Edition <kes>

Heinrich Kersten
Klaus-Werner Schröder

ISO 27001: 2022/2023

Management der Informationssicherheit nach den aktuellen Standards

<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.

Heinrich Kersten · Klaus-Werner Schröder

ISO 27001: 2022/2023

Management der Informationssicherheit nach den aktuellen Standards

Springer Vieweg

Heinrich Kersten
Meckenheim, Deutschland

Klaus-Werner Schröder
IT-Sicherheitsberatung
Remagen, Rheinland-Pfalz, Deutschland

ISSN 2522-0551 ISSN 2522-056X (electronic)
Edition <kes>
ISBN 978-3-658-42243-1 ISBN 978-3-658-42244-8 (eBook)
https://doi.org/10.1007/978-3-658-42244-8

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

Planung/Lektorat: David Imgrund
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

Das Papier dieses Produkts ist recyclebar.

Vorwort

Das vorliegende Buch beschäftigt sich mit der *Informationssicherheit,* d. h. mit Sicherheitsfragen bei der Speicherung, Verarbeitung und Übertragung von Daten.

Das Sicherheitsthema ist seit Jahrzehnten hoch aktuell: Seine Bedeutung für Unternehmen und Behörden („Organisationen"), aber auch für den privaten Bereich nimmt nicht ab – im Gegenteil: Wir werden zurzeit geradezu überschwemmt mit Meldungen über Sicherheitsvorfälle, Spionageaktivitäten und gezielte Attacken auf Organisationen und staatliche Infrastrukturen (Stichwort *Cybersecurity*).

Kann man sich gegen solche Risiken schützen? Sicherlich nicht in vollem Umfang, aber man kann als Organisation einiges tun: ein angemessenes Management der Informationssicherheit einführen und geeignete technisch-administrative Sicherheitsmaßnahmen aufsetzen. Hiermit lassen sich die Risiken erheblich reduzieren.

Die internationale Normung hat dieses Thema vor ca. 20 Jahren aufgegriffen, und zwar durch Herausgabe einer spezifischen Normenreihe: die ISO/IEC 27000. Diese Reihe ist in den vergangenen Jahren ausgebaut worden und beinhaltet aktuell ca. 50 veröffentlichte Einzelnormen. Einige Normen der Reihe haben schon mehrere Aktualisierungen erhalten, um sie an geänderte Rahmenbedingungen und den technologischen Fortschritt anzupassen.

Kern der Reihe ist die Norm ISO 27001, in der das *Management* der Informationssicherheit behandelt wird. In einem Anhang werden weiterhin *Controls* – grob übersetzt: Maßnahmen – aufgelistet, deren Umsetzung für eine Organisation in Frage kommen kann. Der genannte Anhang wird in der umfangreichen (begleitenden) Norm ISO 27002 vertieft.

Im Jahr 2022 sind beide Normen nach entsprechender Überarbeitung in einer dritten Version erschienen (nach 2005 und 2013). Neben Änderungen das Managementsystem betreffend, sind vor allem umfangreiche Änderungen an den Controls vorgenommen worden.

Entsprechende Entwürfe für eine deutsche Übersetzung liegen bereits vor, ihr offizielles Erscheinen in 2023/2024 ist anzunehmen.

Vor diesem Hintergrund erläutert und kommentiert dieses Buch die neuen Normfassungen – mit vielen Beispielen und Hinweisen zur Umsetzung. Dabei werden *alle*

Anforderungen aus der ISO 27001 an das sog. *Managementsystem* eingehend betrachtet und analysiert, ebenso *alle* 93 Controls aus dem Anhang.

In Kap. 1 geben wir einen kurzen Überblick über die Normenreihe und erläutern zentrale Begriffe für die gesamte Reihe in Form eines ausführlichen, im Zusammenhang lesbaren Glossars.

Damit sind wir gut gerüstet für die Analyse der Anforderungen an ein *Managementsystem* für die Informationssicherheit in Kap. 2.

Was mögliche Sicherheitsmaßnahmen anbetrifft, werden in Kap. 3 alle *Controls* aus dem Anhang der ISO 27001 ausführlich kommentiert.

Einen *Fahrplan* zur Umstellung eines vorhandenen Managementsystems auf die neuen Normfassungen stellen wir in Kap. 4 vor.

Die Umstellung bedeutet Aufwand, den man vor allem solchen Organisationen nicht ersparen kann, die nach der ISO 27001 zertifiziert sind – auch wenn hier gewisse Übergangsfristen bestehen. Organisationen, die diese Normen unabhängig von einer Zertifizierung nutzen oder aufgrund anderer Auflagen einhalten müssen, können sich ebenfalls an dem Fahrplan orientieren.

Im Kap. 5 geben wir ergänzend einige Erfahrungen aus Audits wieder, und zwar speziell aus dem Bereich der Energieversorgung als Teil der kritischen Infrastrukturen (KRITIS) in Deutschland. Energieversorger sind nach dem IT-Sicherheitsgesetz bzw. nachgeordneten Sicherheitskatalogen gehalten, ein entsprechendes ISMS zu betreiben.

Noch ein wichtiger Hinweis für die Leser/innen:

Dieses Buch enthält *nicht* die Texte der Normen ISO 27001/27002: Wer sich eher professionell mit der Informationssicherheit beschäftigt, wird diese Normen ohnehin zur Verfügung haben oder kann sie sich bei den entsprechenden Normenverlagen beschaffen. Aber: Zum Verständnis der Normen und ihrer Umsetzung sind die Erläuterungen und Kommentierungen im vorliegenden Buch absolut ausreichend.

An dieser Stelle einen herzlichen Dank an Herrn Imgrund und das Lektorat bei Springer Fachmedien für die gute Betreuung unseres Buchvorhabens.

Im Juni 2023

Heinrich Kersten
Klaus-Werner Schröder

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACL	Access Control List
AGB	Allgemeine Geschäftsbedingungen
BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analysis/Geschäftsauswirkungsanalyse
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CC	Common Criteria
CERT	Computer Emergency Response Team
CSF	Cybersecurity Framework
DAC	Discretionary Access Control
DIN	Deutsches Institut für Normung e. V.
DLP	Data Leakage/Loss Prevention/Protection
DMZ	Demilitarisierte Zone
DNS	Domain Name System
DoS	Denial of Service
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
EVU	Energieversorgungs-Unternehmen
FTP	File Transfer Protocol
GAU	größter anzunehmender Unfall
GPS	Global Positioning System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnologie
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System

ISMS	Information Security Management System/ Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
ITIL	Information Technology Infrastructure Library
IT-SG	IT-Sicherheitsgesetz
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MDM	Mobile Device Management
NDA	Non Disclosure Agreement
NEA	Netzersatzanlage
NTP	Network Time Protocol
OLA	Operational Level Agreement
OTA	Over-the-Air
PDCA	Plan-Do-Check-Act
PIM	Personal Information Management
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTB	Physikalisch-Technische Bundesanstalt
PTP	Precision Time Protocol
QM	Quality Management
RB	Risikobehandlung
RBAC	Role Based Access Control
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RZ	Rechenzentrum
SDK	Software Development Kit
SDM	Standard-Datenschutzmodell
SLA	Service Level Agreement
SoA	Statement of Applicability/Erklärung zur Eignung
SSD	Solid State Drive
SSL	Secure Socket Layer
SÜG	Sicherheitsüberprüfungsgesetz
TAN	Transaktionsnummer
TK	Telekommunikation(s-)
TOM	technisch-organisatorische Maßnahme
TPM	Trusted Platform Module
USB	Universal Serial Bus

USV	Unterbrechungsfreie Stromversorgung
VM	Virtual Machine
VPN	Virtual Private Network
VS	Verschlusssache
WBT	Web-based Training
WLAN	Wireless LAN

Die Normenreihe ISO/IEC 27000 und ihre Grundbegriffe

1

Trailer

In diesem Kapitel geben wir einen Überblick über die Normenreihe ISO/IEC 27000, die eine Vielzahl von Sicherheitsthemen abdeckt und ständig weiterentwickelt wird.

Im Weiteren erläutern wir Grundbegriffe und Zusammenhänge, die für das Verständnis der Normenreihe wesentlich sind.

Die Begriffe sind nicht alphabetisch sortiert, sondern sachlich so angeordnet, dass man den Text der Reihe nach lesen kann, ohne zwischen den Stichwörtern hin- und herspringen zu müssen.

Wir werden in den folgenden Kapiteln auf die erläuterten Stichwörter Bezug nehmen. Wer begrifflich „firm" ist, kann dieses Kapitel überspringen oder später bei Bedarf selektiv lesen.

1.1 Übersicht und Verfügbarkeit

Ursprung der Normenreihe ISO 27000[1] ist der zweiteilige British Standard (BS) 7799 aus den Jahren 1999/2002 – genauer: BS 7799-2 wurde in die ISO 27001 überführt, aus BS7799-1 wurde ISO 27002.

Die Normenreihe beschäftigt sich mit unterschiedlichen Aspekten der Informationssicherheit sowie deren Ausgestaltung in bestimmten Anwendungen und Branchen.

Die englischen Webseiten *ISO27k Information Security* unter www.iso27001security.com vermitteln einen guten Überblick über die Normenreihe insgesamt, den aktuellen

[1] Zur Notation: Zusätze in der Normbezeichnung wie „IEC", „DIN EN" usw. lassen wir im Folgenden zur Vereinfachung weg, wenn keine Missverständnisse zu befürchten sind.

H. Kersten and K.-W. Schröder, *ISO 27001: 2022/2023,* Edition <kes>,
https://doi.org/10.1007/978-3-658-42244-8_1

Stand der Einzelnormen und die laufende Entwicklung der Reihe. Sie umfasst zurzeit[2] ca. 50 veröffentlichte Einzelnormen – darunter einige, die als *Technical Report* (TR) oder *Technical Specification* (TS) gekennzeichnet sind.

Die Normen sind – in allen Ländern – nur gegen Entgelt verfügbar. In Deutschland ist der Beuth-Verlag[3] Anlaufpunkt für den Erwerb der Normen, in Österreich die Austrian Standards[4] und in der Schweiz die Schweizerische Normen-Vereinigung (SNV)[5].

Die in diesem Buch erwähnten Normen der 27000er Reihe sind nicht separat in unseren Literaturverzeichnissen aufgeführt: Wir verweisen dazu auf die genannten Normenverlage bzw. auf die oben genannte Website *ISO27k Information Security.*

1.2 Die Basisnormen

Als *Basisnormen* der Reihe ISO 27000 bezeichnen wir diejenigen, die Modellvorstellungen, Methoden und Verfahren behandeln, welche auf die Informationssicherheit anwendbar sind und den Hintergrund der gesamten Reihe bilden. Das sind nach gegenwärtigem Stand die ersten zehn Normen ISO 27000 bis ISO 27009.

Die erste Norm der Reihe – die Einzelnorm **ISO 27000** – trägt den Titel *Informationssicherheitsmanagementsysteme – Überblick und Terminologie.* Sie gibt eine Einführung in das Management der Informationssicherheit und definiert sodann – in Form eines stichwortartigen Glossars – wesentliche Begriffe, die in der gesamten Reihe zur Anwendung kommen.

Die englische Fassung der ISO 27000 ist die einzige Norm der Reihe, die kostenfrei downloadbar ist[6].

Die **ISO 27001** beschäftigt sich mit den Anforderungen an ein *Informationssicherheits-Managementsystem* (ISMS). Auf diese Norm nehmen alle weiteren Normen der Reihe Bezug, weil die Existenz eines ISMS sozusagen die Grundlage für alle weiteren Überlegungen und Aktivitäten zur Informationssicherheit darstellt.

Während im *Hauptteil* dieser Norm die genannten ISMS-Anforderungen aufgeführt sind, werden im (einzigen) *Anhang A* sog. *Controls* beschrieben: Sie beinhalten typische Anforderungen und Maßnahmen für die Informationssicherheit einer Organisation. Diese Controls sind zu beachten, aber nicht zwingend umzusetzen.

Der *Anhang u*nterscheidet sich von allen früheren Normfassungen durch einen kompletten Umbau, zahlreiche Aktualisierungen sowie einige neue Controls, gleichzeitig ist die *Anzahl* der Control deutlich reduziert worden, und zwar von 114 auf 93 – woraus man aber nicht schließen sollte, dass dadurch für die Umsetzung weniger Arbeit anfällt.

---

[2] Stand Juni 2023.

[3] www.beuth.de.

[4] https://shop.austrian-standards.at/

[5] https://connect.snv.ch/de/

[6] https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.

Die relativ abstrakt gehaltene Darstellung der Controls im Anhang A wird in der umfangreichen Norm **ISO 27002** mit vielen Anmerkungen und Beispielen vertieft.

Zur Umsetzung der ISMS-Anforderungen aus dem Hauptteil der ISO 27001 liefert die **ISO 27003** Begründungen, Erklärungen und vor allem Umsetzungshilfen. Viele Pläne und Ablaufdiagramme erleichtern die Realisierung eines normgerechten ISMS.

Die Norm **ISO 27004** befasst sich mit dem wichtigen Thema der Überwachung, Messung, Analyse und Bewertung eines ISMS – und zwar im Hinblick auf seine Eignung, Wirksamkeit und Angemessenheit. Diese Norm ist sehr hilfreich bei der Umsetzung der entsprechenden Anforderungen aus der ISO 27001: Sie liefert ein Gerüst für die Planung und Umsetzung eines Überwachungs-/Messprogramms für das ISMS einer Organisation.

Eine zentrale und anspruchsvolle Aktivität im Zuge der Einrichtung und des Betriebs eines ISMS ist die Beurteilung und Behandlung von *Risiken:* Hier werden u. a. die für eine Organisation identifizierten Risiken (und Schwachstellen) analysiert und bewertet. Daran schließen sich eine Priorisierung der Risiken und ihre Behandlung an. Die Norm **ISO 27005** bietet einen Leitfaden für das gesamte Risikomanagement – u. a. mit Übersichten und Beispielen für Gefährdungen/Bedrohungen und Risikoklassen.

Die Norm **ISO 27006** besteht aus zwei Teilen: Teil 1 richtet sich an Institutionen, die Audits und/oder Zertifizierungen nach der ISO 27001 anbieten. Es werden die Anforderungen[7] an solche Institutionen und ihr Personal spezifiziert wie z. B. Unabhängigkeit, Kompetenznachweise, Qualitätsmanagement usw. Teil 2 beschreibt analog Anforderungen an Stellen, die Audits/Zertifizierungen für *Datenschutz*-Managementsysteme[8] offerieren.

Für ein normgerechtes ISMS besteht die Verpflichtung, regelmäßig eigene, d. h. *interne* Audits durchzuführen, um die Übereinstimmung des ISMS mit der ISO 27001 sicherzustellen bzw. Defizite zu erkennen. Sofern darüber hinaus eine Zertifizierung beabsichtigt ist, sind auch *externe* Audits durchzuführen, und zwar von Auditoren einer Institution gemäß ISO 27006 Teil 1.

Ob intern oder extern – ein entsprechendes Audit soll den Vorgaben der **ISO 27007** gemäß erfolgen: Es geht hier um Themen wie Personalauswahl, Planung, Durchführung und Ergebnisdarstellung. Wichtig: Die hier gemeinten Audits beziehen sich im Schwerpunkt auf das *Managementsystem (ISMS).*

Dagegen betrachtet die **ISO 27008** Audits hinsichtlich der *Controls* und ihrer Umsetzung – verkürzt ausgedrückt: Es geht schwerpunktmäßig um eher technische Audits. Es ist aber festzuhalten, dass die Durchführung solcher (technischer) Audits weder von der ISO 27001 generell noch im Rahmen einer Zertifizierung gefordert ist. Die Praxis sieht allerdings häufig so aus, dass bei den Management-Audits die Controls und ihre Umsetzung zumindest stichprobenartig überprüft werden. Dabei stehen die korrekte Umsetzung der relevanten Controls und ihre Wirksamkeit im Vordergrund.

---

[7] Die Anforderungen in der ISO 27006-1 sind nicht abschließend: Die genannten Stellen müssen zusätzlich die ISO 17021–1 [1] und die ISO 19011 [2] erfüllen.

[8] Privacy Information Management System (PIMS).

Tab. 1.1 Basisnormen

Norm	Teile	Stand-E	Stand-D
27000		2018-02	2020-06
27001		2022-10	2023-04 (Entwurf)
27002		2022-02	2022-08 (Entwurf)
27003		2017-03	–
27004		2016-12	–
27005		2022-10	
27006	ISO 27006-1 ISO 27006-2	2015-10 + Korrektur 2020 2021-02	2023-05 (Entwurf) –
27007		2020-01	2022-10[9]
27008		2019-01	–
27009		2020-04	2022-09

Da fast alle Basisnormen der Reihe auf einem relativ abstrakten Level gehalten sind, entsteht bei speziellen Themen, in besonderen Branchen oder Markt-Sektoren häufig die Notwendigkeit, die Anforderungen z. B. der ISO 27001 an das ISMS geeignet zu interpretieren, zu verfeinern oder zu ergänzen – was je nach Umfang bedeuten kann, dass de facto ein eigener Standard entwickelt bzw. aus der Norm abgeleitet wird. Dies kann sich auch auf die Controls aus dem Anhang A beziehen, die für bestimmte Anwendungen angepasst und ergänzt werden. Die Norm **ISO 27009** stellt insofern Anleitungen bereit, wie solche branchen- oder sektorspezifischen Standards aus der ISO 27001 abgeleitet werden können, was dabei zu beachten ist – und was auf keinen Fall passieren darf: Widersprüche zur ISO 27001, Wegfall/Abschwächung von Anforderungen usw.

Übersicht

Die folgende Tabelle gibt eine Übersicht über die Basisnormen mit Angaben zum Stand und zur Sprache.

Die Spalte „Stand-E“ gibt Stand des englischen Originals an, „Stand-D“ betrifft die deutsche Fassung, sofern es eine solche gibt. Leider gibt es nur für einen Teil der Normen eine aktuelle deutsche Übersetzung. Den Ausgabestand Jahr-Monat einer Norm geben wir bspw. mit 2018-02 an, wobei 02 den Monat angibt.

Die Tabelle gibt die Daten zum Zeitpunkt Juni 2023 wieder, aktuellere Angaben können ggf. den Webseiten des Beuth-Verlags, der Austrian Standards und der SNV entnommen werden (Tab. 1.1).

[9] Als OENorm 2022–07, als SNV-Norm 2022–01.

1.3 Weitere Normen der Reihe im Überblick

Zählt man die veröffentlichten Normen und solche im Entwurfsstadium („Draft“) zusammen, so nähern wir uns der 100er-Marke. Wir wollen diese nicht einzeln angeben oder kommentieren, sondern ein wenig Ordnung schaffen, indem wir die thematischen Gruppen zusammenstellen und einige Stichwörter geben[10]. Der Zusatz „(mehrteilig)“ zeigt an, dass die entsprechende Norm aus mehreren – getrennt veröffentlichten – Teilen besteht.

Erweiterte Anwendungen der ISO 27001
27013 – Gemeinsame Umsetzung 27001 und ITIL
27701 – ISMS gleichzeitig für Informationssicherheit und Datenschutz
27014 – Governance der Informationssicherheit
27016 – ISMS und Wirtschaftlichkeit
27021 – Kompetenzen, Erfahrungen und Kenntnisse des ISMS-Personals
27022 – Übersicht über ISMS-Prozesse

Normen für spezielle Branchen/Communities
27010 – sektor- und organisationsübergreifende Kommunikation
27011 – Telekommunikationsanbieter
27019 – Energielieferanten und -erzeuger
27036 – Informationssicherheit für Lieferketten (mehrteilig)
27799 – Gesundheitswesen

Technische Themen
27033 – Netzwerksicherheit (mehrteilig)
27034 – Applikationssicherheit (mehrteilig)
27038 – Anforderungen an digitales Schwärzen
27039 – Intrusion Detection and Prevention Systems
27040 – Speicher-Sicherheit
27099 – Public-Key-Infrastrukturen

Cloud Services
27017 – Controls für Cloud Services
27018 – Datenschutz in Public Clouds
27070 – Aufbau von Virtual Roots of Trust in der Cloud mit HSMs
27071 – Vertrauenswürdige Verbindungen zwischen Geräten und (Cloud) Diensten

[10] Die hinter den jeweiligen Nummern angegeben Stichwörter betreffen den Inhalt der Norm, sind aber nicht notwendigerweise identisch mit dem Normtitel.

Cybersecurity
27032 – Cybersecurity/Internet Security
27100 – Cybersecurity-Konzepte: Übersicht
und einige weitere Normen ab der Nummer 27102 (u. a. Cyber-Versicherungen, Ausbildung und Training im Rahmen der Cybersecurity)

Business Continuity
27031 – ICT[11] Widerstandfähigkeit und Wiederherstellung
27035 – (Security) Incident Management (mehrteilig)

Privatheit und Datenschutz
27018 – Personenbeziehbare Daten in Public Clouds
27046 – Informationssicherheit und Datenschutz für "Big Data"
27091 – Privatheit und Datenschutz bei KI-Systemen
und viele weitere Normen zu Datenschutzthemen ab der Nummer 27550 (u. a. Datenschutz-Engineering, biometrische Authentisierung, sichere Löschung, Anonymisierung, Altersverifizierung, Smart City)

Internet of Things (IoT)
27400 – Sicherheit und Privatheit für das Internet of Things
und einige weitere Normen ab der Nummer 27402 (IoT-Sicherheit aus Anwender- und Herstellersicht)

Digitale Beweismittel und Forensik
27037 – Identifizieren, Sammeln und Erhalten digitaler Beweismittel
27041 – eForensic (elektronische Forensik)
27042 – Analyse und Interpretation digitaler Beweismittel
27043 – Untersuchung von Incidents
27050 – eDiscovery (elektronische Erkennung) (mehrteilig)

Big Data
27045 – Framework für "Big Data"
27046 – Anleitung für Sicherheit und Datenschutz bei "Big Data"

Künstliche Intelligenz
27090 – Angriffe auf KI-Systeme
27091 – Datenschutz in KI-Systemen

[11] ICT = **I**nformation and **C**ommunication **T**echnology, im Deutschen meist mit IKT oder IuK abgekürzt.

Wer z. B. im Rahmen eines Normen-Abonnements Zugriff auf die veröffentlichen Titel hat, kann sich hier nach Belieben einlesen. Wer keinen solchen Zugriff hat, müsste sich die einzelnen Normen beschaffen, was preislich schnell in die Höhe geht. Deshalb der wichtige Hinweis: Für die Einrichtung eines ISMS kommt man mit ISO 27001und ISO 27002 bestens aus. Die weiteren Normen ab der Nummer 27010 spezialisieren diese Basisnormen meist nur auf das jeweilige Thema, sind aber nicht verpflichtend anzuwenden bzw. umzusetzen – auch nicht bei einer Zertifizierung.

Es kann jedoch aus geschäftlicher bzw. Marketing-Sicht sinnvoll sein, auch weitere Normen einzubeziehen. Ein Beispiel: Für Cloud-Anbieter könnte es ein Kompetenznachweis sein, neben der 27001 auch die oben unter dem Stichwort *Cloud Services* angegeben Normen umzusetzen – und dann in einem ISO 27001-Zertifikat als mitgeltende Norm erscheinen zu lassen.

1.4 Grundbegriffe und Zusammenhänge

Wir kommentieren folgende Schlüsselbegriffe der Normenreihe ISO 27000 in der angegebenen Reihenfolge:

1. Organisation
2. Prozesse
3. Rollen
4. Ressourcen und Assets
5. Ziele, insbesondere Sicherheitsziele
6. Daten und Klassifizierungen
7. Events und Incidents
8. Dokumentation
9. Aufzeichnungen
10. dokumentierte Information
11. Kontext
12. Interessierte Parteien
13. ISMS und Anwendungsbereich
14. Kontinuierliche Verbesserung
15. Schnittstellen
16. Risiken
17. Risikobeurteilung
18. Risikobehandlung
19. Messen und Überwachen im ISMS
20. Leit- und Richtlinien

Wenn wir im Folgenden von der *Norm* sprechen, meinen wir explizit die ISO 27001.

1. Organisation

In der ISO 27000-Reihe ist häufig die Rede von der *Organisation,* was stellvertretend für ein Unternehmen, eine Behörde oder jede andere Institutionsform steht, die die Norm nutzen bzw. anwenden will.

Was den internen organisatorischen Aufbau anbetrifft, sprechen wir von *Aufbauorganisation,* im Zusammenhang mit den internen Prozessen bzw. Abläufen einer Organisation verwenden wir den Begriff *Ablauforganisation.*

2. Prozesse

Ein Prozess ist eine vernetzte Struktur aus einzelnen Aktivitäten mit einer definierten Verarbeitungsrichtung: Ein Prozess benötigt auf der Eingangsseite gewisse Ressourcen (Input) und liefert unter deren Nutzung ein Ergebnis (Output), z. B. ein Produkt oder eine Dienstleistung. Die Abb. 1.1 visualisiert den Sachverhalt.

Ein Verwaltungsprozess z. B. einer Behörde erbringt in der Regel eine Dienstleistung, die durch gesetzliche Vorgaben festgelegt ist bzw. hiervon gefordert wird. Auch in Unternehmen gibt es solche Verwaltungsprozesse – z. B. das Management der Finanzen und das Personalmanagement. Die Kernaufgabe eines Unternehmens besteht jedoch darin, Produkte und Dienstleistung gegen Entgelt anzubieten, weshalb man auch von *Geschäftsprozessen* spricht: Mit ihrer Hilfe werden z. B. Produkte hergestellt und vertrieben – analog werden Dienstleistungen bereitgestellt und zur Nutzung angeboten.

Da es für die Sicherheit von Prozessen meist unerheblich ist, ob es um einen Verwaltungs– oder Geschäftsprozess geht, wollen wir uns der Einfachheit halber auf *einen* Begriff beschränken und sprechen in diesem Buch – auch im Fall von Behörden oder Verwaltungen – meist nur von ***Geschäftsprozessen.***

Neben den Geschäftsprozessen existieren in Organisationen unterstützende bzw. begleitende Prozesse wie z. B. die Revision, das Qualitätsmanagement, das Controlling und das Management der Informationssicherheit.

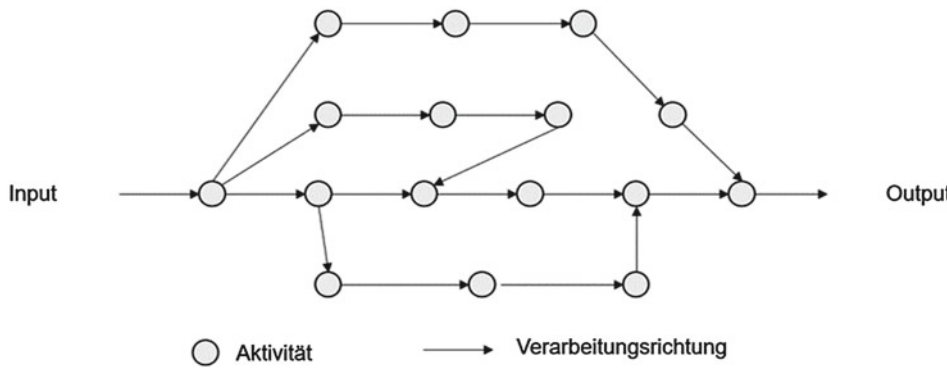

Abb. 1.1 Prozess(ablauf)

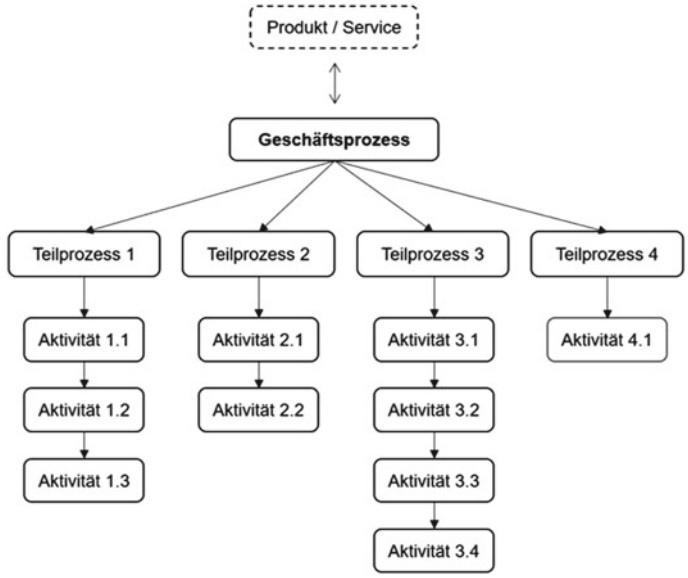

Abb. 1.2 Zerlegung eines Geschäftsprozesses

Einen Prozess – gleich welcher Art – kann man in mehreren Stufen zerlegen (Prozesshierarchie). Meist geschieht dies, um die Übersichtlichkeit zu verbessern, Komplexität zu reduzieren, Abhängigkeiten zu erkennen und Analysen zu vereinfachen. Die Abb. 1.2 gibt ein Beispiel dazu an: Ein Geschäftsprozess ist in 4 Teilprozesse zerlegt worden, in denen einzelne Aktivitäten aneinandergereiht sind. Diesen Aktivitäten könnten in der nächsten Ebene die beteiligten IT-Anwendungen und/oder manuelle Arbeiten zugeordnet sein.

Alle in einer Organisation festgelegten Prozesse bilden gemeinsam die oben schon genannte *Ablauforganisation.* Im Zuge einer gewissen Professionalität gehört zu einem Prozess zunächst eine für alle Belange des Prozesses verantwortliche Stelle[12]. Dann sollte eine Prozessdokumentation[13] vorhanden sein, in der

- Aufgaben und Ziele (u. a. Sicherheitsziele) des Prozesses,
- im Prozess mitwirkenden *Rollen* bzw. Personen sowie deren Aufgaben,
- sonstige benötigte *Ressourcen,* die jeweiligen Abläufe und die erwarteten Ergebnisse beschrieben sind.

Eine zügige Anpassung des Prozesses bei Änderungsbedarf (einschließlich Überarbeitung der Prozessdokumentation) wird geboten sein, ebenso wie eine Überwachung des Prozesses

[12] Rolle, Person oder Organisationseinheit – häufig als Prozessverantwortliche(r), im Englischen als Process Owner bezeichnet.

[13] Prozesshandbücher, Verfahrensbeschreibungen o. ä.

betreffend korrekter Umsetzung, der Ergebnisse und der Zielerreichung. Weiterhin müssen auftretende Probleme, Abweichungen und Fehler behoben werden können – z. B. im Rahmen des Incident Managements (s. weiter unten).

3. Rollen

Unter *Rolle* verstehen wir eine Instanz mit zugewiesenen Aufgaben, Pflichten und Rechten (z. B. der/die Sicherheitsbeauftragte, die System-Administration).

Eine Rolle kann durch *eine* Person oder *mehrere* Personen besetzt sein (Beispiel: die Rolle der System-Administration, die meist mit vielen Administratoren besetzt ist).

Da man für eine Rolle nicht nur *einen* Rolleninhaber, sondern fast immer auch Stellvertretungen benötigt, haben also solche Rollen mindestens zwei Personen als Besetzung. Die betreffenden Personen tragen gemeinsam die Verantwortung dafür, dass die zugewiesenen Aufgaben korrekt und termingerecht erledigt werden.

Ein grundlegendes Prinzip für Rollen besteht darin, Tätigkeiten/Aufgaben ganz oder teilweise an andere Personen delegieren zu können, d. h. der Rolleninhaber macht Vorgaben für die zu delegierende Tätigkeit oder Aufgabe und kontrolliert die Durchführung der Tätigkeit bzw. das Ergebnis der Aufgabe.

Eine Person kann formal mehrere Rollen innehaben – was natürlich nur sinnvoll ist, wenn die Rollenhäufung tatsächlich leistbar ist und wenn es zwischen diesen Rollen keine Interessenkonflikte gibt. Wir nennen zwei Beispiele für solche Konflikte:

1) Sollen die Verantwortlichkeiten für den Datenschutz und die IT-Sicherheit *einer* Person zugewiesen werden? Dieser Punkt wird durchaus kontrovers diskutiert. Betrachten wir folgenden Fall: Zur Aufklärung manipulativer Handlungen könnte sich die Notwendigkeit ergeben, Log- und Zugriffsprotokolle auszuwerten. Diese stellen aber personenbezogene Daten dar. Wäre die gleiche Person für beide Themen zuständig, müsste sie sich sozusagen selbst die Genehmigung zur Einsicht in die Protokolle erteilen oder versagen – eine nicht tragbare Situation. Dies könnte man dadurch auflösen, dass solche Überprüfungsaufgaben auf eine andere Rolle verlagert werden.

2) Kann die IT-Leitung gleichzeitig die Rolle des/der IT-Sicherheitsbeauftragten übernehmen? Bei einem vermuteten Hacker-Angriff könnte die IT-Leitung die Präferenz haben, mit Rücksicht auf die Kunden die IT weiterlaufen zu lassen, während die/der Sicherheitsbeauftragte die IT-Systeme herunterfahren, zumindest aber „vom Netz“ nehmen möchte – ein Interessenkonflikt.

4. Ressourcen und Assets

Jeder Prozess benötigt *Ressourcen*: Daten, Personal, technische Hilfsmittel, informationsverarbeitende Systeme[14], Versorgungen wie Strom, Klimatisierung und Internetzugang,

[14] IT-Systeme, IT-Anwendungen, andere IT-Geräte wie z. B. Speichersysteme, Drucker, Server, Smartphones, Router, Switches, Access Points.

oft auch unterstützende Dienstleistungen von Lieferanten[15] (z. B. Internet-Provider, Cloud Provider) sowie die betrieblich genutzten Liegenschaften und Gebäude.

Viele dieser Ressourcen sind unverzichtbar, weil ohne sie die erwarteten Ergebnisse eines Prozesses nicht erzielt werden können. Damit stellen sie für die Organisation einen *Wert* dar. Solche Ressourcen haben meist auch einen finanziellen Wert, möglicherweise auch einen Wert für das Image der Organisation oder für die Qualität ihrer Produkte usw.

Auch die Geschäftsprozesse selbst stellen Werte dar, ebenso das in der Organisation vorhandene Know-how, besondere Betriebsgeheimnisse usw. Soweit solche Werte im Zusammenhang mit der Informationsverarbeitung stehen, werden sie auch *Informationswerte* genannt.

Für (Informations-)*Wert* wird im Englischen der Begriff (Information) *Asset* verwendet.

In den Werten gibt es eine gewisse Hierarchie: Einige Werte sind mit anderen, sozusagen als Unterstützung, verbunden. Betrachtet man z. B. eine IT-Anwendung als Wert, so werden zu ihrem Betrieb Server und hierfür dann auch Strom benötigt. Server und Stromversorgung wären bei diesem Beispiel mit der IT-Anwendung *verbundene Werte.*

Das Management der Assets ist ein eigener (unterstützender) Prozess: Es ist ein Assetverzeichnis zu erstellen, neue Assets sind hinzuzufügen, ausgemusterte Assets zu entfernen, d. h. das Verzeichnis ist stets aktuell zu halten. Vor allem in größeren Organisationen findet man ein *Asset Management* bzw. die Rolle des *Asset Managers,* der für die skizzierten Aufgaben verantwortlich ist.

5. Ziele, insbesondere Sicherheitsziele

Im Zusammenhang mit der Informationssicherheit werden als *erwartete Ergebnisse* häufig sog. *Sicherheitsziele* formuliert: Die bekanntesten Ziele sind die Vertraulichkeit von Informationen, die Integrität und die Verfügbarkeit von Daten und anderen Objekten.

- Vertraulichkeit: Die betreffenden Informationen dürfen nur einem festgelegten Personenkreis – den Befugten – zur Kenntnis gelangen.
- Integrität: Die betreffenden Daten dürfen nur in beabsichtigter/zugelassener Weise und von dazu autorisiertem Personal verändert werden.
- Verfügbarkeit: Die betreffenden Daten müssen zum beabsichtigten Zeitpunkt für eine Bearbeitung durch autorisiertes Personal bereitgestellt werden können – ggf. kann dabei eine gewisse Verzögerung akzeptiert werden.

In dieser Aufzählung wird zwischen *Information* (bei Vertraulichkeit) und *Daten* (bei Integrität und Verfügbarkeit) unterschieden: Jede Information kann auf viele Arten in Daten umgesetzt und dann gespeichert werden. Hinsichtlich der Vertraulichkeit muss neben solchen Daten auch die Information selbst bzw. als Ganzes betrachtet werden.

[15] *Lieferant* (Supplier) ist der Begriff der Norm für jede Art von Dienstleister, hierunter fallen auch z. B. Produktlieferanten, Wartungstechniker, Entsorgungsdienstleister, Berater.

Bei den eingangs genannten *Objekten* kann es sich um *informationsverarbeitende Einrichtungen*[16] handeln, für die eigene Ziele definiert werden. Typisch sind z. B. die Sicherheitsziele der

- Verfügbarkeit von IT-Anwendungen, IT-Systemen und Netzwerken,
- Integrität von IT-Anwendungen, IT-Systemen und anderer informationsverarbeitender Systeme.

Bei der Integrität geht es dabei um den Ausschluss von unbefugten und unzulässigen Änderungen an der Software oder Hardware.

Neben diesen drei klassischen Zielen gibt es weitere Sicherheitsziele wie z. B. die Authentizität von Daten (beweisbare Quelle und ggf. unveränderte Attribute wie z. B. das Erstellungsdatum), die Authentizität von Personen (beweisbare Identität), die Nicht-Abstreitbarkeit des Sendens oder Empfangs von Daten (Non-Repudiation), die Einhaltung von Service Level Agreements (SLA), die Zuverlässigkeit von Dienstleistungen.

In der Norm werden auch umfassendere bzw. erweiterte Ziele angesprochen, die eine Organisation erreichen möchte[17]. Solche Ziele können auf unterschiedlichen Ebenen und für sehr verschiedene Sachverhalte formuliert sein. Wir geben einige Beispiele:

- Die eigene Organisation könnte sich das Ziel setzen, ein „sehr schnelles“ Incident Management aufzusetzen *(Strategieebene)*.
- Aus externen Vorgaben (z. B. Gesetze) ergibt sich möglicherweise, dass unsere Organisation für bestimmte Tätigkeiten Aufzeichnungen zu erstellen hat, etwa als Nachweis gegenüber Aufsichtsbehörden. Die Verantwortlichen könnten insofern entscheiden, die Nachweisführung in alle betroffenen Prozesse einzubauen *(Prozessebene)*.
- Kunden könnten z. B. Anforderungen an die Kompatibilität von Datenformaten oder die Interoperabilität mit bestimmten Kundensystemen oder -anwendungen stellen, was dann in entsprechende Ziele der Organisation einfließt *(Daten-/Systemebene)*.

Solche erweiterten Ziele können einen Einfluss auf die Informationssicherheit haben oder durch die Informationssicherheit – sozusagen als Nebeneffekt – realisiert werden. Man kann sie deshalb nicht vom ISMS trennen.

6. Daten und Klassifizierungen

Im Zusammenhang mit der Vertraulichkeit kommt die Klassifizierung[18] von Daten und damit verbundenen Werten ins Spiel. Was versteht man darunter?

---

[16] Informationsverarbeitende Systeme, Dienste, Standorte, Versorgungseinrichtungen.

[17] In der Norm wird u. a. die Formulierung „intended outcome“ als Zusammenfassung der Ziele (oder Erwartungen) verwendet.

[18] Solche Klassifizierungen existieren auch für die Integrität von Daten, sind aber in der Praxis weniger gebräuchlich.

Ein sehr einfaches Beispiel stellt die Klassifizierung nach OFFEN und VERTRAULICH dar: Unterlagen, die intern zu halten sind und nicht an die Öffentlichkeit gelangen sollen, werden mit dem Stempel VERTRAULICH versehen. Unterlagen ohne Stempel sind grundsätzlich als OFFEN anzusehen – bedürfen also hinsichtlich der Vertraulichkeit keines weiteren Schutzes.

Diese zweistufige Klassifizierung ist für manche Bereiche zu grob: Man möchte Dokumente detaillierter klassifizieren bzw. *einstufen*. Im behördlichen Geheimschutz verwendet man vier Stufen mit den Bezeichnungen VS-NfD[19], VERTRAULICH, GEHEIM, STRENG GEHEIM. Diese Stufen deuten an, wie kritisch ein Dokument in punkto Vertraulichkeit ist: Je höher die Einstufung, desto höher der Schaden für die Organisation, falls das Dokument in die falschen Hände gelangt.

Um dies auszuschließen, werden Regeln u. a. für das Lesen und Schreiben von eingestuften Dateien festgelegt. Eine Person, die z. B. für die Stufe VERTRAULICH *ermächtigt* ist, darf Dokumente dieser Stufe und niedrigerer Stufen lesen (Read Down). Schreiben dagegen ist nur erlaubt in Dateien der Stufe VERTRAULICH und höherer Stufen (Write Up): Die Schreibregel verhindert, dass man höher eingestufte Daten in eine niedriger eingestufte Datei schreibt und sie damit sozusagen „herabstuft" – eine im diesem Umfeld unzulässige Operation. Wendet man die Lese- und Schreibregeln gleichzeitig an, darf unsere Beispiel-Person eine Datei nur dann nach Belieben lesen, ändern und ergänzen, wenn diese Datei als **VERTRAULICH** eingestuft wurde, d. h. wenn Einstufung der Datei und Ermächtigung der Person übereinstimmen. (Abb. 1.3)

Soll nun ein solches eingestuftes Dokument als Datei auf einem Datenträger gespeichert, in einem IT-System bearbeitet, ausgedruckt oder in einem Netzwerk transportiert werden, ist dies nur zulässig, wenn diese Einrichtung (Speicher, IT-System, Drucker, Netzwerk) für die jeweilige Einstufung geeignet und zugelassen ist. Keinesfalls darf es passieren, dass bspw. ein als GEHEIM eingestuftes Dokument in einem nur für VERTRAULICH freigegebenem Netzwerk übertragen wird. Dies könnte allenfalls dann gestattet werden, wenn das Dokument ausreichend sicher verschlüsselt ist – eben mit einem für GEHEIM freigegeben Algorithmus. Die Eignung von Geräten und Netzwerken bzw. Netzwerkstrecken für

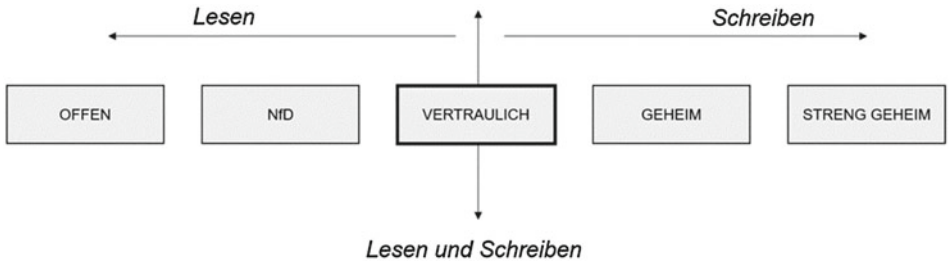

Abb. 1.3 Lese- und Schreibregeln im VS-Bereich

[19] NfD = Nur für den Dienstgebrauch, VS = Verschlusssache.