längliche Anhang A der ISO 27001 enthält 114 sogenannte *Controls*, und zwar nach einem themenbezogenen Ordnungsraster. Auch wenn die deutschen Normfassungen hier von *Maßnahme* als Übersetzung von *Control* sprechen: Es handelt sich um einzelne *Sicherheitsanforderungen*, die eine Organisation zu erfüllen hat – und zwar immer dann, wenn die betreffende Anforderung im geschäftlichen Umfeld der Organisation

relevant ist. Falls ein Control als irrelevant betrachtet wird, ist dies zumindest zu begründen.⁹

Welche konkreten Maßnahmen sind nun geeignet, diese Sicherheitsanforderungen aus dem Anhang A umzusetzen?

- Beispiele (!) für solche Maßnahmen findet man zunächst in der ISO 27002, und zwar nach dem gleichen Ordnungsraster wie im Anhang A.
- Findet man hier nichts Passendes, wird das eigene Sicherheitspersonal technische/organisatorische Maßnahmen entwerfen bzw. konzipieren.
- Darüber hinaus sind natürlich auch andere Quellen einsetzbar – z. B. die Kataloge des IT- Grundschatzes bzw. des neuen Grundschatz-Kompendiums¹⁰ oder die Expertise externer Berater.

Streng genommen muss man die 114 Controls für jedes Asset aus der Inventarisierung abarbeiten: Die zugeordneten Maßnahmen zur Umsetzung eines Controls könnten bei bestimmten Assets unterschiedlich sein. Das verursacht natürlich einen erheblichen Aufwand. Hat man jedoch bei der Inventarisierung eine Hierarchie mit Top Level Assets und Ressourcen eingeführt, kann man die Vorgehensweise vereinfachen: Die Praxis hat gezeigt, dass es ausreicht, die Controls für die einzelnen Top Level Assets durchzuspielen – was fast immer eine überschaubare Liste darstellt.

Ist in der Organisation allerdings keine Prozess-Sicht eingeführt, wird es schwieriger. Eine IT-Abteilung könnte sich stattdessen an ihren IT-Anwendungen als Top Level Assets orientieren. Ist der Anwendungsbereich des ISMS aber die gesamte Organisation, dürfte dieser Ansatz nur eben den IT-Bereich abdecken und somit zu kurz greifen.

Die praktische Vorgehensweise sieht nun so aus, dass eine Tabelle erzeugt wird, in der in der ersten Spalte die 114 Controls eingetragen werden und anschließend für jedes Top Level Asset eine weitere Spalte vorgesehen wird. Für jedes Top Level Asset und jedes Control wird dann in das entsprechende Feld eingetragen, ob das betreffende Control relevant ist:

- wenn nein: eine Begründung,
- wenn ja: welche konkreten Maßnahmen (ggf. auch Optionen) zur Umsetzung des Controls geplant oder bereits vorhanden sind.

Da längliche Texte in einzelnen Tabellenfeldern unhandlich sind, trägt man besser nur Verweise auf ein Tabellenblatt mit Begründungen bzw. auf ein Tabellenblatt mit Maßnahmen ein.

⁹Die erforderlichen Angaben sind in dem „Technical Corrigendum 2“ [9] zur 2015-er (deutschen) Normfassung präzisiert worden, vgl. dazu den Abschn. 8.2 in diesem Buch.

¹⁰Allerdings hat der IT-Grundschatz ein anderes Ordnungsraster, d. h. man muss hier zunächst eine Zuordnung zwischen den Controls und den Baustein- und Maßnahmengruppen in den BSI-Unterlagen herstellen. Dabei unterstützt die Zuordnungsliste [10] des BSI.

In der Maßnahmentabelle kann man auch weitere Spalten vorsehen, um klarzustellen, ob eine Maßnahme bereits vorhanden ist, teilweise vorhanden ist oder vollständig fehlt. Hieraus lassen sich weitere Daten (Umsetzungs- und Prüfpläne) generieren.

Es kann sein, dass für eine konkrete Organisation die 114 Controls und die darin behandelten Sicherheitsaspekte nicht alle Sicherheitsziele der Organisation abdecken. Die Lösung besteht dann darin, der obigen Tabelle der Controls sozusagen eigene Controls für die fehlenden Aspekte hinzuzufügen und damit bei den einzelnen Assets analog vorzugehen.

Dieses Tabellenkonstrukt ist nach Fertigstellung der zentrale Baustein für die Risikobehandlung. Für die geplanten Optionen und Maßnahmen lassen sich auch Kostenschätzungen ableiten (in die Maßnahmentabelle aufnehmen?), die wiederum in den Genehmigungsprozess bei der Leitung einfließen müssen.

Die Zusammenfassung dieser Daten wird als *Statement of Applicability*¹¹ (SoA) bezeichnet.

1.5 ISMS und Auslagerung

Betrachten wir die Informationsverarbeitung in einer Organisation, so wird schnell deutlich, dass man dabei von vielen Lieferanten und Dienstleistern abhängt. Wir nennen einige Stichwörter: Lieferanten für Hard- und Software, Wartungstechniker, EVU, Netzbetreiber, Internet-Provider, Outsourcing-Nehmer, Cloud-Dienstleister, Reinigungskolonnen, Bewachungspersonal usw.

Für alle diese Fälle verwendet die Norm im Anhang A den Begriff *Lieferanten* und spricht von *Lieferantenbeziehungen*, die es zu managen gilt.

Die Frage ist, wie sich diese Gegebenheiten auf das ISMS der Organisation auswirken: Zunächst bleibt aus Sicht des ISMS die Gesamtverantwortung stets bei der Organisation selbst. Sicherheitsziele der Organisation müssen auf die einzelnen Lieferanten heruntergebrochen und dann vertraglich fixiert werden. Aus der Gesamtverantwortung ergibt sich aber weiter die Anforderung, die Einhaltung von Verträgen und Vereinbarungen regelmäßig (= gemäß einer festzulegenden Regel) zu überwachen.

Dies kann auf verschiedene Weise gelöst werden:

- Bei zertifizierten Lieferanten kann man möglicherweise mit Hinweis auf deren Zertifizierung (und die damit verbundene regelmäßige Auditierung) auf eine nochmalige Überprüfung verzichten.
- Hat man sich im Vertrag ein Inspektions- oder Prüfrecht vorbehalten, kann man die Überprüfung selbst oder mit einem beauftragten Auditor durchführen.

¹¹ Wie soll man das übersetzen? „Bericht zur Eignung“ wäre ganz gut. Meist wird einfach von „SoA“ gesprochen.

- Eventuell besteht auch die Möglichkeit, bestimmte Charakteristika einer Dienstleistung durch Messungen (Protokolle, Tickets, Aufzeichnungen) zu ermitteln, was in Verbindung mit einer entsprechenden Auswertung bereits zielführend sein kann.

Im Hinblick auf das ISMS kommt also die Aufgabe hinzu, die Vertragsbeziehungen zu managen, und zwar bei der Vertragsgestaltung, der Vertragsüberwachung und – nicht zu vergessen – auch bei der Vertragsbeendigung. Diese Punkte findet man im Anhang A in einer spezifischen Gruppe von Controls.

Für alle Vorgaben aus dem Hauptteil der Norm gilt, dass sie unverändert auf alles anzuwenden sind, was mit den Dienstleistungsbeziehungen zusammenhängt. Wir geben einige Beispiele:

- Die Prozesse der Risikobeurteilung sind auch für die Dienstleistungsbeziehungen anzuwenden.
- In die Lenkung dokumentierter Informationen sind alle Unterlagen und Aufzeichnungen über die Dienstleistungsbeziehungen aufzunehmen.
- Interne Audits und Management-Bewertungen müssen auch die Dienstleistungsbeziehungen berücksichtigen.

1.6 Checkliste

Bevor wir an die konkrete Ausgestaltung unseres ISMS herangehen, ist es sinnvoll, zur Vorbereitung die Punkte der Checkliste in der Tab. 1.2 zu klären.

Tab. 1.2 Checkliste zur Vorbereitung

Aktion	Gegenstand	Ja	Teilweise	Nein
1	Sind die Normen (27000, 27001, 27002) in aktueller elektronischer Form vorhanden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Sind die Vorteile und der Nutzen eines ISMS erläutert worden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Ist ein Grob-Abgleich mit ISO 27001 erfolgt? (Ziel: erste Aufwandsabschätzung)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Ist eine Entscheidung zur Orientierung an der ISO 27001 getroffen worden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Denken wir in Management-Systemen? Existieren schon andere Management-Systeme?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Ist der Begriff ISMS eingeführt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Denken wir in Geschäftsprozessen und IT-Anwendungen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Ist der Anwendungsbereich des ISMS (Scope) zumindest grob skizziert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Sind zumindest die Top Level Assets und deren Asset/Risk Owner erfasst worden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	Wurden – zumindest grob – Sicherheitsziele für diese Assets festgelegt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Zusammenfassung

Nachdem wir nun einen Einblick in die ISO 27001 gewonnen und uns insbesondere eine Vorstellung von einem ISMS verschafft haben, sind wir gerüstet, im folgenden Kap. 2 die detaillierten Anforderungen an das ISMS durchzuarbeiten.

Literatur

1. DIN ISO/IEC 27001 (2017–06) Informationstechnik – IT-Sicherheitsverfahren: Informationssicherheits-Managementsysteme – Anforderungen (Hinweis: Diese aktuelle deutsche Normfassung enthält die frühere Fassung 2015-03 mit der Korrektur [9].)
2. DIN ISO/IEC 27002 (2017–06) Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management (Hinweis: Diese aktuelle deutsche Normfassung enthält die frühere Fassung 2016-11 und berücksichtigt die Korrektur [8].)
3. BS 7799-1 (1999) Information Security Management – Part 1: Code of Practice for Information Security Management, www.bsi-global.com
4. BS 7799-2 (2002) Specification for Information Security Management, www.bsi-global.com
5. DIN EN ISO 9001 (2015–11) Qualitätsmanagementsysteme – Anforderungen
6. BDSG: Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)
7. Datenschutz-Grundverordnung: VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, Amtsblatt der Europäischen Union L 119/1 vom 4.5.2016
8. International Standard ISO/IEC 27001:2014: TECHNICAL CORRIGENDUM 1 vom 15.09.2014
9. International Standard ISO/IEC 27001:2014: TECHNICAL CORRIGENDUM 2 vom 01.12.2015
10. Zuordnung ISO/IEC 27001 sowie ISO/IEC 27002 zum modernisierten IT-Grundschutz, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/Zuordnung_ISO_und_modernisierter_IT_Grundschutz.html vom 20.04.2018