

# HANSER



## Leseprobe

zu

## „Informationssicherheit und Datenschutz – einfach & effektiv“

von Inge Hanschke

Print-ISBN: 978-3-446-45818-5

E-Book-ISBN: 978-3-446-45973-1

E-Pub-ISBN: 978-3-446-46300-4

Weitere Informationen und Bestellungen unter

<http://www.hanser-fachbuch.de/978-3-446-45818-5>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Inhalt

<b>Vorwort</b> .....	<b>VII</b>
Wegweiser durch dieses Buch.....	IX
<b>1 Herausforderungen in Informationssicherheit und Datenschutz</b> .....	<b>1</b>
1.1 Einordnung von Informationssicherheit und Datenschutz .....	3
1.2 Anforderungen an Informationssicherheit und Datenschutz .....	6
1.2.1 Wesentliche Normen und gesetzliche Vorschriften .....	7
1.2.2 Cyber-Security .....	15
1.2.3 ISO/IEC 27001 .....	17
1.2.4 IT-Grundschutz .....	37
1.2.4.1 Bestandteile des IT-Grundschutzes.....	38
1.2.4.2 Die IT-Grundschutz-Methodik.....	40
1.2.4.3 Der Sicherheitsprozess entsprechend IT-Grundschutz.....	41
1.2.5 EU-DSGVO.....	44
1.2.5.1 DSGVO-Grundsätze als Teil des Datenschutzkozepts .....	49
1.2.5.2 Umsetzung der Anforderungen.....	51
<b>2 Integriertes Managementsystem für Datenschutz und Informationssicherheit</b> .....	<b>55</b>
2.1 Was ist ein Managementsystem für Datenschutz und Informationssicherheit?.....	57
2.2 Bestandteile eines integrierten Managementsystems.....	61
2.2.1 Warum? – Strategie: Datenschutzpolitik und Informationssicherheitsstrategie.....	62
2.2.2 Was? – Anforderungen: Festlegung der umzusetzenden Kontrollen .....	63
2.2.3 Wie? – Sicherheitsorganisation und Sicherheitskonzept .....	63
2.2.4 Nachweis – Überwachung der Maßnahmendurchführung sowie regelmäßige interne oder externe Audits, um Konformität und Wirksamkeit zu gewährleisten .....	65
2.3 Erfolgsfaktoren für ein wirksames integriertes Instrumentarium für Datenschutz und Informationssicherheit .....	71
<b>3 Schritt-für-Schritt-Leitfaden</b> .....	<b>77</b>
3.1 Vorgehensweise zum Aufbau eines integrierten DS & ISMS .....	78
3.2 Detaillierter Leitfaden für den Aufbau .....	84
3.2.1 Datenschutz- und Informationssicherheitsleitlinie und -organisation .....	85
3.2.2 Konzeption des integrierten Managementsystems.....	87

3.2.2.1	Teilschritte bei der Konzeption des Instrumentariums .....	88
3.2.2.2	Umsetzen der Konzeption für das integrierte DS & ISMS und Inbetriebnahme .....	92
3.3	Fazit .....	92
<b>4</b>	<b>Best-Practices .....</b>	<b>95</b>
4.1	Schutzziele und Schutzbedarfsfeststellung .....	97
4.1.1	Schutzziele .....	98
4.1.1.1	Vertraulichkeit .....	98
4.1.1.2	Integrität .....	102
4.1.1.3	Verfügbarkeit .....	103
4.1.1.4	Weitere Schutzziele, z. B. Authentizität .....	104
4.1.2	Schutzbedarfsfeststellung .....	106
4.1.2.1	Schadensszenarien .....	106
4.1.2.2	Kronjuwelen .....	109
4.1.2.3	Vorgehen bei der Schutzbedarfsfeststellung .....	110
4.1.2.4	Zonenkonzept .....	114
4.1.2.5	Schutzbedarfsfeststellung für Geschäftsprozesse und die dazugehörigen Informationen .....	117
4.2	Risikomanagement .....	120
4.3	Notfallmanagement .....	128
4.4	ISMS-Reporting .....	134
4.5	Sicherheits- und Datenschutzorganisation .....	137
<b>5</b>	<b>Integration von EAM, IT-Servicemanagement und Informations- sicherheit .....</b>	<b>143</b>
5.1	EAM und Informationssicherheit .....	145
5.1.1	Enterprise Architecture Management .....	145
5.1.2	Zusammenspiel von EAM und DS & ISMS .....	151
5.1.3	Tool-Unterstützung für DS & ISMS .....	154
5.2	IT-Servicemanagement und Informationssicherheit .....	157
<b>Glossar .....</b>		<b>163</b>
<b>Abkürzungen .....</b>		<b>195</b>
<b>Literatur .....</b>		<b>197</b>
<b>Stichwortverzeichnis .....</b>		<b>201</b>

# Vorwort



*Am besten erledigt man die Dinge systematisch.*

*Hesiod von Böotien (um 700 v. Chr.)*

Anforderungen an die Informationssicherheit (u. a. ISO 27001 oder BSI), den Datenschutz (EU-Datenschutz-Grundverordnung) und Sicherheitsbedrohungen sowie die durch diese verursachten Schäden nehmen immer weiter zu. Ein in alle Planungs-, Entscheidungs- und Durchführungsprozesse verankertes, handhabbares und integriertes Managementinstrumentarium ist für deren nachhaltige Bewältigung notwendig. Im Buch werden sowohl die Herausforderungen adressiert als auch Hilfestellungen für eine systematische Gestaltung und nachhaltige Verankerung in der Organisation gegeben.

Im Buch werden sowohl die Anforderungen der EU-Datenschutz-Grundverordnung als auch die aus dem Kontext Informationssicherheit sowie wesentliche Normen und gesetzliche Regelungen eingeführt. Wegen der ständig zunehmenden Bedrohungslage im Cyberspace wird auch das Themenfeld Cyber-Security adressiert, um dessen wachsender Bedeutung gerecht zu werden. Cyber-Security beschreibt den Schutz vor technischen, organisatorischen und naturbedingten Bedrohungen, die die Sicherheit des Cyberspace inklusive Infrastruktur- und Datensicherheit gefährden. Es beinhaltet alle Konzepte und Maßnahmen, um Gefährdungen<sup>1</sup> zu erkennen, zu bewerten, zu verfolgen, vorzubeugen sowie Handlungs- und Funktionsfähigkeit möglichst schnell wiederherzustellen.

Neben den Herausforderungen für Datenschutz und Informationssicherheit finden Sie in diesem Buch sowohl Best-Practices für ein integriertes und ganzheitliches einfaches und effektives Management-Instrumentarium für Datenschutz und Informationssicherheit als auch einen Leitfaden, um Ihr individuelles Instrumentarium abzuleiten. Mithilfe eines

---

<sup>1</sup> Gefährdung = Bedrohung und Schwachstelle

Schritt-für-Schritt-Leitfadens werden Hilfestellungen für die individuelle Ableitung und für die Umsetzung gegeben. Die Schritte werden anhand von Beispielen erläutert.

Sowohl der Datenschutz als auch die Informationssicherheit, einschließlich der Cyber-Security, benötigen eine möglichst vollständige, konsistente und aktuelle Aufstellung aller Assets (fachliche und technische Werte des Unternehmens wie Geschäftsprozesse, Organisationsstrukturen, Applikationen, technische Bausteine und Configuration Items) für Analysen und Schutzbedarfsfeststellung.

So sind für den Datenschutz Informationen über die Verwendung von Daten (Geschäftsobjekte) in Prozessen oder Applikationen essenziell. Fragestellungen wie „Welche Prozesse oder Applikationen verwenden personenbezogene Daten in welcher Art und Weise?“ sind relevant. Auf Basis des Asset-Registers erfolgen zudem die Schutzbedarfsfeststellung und die Gefährdungsanalyse sowie die Analyse von Abhängigkeiten und Auswirkungen von technischen Schwachstellen (siehe Abschnitte 4.1 und 4.2).

Das Asset-Management kann maßgeblich durch Enterprise Architecture Management (EAM) und eine Configuration Management Database (CMDB) unterstützt werden. Durch die Kombination vom integrierten Managementsystem für Datenschutz und Informationssicherheit mit EAM und einer CMDB werden sowohl die Wirksamkeit als auch die Effizienz deutlich erhöht. Daher wird diesem Zusammenspiel ein eigenes Kapitel in diesem Buch gewidmet.

Hier setzt dieses Buch an. Das Buch liefert einerseits einen ganzheitlichen schlanken und handhabbaren Ordnungsrahmen und andererseits einen Schritt-für-Schritt-Leitfaden für die systematische maßgeschneiderte Ableitung Ihres individuellen Datenschutz- und Informationssicherheitsinstrumentariums sowie deren Operationalisierung durch direkt anwendbare Hilfestellungen.

München, im Herbst 2019

*Inge Hanschke*

## **Danksagung**

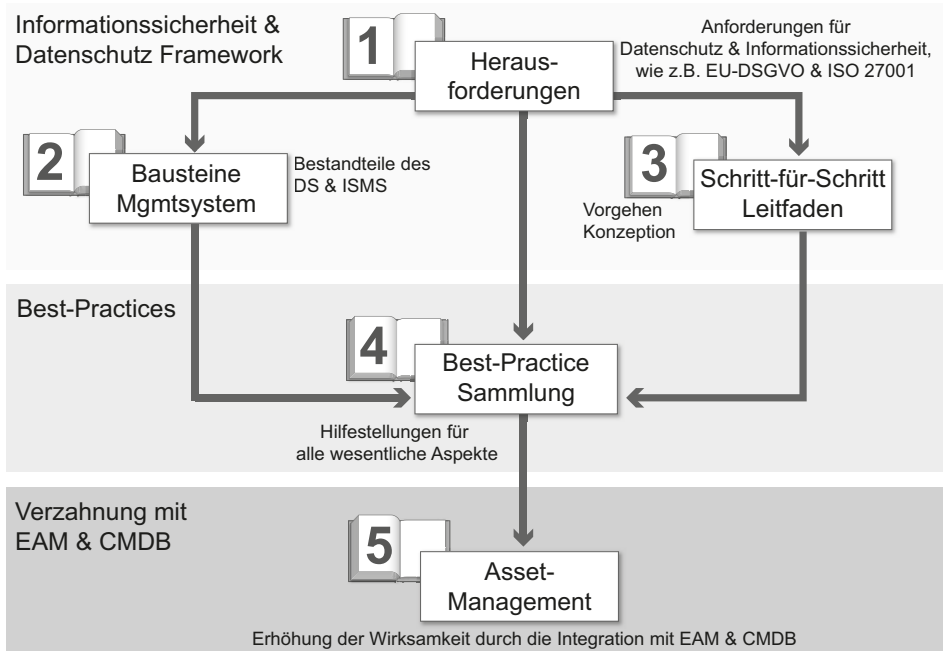
Vielen Dank an die vielen Datenschutz- und Informationssicherheitsexperten und Kollegen aus befreundeten Unternehmen für den intensiven Austausch.

Danke an meine Diskussionspartner, Reviewer und Unterstützer, die durch wertvolle Kommentare und Feedback das Buch maßgeblich mitgestaltet haben. Hier sind insbesondere Sebastian Hanschke, Christiane Charrad und auch Frau Brigitte Bauer-Schiewek sowie Frau Irene Weilhart vom Hanser-Verlag für ihr wertvolles Feedback und ihre Unterstützung zu nennen.

Besonderen Dank an Jörg Krüger, meine Familie und Freunde, die mir den Rücken freigehalten haben und mich auch durch Feedback tatkräftig unterstützt haben.

## ■ Wegweiser durch dieses Buch

Die Gliederung des Buchs ist im folgenden Bild dargestellt. Sie können die Kapitel in der genannten Reihenfolge oder aber auch selektiv lesen. Sie sind inhaltlich in sich abgeschlossen.



**Bild 1** Kapitelstruktur

- Kapitel 1 erläutert die Herausforderungen im Datenschutz und in der Informationssicherheit mit allen relevanten Sicherheitsvorgaben, wie z. B. ISO 27001, IT-Grundschutz und EU-DSGVO sowie der Cyber-Security.
- Kapitel 2 skizziert die Bausteine eines integrierten Datenschutz- und Informationssicherheitssystems.
- In Kapitel 3 finden Sie den Schritt-für-Schritt-Leitfaden für die Konzeption Ihres integrierten Instrumentariums.
- Kapitel 4 liefert Ihnen eine Best-Practice-Sammlung zur Operationalisierung Ihres Instrumentariums.
- Kapitel 5 widmet sich dem Asset-Management mit Hilfe vom Enterprise Architecture Management und einer CMDB.

Jedes Kapitel enthält darüber hinaus zahlreiche Literaturhinweise als Empfehlung für die Vertiefung des jeweiligen Themas.

## Wer sollte dieses Buch lesen?

Das Buch adressiert alle Personengruppen im Kontext Informationssicherheit und Datenschutz, die „Kümmerer“ und die „Betroffenen“, wie z. B. der Datenschutz- oder Informationssicherheitsbeauftragte sowie die Bereiche Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge. Folgende Personengruppen werden besonders adressiert:

- *Chief Information Security Officer (CISO), Informationssicherheitsbeauftragter (ISB), Beauftragte für IT-Sicherheit, Bereichs- oder Projektsicherheitsbeauftragter*
  - Wie kann das ISMS initiiert, implementiert und überwacht werden?
  - Welche Sicherheitsanforderungen bestehen? Welche Normen, wie z. B. ISO 27001, sind für das Unternehmen relevant?
  - Wie werden Sicherheitsziele und Geltungsbereich festgelegt?
  - Welche Sicherheitsmaßnahmen sind zur Umsetzung der Anforderungen erforderlich?
  - Welche Dokumente sind unter welchen Vorgaben verpflichtend? Welche Inhalte haben die Dokumente, wie z. B. die Informationssicherheitsleitlinie? Wie können diese handhabbar gestaltet werden?
  - Wie muss eine Sicherheitsorganisation für den jeweiligen Kontext gestaltet werden?
  - Wie sieht ein Sicherheitskonzept aus? Welche Best-Practices gibt es hierzu?
  - Wie kann wirksam ein Instrumentarium aufgebaut und betrieben werden?
  - Wie erfolgt die Erstellung von Plänen zur Umsetzung und Kontrolle von Sicherheitsmaßnahmen?
  - Wie kann die Wirksamkeit überprüft werden?
  - Wie kann ein ausreichendes Sicherheitsniveau definiert und implementiert werden?
  - Wie kann Informationssicherheit effizient und effektiv kontinuierlich sichergestellt werden?
  - In welche Prozesse, wie z. B. Risikomanagement, und organisatorische Strukturen muss sich das Instrumentarium verzahnen? Auf welche Art und Weise?
- *Datenschutzbeauftragte (DSB)*
  - Wie kann der Datenschutzbeauftragte der obersten Leitungsebene bei der Wahrung der Persönlichkeitsrechte und der Vermeidung von Zwischenfällen, die dem Ansehen des Unternehmens schaden, unterstützen?
  - Wie sieht ein Datenschutzkonzept aus?
  - Welche Dokumente/Meldewege sind verpflichtend? Welche Inhalte und Struktur haben diese Dokumente? Wie können diese handhabbar gestaltet werden?
  - Welche technischen und organisatorischen Maßnahmen sind relevant für die Umsetzung des Datenschutzkonzepts? Wie kann deren Wirksamkeit überprüft werden?
  - Welche organisatorischen Voraussetzungen müssen geschaffen werden?
  - Wie kann ein ausreichendes Datenschutzniveau definiert und implementiert werden?
  - Wie kann Datenschutz effizient und effektiv kontinuierlich sichergestellt werden?
  - In welche Prozesse, wie z. B. Risikomanagement, muss sich das Instrumentarium verzahnen? Auf welche Art und Weise?

- *Betriebsrat*
  - Wie können die Mitbestimmungsrechte gewahrt werden?
  - Wie können Mitarbeiter vor Sanktionen geschützt werden?
  - Wie können Mitarbeiter vor unklaren Regelungen und einschränkenden Maßnahmen geschützt werden?
- *Oberste Leitungsebene („Informationssicherheit und Datenschutz ist Chefsache“)*
  - Ist ein ISMS im Wettbewerb ein Vorteil oder ein Hygienefaktor?
  - Wie können die Unternehmenswerte hinreichend gesichert werden?
  - Wie können die Unternehmensrisiken und persönlichen Risiken beherrscht werden?
  - Wie können Informationssicherheit und Datenschutz hinreichend umgesetzt werden? Mit welcher Organisation? Ohne zu viele Aufwände? Ohne zu viele Formalismen? Wie viele Rollen und Ressourcen sind notwendig?
  - Welche Aufgaben bestehen für die oberste Leitungsebene? Welche Aufgaben können delegiert werden? Welche Verantwortung verbleibt?
- *Leiter Organisation und Führungskräfte*
  - Welche organisatorischen Voraussetzungen müssen für Informationssicherheit und Datenschutz geschaffen werden?
  - Welche organisatorischen und personellen Anforderungen bestehen und wie können diese durch angemessene Sicherheitsmaßnahmen umgesetzt werden?
  - Wie können Datenschutz- und Informationssicherheitsrisiken in das unternehmensübergreifende Risikomanagement integriert werden?
- *Einkauf*
  - Wie kann das Sicherheitsrisiko durch Lieferanten gesenkt werden? Wie können Auftragnehmer zu den für das Unternehmen festgelegten Sicherheits- und Datenschutzrichtlinien verpflichtet und in geeigneter Weise zur Einhaltung „gezwungen“ werden?
  - Wie stellt man sicher, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber unverzüglich informiert?
  - Wie kann der Aufwand bei der Lieferanten-Auditierung reduziert werden?
- *Fachverantwortliche für Geschäftsprozesse und Fachverfahren*
  - Wie können die geschäftliche Relevanz/Kritikalität der verarbeitenden Informationen, der Verarbeitungen und deren Schutzbedarf festgelegt werden?
  - Welche Sicherheits- und Kontrollmaßnahmen sind zur Verwaltung und zum Schutz der im Verantwortungsbereich befindlichen Informationen zu implementieren?
  - Wie können durch den Fachverantwortlichen der Zugang zu Informationen sowie der Umfang und die Art der Autorisierung in den Verarbeitungen definiert werden? Was ist dabei zu berücksichtigen? Wie ist die Autorisierung zu dokumentieren?
  - Welche Informationen haben welche geschäftliche Relevanz und wie können diese adäquat geschützt werden?
  - Welche Aufbewahrungsfristen müssen entsprechend der gesetzlichen Vorschriften eingehalten werden?



- *Mitarbeiter*
  - Welche Verhaltensregeln gibt es im Kontext Informationssicherheit und Datenschutz?
  - Was muss beachtet werden? Wo findet man die jeweils gültige Richtlinie und Verfahrensanweisung?
- *IT-Verantwortliche*
  - Welche Richtlinien und Verfahrensanweisungen sind für sichere IT-Unterstützung der Geschäftsprozesse relevant? Wie können diese mit den vorhandenen IT-Prozessen integriert werden?
  - Wie können IT-Servicemanagement und Informationssicherheit zusammenwirken?
  - Wie sollte eine ordnungsgemäße IT-Administration erfolgen? Welche Verhaltensregeln und Sicherheitshinweise sollten für Administratoren festgelegt werden?
  - Wie können über Sicherheitsgateways oder Firewalls Schutzzonen erstellt werden? Welche sind erforderlich?
  - Wie kann ein hinreichender Virenschutz zum Schutz vor Schadprogrammen erreicht werden?
  - Wie kann die Notfallvorsorge aussehen?
  - Was ist bei der Datensicherung zu beachten?
  - Welche Daten sind zu archivieren? Welche Aufbewahrungsfristen gelten?
  - Wie kann die sichere Nutzung von E-Mail und Groupware gewährleistet werden?
  - Was ist bei Outsourcing und externen Dienstleistern zu beachten?

### **Webseite zum Buch**

Weitergehende Informationen zum Buch finden Sie auf den Webseiten <https://Lean42.com> und <https://LeanISMS.de>, außerdem unter <https://www.hanser-fachbuch.de/978-3-446-45818-5>. Auf dieser Buchdetailseite klicken Sie auf die Registerkarte LINKS.

# Stichwortverzeichnis

## A

Access Management 27  
Agilität 163  
Anforderungsmanagement 163  
Anwendungsentwicklung 163  
Anwendungsfeld 163  
API-Management 163  
Applikationsarchitektur 146  
Arbeitsanweisung 65, 163  
Areal 163  
Asset 163  
Asset-Management 88, 98  
Auftragskontrolle 59  
Auftragsverarbeitung 48, 163  
Authentisierung 164  
Authentizität 104  
Autorisierung 164

## B

Baseline 164  
Basis-Absicherung 40  
Basis-Infrastruktur 164  
Beauftragte für Informationssicherheit (ISB) 86  
Bebauung 164  
Bebauungsplan 164  
Bebauungsplaner 164  
Bebauungsplangrafik 165  
Bebauungsplanung 165  
Bedrohung 165  
Benchmark 165  
Best Practices 165  
Betriebsinfrastrukturarchitektur 146  
BI 166  
Blueprint 165  
BSI-Standards 38  
Budgetierung 165  
Business-Alignment der IT 150, 165  
Business-Analyse 165  
Business-Analyst 165

Business Analytics 166  
Business Capability 166  
Business Capability Management 166  
Business Capability Map 166  
Business Continuity Management 68, 166  
Business Intelligence 166  
Business-IT 166  
Business-IT-Koordination 167  
Business-Plan 167  
Business-Planung 167  
Business-Service 167  
Business-Transformation 167  
BYOD 30

## C

Change Management 167  
Change Request 167  
Chatbots 167  
Chief Digital Officer 168  
CIO 168  
Cloud-Computing 168  
Cluster-Analyse 168  
CMDB 169  
CMMI 168  
CobiT 168  
Cockpit 168  
Commodity 168  
Compliance 14, 169  
Consumerisation 30, 169  
Controlling 169  
COTS 168  
Cyber-Physical Systeme (CPS) 169  
Cyber-Security 15  
Cyber-Sicherheit 3, 179

## D

Data Governance 169  
Data Lake 170  
Data Profiling 171

- Data Scientist 171
  - Data Steward 171
  - Daten-Cluster 170
  - Datenmanagement 170
  - Datenminimierung 50, 105
  - Datenschutz 3, 104, 108, 171
  - Datenschutzbeauftragter (DSB) 47, 71, 138
  - Datenschutz-Folgenabschätzung 51
  - Datenschutz-Grundverordnung (DSGVO) 8, 44
  - Datenschutzpolitik 62
  - Datensicherung 171
  - Datentransparenz 50
  - Demand Management 171
  - DevOps 171
  - Dienst 188
  - Dienstleistungs- und Produktportfolio 171
  - Digitalisierung 171
  - Disruption 171
  - Disziplin 171
  - Dokumentenlenkung 20, 100, 172
  - Dokumentenpyramide 62
  - Domäne 172
  - DS & ISMS 172
    - Integriertes Managementsystem für Daten-  
schutz und Informationssicherheit 61, 172
  - Due Diligence 172
- E**
- EAM 172
  - Eingabekontrolle 59
  - Einwilligung des Betroffenen 49
  - End-to-end 172
  - Enterprise Architecture 192
  - Enterprise Architecture Framework 172
  - Enterprise Architecture Management 147, 172
  - Ergebnistyp 172
  - Erklärung zur Anwendbarkeit 25
  - EU-Datenschutz-Grundverordnung 6
  - EU-DSGVO 6, 8, 44
- F**
- Fachliche Bebauung 172
  - Fachliche Domäne 173
  - Fachliches Domänenmodell 173
  - Fachliche Funktion 173
  - Fachliches Klassenmodell 173
  - Fachliches Komponentenmodell 173
  - FAIT 11
  - Fertigungstiefe 173
  - Fragestellungen 147
- G**
- GAP-Analyse 89
  - Gefahr 173
  - Gefährdung 173
  - Geheimchutz 11
  - Geschäftsanforderung 174
  - Geschäftsarchitektur 146, 174
  - Geschäftseinheit 174
  - Geschäftsfunktion 167
  - Geschäftsmodell 174
  - Geschäftsobjekt 174
  - Geschäftspartner 174
  - Geschäftsprozess 175
  - Geschäftsregel 175
  - Geschäftstreiber 175
  - Goldene Regeln der Informationssicherheit 44
  - Governance 175
  - Granularität 175
  - Gremium 175
- H**
- Handlungsbedarf 175
- I**
- Identity Management 27
  - Identity- und Accessmanagement (IAM) 27
  - Incident Management 175
  - Indikator 175
  - Informationsflussgrafik 175
  - Informationsklassifizierung 99
  - Informationssicherheit 3, 175
  - Informationssicherheitsbeauftragter (ISB) 71, 138
  - Informationssicherheitsleitlinie 22, 81, 176
  - Informationssicherheitsmanagementsystem (ISMS) 17
  - Informationssicherheitsstrategie 62, 176
  - Informationssicherheitssystem 176
  - Informationssystem 176
  - Informationssystembebauung 176
  - Infrastrukturbebauung 176
  - Infrastrukturelemente 176
  - Infrastruktur-Service 176
  - Infrastruktursysteme 177
  - Insourcing 177
  - Integrationsarchitektur 177
  - Integrität 97, 102
  - Intervenierbarkeit 105
  - Investitionsplanung 177
  - IS-Bebauung 176

IS-Domäne 177  
 IS-Kategorie 177  
 IS-Landschaft 177  
 Ist-Bebauung 177  
 Ist-Zustand 177  
 IT-Architektur 178  
 IT-Bebauungsmanagement 178  
 IT-Board 178  
 IT-Commodity 178  
 IT-Dienstleistungs- und Produktportfolio 178  
 IT-Funktion 178  
 IT-Funktionalität 178  
 IT-Governance 178  
 IT-Grundschatz-Kompodium 38  
 IT-Kaufprodukt 179  
 IT-Konsolidierung 179  
 IT-Koordinatoren-Gremium 179  
 IT-Landschaft 179  
 IT-Management 179  
 IT-Nutzerrichtlinie 70  
 IT-Produkt 179  
 IT-Projektportfolio 179  
 IT-Revision 179  
 IT-Sicherheit 3, 179  
 IT-Strategie 180  
 IT-Strategieentwicklung 180  
 IT-System 180  
 Iteration 180  
 ITIL 180

## K

Katastrophe 130, 180  
 Kennzahl 180  
 Kennzahlensystem 181  
 Kern-Absicherung 41  
 Kernkompetenz 181  
 Kernprozesse 181  
 Key-User 181  
 Kommunikationsplan 20, 141  
 Kontrolle 181  
 KPI 181  
 Krise 129, 181  
 Kronjuwelen 41, 109  
 Kryptokonzept 68, 114, 181  
 Kumulationseffekt 111  
 KVP 73

## L

Laufzeitumgebung 181  
 Leitlinie 181

Lieferantenmanagement 182  
 Lifecycle 182  
 Lokation 182  
 Löschkonzept 32

## M

Managementsystem für Informationssicherheit  
 und Datenschutz (DS & ISMS) 77  
 Mandant 182  
 Maßnahme 182  
 Masterplan 182  
 Masterplan-Grafik 182  
 Maturity Level 182  
 Maximumprinzip 111  
 Methode 182  
 Migrationsstrategie 182  
 Mittelfristplanung 182  
 Modell 183  
 Modernisierter IT-Grundschatz 37, 85  
 Monitoring 183  
 Multiprojektmanagement 183  
 MVP *siehe* Minimum Viable Product

## N

Nichtabstreitbarkeit 104  
 Nichtverkettung 105  
 Notfall 129, 183  
 Notfallhandbuch 132  
 Notfallkonzept 132  
 Notfallmanagement 166  
 Notfallorganisation 128, 131  
 Notfallvorsorgekonzept 132

## O

Offshoring 183  
 Operational Excellence 183  
 Operational Model 183  
 Operative Ausrichtung 184  
 Operatives Prozessmanagement 184  
 Opportunitätskosten 184  
 Organisationseinheit 184  
 Organisationsstruktur 184  
 O-Ton Kunde 184  
 Outsourcing 184  
 Owner 184

## P

Penetrationstest 184  
 Performance Management 184  
 Pflegekonzept 184

- Planung 185
  - Plattform 185
  - Plattform-API 185
  - Portfolio 185
  - Portfolioanalyse 185
  - Portfoliografik 185
  - Portfoliomanagement 185
  - Prämisse 185
  - Prinzipien 185
  - Privacy by design und by default 50
  - Produkt 185
  - Produkt-Lifecycle 185
  - Produktmanagement 186
  - Produktmanager 186
  - Produktplanung 186
  - Profiling 49
  - Programm 186
  - Projekt 186
  - Projektantrag 186
  - Projektidee 186
  - Projektportfolio 186
  - Projektportfolio-Board 186
  - Projektportfoliomanagement 187
  - Projektportfolioplanung 187
  - Projektsteuerkreis 187
  - Provisioning 27
  - Prozesslandkarte 187
  - Prozessmanagement 187
- Q**
- Qualitätsmanagement 187
  - Quality Gate 187
  - Quick Win 188
- R**
- Rechtmäßigkeit der Verarbeitung 49
  - Reifegradmodell 43, 188
  - Release 188
  - Releasemanagement 188
  - Richtlinie 64, 188
  - Risiko 188
  - Risikoakzeptanzkriterien 125
  - Risikoappetit 5, 125
  - Risikobehandlung 125
  - Risikofolgenabschätzung 48
  - Risikoidentifikation 123
  - Risikomanagement 121, 188
  - Risikoreduzierung 125
  - Risikotransfer 125
  - Risikoübernahme 126
- Risikovermeidung 125
- S**
- Schnittstelle 188
  - Schutzbedarf 106
  - Schutzbedarfsfeststellung 89, 106
  - Schutzbedarfskategorien 98
  - Schutzziel 98
  - Schwachstelle 188
  - Schwachstellenmanagement 127
  - Service 188
  - Service-IT 189
  - Service-Level-Management 189
  - Servicemanagement 189
  - Sicherheitsarchitektur 189
  - Sicherheitsereignis 189
  - Sicherheitsniveau, Risikoappetit 5
  - Sicherheitsnotfall 189
  - Sicherheitsorganisation 42
  - Sicherheitsvorfall 189
  - SLA 189
  - SoA 25
  - Sourcing-Strategie 189
  - Sponsor 189
  - Stakeholder 189
  - Stakeholder-Analyse 189
  - Stakeholder-Gruppe 189
  - Standard-Absicherung 40
  - Standard-Datenschutzmodell (SDM) 53
  - Stellgröße 190
  - Steuerkreis 190
  - Steuerungsgröße 190
  - Steuerungsinstrumentarium 190
  - Steuerungsobjekt 190
  - Störung 129, 190
  - Strategic Excellence 190
  - Strategie 190
  - Strategiebeitrag 191
  - Strategien 191
  - Strategische Ausrichtung 191
  - Strategisches IT-Controlling 191
  - Strategische IT-Maßnahmenplanung 191
  - Strategisches IT-System 191
  - Szenario 191
- T**
- Tailoring 191
  - Taktische Ausrichtung 191
  - Technische Architektur 146
  - Technische Bausteine 191

- Technische Bebauung 191
  - Technische Domäne 191
  - Technische Standardisierung 192
  - Themenbereich 192
  - Transparenz 105
  - Trennungsgebot 59
  - Trusted Zone 115
- U**
- Unternehmensarchitektur 192
  - Unternehmensplanung 192
  - Unternehmenssteuerung 192
  - Unternehmensstrategie 193
  - Unternehmensstrategieentwicklung 193
  - Unterstützende Prozesse 193
  - Use-Case 193
- V**
- Verantwortlichkeit 193
  - Verbindlichkeit 193
  - Verfahren 193
  - Verfahrensweisung 65, 193
  - Verfügbarkeit 97, 103
  - Verfügbarkeitskontrolle 59
  - Verschlusssache 11
  - Verteilungseffekt 111
- Vertraulichkeit 97, 98
  - Verzeichnis der Verarbeitungstätigkeiten 46
  - Vision 194
  - Vorhaben 194
  - Vulnerability 16
- W**
- Wartung 194
  - Wartungsmaßnahme 194
  - Weitergabekontrolle 59
  - Wertbeitrag 194
  - Wertschöpfungskette 194
  - Wiederanlaufpunkt (RPO) 103
  - Wiederanlaufzeit (RTO) 103
  - Wiederherstellzeit (RTO) 103
  - Wissensmanagement 194
- Z**
- Ziel 194
  - Zonenkonzept 114
  - Zugangskontrolle 58
  - Zugriffskontrolle 58
  - Zurechenbarkeit 104
  - Zuständigkeit 194
  - Zutrittskontrolle 58
  - Zweckbindung 50