

## 19 Abbildungsverzeichnis

Abbildung 2-1:	Pyramidenmodell® .....	28
Abbildung 5-1:	ISO-27000-Familie (Teil 1/2).....	94
Abbildung 5-2:	ISO-27000-Familie (Teil 2/2).....	95
Abbildung 6-1:	Schutzobjektclassen .....	128
Abbildung 6-2:	Detaillierter Sicherheitsdreiklang <sup>Dr.-Ing. Müller</sup> .....	130
Abbildung 6-3:	Detaillierter Risikodreiklang <sup>Dr.-Ing. Müller</sup> .....	132
Abbildung 7-1:	Sicherheitspyramide <sup>Dr.-Ing. Müller</sup> , Version V bzw. Sicherheitsmanagementpyramide <sup>Dr.-Ing. Müller</sup> , Version V.....	139
Abbildung 10-1:	House of Occ. Health, Safety, Security and Continuity (HHSSC) .....	192
Abbildung 10-2:	Occ. Health, Safety, Security and Continuity Function Deployment (OHSSCFD) .....	193
Abbildung 11-1:	Risikolandkarte und Risikoklassen (Beispiel) .....	211
Abbildung 11-2:	Prinzipielles Kontext-Diagramm zur Pfadanalyse .....	222
Abbildung 11-3:	Kern-, Support- und Begleitprozesse im Lebenszyklus .....	242
Abbildung 11-4:	Begleitprozesse (Managementdisziplinen).....	249
Abbildung 11-5:	Risiko(management)pyramide <sup>Dr.-Ing. Müller</sup> , Version V .....	265
Abbildung 11-6:	Risikoermittlung auf Basis des Risikodreiklangs <sup>Dr.-Ing. Müller</sup> .....	267
Abbildung 11-7:	Business Continuity Management mit der Sicherheitspyramide V ...	302
Abbildung 11-8:	Kontinuitätspyramide <sup>Dr.-Ing. Müller</sup> , Version V bzw. Kontinuitätsmanagementpyramide <sup>Dr.-Ing. Müller</sup> , Version V.....	303
Abbildung 11-9:	Business Continuity Pyramid <sup>Dr.-Ing. Müller</sup> , Version V or BCM pyramid <sup>Dr.-Ing. Müller</sup> , Version V .....	304
Abbildung 11-10:	Datensicherungsmethoden .....	323
Abbildung 11-11:	Über-Kreuz-Sicherung.....	327
Abbildung 11-12:	Allgemeines Sicherheitsschalenmodell <sup>Dr.-Ing. Müller</sup> .....	330
Abbildung 11-13:	Elemente des Securitymanagements gemäß Sicherheitsschalen- modell <sup>Dr.-Ing. Müller</sup> .....	335
Abbildung 11-14:	Berechtigungswürfel bzw. -kubus .....	336
Abbildung 11-15:	Subjekt-Subjektgruppe-Recht-Objektgruppe-Objekt-Modell.....	337
Abbildung 11-16:	Taschenauthenticator (Prinzipdarstellung) .....	348
Abbildung 11-17:	Verschlüsselungsverfahren.....	363
Abbildung 11-18:	Speichermedien .....	394
Abbildung 11-19:	DAS, NAS, SAN .....	399
Abbildung 11-20:	Firewallebenen (Prinzipdarstellung).....	403
Abbildung 11-21:	Interdependenznetz (prinzipielles und vereinfachtes Beispiel).....	418
Abbildung 12-1:	Notfallablauf.....	456
Abbildung 12-2:	Eskalationstrichter <sup>Dr.-Ing. Müller</sup> .....	458
Abbildung 16-1:	Sicherheits-/RiSiKo-Studie/-Analyse .....	499
Abbildung 16-2:	Sicherheitsregelkreis .....	504
Abbildung 17-1:	Reifegradmodell <sup>Dr.-Ing. Müller</sup> , hier für Sicherheit und RiSiKo .....	521
Abbildung 18-1:	Sicherheits-(management-)prozess <sup>Dr.-Ing. Müller</sup> .....	529

## 20 Tabellenverzeichnis

Tabelle 3-1:	Zehn Schritte zum Sicherheitsmanagement.....	35
Tabelle 9-1:	Primäre und sekundäre Sicherheitskriterien.....	177
Tabelle 9-2:	Schadensszenarien.....	182
Tabelle 11-1:	Sicherheitszonen-Maßnahmen-Matrix.....	229
Tabelle 11-2:	Prinzipien versus Sicherheitskriterien.....	240
Tabelle 11-3:	Datenschutzkontrollen.....	259
Tabelle 11-4:	Prozentuale Verfügbarkeit und maximale Ausfalldauer.....	307
Tabelle 11-5:	Vor- und Nachteile von Datensicherungsmethoden.....	324
Tabelle 11-6:	Verschlüsselungsverfahren und Standards.....	364
Tabelle 11-7:	Sicherheits-Hash-Algorithmen.....	366
Tabelle 11-8:	Sicherheitskriterien und Schutzmaßnahmen.....	369
Tabelle 11-9:	Präventive Datenträgererneuerung.....	395
Tabelle 11-10:	Schutzmaßnahmen und Sicherheitsklassen (Gebäude, Räume, Versorgung).....	415
Tabelle 11-11:	RiSiKo-Architekturmatrix.....	419
Tabelle 12-1:	Definitionen für Störung, Notfall, Krise, Katastrophe im Überblick.....	444
Tabelle 18-1:	RiSiKo-Managementprozess (Input, Aktivitäten, Methoden, Ergebnisse) ... .....	534

## 21 Verzeichnis der Checklisten

Checkliste 8-1:	Kontrollen zur Sicherheits-, Kontinuitäts- und Risikopolitik.....	158
Checkliste 11-1:	Kontrollen zum Konformitätsmanagement (Compliance Management).....	254
Checkliste 11-2:	Kontrollen zum Datenschutzmanagement.....	261
Checkliste 11-3:	Kontrollen zum Kontinuitätsmanagement.....	328
Checkliste 17-1:	Reifegradmodell <sup>Dr.-Ing. Müller</sup> .....	527

## 22 Verzeichnis der Beispiele

Beispiel 8-1:	Sicherheits-, Kontinuitäts- und Risikopolitik .....	166
Beispiel 9-1:	Tabelle Schutzbedarf der Prozesse.....	183
Beispiel 9-2:	IKT-Schutzbedarfsanalyse.....	188
Beispiel 9-3:	Schutzbedarfsklassen in Tabellenform .....	189
Beispiel 9-4:	Schutzbedarfsklassen in Matrixform .....	190
Beispiel 10-1:	Sicherheitskriterium Verfügbarkeit: Einflussfaktoren (Auszug) .....	197
Beispiel 10-2:	Maßnahmen-Klassen-Matrix (MKM) .....	199
Beispiel 11-1:	Bedrohungslandkarte (Auszug) .....	206
Beispiel 11-2:	Physische Sicherheitszonen (schematisch).....	227
Beispiel 11-3:	Risikoinventar (Auszug) .....	268
Beispiel 11-4:	Bruttoisikomatrix.....	271
Beispiel 12-1:	Richtlinie Sourcing .....	430
Beispiel 12-2:	Richtlinie Fax-Nutzung .....	431
Beispiel 12-3:	IKT-Benutzerordnung.....	433
Beispiel 12-4:	Richtlinie E-Mail-Nutzung .....	435
Beispiel 12-5:	Richtlinie Internet-Nutzung.....	437
Beispiel 12-6:	Sicherheits-, Kontinuitäts- und Risikomanagement: Struktur .....	440
Beispiel 12-7:	Richtlinie Kapazitätsmanagement .....	441
Beispiel 12-8:	Anforderungen an sicherheitsrelevante Räumlichkeiten.....	449
Beispiel 12-9:	Richtlinie Datensicherung .....	451
Beispiel 12-10:	Gliederungsstruktur Notfallhandbuch (Auszug) .....	455
Beispiel 12-11:	Richtlinie Vorbeugender Brandschutz (Auszug).....	459
Beispiel 12-12:	Formblatt Drohanruf.....	460
Beispiel 12-13:	Richtlinie Berichtswesen Kontinuitätsmanagement .....	463
Beispiel 12-14:	Richtlinie Zufahrtsschutz .....	466
Beispiel 12-15:	Richtlinie Zutrittsschutz .....	469
Beispiel 12-16:	Richtlinie für den Umgang mit Schlüsseln und Zutrittskarten .....	470
Beispiel 12-17:	Richtlinie Benutzererkennung .....	470
Beispiel 12-18:	Passwortregeln: Gebote .....	471
Beispiel 12-19:	Passwortregeln: Verbote.....	472
Beispiel 12-20:	Passwortheigenschaften: Verbote.....	472
Beispiel 12-21:	Richtlinie zum Schutz vor Schadsoftware.....	473
Beispiel 12-22:	Richtlinie Leseschutz .....	474
Beispiel 12-23:	Protokollierungsanforderungen je Sicherheitsklasse .....	474
Beispiel 12-24:	Protokolldaten je Sicherheitselement.....	475
Beispiel 12-25:	Richtlinie Architekturmanagement (Unternehmen).....	475
Beispiel 12-26:	Richtlinie Zutrittskontrollsystem / Zutrittskontrollanlage .....	476
Beispiel 12-27:	Passwortbezogene Systemanforderungen .....	477
Beispiel 12-28:	Funktionen, Rollen und Tätigkeiten im Sicherheitsmanagement.....	477
Beispiel 13-1:	Dokumentationsvorlage Datensicherung .....	480
Beispiel 13-2:	Systemspezifische Passwordeinstellungen .....	481
Beispiel 14-1:	Protokoll der Passwordeinstellungen .....	482
Beispiel 16-1:	HAZOP-Matrix.....	501
Beispiel 16-2:	Kennzahlcharakteristika.....	509

## 23 Verzeichnis der Tipps

Tipp 4-1:	Datenschutz: Internationale Unternehmen.....	50
Tipp 4-2:	Organisationsrichtlinien: Prinzip des sachverständigen Dritten.....	72
Tipp 4-3:	ISMS-Vorgehensweise.....	73
Tipp 4-4:	Outsourcing: Datenschutz.....	78
Tipp 4-5:	Mindestanforderungen: MaRisk BA und VA.....	86
Tipp 4-6:	Compliance-Risiko.....	88
Tipp 9-1:	Prozessinformationsdatenbank.....	173
Tipp 11-1:	Probleme erst im Betrieb.....	288
Tipp 11-2:	Notfallübung, Zielvereinbarung, Eskalation.....	315
Tipp 11-3:	Schutz mobiler Daten.....	364
Tipp 11-4:	Quellcode in neutraler Hand.....	380
Tipp 11-5:	Vertrags- und Services-Datenbank.....	381
Tipp 11-6:	Speichermedien: Präventive Wartung.....	395

## 24 Verzeichnis der Informationen

Information 1-1:	Ausfälle und Bedrohungen.....	17
Information 1-2:	Ausfälle und Sicherheitsverletzungen: Folgen und Kosten .....	22
Information 4-1:	Vorstand und Aufsichtsrat: Mögliche Pflichtverletzung .....	38
Information 4-2:	Compliance Officer: Garantienpflicht.....	40
Information 4-3:	Datenschutzverletzungen: Hohe Strafen .....	50
Information 4-4:	Datenschutz: Safe-Harbour-Abkommen.....	52
Information 8-1:	BCM-Planungshorizont, Mindestszenarien, Kontinuitätsmanagement .....	155
Information 11-1:	Technologischer Wandel .....	208
Information 11-2:	Entfernung zwischen redundanten Räumlichkeiten.....	237
Information 11-3:	Arbeitsunfälle .....	255
Information 11-4:	Sicherheit bei der E-Mail-Übertragung .....	257
Information 11-5:	Unerkannte Risiken .....	262
Information 11-6:	Auslagerungen bei Banken .....	275
Information 11-7:	Ausfallkosten .....	308
Information 11-8:	Interner Alarm- und Gefahrenabwehrplan .....	311
Information 11-9:	Biometrie .....	346
Information 11-10:	Körperscanner an deutschen Flughäfen.....	359
Information 11-11:	Erkennung von Sprengstoffen und gefährlichen Objekten .....	360
Information 11-12:	GoBD.....	361
Information 11-13:	Passwort-Knacken.....	365
Information 11-14:	Transportsicherheit .....	371
Information 11-15:	Forensische Codes und digitaler Fingerabdruck .....	374
Information 11-16:	Screening zur Terrorismusbekämpfung .....	385
Information 11-17:	Spear-Phishing.....	386
Information 11-18:	Speichermedien: Risiko veralteter Speichertechnologien.....	395
Information 11-19:	Steigender Speicherplatzbedarf .....	398
Information 12-1:	Hash-Algorithmen: Sicherheit.....	474
Information 17-1:	Unerkannte Risiken und Unvorhergesehenes.....	523

## 25 Markenverzeichnis

Die folgenden Angaben erfolgen ohne Gewähr und ohne Haftung. Es gelten stets die entsprechenden Schutzbestimmungen und -rechte in ihrer jeweils aktuellen Fassung.

AICPA® ist eine eingetragene Marken des American Institute of Certified Public Accountants.

Balanced Pyramid Scorecard® ist eine eingetragene Marke von Dr.-Ing. Klaus-Rainer Müller. CERT® und CERT Coordination Center® (CERT®/CC) sind eingetragene Marken der Carnegie Mellon University.

Certified Information Security Manager®, CISM®, Certified Information Security Auditor™, CISA®, Certified in the Governance of Enterprise IT®, CGEIT®, Certified in Risk and Information Systems Control™ und CRISC™, sind Marken bzw. eingetragene Marken der Information Systems Audit and Control Association®, Inc. (ISACA®).

CMM®, CMMI®, Capability Maturity Model®, Capability Maturity Model Integration® sind eingetragene Marken der Carnegie Mellon University.

COBIT® ist eine eingetragene Marke der Information Systems Audit and Control Association® (ISACA®) und des IT Governance Institute®.

DMTF® ist eine eingetragene Marke der DMTF Distributed Management Task Force, Inc.

Excel® ist eine eingetragene Marke der Microsoft Corporation.

GAMP® ist eine eingetragene Marke der International Society for Pharmaceutical Engineering.

IDEA™ ist eine Marke der Ascom Systec Ltd.

Information Systems Audit and Control Association® und ISACA® sind eingetragene Marken der Information Systems Audit and Control Association®.

IT Governance Institute® und ITGI® sind eingetragene Marken der Information Systems Audit and Control Association®.

ITIL® ist eine eingetragene Marke der AXELOS Limited.

Kerberos™ ist eine Marke des Massachusetts Institute of Technology (MIT).

Microsoft®, Windows®, NT® sind eingetragene Marken der Microsoft Corporation.

Mind Map® ist eine eingetragene Marke der Buzan Organisation Ltd.

MISRA® und MISRA C® sind eingetragene Marken der MIRA Ltd.

Nagios® ist eine eingetragene Marke von Nagios Enterprises.

OCTAVE® ist eine eingetragene Marke der Carnegie Mellon University.

PRINCE® und PRINCE2® sind eingetragene Marken der AXELOS Limited.

Pyramidenmodell® ist eine eingetragene Marke von Dr.-Ing. Klaus-Rainer Müller.

RC5™ ist eine Marke der RSA Security Inc.

SA8000® ist eine eingetragene Marke von Social Accountability International (SAI).

SOC 1®, SOC 2® sind eingetragene Marken des American Institute of Certified Public Accountants.

SOC 3<sup>SM</sup> ist eine eingetragene Service-Marke des American Institute of Certified Public Accountants.

Stratus® und Continuous Processing® sind eingetragene Marken von Stratus Technologies Bermuda Ltd.

TOGAF® ist eine eingetragene Marke der „The Open Group“.

UNIX® ist eine eingetragene Marke der „The Open Group“.

Wi-Fi® ist eine eingetragene Marke der Wi-Fi Alliance.

## 26 Verzeichnis über Gesetze, Vorschriften, Standards, Normen

Die folgenden Unterkapitel nennen einige Gesetze, Verordnungen, Ausführungsbestimmungen, Grundsätze, Vorschriften, Standards und Normen, die im Zusammenhang mit dem Thema Sicherheits-, Kontinuitäts- und Risikomanagement eine Rolle spielen. Diese sind teils branchenübergreifend und teils branchenspezifisch. Sie behandeln z. B. Themen wie Sorgfaltspflicht der Vorstandsmitglieder, Überwachungssystem, Risiken, Notfallplanung, Datenschutz und Ordnungsmäßigkeit.

### Lagebericht zur Informationssicherheit 2014 der <kes> [84]

Aufgrund der in [84] erhobenen Informationen ist das Bundesdatenschutzgesetz (BDSG) bei den Teilnehmern an der Sicherheitsstudie mit rund 95% am bekanntesten und für über 90% der Befragten auch relevant. Demgegenüber sind z. B. das Telekommunikationsgesetz (TKG) und die Telekommunikations-Überwachungsverordnung (TKÜV) knapp über 80%, das Telemediengesetz (TMG) rund 74% sowie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) nur noch weniger als 70% der Befragten bekannt. Dies ist insofern ein wenig ernüchternd, als Gesetze und Verordnungen z. B. für die Protokollierung auf Firewalls, Web- und Mail-Servern (s. a. [85]) eine hohe Bedeutung besitzen und das KonTraG die Einrichtung eines Risikomanagementsystems fordert.

## 26.1 Gesetze, Verordnungen, Richtlinien

### 26.1.1 Deutschland: Gesetze, Verordnungen

AO	Abgabenordnung
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
AMG	Arzneimittelgesetz
AMWHV	Arzneimittel- und Wirkstoffherstellungsverordnung
ArbSchG	Arbeitsschutzgesetz
ASiG	Arbeitssicherheitsgesetz
ArbStättV	Arbeitsstättenverordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BImSchG	Bundes-Immissionsschutzgesetz (Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge)
BImSchV 12	Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes
BSiG	BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik)

<i>ChemG</i>	Chemikaliengesetz
<i>EnWG</i>	Energiewirtschaftsgesetz
<i>GmbHG</i>	GmbH-Gesetz
<i>GwG</i>	Geldwäschegesetz
<i>HGB</i>	Handelsgesetzbuch
<i>KAGB</i>	Kapitalanlagegesetzbuch
<i>KAVerOV</i>	Kapitalanlage-Verhaltens- und -Organisationsverordnung
<i>KonTraG</i>	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
<i>KWG</i>	Kreditwesengesetz
<i>PatG</i>	Patentgesetz
<i>PfandBG</i>	Pfandbriefgesetz
<i>ProdHaftG</i>	Produkthaftungsgesetz
<i>ProdSG</i>	Produktsicherheitsgesetz
<i>SGB</i>	Sozialgesetzbuch
<i>SGB IV</i>	Viertes Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung
<i>SGB VII</i>	Siebtes Sozialgesetzbuch – Gesetzliche Unfallversicherung
<i>SGB X</i>	Zehntes Sozialgesetzbuch – Sozialverfahren und Sozialdatenschutz
<i>SigG</i>	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
<i>SigV</i>	Verordnung zur elektronischen Signatur (Signaturverordnung)
<i>SolvV</i>	Solvabilitätsverordnung
<i>TKG</i>	Telekommunikationsgesetz
<i>TKÜV</i>	Telekommunikations-Überwachungsverordnung (Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation)
<i>TMG</i>	Telemediengesetz
<i>UMAG</i>	Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts
<i>UmweltHG</i>	Umwelthaftungsgesetz
<i>UrhG</i>	Urheberrechtsgesetz
<i>VAG</i>	Versicherungsaufsichtsgesetz (Gesetz über die Beaufsichtigung der Versicherungsunternehmen)
<i>WpHG</i>	Wertpapierhandelsgesetz (Gesetz über den Wertpapierhandel)
<i>ZAG</i>	Zahlungsdienstenaufsichtsgesetz

### 26.1.2 Österreich: Gesetze, Verordnungen

<i>BWG</i>	Bankwesengesetz (Bundesgesetz über das Bankwesen)
<i>DSG 2000</i>	Datenschutzgesetz 2000



<i>InfoSiG</i>	Informationssicherheitsgesetz (Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen)
<i>InfoSiV</i>	Informationssicherheitsverordnung (Verordnung der Bundesregierung über die Informationssicherheit)
<i>VAG</i>	Versicherungsaufsichtsgesetz

### 26.1.3 Schweiz: Gesetze, Verordnungen, Rundschreiben

<i>ArG</i>	Arbeitsgesetz
<i>BankG</i>	Bankengesetz (Bundesgesetz über die Banken und Sparkassen)
<i>BankV</i>	Bankenverordnung (Verordnung über die Banken und Sparkassen)
<i>BEHG</i>	Börsengesetz (Bundesgesetz über die Börsen und den Effektenhandel)
<i>DSG</i>	Bundesgesetz über den Datenschutz
<i>EnG</i>	Energiegesetz
<i>FINMA-RS 08/7</i>	Rundschreiben 2008/7, Outsourcing Banken – Auslagerung von Geschäftsbereichen bei Banken, Stand: 6. Dezember 2012
<i>FINMA-RS 08/21</i>	Rundschreiben 2008/21, Operationelle Risiken Banken – Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken, Stand: 27. März 2014
<i>FINMA-RS 08/24</i>	Überwachung und interne Kontrolle Banken – Überwachung und interne Kontrolle bei Banken, Stand: 6. Dezember 2012
<i>FINMA-RS 08/32</i>	Rundschreiben 2008/32, Corporate Governance Versicherer – Corporate Governance, Risikomanagement und Internes Kontrollsystem bei Versicherern
<i>FINMA-RS 08/35</i>	Rundschreiben 2008/35, Interne Revision Versicherer – Interne Revision bei Versicherern, Stand: 6. Dezember 2012
<i>GeBüV</i>	Geschäftsbücherverordnung (Verordnung über die Führung und Aufbewahrung der Geschäftsbücher)
<i>GwG</i>	Geldwäschereigesetz (Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung im Finanzsektor)
<i>GwV-FINMA</i>	Geldwäschereiverordnung-FINMA (Verordnung der Eidgenössischen Finanzmarktaufsicht über die Verhinderung von Geldwäscherei und Terrorismusfinanzierung)
<i>KAG</i>	Kollektivanlagengesetz (Bundesgesetz über die kollektiven Kapitalanlagen)
<i>PfG</i>	Pfandbriefgesetz
<i>UVG</i>	Bundesgesetz über die Unfallversicherung
<i>VAG</i>	Versicherungsaufsichtsgesetz (Bundesgesetz betreffend die Aufsicht über Versicherungsunternehmen)
<i>VDSG</i>	Verordnung zum Bundesgesetz über den Datenschutz
<i>VUV</i>	Verordnung über die Unfallverhütung

### 26.1.4 Großbritannien: Gesetze, Vorschriften

<i>FoIA</i>	Freedom of Information Act (FoIA) 2000
<i>HASAW,</i> <i>HSW,</i> <i>HSWA</i>	The Health and Safety at Work etc Act 1974, hinsichtlich Strafen geändert durch The Health and Safety (Offences) Act 2008
	Management of Health and Safety at Work Regulations
	Workplace Regulations

### 26.1.5 Europa: Entscheidungen, Richtlinien, Practices

<i>Entscheidung</i> <i>2000/520/EG</i>	Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/520/EG
<i>Entscheidung</i> <i>2002/16/EG</i>	Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG
<i>Richtlinie</i> <i>89/654/EWG</i>	Richtlinie 89/654/EWG des Rates vom 30. November 1989 über Mindestvorschriften für Sicherheit und Gesundheitsschutz in Arbeitsstätten (Erste Einzelrichtlinie im Sinne des Artikels 16 Absatz 1 der Richtlinie 89/391/EWG)
<i>Richtlinie</i> <i>95/46/EG</i>	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
<i>Richtlinie</i> <i>2000/31/EG</i>	Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“)
<i>Richtlinie</i> <i>2001/20/EG</i>	Richtlinie 2001/20/EG des Europäischen Parlaments und des Rates vom 4. April 2001 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Anwendung der guten klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Humanarzneimitteln
<i>Richtlinie</i> <i>2002/58/EG</i>	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)
<i>Richtlinie</i> <i>2002/87/EG</i>	Richtlinie 2002/87/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2002 über die zusätzliche Beaufsichtigung der Kreditinstitute, Versicherungsunternehmen und Wertpapierfirmen eines Finanzkonglomerats und zur Änderung der Richtlinien 73/239/EWG, 79/267/EWG, 92/49/EWG, 92/96/EWG, 93/6/EWG und 93/22/EWG des Rates und der Richtlinien 98/78/EG und 2000/12/EG des Europäischen Parlaments und des

## Rates

- Richtlinie*  
2005/28/EG Richtlinie 2005/28/EG der Kommission vom 8. April 2005 zur Festlegung von Grundsätzen und ausführlichen Leitlinien der guten klinischen Praxis für zur Anwendung beim Menschen bestimmte Prüfpräparate sowie von Anforderungen für die Erteilung einer Genehmigung zur Herstellung oder Einfuhr solcher Produkte
- Richtlinie*  
2006/42/EG Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung) (Maschinenrichtlinie)
- Richtlinie*  
2006/43/EG  
*EuroSOX* Richtlinie 2006/43/EG des europäischen Parlaments und der Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen (EuroSOX)
- Richtlinie*  
2006/48/EG Richtlinie 2006/48/EG des europäischen Parlaments und der Rates vom 14. Juni 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (Neufassung)
- Richtlinie*  
2007/64/EG Richtlinie 2007/64/EG des europäischen Parlaments und der Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (Zahlungsdiensterichtlinie)
- Richtlinie*  
2009/104/EG Richtlinie 2009/104/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über Mindestvorschriften für Sicherheit und Gesundheitsschutz bei Benutzung von Arbeitsmitteln durch Arbeitnehmer bei der Arbeit (Zweite Einzelrichtlinie im Sinne des Artikels 16 Absatz 1 der Richtlinie 89/391/EWG)
- Richtlinie*  
2009/136/EG Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz
- Richtlinie*  
2009/138/EG Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II)
- Richtlinie*  
2013/36/EU Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG
- Verordnung*  
(EU) Nr.  
575/2013 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012  
Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum

freien Datenverkehr (Allgemeine Datenschutzverordnung) (in Arbeit)

European Communities: Guidelines on best practices for using electronic information, 1997

*PIC/S*  
*PE 009-11* Guide to Good Manufacturing Practice for Medicinal Products, Annexes, PE 009-11, PIC/S, 01. März 2014

*PIC/S*  
*PI 011-2* Good Practices for Computerised Systems in Regulated „GxP“ Environments, PI 011-3, PIC/S, 25. September 2007

### 26.1.6 USA: Gesetze, Practices, Prüfvorschriften

*16 CFR,*  
*Part 312,* Children’s Online Privacy Protection Act, Code of Federal Regulations, Title 16, Part 312

*21 CFR*  
*Part 11* Electronic Records; Electronic Signatures, Code of Federal Regulations; Title 21, Part 11

*21 CFR*  
*Part 58* Good Laboratory Practice for Nonclinical Laboratory Studies, Code of Federal Regulations, Title 21, Part 58

*21 CFR*  
*Part 110* Current Good Manufacturing Practice in Manufacturing, Packing, or Holding Human Food, Code of Federal Regulations, Title 21, Part 110

*21 CFR*  
*Part 211* Current Good Manufacturing Practice for Finished Pharmaceuticals, Code of Federal Regulations, Title 21, Part 211

*21 CFR*  
*Part 820* Quality System Regulation, Code of Federal Regulations, Title 21, Part 820

*34 CFR*  
*Part 99* Family Educational Rights and Privacy Act

*COSO:*  
*Enterprise*  
*Risk*  
*Management* Enterprise Risk Management – Integrated Framework (2004), Aktualisierungsprojekt seitens COSO am 21.10.2014 angekündigt)

*COSO:*  
*Internal*  
*Control* Internal Control — Integrated Framework (2013)

*DPPA* Drivers Privacy Protection Act

*ECPA* Electronic Communications Privacy Act

*FDIC,*  
*Managing*  
*Multiple*  
*Service*  
*Providers* Technology Outsourcing, Techniques for Managing Multiple Service Providers, neu herausgegeben 7. April 2014

*FDIC,*  
*Selecting a*  
*Service*  
*Provider* Technology Outsourcing, Effective Practices for Selecting a Service Provider, neu herausgegeben 7. April 2014

*FFIEC, BCP* IT Examination Handbook, Business Continuity Planning, Februar 2015

<i>FFIEC, D&amp;A</i>	IT Examination Handbook, Development and Acquisition, April 2004
<i>FFIEC, IS</i>	IT Examination Handbook, Information Security, Juli 2006
<i>FFIEC, MGT</i>	IT Examination Handbook, Management (IT Risk Management Process), Juni 2004
<i>FFIEC, OPS</i>	IT Examination Handbook, Operations, Juli 2004
<i>FFIEC, OT</i>	IT Examination Handbook, Outsourcing Technology Services, Juni 2004
<i>FFIEC, TSP</i>	IT Examination Handbook, Supervision of Technology Service Providers (TSP), Oktober 2012
<i>FISMA</i>	Federal Information Security Management Act of 2002, der im April 2013 durch The Federal Information Security Amendments Act, H.R. 1163, geändert wurde
<i>GLBA</i>	Gramm-Leach-Bliley Act
<i>HMTA</i>	Hazardous Materials Transportation Act
<i>HIPAA</i>	Health Insurance Portability and Accountability Act
<i>HITECH Act</i>	Health Information Technology for Economic and Clinical Health Act
<i>OSH Act</i>	Occupational Safety and Health Act
	Privacy Act
<i>PCAOB, Auditing Standards</i>	Auditing Standards: <ul style="list-style-type: none"> <li>• Auditing Standard 1: References in Auditors' Reports to the Standards of the Public Company Accounting Oversight Board</li> <li>• Auditing Standard 3: Audit Documentation</li> <li>• Auditing Standard 4: Reporting on Whether a Previously Reported Material Weakness Continues to Exist</li> <li>• Auditing Standard 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements</li> <li>• Auditing Standard 6: Evaluating Consistency of Financial Statements</li> <li>• Auditing Standard 7: Engagement Quality Review</li> <li>• Auditing Standard 8: Audit Risk</li> <li>• Auditing Standard 9: Audit Planning</li> <li>• Auditing Standard 10: Supervision of the Audit Engagement</li> <li>• Auditing Standard 11: Consideration of Materiality in Planning and Performing an Audit</li> <li>• Auditing Standard 12: Identifying and Assessing Risks of Material Misstatement</li> <li>• Auditing Standard 13: The Auditor's Responses to the Risks of Material Misstatement</li> <li>• Auditing Standard 14: Evaluating Audit Results</li> <li>• Auditing Standard 15: Audit Evidence</li> <li>• Auditing Standard 16: Communications with Audit Committees</li> <li>• Auditing Standard 17: Auditing Supplemental Information Accompanying Audited Financial Statements</li> <li>• Auditing Standard 18: Related Parties</li> </ul>
<i>SOX</i>	Sarbanes-Oxley Act

SSA	Social Security Act
TSCA	Toxic Substances Control Act
	Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations

## 26.2 Ausführungsbestimmungen, Grundsätze, Vorschriften

<i>Basel II</i>	Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen
<i>Basel III</i>	A global regulatory framework for more resilient banks and banking systems
<i>DGUV Regelwerk</i>	DGUV-Regelwerk unterscheidet die folgenden vier Kategorien: <ul style="list-style-type: none"> <li>• DGUV Vorschriften</li> <li>• DGUV Regeln</li> <li>• DGUV Informationen</li> <li>• DGUV Grundsätze</li> </ul>
<i>GoB</i>	Grundsätze ordnungsmäßiger Buchführung
<i>GoBD</i>	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
<i>GoDV</i>	Grundsätze ordnungsmäßiger Datenverarbeitung [12]
<i>IDW PS 330</i>	Abschlussprüfung bei Einsatz von Informationstechnologie, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 24.09.2002
<i>IDW PS 525</i>	Die Beurteilung des Risikomanagements von Kreditinstituten im Rahmen der Abschlussprüfung, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 26.06.2010
<i>IDW PS 880</i>	Die Prüfung von Softwareprodukten, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 11.03.2010
<i>IDW PS 951</i>	Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 16.10.2013
<i>IDW PS 980</i>	Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 11.03.2011
<i>IDW RS FAIT 1</i>	Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 24.09.2002
<i>IDW RS FAIT 2</i>	Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 24.09.2003
<i>IDW RS FAIT 3</i>	Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 11.07.2006

<i>IDW RS FAIT 4</i>	Anforderung an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 08.08.2012
<i>InvMaRisk</i>	Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk)
<i>MaDSB</i>	Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG), Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Düsseldorfer Kreis, 24./25. November 2010
<i>MaIuK</i>	Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – IuK-Mindestanforderungen
<i>MaRisk BA</i>	Mindestanforderungen an das Risikomanagement (Bankenaufsicht)
<i>MaRisk VA</i>	Aufsichtsrechtliche Mindestanforderungen an das Risikomanagement (Versicherungsaufsicht)
<i>MaComp</i>	Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG
Rund- schreiben 6/2013 (BA)	Anforderungen an Systeme und Kontrollen für den Algorithmushandel von Instituten (Bankenaufsicht)

## 26.3 Standards, Normen, Leitlinien und Rundschreiben

<i>AICPA® SOC 1® Report</i>	Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SSAE 16)
<i>AICPA® SOC 2® Report</i>	Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
<i>AICPA® SOC 3<sup>SM</sup> Report</i>	Trust Services Report for Service Organizations
<i>AICPA® SSAE 16</i>	Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
<i>ANSI/AIHA/ASSE Z10-2012</i>	Occupational Health and Safety Management Systems
<i>ANSI/TIA 606-B-2012</i>	Administration Standard for Telecommunications Infrastructure
<i>ANSI/TIA 942-A-2012</i>	Telecommunications – Infrastructure Standard for Data Centers
<i>ANSI/TIA 1179-2010</i>	Healthcare Facility Telecommunications Infrastructure Standard
<i>ANSI/BICSI 002-2011</i>	Data Center Design and Implementation Best Practices
<i>BCBS 98, Risk Management Principles Electron- ic Banking, Juli 2003</i>	Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision

BCBS 113, <i>Compliance,</i> <i>April 2005</i>	Compliance and the compliance function in banks, Basel Committee on Banking Supervision
BCBS 155, <i>Stress Testing,</i> <i>Mai 2009</i>	Principles for sound stress testing practices and supervision, Basel Committee on Banking Supervision
BCBS 176, <i>Governance Principles,</i> <i>Oktober 2010</i>	Principles for enhancing corporate governance, Basel Committee on Banking Supervision Überarbeitete Fassung "Corporate governance principles for banks" zur Konsultation bereitgestellt am 10.10.2014, BCBS 294
BCBS 195, <i>Risk Management Principles,</i> <i>Juni 2011</i>	Principles for the Sound Management of Operational Risk, Basel Committee on Banking Supervision
BCBS 239, <i>Risk Data Aggregation,</i> <i>Januar 2013</i>	Principles for effective risk data aggregation and risk reporting, Basel Committee on Banking Supervision
BCBS 292, <i>Review of Risk Management Principles,</i> <i>Oktober 2014</i>	Review of the Principles for the Sound Management of Operational Risk, Basel Committee on Banking Supervision
BCBS joint 12, <i>Outsourcing,</i> <i>Februar 2005</i>	Outsourcing in Financial Services, Basel Committee on Banking Supervision, The Joint Forum
BCBS joint 17, <i>Business Continuity,</i> <i>August 2006</i>	High-level principles for business continuity, Basel Committee on Banking Supervision, The Joint Forum
BS 10012:2009	Data protection. Specification for a personal information management system (PIMS)
BS 10500:2011	Specification for an anti-bribery management system (ABMS)
BS 11000-1:2010	Collaborative business relationships. A framework specification
BS 11000-2:2011	Collaborative business relationships. Guide to implementing BS 11000-1
BS 11200:2014	Crisis management. Guidance and good practice
BS OHSAS	Occupational Health and Safety Assessment Series
BS OHSAS 18001:2007	Occupational health and safety management systems – Requirements
BS OHSAS 18002:2008	Occupational health and safety management systems – Guidelines for the implementation of OHSAS 18001:2007
BS 65000:2014	Guidance on organizational resilience
BS PAS 99:2012	Specification of common management system requirements as a framework for integration



<i>bsi BIP 2217:2011</i>	Business continuity management for small and medium sized enterprises. How to survive a major disaster or failure
<i>bsi PD 25111:2010</i>	Business continuity management. Guidance on human aspects of business continuity
<i>bsi PD 25222:2011</i>	Business continuity management. Guidance on supply chain continuity
<i>bsi PD 25666:2010</i>	Business continuity management. Guidance on exercising and testing for continuity and contingency programmes
<i>bsi PD 25888:2011</i>	Business continuity management. Guidance on organization recovery following disruptive incidents
<i>BSI-Standard 100-1:2008</i>	Managementsysteme für Informationssicherheit (ISMS), Version 1.5, Mai 2008
<i>BSI-Standard 100-2:2008</i>	IT-Grundschutz-Vorgehensweise, Version 2.0, Mai 2008
<i>BSI-Standard 100-3:2008</i>	Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5, Mai 2008
<i>BSI-Standard 100-3:2008, Ergänzung 2011</i>	Ergänzung zum BSI-Standard 100-3, Version 2.5, Verwendung der elementaren Gefährdungen aus den IT-Grundschutz-Katalogen zur Durchführung von Risikoanalysen, Stand: 03.08.2011
<i>BSI-Standard 100-4:2008</i>	Notfallmanagement, Version 1.0, November 2008
<i>BSI</i>	Technische Richtlinie TR-03109
<i>TR-03109-1</i>	• TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems
<i>TR-03109-2</i>	• TR-03109-2: Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls
<i>TR-03109-3</i>	• TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen
<i>TR-03109-4</i>	• TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways
<i>CC, V 3.1, R4</i>	Common Criteria, Version 3.1, Revision 4, September 2012
<i>CEM, V 3.1, R4</i>	Common Methodology for Information Security Evaluation, Version 3.1, Revision 4, September 2012
<i>CMM®</i>	Capability Maturity Model® (Vorgänger des CMMI®)
<i>CMMI®</i>	Capability Maturity Model Integration®
<i>COBIT®</i>	Control Objectives for Information and related Technology
<i>CSPP-OS</i>	COTS Security Protection Profile – Operating Systems
	Deutscher Corporate Governance Kodex
<i>DIN EN 3-7</i>	Tragbare Feuerlöscher – Teil 7: Eigenschaften, Löschleistung, Anforderungen und Prüfung
<i>DIN EN 179:2014</i>	Schlösser und Baubeschläge – Notausgangsverschlüsse mit Drücker oder Stoßplatte für Türen in Fluchtwegen – Anforderungen und Prüfverfahren; Deutsche Fassung prEN 179:2014
<i>DIN VDE 0833-1:2014</i>	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall
<i>0833-2:2009</i>	• Teil 1: Allgemeine Festlegungen
<i>0833-3:2009</i>	• Teil 2: Festlegungen für Brandmeldeanlagen (BMA)

0833-4:2014	<ul style="list-style-type: none"> <li>• Teil 3: Festlegungen für Einbruch- und Überfallmeldeanlagen</li> <li>• Teil 4: Festlegungen für Anlagen zur Sprachalarmierung im Brandfall</li> </ul>
DIN EN 1047-1 1047-2:2013	Wertbehältnisse – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand <ul style="list-style-type: none"> <li>• Teil 1: Datensicherungsschränke und Disketteneinsätze; Deutsche Fassung der EN 1047-1:2005</li> <li>• Teil 2: Datensicherungsräume und Datensicherungscontainer; Deutsche Fassung der EN 1047-2:2009+A1:2013</li> </ul>
DIN EN 1125:2014	Schlösser und Baubeschläge – Paniktürverschlüsse mit horizontaler Betätigungsstange, für Türen in Rettungswegen – Anforderungen und Prüfverfahren
DIN EN 1627:2011	Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse – Einbruchhemmung – Anforderungen und Klassifizierung; Deutsche Fassung der EN 1627:2011
DIN 4102	Brandverhalten von Baustoffen und Bauteilen
DIN EN ISO 9001:2008	Qualitätsmanagementsysteme – Anforderungen
DIN ISO 9735-9	Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene – Teil 9: Sicherheitsschlüssel- und Zertifikatsverwaltung
DIN EN 12251	Medizinische Informatik – Sichere Nutzeridentifikation im Gesundheitswesen – Management und Sicherheit für die Authentifizierung durch Passwörter, englische Fassung; 2004-01
DIN EN 12600	Glas im Bauwesen – Pendelschlagversuch – Verfahren für die Stoßprüfung und Klassifizierung von Flachglas
DIN 14096:2014	Brandschutzordnung – Regeln für das Erstellen und Aushängen
DIN EN 15975-1:2011-06 15975-2:2013-12	Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement <ul style="list-style-type: none"> <li>• Teil 1: Krisenmanagement; Deutsche Fassung EN 15975-1:2011</li> <li>• Teil 2: Risikomanagement; Deutsche Fassung EN 15975-2:2013</li> </ul>
DIN 16557-4:2002	Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Teil 4: Regeln zur Auszeichnung von UN/EDIFACT-Übertragungsdateien mit der eXtensible Markup Language (XML) unter Einsatz von Document Type Definitions (DTD's)
DIN 16560-15:2003	EDIFACT – Anwendungsregeln – Teil 15: Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen über versendete Nutzdaten
DIN EN 16602-30-02:2014-12	Raumfahrtproduktsicherung – Fehlermöglichkeits-, Einfluss- (und Kritikalitäts-)Analyse (FMEA/FMECA); Englische Fassung EN 16602-30-02:2014

DIN 18095-2	Türen; Rauchschutztüren; Bauprüfungen der Dauerfunktionstüchtigkeit und Dichtheit
DIN ISO 23601:2010-12	Sicherheitskennzeichnung – Flucht- und Rettungspläne (ISO 23601:2009)
DIN 25424	Fehlerbaumanalyse, Teil 1: Methode und Bildzeichen, Teil 2: Handrechenverfahren zur Auswertung eines Fehlerbaumes
DIN 40041	Zuverlässigkeit; Begriffe
DIN EN 50126:2000	Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) {RAMS = Reliability, Availability, Maintainability, Safety}
DIN EN 50128:2012	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung der EN 50128:2011
DIN EN 50129:2003	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik
DIN EN 50130 Beiblatt 1	Alarmanlagen – Leitfaden für Einrichtungen von Alarmanlagen zur Erreichung der Übereinstimmung mit EG-Richtlinien; Deutsche Fassung CLC/TR 50456:2008
DIN EN 50131	Alarmanlagen – Einbruch- und Überfallmeldeanlagen
DIN EN 50132	Alarmanlagen – CCTV-Überwachungsanlagen für Sicherungsanwendungen
DIN EN 50133	Alarmanlagen – Zutrittskontrollanlagen für Sicherungsanwendungen
DIN EN 50134-1:2003-05 50134-2:2000-01 50134-3:2012-11 50134-5:2005-08	Alarmanlagen – Personen-Hilferufanlagen <ul style="list-style-type: none"> <li>• Teil 1: Systemanforderungen; Deutsche Fassung EN 50134-1:2002</li> <li>• Teil 2: Auslösegeräte; Deutsche Fassung EN 50134-2:1999</li> <li>• Teil 3: Örtliche Zentrale und Übertragungsgerät; Deutsche Fassung EN 50134-3:2012</li> <li>• Teil 5: Verbindungen und Kommunikation; Deutsche Fassung EN 50134-5:2004</li> <li>• Teil 7: Anwendungsregeln; Deutsche Fassung CLC/TS 50134-7:2003</li> </ul>
DIN CLC/TS 50134-7:2004-08	
DIN EN 50600-1:2013 50600-2-1:2014 50600-2-2:2014 50600-2-3:2013 50600-2-4:2014 50600-2-5:2014 50600-2-6:2014	Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren <ul style="list-style-type: none"> <li>• Teil 1: Allgemeine Konzepte; Deutsche Fassung der EN 50600-1:2012</li> <li>• Teil 2-1: Gebäudekonstruktion; Deutsche Fassung der EN 50600-2-1:2014</li> <li>• Teil 2-2: Stromversorgung; Deutsche Fassung der EN 50600-2-2:2014</li> </ul>

- Teil 2-3: Überwachung der Umgebung;  
Deutsche Fassung der prEN 50600-2-3:2013
  - Teil 2-4: Infrastruktur der Telekommunikationsverkabelung;  
Deutsche Fassung der prEN 50600-2-4:2013
  - Teil 2-5: Sicherungssysteme;  
Deutsche Fassung der prEN 50600-2-5:2014
  - Teil 2-6: Informationen für das Management und den Betrieb;  
Deutsche Fassung der prEN 50600-2-6:2014
- DIN EN*  
60812:2006      Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006); Deutsche Fassung EN 60812:2006
- DIN EN*  
62040-3:2011      Unterbrechungsfreie Stromversorgungssysteme (USV) – Teil 3: Methoden zur Festlegung der Leistungs- und Prüfungsanforderungen (IEC 62040-3:2011); Deutsche Fassung EN 62040-3:2011
- DIN*  
66399-1:2012  
66399-2:2012  
SPEC 66399-3:2013      Büro- und Datentechnik – Vernichten von Datenträgern
- Teil 1: Grundlagen und Begriffe
  - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern
  - Teil 3: Prozesse der Datenträgervernichtung
- DIN EN*  
80001-1:2011      Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010); Deutsche Fassung der EN 80001-1:2011
- FinTS, V4.1*  
*GAMP® 5*      Financial Transaction Services  
The Good Automated Manufacturing Practice (GAMP®) 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, Stand Februar 2008
- GERM*  
*ISO*  
*Guide 73:2009*      Good Electronic Records Management  
Risikomanagement – Vokabular
- ISO/IEC*  
2382-8:1998      Informationstechnik – Begriffe – Teil 8: Sicherheit
- ISO*  
10007:2003      Quality management systems – Guidelines for configuration management
- ISO/IEC*  
12207:2008      Systems and software engineering – Software life cycle processes
- ISO*  
TR 13569:2005      Financial services – Information security guidelines
- ISO*  
14001:2004,  
Cor. 1:2009      Environmental management systems – Requirements with guidance for use  
Die überarbeitete Fassung der ISO 14001 hat die ISO für Ende 2015 angekündigt.
- ISO*  
14971:2007      Medical devices – Application of risk management to medical devices

- ISO  
15000-5:2014 Electronic business eXtensible Markup Language (ebXML)
- Part 5: ebXML Core Components Specification
- ISO/IEC  
15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security s. a. Common Criteria
- 15408-2:2008
- 15408-3:2008
- Part 1: Introduction and general model
  - Part 2: Security functional components
  - Part 3: Security assurance components
- ISO/IEC  
TR 15443-1:2012 Information technology – Security techniques – Security assurance framework
- TR 15443-2:2012
- Part 1: Introduction and concepts
  - Part 2: Analysis
- ISO/IEC  
TR 15446:2009 Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets
- ISO  
15489-1:2001, Information and documentation: Records management
- TR 15489-2:2001
- Part 1: General
  - Part 2: Guidelines
- ISO/IEC  
15504-1:2004 Information technology – Process assessment
- 15504-2:2003
- 15504-3:2004
- 15504-4:2004
- 15504-5:2012
- 15504-6:2013
- TR 15504-7:2008
- TS 15504-8:2012
- TS 15504-9:2011
- TS 15504-10:2011
- Part 1: Concepts and vocabulary
  - Part 2: Performing an assessment; Cor 1: 2004
  - Part 3: Guidance on performing an assessment
  - Part 4: Guidance on use for process improvement and process capability determination
  - Part 5: An exemplar software life cycle process assessment model
  - Part 6: An exemplar system life cycle process assessment model
  - Part 7: Assessment of organizational maturity
  - Part 8: An exemplar process assessment model for IT service management
  - Part 9: Target process profiles
  - Part 10: Safety extension
- ISO/IEC  
16085:2006 Systems and software engineering – Life cycle processes – Risk management
- ISO  
17090-1:2013 Health informatics – Public key infrastructure
- 17090-2:2008
- 17090-3:2008
- 17090-4:2014
- Part 1: Overview of digital certificate services
  - Part 2: Certificate profile
  - Part 3: Policy management of certification authority
  - Part 4: Digital Signatures for healthcare documents
- ISO/IEC  
17789:2014 Information technology – Cloud computing – Reference architecture
- ISO/IEC  
18028-4:2005 Information technology – Security techniques – IT network security
- Part 4: Securing remote access
- ISO/IEC  
18045:2008 Information technology – Security techniques – Methodology for IT security evaluation

<i>ISO TR 18307:2001</i>	Health informatics – Interoperability and compatibility in messaging and communication standards – Key characteristics
<i>ISO 18308:2011</i>	Health informatics – Requirements for an electronic health record architecture
<i>ISO 19011:2011</i>	Guidelines for auditing management systems
<i>ISO 19092:2008</i>	Financial services – Biometrics – Security framework
<i>ISO 19600:2014</i>	Compliance management systems – Guidelines
<i>ISO/IEC 19770-1:2012 19770-2:2009 DIS 19770-3 19770-5:2013 AWI 19770-7</i>	Information technology – Software asset management <ul style="list-style-type: none"> <li>• Part 1: Processes and tiered assessment of conformance</li> <li>• Part 2: Software identification tag</li> <li>• Part 3: Software entitlement schema</li> <li>• Part 5: Overview and vocabulary</li> <li>• Part 7: Tag management</li> </ul>
<i>ISO/IEC 19792:2009</i>	Information technology – Security techniques – Security evaluation of biometrics
<i>ISO/IEC 20000-1:2011 20000-2:2012 20000-3:2012 TR 20000-4:2010 TR 20000-5:2013 WD 20000-6 WD 20000-8 TR 20000-9:2015 TR 20000-10:2013 PDTR 20000-11</i>	Information technology – Service management <ul style="list-style-type: none"> <li>• Part 1: Service management system requirements</li> <li>• Part 2: Guidance on the application of service management systems</li> <li>• Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1</li> <li>• Part 4: Process reference model</li> <li>• Part 5: Exemplar implementation plan for ISO/IEC 20000-1</li> <li>• Part 6: Requirements for bodies providing audit and certification of service management systems</li> <li>• Part 8: Guidance on the application of service management systems for smaller organizations</li> <li>• Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services</li> <li>• Part 10: Concepts and terminology</li> <li>• Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks</li> </ul>
<i>ISO/IEC TR 20004:2012</i>	Information technology – Security techniques – Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
<i>ISO/IEC 20006-1:2014 FDIS 20006-2 PDTS 20006-3</i>	Information technology for learning, education and training – Information model for competency <ul style="list-style-type: none"> <li>• Part 1: Competency general framework and information model</li> <li>• Part 2: Proficiency level information model</li> <li>• Part 3: Guidelines for the aggregation of competency information and data</li> </ul>

ISO TR 20514:2005	Health informatics – Electronic health record – Definition, scope and context
ISO/IEC 21000-5:2004	Information technology – Multimedia framework (MPEG-21) – Part 5: Rights Expression Language, Amd 1:2007, Amd 2:2007, Amd 3:2008
ISO 21091:2013	Health informatics – Directory services for healthcare providers, subjects of care and other entities
ISO TS 21298:2008	Health informatics – Functional and structural roles
ISO/IEC 21827:2008	Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model <sup>®</sup> (SSE-CMM <sup>®</sup> )
ISO 22000:2005	Food safety management systems – Requirements for any organization in the food chain, Cor 1:2006
ISO TS 22002-1:2009 TS 22002-2:2013 TS 22002-3:2011	Prerequisite programmes on food safety <ul style="list-style-type: none"> <li>• Part 1: Food manufacturing</li> <li>• Part 2: Catering</li> <li>• Part 3: Farming</li> </ul>
ISO TS 22003:2013	Food safety management systems – Requirements for bodies providing audit and certification of food safety management systems
ISO 22004:2014	Food safety management systems – Guidance on the application of ISO 22000
ISO 22005:2007	Traceability in the feed and food chain – General principles and basic requirements for system design and implementation
ISO 22006:2009	Quality management systems – Guidelines for the application of ISO 9001:2008 to crop production
ISO TR 22221:2006	Health informatics – Good principles and practices for a clinical data warehouse
ISO 22300:2012	Societal security – Terminology
ISO 22301:2012	Societal security – Business continuity management systems – Requirements
ISO 22307:2008	Financial services – Privacy impact assessment
ISO 22311:2012	Societal security – Video-surveillance – Export Interoperability
ISO TR 22312:2011	Societal security – Technological Capabilities
ISO 22313:2012	Societal security – Business continuity management systems – Guidance
ISO 22315:2014	Societal security – Mass evacuation – Guidelines for planning
ISO CD 22316	Societal security – Organizational resilience – Principles and guidelines
ISO 22320:2011	Societal security – Emergency management – Requirements for incident response

ISO PRF 22322	Societal security – Emergency management – Guidelines for public warning
ISO DIS 22324	Societal security – Emergency management – Guidelines for colour-coded alert
ISO 22398:2013	Societal security – Guidelines for exercises
ISO 22600-1:2014 22600-2:2014 22600-3:2014	Health informatics – Privilege management and access control <ul style="list-style-type: none"> <li>• Part 1: Overview and policy management</li> <li>• Part 2: Formal models</li> <li>• Part 3: Implementations</li> </ul>
ISO/IEC 23026:2006	Software Engineering – Recommended Practice for the Internet – Web Site Engineering, Web Site Management, and Web Site Life Cycle
ISO/IEC/IEEE FDIS 23026	Systems and software engineering – Engineering and management of websites for systems, software, and services information
ISO/IEC 24745:2011	Information technology – Security techniques – Biometric information protection
ISO/IEC 24759:2014	Information technology – Security techniques – Test requirements for cryptographic modules
ISO/IEC 24760-1:2011 FDIS 24760-2 CD 24760-3	Information technology – Security techniques – A Framework for Identity Management <ul style="list-style-type: none"> <li>• Part 1: Terminology and concepts</li> <li>• Part 2: Reference architecture and requirements</li> <li>• Part 3: Practice</li> </ul>
ISO/IEC 24761:2009	Information technology – Security techniques – Authentication context for biometrics (ACBio), Cor 1: 2013
ISO/IEC TR 24763:2011	Information technology – Learning, education and training – Conceptual Reference Model for Competency Information and Related Objects
ISO/IEC 24764:2010, Amd 1:2014	Information technology – Generic cabling systems for data-centres. Amd 1:2014
ISO/IEC 24775-1:2014 24775-2:2014 24775-3:2014 24775-4:2014 24775-5:2014 24775-6:2014 24775-7:2014 24775-8:2014	Information technology – Storage management <ul style="list-style-type: none"> <li>• Part 1: Overview</li> <li>• Part 2: Common Architecture</li> <li>• Part 3: Common Profiles</li> <li>• Part 4: Block Devices</li> <li>• Part 5: File systems</li> <li>• Part 6: Fabric</li> <li>• Part 7: Host Elements</li> <li>• Part 8: Media Libraries</li> </ul>
ISO/IEC 25000:2014	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE



<i>ISO/IEC</i> <i>25001:2014</i>	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Planning and management
<i>ISO/IEC</i> <i>25010:2011</i>	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models
<i>ISO/IEC</i> <i>25012:2008</i>	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model
<i>ISO/IEC</i> <i>25020:2007</i>	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Measurement reference model and guide
<i>ISO/IEC</i> <i>25030:2007</i>	Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Quality requirements
<i>ISO/IEC</i> <i>25040:2011</i>	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation process
<i>ISO/IEC</i> <i>25041:2012</i>	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation guide for developers, acquirers and independent evaluators
<i>ISO/IEC</i> <i>25045:2010</i>	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation module for recoverability
<i>ISO/IEC</i> <i>TR 25060:2010</i>	Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: General framework for usability-related information
<i>ISO</i> <i>26000:2010</i>	Guidance on social responsibility
<i>ISO</i> <i>26262-1:2011</i>	Road vehicles – Functional safety
<i>26262-2:2011</i>	<ul style="list-style-type: none"> <li>• Part 1: Vocabulary</li> </ul>
<i>26262-3:2011</i>	<ul style="list-style-type: none"> <li>• Part 2: Management of functional safety</li> </ul>
<i>26262-4:2011</i>	<ul style="list-style-type: none"> <li>• Part 3: Concept phase</li> </ul>
<i>26262-5:2011</i>	<ul style="list-style-type: none"> <li>• Part 4: Product development at the system level</li> </ul>
<i>26262-6:2011</i>	<ul style="list-style-type: none"> <li>• Part 5: Product development at the hardware level</li> </ul>
<i>26262-7:2011</i>	<ul style="list-style-type: none"> <li>• Part 6: Product development at the software level</li> </ul>
<i>26262-8:2011</i>	<ul style="list-style-type: none"> <li>• Part 7: Production and operation</li> </ul>
<i>26262-9:2011</i>	<ul style="list-style-type: none"> <li>• Part 8: Supporting processes</li> </ul>
<i>26262-10:2012</i>	<ul style="list-style-type: none"> <li>• Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses</li> <li>• Part 10: Guideline on ISO 26262</li> </ul>
<i>ISO/IEC/IEEE</i> <i>26511:2011</i>	Systems and software engineering – Requirements for managers of user documentation
<i>ISO/IEC</i> <i>27000:2014</i>	Information technology – Security techniques – Information security management systems – Overview and vocabulary
<i>ISO/IEC</i> <i>27001:2013,</i> <i>Cor 1:2014</i>	Information technology – Security techniques – Information security management systems – Requirements, Cor 1:2014

<i>ISO/IEC 27002:2013, Cor 1:2014</i>	Information technology – Security techniques – Code of practice for information security controls, Cor 1:2014
<i>ISO/IEC 27003:2010</i>	Information technology – Security techniques – Information security management system implementation guidance
<i>ISO/IEC 27004:2009</i>	Information technology – Security techniques – Information security management – Measurement
<i>ISO/IEC 27005:2012</i>	Information technology – Security techniques – Information security risk management
<i>ISO/IEC 27006:2011</i>	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
<i>ISO/IEC 27007:2011</i>	Information technology – Security techniques – Guidelines for information security management systems auditing
<i>ISO/IEC TR 27008:2011</i>	Information technology – Security techniques – Guidelines for auditors on information security controls
<i>ISO/IEC CD 27009</i>	The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications
<i>ISO/IEC 27010:2012</i>	Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications
<i>ISO/IEC 27011:2008</i>	Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
<i>ISO/IEC 27013:2012</i>	Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
<i>ISO/IEC 27014:2013</i>	Information technology – Security techniques – Governance of information security
<i>ISO/IEC TR 27015:2012</i>	Information technology – Security techniques – Information security management guidelines for financial services
<i>ISO/IEC TR 27016:2014</i>	Information technology – Security techniques – Information security management – Organizational economics
<i>ISO/IEC DIS 27017</i>	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
<i>ISO/IEC 27018:2014</i>	Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
<i>ISO/IEC TR 27019:2013</i>	Information technology – Security techniques – Information security management – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
<i>ISO/IEC 27031:2011</i>	Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

<i>ISO/IEC</i> <i>27032:2012</i>	Information technology – Security techniques – Guidelines for cyberse- curity
<i>ISO/IEC</i> <i>27033-1:2009</i> <i>27033-2:2012</i> <i>27033-3:2010</i> <i>27033-4:2014</i> <i>27033-5:2013</i> <i>DIS 27033-6</i>	Information technology – Security techniques – Network security <ul style="list-style-type: none"> <li>• Part 1: Overview and concepts</li> <li>• Part 2: Guidelines for the design and implementation of network security</li> <li>• Part 3: Reference networking scenarios – Threats, design techniques and control issues</li> <li>• Part 4: Securing communications between networks using security gateways</li> <li>• Part 5: Securing communications across networks using Virtual Private Networks (VPNs)</li> <li>• Part 6: Securing wireless IP network access</li> </ul>
<i>ISO/IEC</i> <i>27034-1:2011,</i> <i>Cor 1:2014</i> <i>DIS 27034-2</i> <i>NP 27034-3</i> <i>CD 27034-4</i> <i>CD 27034-5</i> <i>NP 27034-5-1</i> <i>CD 27034-6</i> <i>NP 27034-7</i>	Information technology – Security techniques – Application security <ul style="list-style-type: none"> <li>• Part 1: Overview and concepts, Cor 1:2014</li> <li>• Part 2: Organization normative framework</li> <li>• Part 3: Application security management process</li> <li>• Part 4: Application security validation</li> <li>• Part 5: Protocols and application security controls data structure</li> <li>• Part 5-1: Protocols and application security controls data structure – XML schemas</li> <li>• Part 6: Security guidance for specific applications</li> <li>• Part 7: Application security assurance prediction</li> </ul>
<i>ISO/IEC</i> <i>27035:2011</i>	Information technology – Security techniques – Information security incident management
<i>ISO/IEC</i> <i>27036-1:2014</i> <i>27036-2:2014</i> <i>27036-3:2013</i> <i>WD 27036-4</i>	Information technology – Security techniques – Information security for supplier relationships <ul style="list-style-type: none"> <li>• Part 1: Overview and concepts</li> <li>• Part 2: Requirements</li> <li>• Part 3: Guidelines for ICT supply chain security</li> <li>• Part 4: Guidelines for security of cloud services</li> </ul>
<i>ISO/IEC</i> <i>27037:2012</i>	Information technology – Security techniques – Guidelines for identifi- cation, collection, acquisition and preservation of digital evidence
<i>ISO/IEC</i> <i>27038:2014</i>	Information technology – Security techniques – Specification for digital redaction
<i>ISO/IEC</i> <i>27039:2015</i>	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)
<i>ISO/IEC</i> <i>27040:2015</i>	Information technology – Security techniques – Storage security
<i>ISO/IEC</i> <i>FDIS 27041</i>	Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigation methods
<i>ISO/IEC</i> <i>DIS 27042</i>	Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence
<i>ISO/IEC</i> <i>27043:2015</i>	Information technology – Security techniques – Incident investigation principles and processes

<i>ISO/IEC WD 27044</i>	Information technology – Security techniques – Guidelines for Security Information and Event Management (SIEM)
<i>ISO/IEC CD 27050-1 NP 27050-2 NP 27050-3 NP 27050-4</i>	Information technology – Security techniques – Electronic discovery <ul style="list-style-type: none"> <li>• Part 1: Overview and concepts</li> <li>• Part 2: Guidance for governance and management of electronic discovery</li> <li>• Part 3: Code of Practice for electronic discovery</li> <li>• Part 4: ICT readiness for electronic discovery</li> </ul>
<i>ISO 27789:2013</i>	Health informatics – Audit trails for electronic health records
<i>ISO 27799:2008</i>	Health informatics – Information security management in health using ISO/IEC 27002
<i>ISO 28000:2007</i>	Specification for security management systems for the supply chain
<i>ISO 28001:2007</i>	Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
<i>ISO 28002:2011</i>	Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
<i>ISO 28003:2007</i>	Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems
<i>ISO 28004-1:2007, Cor 1:2012 28004-2:2014 28004-3:2014 28004-4:2014</i>	Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 <ul style="list-style-type: none"> <li>• Part 1: General principles, Cor 1:2012</li> <li>• Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations</li> <li>• Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)</li> <li>• Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective</li> </ul>
<i>ISO 28005-1:2013 28005-2:2011</i>	Security management systems for the supply chain – Electronic port clearance (EPC) <ul style="list-style-type: none"> <li>• Part 1: Message structures</li> <li>• Part 2: Core data elements</li> </ul>
<i>ISO/IEC 29100:2011</i>	Information technology – Security techniques – Privacy framework
<i>ISO/IEC 29101:2013</i>	Information technology – Security techniques – Privacy architecture framework
<i>ISO/IEC/IEEE 29119-1:2013 29119-2:2013</i>	Software and systems engineering – Software testing <ul style="list-style-type: none"> <li>• Part 1: Concepts and definitions</li> <li>• Part 2: Test processes</li> </ul>

29119-3:2013	• Part 3: Test documentation
FDIS 29119-4	• Part 4: Test techniques
DIS 29119-5	• Part 5: Keyword-Driven Testing
ISO/IEC TR 29125:2010	Information technology – Telecommunications cabling requirements for remote powering of terminal equipment
ISO/IEC PRF 29190	Information technology – Security techniques – Privacy capability assessment model
ISO/IEC 29361:2008	Information technology – Web Services Interoperability – WS-I Basic Profile Version 1.1
ISO/IEC 29362:2008	Information technology – Web Services Interoperability – WS-I Attachments Profile Version 1.0.
ISO/IEC 29363:2008	Information technology – Web Services Interoperability – WS-I Simple SOAP Binding Profile Version 1.0
ISO 31000:2009	Risk management – Principles and guidelines
ISO TR 31004:2013	Risk management – Guidance for the implementation of ISO 31000
ISO/IEC 31010:2009	Risk management – Risk assessment techniques
ISO/IEC 38500:2008	Corporate governance of information technology
ISO/IEC/IEEE 42010:2011	Systems and software engineering – Architecture description
ISO CD 45001	Occupational health and safety management systems – Requirements. Der Draft basiert auf der BS OHSAS 18001
ISO 55001:2014	Asset management – Management systems – Requirements
ISO 55002:2014	Asset management – Management systems – Guidelines for the application of ISO 55001
ISO/IEC TR 90006:2013	Information technology – Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011
IT-GSK	IT-Grundschutzkataloge des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI)
ITIL®	IT Infrastructure Library
ITSEC	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Bundesanzeiger, Stand: Juni 1991
LASI LV 58, AMS	Beratung der Länder zu und Umgang der Länder mit Arbeitsschutzmanagementsystemen (AMS), Länderausschuss für Arbeitsschutz und Sicherheitstechnik (LASI)
MISRA C®:2012	Guidelines for the use of the C language in critical systems (MISRA C3)
MISRA®-C++:2008	Guidelines for the use of the C++ language in critical systems
NIST IR 7298, Rev 2	Glossary of Key Information Security Terms, Revision 2, NIST, Mai 2013

- NIST*  
*SP 800-16* Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998
- A Role-Based Model for Federal Information Technology/Cyber Security Training, NIST Special Publication 800-16, Revision 1 (2<sup>nd</sup> Draft, Version 2), October 2013
- NIST*  
*SP 800-27, Rev. A* Engineering Principles for IT Security, Revision A, NIST, Juni 2004
- NIST*  
*SP 800-30, Rev. 1* Guide for Conducting Risk Assessments, NIST, September 2012
- NIST*  
*SP 800-36* Guide to Selecting Information Technology Security Products, NIST, Oktober 2003
- NIST*  
*SP 800-39* Managing Information Security Risk, NIST, März 2011
- NIST*  
*SP 800-41, Revision 1* Guidelines on Firewalls and Firewall Policy, Revision 1, NIST, September 2009
- NIST*  
*SP 800-53, Revision 4* Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, NIST, April 2013
- NIST*  
*SP 800-53A, Revision 4* Assessing Security and Privacy Controls in Federal Information Systems and Organizations, NIST, Dezember 2014
- NIST*  
*SP 800-55, Revision 1* Performance Measurement Guide for Information Security, NIST, Juli 2008
- NIST*  
*SP 800-61, Revision 2* Computer Security Incident Handling Guide, NIST, August 2012
- NIST*  
*SP 800-88, Revision 1* Guidelines for Media Sanitization, NIST, Dezember 2014
- NIST*  
*SP 800-94, Rev 1, DRAFT* Guide to Intrusion Detection and Prevention Systems (IDPS), NIST, Februar 2007
- Guide to Intrusion Detection and Prevention Systems (IDPS), DRAFT, NIST, Juli 2012
- NIST*  
*SP 800-95* Guide to Secure Web Services, NIST, August 2007
- NIST*  
*SP 800-100* Information Security Handbook: A Guide for Managers, NIST, Oktober 2006
- NIST*  
*SP 800-115* Technical Guide to Information Security Testing and Assessment, NIST, September 2008

<i>NIST</i> <i>SP 800-121,</i> <i>Revision 1</i>	Guide to Bluetooth Security, NIST, Juni 2012,
<i>NIST</i> <i>SP 800-123</i>	Guide to General Server Security, NIST, Juli 2008
<i>NIST</i> <i>SP 800-124,</i> <i>Revision 1</i>	Guidelines for Managing the Security of Mobile Devices in the Enterprise, Revision 1, NIST, Juni 2013
<i>NIST</i> <i>SP 800-125</i>	Guide to Security for Full Virtualization Technologies, NIST, Januar 2011
<i>NIST</i> <i>SP 800-128</i>	Guide for Security-Focused Configuration Management of Information Systems, NIST, August 2011
<i>NIST</i> <i>SP 800-137</i>	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST, September 2011
<i>NIST</i> <i>SP 800-144</i>	Guidelines on Security and Privacy in Public Cloud Computing, NIST, Dezember 2011
<i>NIST</i> <i>SP 800-145</i>	The NIST Definition of Cloud Computing, NIST, September 2011
<i>NIST</i> <i>SP 800-153</i>	Guidelines for Securing Wireless Local Area Networks (WLANs), NIST, Februar 2012
<i>NIST</i> <i>SP 800-161,</i> <i>2nd DRAFT</i>	Supply Chain Risk Management Practices for Federal Information Systems and Organizations, 2nd DRAFT, NIST, Juni 2014
<i>NIST</i> <i>SP 800-164,</i> <i>DRAFT</i>	Guidelines on Hardware-Rooted Security in Mobile Devices, DRAFT, NIST, Oktober 2012
<i>NIST</i> <i>800-167, DRAFT</i>	Guide to Application Whitelisting, DRAFT, NIST, August 2014
<i>OECD</i> <i>cGLP:1995</i>	The Application of the Principles of GLP to Computerised Systems, OECD series on principles of good laboratory practice and compliance monitoring Number 10
<i>OECD</i> <i>cGLP:2014,</i> <i>DRAFT</i>	The Application of GLP Principles to Computerised Systems, DRAFT
<i>OECD GLP</i>	OECD-Grundsätze der Guten Laborpraxis, Schriftenreihe über die Grundsätze der Guten Laborpraxis und Überwachung ihrer Einhaltung, Nummer 1
<i>OECD Corporate</i> <i>Governance: 2004</i>	OECD-Grundsätze der Corporate Governance
<i>OECD Corporate</i> <i>Governance: 2014,</i> <i>DRAFT</i>	Principles of corporate governance, DRAFT
<i>OECD</i> <i>Risk Management</i> <i>and Corporate</i> <i>Governance: 2014</i>	Risk Management and Corporate Governance

<i>OENORM S 2400:2009</i>	Business Continuity und Corporate Security Management – Benennungen und Definitionen
<i>OENORM S 2401:2009</i>	Business Continuity und Corporate Security Management – Systemaufbau und Business Continuity und Corporate Security Policy
<i>OENORM S 2402:2009</i>	Business Continuity und Corporate Security Management – Business Continuity Management
<i>OENORM S 2403:2009</i>	Business Continuity und Corporate Security Management – Corporate Security Management
<i>OHRIS:2010</i>	Occupational Health and Risk Management System, Bayerisches Staatsministerium für Umwelt, Gesundheit und Verbraucherschutz
<i>ONR 49000:2014</i>	Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen – Umsetzung von ISO 31000 in die Praxis
<i>ONR 49001:2014</i>	Risikomanagement für Organisationen und Systeme – Risikomanagement – Umsetzung von ISO 31000 in die Praxis
<i>ONR 49002-1:2014 49002-2:2014 49002-3:2014</i>	Risikomanagement für Organisationen und Systeme <ul style="list-style-type: none"> <li>• Teil 1: Leitfaden für die Einbettung des Risikomanagements ins Managementsystem – Umsetzung von ISO 31000 in die Praxis</li> <li>• Teil 2: Leitfaden für die Methoden der Risikobeurteilung – Umsetzung von ISO 31000 in die Praxis</li> <li>• Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement – Umsetzung von ISO 31000 in die Praxis</li> </ul>
<i>ONR 49003:2014</i>	Risikomanagement für Organisationen und Systeme – Anforderungen an die Qualifikation des Risikomanagers – Umsetzung von ISO 31000 in die Praxis
<i>PCI DSS Version 3.0, 2013</i>	Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures
<i>SAI SA8000®:2014</i>	Social Accountability 8000, Social Accountability International
<i>SCAMPI<sup>SM</sup></i>	Standard CMMI® Appraisal Method for Process Improvement (SCAMPI <sup>SM</sup> ) A, Version 1.3: Method Definition Document, Carnegie Mellon University, März 2011
<i>SERA</i>	Introduction to the Security Engineering Risk Analysis (SERA) Framework, Carnegie Mellon University, November 2014
<i>SPICE</i>	Software Process Improvement and Capability dEtermination, s. a. ISO/IEC TR 15504
<i>SSE-CMM<sup>®</sup></i>	Information technology – Systems Security Engineering – Capability Maturity Model (ISO/IEC 21827:2008)
<i>TOGAF® 9.1</i>	Enterprise architecture methodology and framework, The Open Group
<i>VDI 7000:2015-01</i>	Frühe Öffentlichkeitsbeteiligung bei Industrie- und Infrastrukturprojekten
<i>VdS 2000:2010-12</i>	Leitfaden für den Brandschutz im Betrieb
<i>VdS 2007:2004-08</i>	Anlagen der Informationstechnologie (IT-Anlagen) – Merkblatt zur Schadenverhütung



VdS 2008:2009-07	Feuergefährliche Arbeiten – Richtlinien für den Brandschutz
VdS 2036:2009-07	Erlaubnisschein für feuergefährliche Arbeiten
VdS 2037EF:2013-05	Grafische Symbole für die Erstellung von Feuerwehrplänen (gemäß DIN 14095), Flucht- und Rettungsplänen (gemäß DIN ISO 23601) und zur Sicherheits- und Gesundheitsschutzkennzeichnung von Arbeitsstätten (gemäß ASR A1.3)
VdS 2095:2010-05	Automatische Brandmeldeanlagen – Planung und Einbau
VdS 2170:2010-11	Installationsattest für Einbruchmeldeanlagen
VdS 2247-2:2013-12 2247-S:2006-12	VdS-Richtlinien für Einbruchmeldeanlagen – Prüfungsfragen Einbruchmeldeanlagen <ul style="list-style-type: none"> <li>• Teil 2: Einbruchmeldetechnik</li> <li>• Teil S: Zusatzfragen zur mechanischen Sicherungstechnik</li> </ul>
VdS 2263:2013-09	Betriebsbuch für Einbruch- und Überfallmeldeanlagen
VdS 2311:2010-11 2311-S1:2013-08	VdS-Richtlinien für Einbruchmeldeanlagen – Planung und Einbau <ul style="list-style-type: none"> <li>• Ergänzung S1: Korrekturen, Änderungen und Ergänzungen</li> </ul>
VdS 2333:2014-09	Sicherungsrichtlinien für Geschäfte und Betriebe
VdS 2366:2013-08	VdS-Richtlinien für Videoüberwachungsanlagen – Planung und Einbau
VdS 2367:2004-06	VdS-Richtlinien für Zutrittskontrollanlagen – Planung und Einbau
VdS 2463:2007-08	VdS-Richtlinien für Gefahrenmeldeanlagen – Übertragungseinrichtungen für Gefahrenmeldungen (ÜE) – Anforderungen
VdS 2465:1999-03 2465-S1:2001-05 2465-S2:2006-06 2465-S3:2008-10	Richtlinien für Gefahrenmeldeanlagen – Übertragungsprotokoll für Gefahrenmeldungen, Version 2 <ul style="list-style-type: none"> <li>• Ergänzung S1: Korrektur und Anpassung von Satztypen</li> <li>• Ergänzung S2: Protokollerweiterung zur Anschaltung an Netze der Protokollfamilie TCP</li> <li>• Ergänzung S3: Protokollerweiterung zur Anschaltung von Videoüberwachungsanlagen an Gefahrenmeldeanlagen</li> </ul>
VdS 2472:2007-11	Sicherungsrichtlinien für Banken, Sparkassen und sonstige Zahlstellen
VdS 2493:2004-06	Attest über die Installation einer VdS-anerkannten Zutrittskontrollanlage
VdS 2833:2003-11	Schutzmaßnahmen gegen Überspannung für Gefahrenmeldeanlagen, Richtlinien
VdS 3143:2012-09	Sicherungsleitfaden Perimeter

<i>VdS</i> 3172:2013-04	Merkblatt – Worauf es bei der Planung sowie Errichtung von Einbruch- und Überfallmeldeanlagen in Verbindung mit der DIN VDE 0833-3 und den Richtlinien VdS 2311 zu achten gilt.
<i>VdS</i> 3425:2008-07	Betriebsbuch für Videoüberwachungsanlagen
<i>VdS</i> 3426:2013-07	Installationsattest für eine Videoüberwachungsanlage (VÜA)
<i>VdS</i> 3436:2005-08	Betriebsbuch für Zutrittskontrollanlagen
<i>VdS</i> 3534:2013-03	Gefahrenmanagementsysteme für sicherungstechnische Anlagen – Anforderungen und Prüfmethode
<i>VS-ITR</i>	Verwaltungsvorschrift des Innenministeriums zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik (VS-IT-Richtlinien - VSITR), 20.12.2004 - Az.: 5-0214.3/77

## 27 Literatur- und Quellenverzeichnis

- [1] Müller, Klaus-Rainer: IT-Sicherheitsmanagement und die Rolle der Unternehmensberater, Datensicherheitstage, 5. Oktober 1995
- [2] Müller, Klaus-Rainer: IT-Sicherheit mit System, VIEWEG, Juli 2003
- [3] <kes>/Microsoft-Studie 2014, Lagebericht zur Informations-Sicherheit, Teil 2, <kes>, 5/2014, S. 70ff.
- [4] Müller, Klaus-Rainer: Unternehmensberater – Ungeliebte Zaungäste?, KES, 2/1996, S. 6ff.
- [5] Müller, Klaus-Rainer: Risiken vermeiden, Business Computing, 7/1996, S. 46ff.
- [6] Müller, Klaus-Rainer: Sicherheits- und Qualitätsmanagement – zwei Seiten einer Medaille?, KES, 3/1996, S. 111ff.
- [7] Bundesministerium der Justiz: Entwurf eines Gesetzes zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG), Januar 2004
- [8] Müller, Klaus-Rainer: Information Security – eine unternehmerische Aufgabe, Information Security Management, TÜV Media, März 2008
- [9] Von der Crone, Hans Caspar und Roth, Katja: Der Sarbanes-Oxley Act und seine extraterritoriale Bedeutung, AJP/PJA, 2/2003, S. 131 ff.
- [10] Deutscher Bundestag: Bundestag-Drucksache 13/9712, Anlage 1, Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- [11] Baseler Ausschuss für Bankenaufsicht: Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen, Überarbeitete Rahmenvereinbarung, Juni 2004
- [12] Schuppenhauer, Rainer: GoDV-Handbuch: Grundsätze ordnungsmäßiger Datenverarbeitung und DV-Revisionen, Beck Juristischer Verlag, Januar 2007
- [13] Institut der Wirtschaftsprüfer: Rechnungslegung und Prüfung beim Einsatz von Informationstechnologie, 3., aktualisierte und erweiterte Auflage, IDW Sonderdruck, IDW-Verlag GmbH, Juni 2009
- [14] Europäisches Parlament und Rat: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- [15] Kommission der Europäischen Gemeinschaft: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/520/EG
- [16] Bundesanstalt für Finanzdienstleistungsaufsicht: Veröffentlichung der Endfassung der MaRisk, BA 17 – GS 5201 – 1/2005, 20.12.2005
- [17] Bundesanstalt für Finanzdienstleistungsaufsicht: Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben 10/2012, 14.12.2012
- [18] Baseler Ausschuss für Bankenaufsicht: Enhancements to the Basel II framework, Juli 2009
- [19] Basel Committee on Banking Supervision: Sound Practices for the Management and Supervision of Operational Risk, February 2003
- [20] Baseler Ausschuss für Bankenaufsicht: Management operationeller Risiken – Praxisempfehlungen für Banken und Bankenaufsicht, Februar 2003

- [21] Bundesanstalt für Finanzdienstleistungsaufsicht: Solvency II: Aufbau und Gesetzgebung, Webseite, Einsichtnahme 01.06.2014
- [22] Müller, Klaus-Rainer: Lebenszyklus- und prozessimmanente IT-Sicherheit, <kes>, 3/2004, S. 72ff.
- [23] Alberts, Christopher, Dorofee, Audrey, Stevens, James, Woody, Carol: Introduction to the OCTAVE<sup>®</sup> Approach, Carnegie Mellon University, August 2003
- [24] Alberts, Christopher und Dorofee, Audrey: Managing Information Security Risks, Addison-Wesley, 2002
- [25] PIC/S: Guide to Good Manufacturing Practice for Medicinal Products, Annexes, PE 009-11, 01.03.2014
- [26] PIC/S: Good Practices for Computerised Systems in Regulated „GxP“ Environments, PI 011-3, 25. September 2007
- [27] GAMP<sup>®</sup> 5: A Risk-Based Approach to Compliant GxP Computerized Systems, [http://www.ispe.org/cs/gamp\\_publications\\_section/gamp\\_publications\\_overview](http://www.ispe.org/cs/gamp_publications_section/gamp_publications_overview), Einsichtnahme 19.09.2009
- [28] Carnegie Mellon University: Systems Security Engineering Capability Maturity Model, Model Description Document, Version 3.0, 15. Juni 2003
- [29] Anderson, Ross: Security Engineering, Wiley, 2001
- [30] Müller, Klaus-Rainer: Risikoanalyse diktiert die Handlung, Computerzeitung, 38/2004, S. 17
- [31] Brockhaus, die Enzyklopädie in 24 Bänden, Studienausgabe, Band 18, Brockhaus, 2001
- [32] Masing, Walter (Hrsg.): Handbuch Qualitätsmanagement, 3. Auflage, Carl Hanser Verlag, 1994
- [33] Suzaki, Kiyoshi: Die ungenutzten Potentiale, Carl Hanser Verlag, 1994
- [34] DeMarco, Tom: Structured Analysis and System Specification, New York, Yourdon Press, 1978
- [35] The Federal Reserve Board: Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations, September 1997
- [36] Bundesamt für Sicherheit in der Informationstechnik: Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren, datumsfreie pdf-Unterlage, eingesehen am 5. Oktober 2006
- [37] Müller, Klaus-Rainer: Biometrie-Update 2009 – Verfahren, Trends, Chancen und Risiken – Teil 2, hakin9, 5/2009
- [38] Müller, Klaus-Rainer: IT-Sicherheit mit System, Springer Vieweg, 5. Auflage, März 2014
- [39] Kaplan, Robert S., Norton, David P.: Balanced Scorecard, Schäffer-Poeschel, 1997
- [40] Kamiske, Gerd F. und Brauer, Jörg-Peter: Qualitätsmanagement von A bis Z, Carl Hanser Verlag, 1993
- [41] Müller, Klaus-Rainer: In oder Out? – Sourcing mit System, geldinstitute, 3/2004, S. 32ff.
- [42] Sherman, Larry: Stratus<sup>®</sup> Continuous Processing<sup>®</sup> Technology<sup>®</sup>, 2003
- [43] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Bundesanzeiger, Stand: Juni 1991
- [44] Neuber, Dirk: Lösung für unterschiedliche Brandrisiken, WIK 2/2005, S. 43ff.

- [45] Müller, Klaus-Rainer: Biometrie-Update 2009 – Verfahren, Trends, Chancen und Risiken – Teil 1, hakin9, 4/2009
- [46] "Password" unseated by "123456" on SplashData's annual "Worst Passwords" list, SplashData Inc., Los Gatos, CA
- [47] Medvinsky, Sasha und Lalwaney, Poornima: Kerberos V Authentication Mode for Uninitialized Clients, 29. August 2000, [www.ietf.org/proceedings/00jul/SLIDES/dhckkerberos/sld000.htm](http://www.ietf.org/proceedings/00jul/SLIDES/dhckkerberos/sld000.htm)
- [48] Cheswick, William R. und Bellovin, Steven M.: Firewalls und Sicherheit im Internet, Addison-Wesley, 1996
- [49] Liberty Alliance Project: Business Benefits of Federated Identity, April 2003
- [50] Liberty Alliance Project: Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, März 2003
- [51] Liberty Alliance Project: Liberty ID-FF Architecture Overview, Version 1.2
- [52] Liberty Alliance Project: Privacy and Security Best Practices, Version 2.0, November 12, 2003
- [53] Federal Information Processing Standards Publication 197 (FIPS PUBS 197): Advanced Encryption Standard (AES), 26. November 2001
- [54] Baldwin, R. und Rivest, R.: RFC 2040, The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithm, Oktober 1996, Category: Informational
- [55] Callas, J., Donnerhacke, L., Finney, H., Thayer, R.: RFC 2440, OpenPGP Message Format, November 1998
- [56] Gutmann, Peter: Secure Deletion of Data from Magnetic and Solid-State Memory, 6. USENIX Security Symposium Proceedings, 22.-25. Juli 1996
- [57] Sikora, Axel: Netzwerk-Sicherheit, in IT-Security, tecCHANNEL compact, 2/2003, S. 100ff.
- [58] Farmer, Dan und Venema, Wietse: The Coroner's Toolkit, [www.porcupine.org/forensics/tct.html](http://www.porcupine.org/forensics/tct.html), eingesehen am 28.3.2010
- [59] Müller, Klaus-Rainer: IT für Manager, VIEWEG+TEUBNER, 2008
- [60] Müller, Klaus-Rainer: Der Architekturtrichter, geldinstitute, 6/2002, S. 44ff.
- [61] European Communities: Guidelines on best practices for using electronic information, 1997
- [62] Van Bogart, John W. C.: Media Stability, National Media Laboratory, 1996
- [63] Informationweek: Die 21 Stufen zur Datensicherheit, Informationweek, 13/2000
- [64] Storage Networking Industry Association (SNIA): Common RAID Disk Data Format Specification, Version 2.0, Revision 19, 27. März 2009
- [65] RAID Advisory Board: RAB Classification For Disk Systems, 19. November 1997, [www.raid-advisory.com/classinfo.html](http://www.raid-advisory.com/classinfo.html)
- [66] Auspex Systems: A Storage Architecture Guide, White Paper
- [67] Lange, Rolf: Speicherkonzepte mit viel Feingefühl fusionieren, ntz, 11/2002, S. 48ff.
- [68] Török, Elmar: Entwicklung der Speicherkomponenten, lanline, 2/2003, S. 42ff.
- [69] Storage Networking Industry Association (SNIA) Technical Position: Storage Management Initiative Specification (SMI-S), Version 1.6.0, Revision 5, 2. Sept. 2014
- [70] J. Satran, K. Meth, IBM, C. Sapuntzakis, Cisco Systems, M. Chadalapaka, Hewlett-Packard Co., E. Zeidner, IBM: Internet Small Computer Systems Interface (iSCSI), RFC 3720, April 2004
- [71] M. Rajagopal, E. Rodriguez, R. Weber: Fibre Channel over TCP/IP (FCIP), RFC 3821, Juli 2004
- [72] Lange, Christoph: Trends im Speicherbereich, LANline, 5/2007, S. 52ff.

- [73] Storage Networking Industry Association (SNIA): SNIA Storage Security, Best Current Practices (BCPs) Version 2.1.0, 4.09.2008
- [74] Dembeck, Michael: Firewalls – Gegen virtuelle Katastrophen, KES, 4/1999, S. 23ff.
- [75] Kyas, Othmar und a Campo, Markus: IT-Crackdown, mitp-Verlag, 2002
- [76] Wack, John und Cutler, Ken sowie Pole, Jamie: Guidelines on Firewalls and Firewall Policy, National Institute of Standards and Technology (NIST), NIST Special Publication 800-41, Januar 2002
- [77] Schneier, Bruce: Secrets & Lies, dpunkt.verlag, 2001
- [78] Lipinski, Klaus: Lexikon der Datenkommunikation, DATACOM Buchverlag GmbH, 3. Auflage, 1995
- [79] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschrift-Kataloge, November 2009
- [80] Wurm, Andreas: Überwachungssysteme in Netzwerken, tecCHANNEL compact, 4/5/6/2007, S. 31ff.
- [81] Müller, Klaus-Rainer: Notfallübung – Geplant, geübt, für gut befunden, IT magazin, Heft 1/2007, März 2007, S. 38ff.
- [82] National Institute of Standards and Technology (NIST): Guide for Assessing the Security Controls in Federal Information Systems, Special Publication 800-53A, Juli 2008
- [83] Bundesamt für Sicherheit in der Informationsverarbeitung: Open Vulnerability Assessment System (OpenVAS), [https://www.bsi.bund.de/DE/Themen/ProdukteTools/OpenVAS/OpenVAS\\_node.html](https://www.bsi.bund.de/DE/Themen/ProdukteTools/OpenVAS/OpenVAS_node.html), eingesehen am 02.01.2015
- [84] <kes>/Microsoft-Studie 2014, Lagebericht zur Informations-Sicherheit, Teil 2, <kes>, 5/2014, S. 70ff.
- [85] Jaeger, Stefan: Verbotene Protokolle, KES, 5/2000, S. 6ff.
- [86] Harvard Research Group, Inc.: Highly available servers market assumptions 2000 – 2005, 2001

## 28 Glossar und Abkürzungsverzeichnis

### A

#### AIHA

American Industrial Hygiene Association

#### Alarm – Alert

Ein Alarm ist ein optisches, akustisches, olfaktorisches oder sensorisches Signal, das die Zuständigen oder Hilfe leistenden Stellen aufmerksam machen und zu Gegenmaßnahmen anhalten soll.

#### ANSI

American National Standards Institute

#### Appliance

Eine Appliance (engl. für {Haushalts-}gerät) ist ein Computer, der als eine Art „Black Box“ schlüsselfertig bestimmte festgelegte Funktionalitäten in sich birgt

#### ASSE

The American Society of Safety Engineers

#### Auslöser

Ein „Auslöser“ ist ein Ereignis, durch das der reguläre Geschäftsbetrieb beeinträchtigt wird. Je nach Schwere des Auslösers kann hieraus eine Störung, ein Notfall, eine Krise oder eine Katastrophe entstehen. Auslöser sind beispielsweise technische Defekte, wie Hardware-Ausfall, Naturereignisse wie Sturm, Flut, Tsunami, Erdbeben, kriminelle Handlungen, wie Sabotage, oder menschliches Versagen, wie Fehlbedienungen.

#### Authentifizierung – Authentication

Durch Authentifizierung wird die Echtheit, z. B. der Identität oder einer Information, im Rahmen einer Prüfung bestätigt.

#### Authentisierung – Authentication

Durch Authentisierung wird eine Information glaubwürdig bzw. rechtskräftig gemacht.

#### Autorisierung – Authorization

Die Autorisierung stellt eine Bevollmächtigung oder Genehmigung dar.

### B

#### BCP

1. Business Continuity Plan
2. Best Current Practice

#### Bedrohung – Threat

Eine Bedrohung ist die potenzielle Möglichkeit eines (unerwünschten) Schadens für Prozesse, Ressourcen (z. B. Anlagen, Systeme, Sachen und Menschen), Organisationen, Produkte und Leistungen.

#### Betriebseinflussanalyse – Operational Impact Analysis (OIA)

Mittels der Betriebseinflussanalyse (Operational Impact Analysis {OIA}) wird erhoben, welche Auswirkungen der Ausfall oder die gravierende Beeinträchtigung eines Schutzobjektes, wie z. B. eines IT-Systems, einer Anlage, eines Gebäudes oder eines Services, durch ein Ereignis hat.

#### Brandmeldeanlage (BMA) – Fire Alarm System

Brandmeldeanlagen (BMA) gehören zu den Gefahrenmeldeanlagen. Sie dienen dazu, Brände zu einem frühen Zeitpunkt zu erkennen und zu melden sowie direkte Hilferufe bei Brandgefahren abzusetzen.

**Brute-Force-Attacke**

Brute-Force-Attacken, also Angriffe die auf „roher Gewalt“ beruhen, versuchen auf alle möglichen Arten, das Objekt der Attacke zu „knacken“. Beispiele sind das Aufsprengen von Safes, das Aufbrechen von Fenstern und Türen mittels Brecheisen, etc. Brute-Force-Attacken zum Knacken von Passwörtern probieren beispielsweise alle möglichen Zeichenkombinationen (Buchstaben, Ziffern, Sonderzeichen) aus, bis das gewünschte Passwort ermittelt ist. Bei Vorliegen eines gehashten Passwortes kann durch rechenintensives Erzeugen und Hashen jedes potenziellen Passwortes nach dem gleichen Algorithmus so lange probiert werden, bis das gehashte Ergebnis dem vorliegenden gehashten Passwort entspricht. Aufgrund des Aufwands gelangen hierfür daher „social engineering“ und Wörterbuchattacken eher zum Einsatz.

**BSI**

1. British Standards Institution
2. Bundesamt für Sicherheit in der Informationstechnik

**C****Certified Information Security Auditor™ (CISA®)**

CISA® ist eine Bezeichnung für Sicherheitsauditoren von Informationssystemen, die von der Information Systems Audit and Control Association (ISACA®) zertifiziert wurden.

**Certified Information Security Manager® (CISM®)**

CISM® ist eine Bezeichnung für Sicherheitsmanager von Informationssystemen, die von der Information Systems Audit and Control Association (ISACA®) zertifiziert wurden.

**Certified in the Governance of Enterprise IT® (CGEIT®)**

CGEIT® ist eine Bezeichnung für Personen, die hinsichtlich der Governance der Unternehmens-IT von der Information Systems Audit and Control Association (ISACA®) zertifiziert wurden.

**Certified in Risk and Information Systems Control™ (CRISC™)**

CRISC™ ist eine Bezeichnung für Personen, die hinsichtlich der Risiko- und Informationssystemkontrollelemente von der Information Systems Audit and Control Association (ISACA®) zertifiziert wurden.

**Chief Compliance Officer (CCO)**

Leiter jener Unternehmenseinheit, welche für die Konformität des Unternehmens verantwortlich ist, also für die Bekanntheit und Einhaltung gesetzlicher, aufsichtsbehördlicher und gegebenenfalls normativer Anforderungen.

**Chief Risk Officer (CRO)**

Leiter jener Unternehmenseinheit, welche für das Risikomanagement im Unternehmen verantwortlich ist.

**CIA**

Akronym für Confidentiality, Integrity, Availability

**CIA<sup>2</sup>**

Akronym für Confidentiality, Integrity, Availability, Accountability

**Computer Emergency Response Team (CERT®)**

Das Computer Emergency Response Team (CERT®) Coordination Center (CERT/CC) des Software Engineering Institute (SEI) an der Carnegie Mellon Universität wurde 1988 eingerichtet. Es ist ein Zentrum für Internet-Sicherheits-Expertise. Darüber hinaus



haben Unternehmen ihre eigenen „CERTs“ etabliert, die präventiv und in kritischen Situationen kurzfristig auf Gefährdungen und Angriffe reagieren sollen. Für die Bundesverwaltung in Deutschland existiert seit 1. September 2001 das CERT-Bund. Europäische Behörden-CERTs haben sich in der European Government CERTs (EGC) Group informell zusammengeschlossen.

**Computervirus** – computer virus

Ein Computervirus ist ein nicht selbständig ausführbarer Programmteil, der ein Wirtsprogramm benötigt sowie sich bei Aktivierung selbst vervielfältigen und Schaden verursachen kann, z. B. durch das Löschen von Dateien. Ein Computervirus zeigt in diesen drei Punkten, nämlich der Notwendigkeit eines Wirts, der eigenständigen Verbreitung und der Schadensverursachung Parallelen zu biologischen Viren. Ein Computervirus besteht aus vier prinzipiellen Teilen: einer Viruserkennung, dem Infektionsteil, dem Schadensteil und dem Sprungbefehl. Ist ein Programm infiziert, so ändert sich dessen Größe und Prüfsumme. Nach dem Start eines infizierten Programms und Aufruf des Computervirus sucht der Infektionsteil nach anderen noch nicht infizierten Programmen und kopiert sich dort hinein. Anschließend führt er seine Schadfunktion aus und springt gegebenenfalls in den Programmcode zurück.

**Content-Security-System** – Content Security System

Content-Security-Systeme prüfen anhand eines unternehmensspezifisch festgelegten Regelwerks den Inhalt ein- und ausgehender E-Mails.

**Cracker**

Unter einem Cracker versteht man einen technisch sehr versierten Angreifer, dessen Angriffe darauf abzielen, sich einen Nutzen zu verschaffen und Dritten Schaden zuzufügen.

## D

**Digitales Wasserzeichen** - Digital Watermarking

Digitale Wasserzeichen sind zusätzliche Informationen, die mittels Steganografie in digitale Dateien eingebracht werden, um Urheberfragen klären und damit Urheberrechte schützen zu können.

**Dokumentenlebenszyklusmanagement (DLM)** – Document Lifecycle Management (DLM)

Dokumentenlebenszyklusmanagement bezeichnet die Steuerung, Verfolgung und Verwaltung von Dokumenten während ihres Lebenszyklus von der Erstellung über die Aufnahme, Speicherung, Archivierung, Auffindung, Nutzung und Aussonderung bis hin zur Vernichtung.

**Domain Name Services (DNS)**

Domain Name Services (DNS) übersetzen alphanumerische Internetadressen (URL) in eine IP-Adressen. DNS-Server sind also das „Telefonbuch“ des Internet und damit dessen Rückgrat.

**DoS-Angriff** – Denial of Service (DoS) Attack

Angriff, bei dem ein Zielsystem oder –Netzwerk lahmgelegt wird.

## E

**Einbruchmeldeanlage (EMA)** – burglar alarm system

Einbruchmeldeanlagen (EMA) gehören zu den Gefahrenmeldeanlagen. Sie dienen dazu, Flächen und Räume auf unbefugtes Eindringen sowie Gegenstände auf unbefugte Wegnahme zu überwachen.

**Eintrittswahrscheinlichkeit** – probability of occurrence

Die Wahrscheinlichkeit, mit der ein Ereignis eintritt, heißt Eintrittswahrscheinlichkeit. Sie wird bei der Bewertung des als Schadensausmaß  $\times$  Eintrittswahrscheinlichkeit de-

finierten Bruttoisikos bzw. der Kosten-Nutzen-Abwägung zur Festlegung des Umfangs von Sicherheits- und Kontinuitätsmaßnahmen genutzt. Hierbei muss beachtet werden, dass Eintrittswahrscheinlichkeiten oftmals retrospektiv (ex post) ermittelt werden. D. h. die Eintrittswahrscheinlichkeit wird anhand der zurückliegenden Ereignisse innerhalb eines vorgegebenen Zeitraums ermittelt. Generell ist bei Wahrscheinlichkeiten daran zu denken, dass ein Ereignis, das z. B. alle 100 Jahre auftritt, auch morgen, heute oder jetzt auftreten kann.

**Elektronische Lautsprecheranlage (ELA)**

Elektronische Lautsprecheranlagen (ELA) in Gebäuden dienen dazu, Personen zu alarmieren bzw. zu informieren.

**Entmilitarisierte Zone – Demilitarized Zone (DMZ)**

Eine entmilitarisierte Zone ist der Bereich zwischen einer äußeren und einer inneren Firewall. In dieser Zone werden beispielsweise Web-Server angesiedelt.

**Exploit**

Exploits sind Programme, die Sicherheitslücken oder Fehlfunktionen von Computerprogrammen nutzen, um in diese einzudringen. Sie werden von Hackern bzw. Crackern geschrieben und auch als Hack-Werkzeuge bezeichnet.

**F**

**Falsch negativ – False negative**

Ist das Ergebnis einer Prüfung, z. B. zur Zutritts- oder Zugangskontrolle, falsch negativ, so erfolgt fälschlicherweise eine Ablehnung.

**Falsch positiv – False positive**

Ist das Ergebnis einer Prüfung, z. B. zur Zutritts- oder Zugangskontrolle, falsch positiv, so erfolgt fälschlicherweise eine Freigabe.

**False Acceptance Rate (FAR)**

Die False Acceptance Rate (FAR) bzw. Falsch-Akzeptanzrate gibt an, wie oft statistisch ein Objekt fälschlicherweise akzeptiert wird. Beim Einsatz biometrischer Verfahren, beispielsweise zur Zutritts- oder Zugangskontrolle, ist diese Angabe extrem sicherheitsrelevant, da eine fälschliche Erkennung unberechtigten Personen Zutritt oder Zugang ermöglicht.

**False Rejection Rate (FRR)**

Die False Rejection Rate (FRR) bzw. Falsch-Rückweisungsrate gibt an, wie oft statistisch ein Objekt fälschlicherweise abgelehnt wird. Beim Einsatz biometrischer Verfahren, beispielsweise zur Zutritts- oder Zugangskontrolle, bedeutet dies, dass berechtigte Personen fälschlicherweise abgewiesen werden. Dies mindert potenziell die Akzeptanz eines solchen Systems und kann zu kritischen Situationen führen.

**Fibre Channel (FC)**

Fibre Channel umfasst einen Satz von Standards für eine Technologie, die Hochgeschwindigkeitsdatenübertragung zwischen Computern ermöglicht. FC unterstützt Punkt-zu-Punkt-, Switch- und Loop-Technologien.

**Financial Transaction Services (FinTS)**

Die Financial Transaction Services (FinTS) sind ein Standard des Zentralen Kreditausschusses (ZKA). Er dient der Vereinheitlichung der Schnittstelle zwischen Bankkunde und Finanzinstitut. Die Version 4.1 der FinTS liegt seit Januar 2014 vor. Sie besteht aus FinTS Formals, XML Syntax, FinTS Messages und FinTS Security. FinTS Formals enthält Festlegungen zur Syntax, Kommunikationsszenarien, Kommunikati-

onsverfahren, FinTS Dialoge und FinTS Datagramme. FinTS Messages spezifiziert Geschäftsvorfälle. FinTS Security beschreibt das PIN/TAN- (FinTS PIN/TAN) und das HBCI-Legitimationsverfahren (FinTS HBCI). FinTS HBCI ermöglicht die digitale Signatur, z. B. per Chipkarte.

**Fingerabdrucknehmen** – fingerprinting

Der IP-Stack jedes Rechners hat Eigenheiten, die sich insbesondere in der Antwort des Betriebssystems auf fehlerhafte Pakete bemerkbar macht. Es hinterlässt sozusagen einen Fingerabdruck. Um über das Netz an Informationen über das Betriebssystem zu gelangen, dient das „Fingerabdrucknehmen“. Beim aktiven Fingerabdrucknehmen werden fehlgeformte Pakete an das Zielsystem gesendet und die Antwort mit einer Datenbank verglichen, in der die Reaktionen verschiedener Betriebssysteme auf fehlgeformte Pakete zuvor eingetragen wurden. Beim passiven Fingerabdrucknehmen werden die Spuren des sendenden Betriebssystems in den ankommenden Paketen analysiert. Charakteristika sind beispielsweise die „time to live“ (TTL) ausgehender Pakete, die „window size“, das „don't fragment bit“ (DF) und die Festlegung des „type of service“ (TOS).

**Firewall**

Eine Firewall („Brandschutzmauer“) ist eine Netzkomponente, die zwei Netze mit unterschiedlichem Sicherheitsniveau so miteinander verbinden soll, dass das zu schützende Netz vor Übergriffen aus dem anderen Netz geschützt wird.

**Forensische Informatik**

Die forensische Informatik beschäftigt sich mit der Spurensuche auf Computern, z. B. im Rahmen staatsanwaltlicher Ermittlungen oder nach erfolgreichen Angriffen.

**Forum of Incident Response and Security Teams (FIRST)**

Das globale Forum of Incident Response and Security Teams (FIRST) bringt eine Vielzahl von Computer Security Incident Response Teams aus öffentlichen und kommerziellen sowie Bildungsbereichen zusammen. Ziel ist die Förderung der Zusammenarbeit und Koordination im Hinblick auf die Vorbeugung gegenüber sicherheitsrelevanten Ereignissen, die schnelle Reaktion darauf sowie der Informationsaustausch.

**Funk-LAN** – Wireless Local Area Network (WLAN)

Funk-LANs (WLAN) stellen ein drahtloses lokales Netz dar. Sie basieren auf dem vom Institute of Electrical and Electronics Engineers (IEEE) 1997 festgelegten Standard IEEE 802.11. Da sie einfach zu installieren sind, kommen sie sowohl bei temporären Installationen zum Einsatz, z. B. auf Messen, aber auch bei langfristigerer Nutzung, z. B. auf Flughäfen und Bahnhöfen sowie in Unternehmen und bei Privatpersonen. Der Netzzugang erfolgt über öffentliche Hot Spots bzw. über Access Points. Die Kompatibilität von Produkten zu IEEE 802.11 dokumentiert die Herstellervereinigung Wireless Ethernet Compatibility Alliance (WECA) durch Vergabe des Wi-Fi<sup>®</sup>-Zertifikats.

IEEE 802.11i beschreibt die Sicherheitsarchitektur Robust Security Network (RSN), das zur Authentisierung das Extensible Authentication Protocol (EAP) und zur Verschlüsselung AES nutzt. IEEE 802.11-2007 integriert die IEEE 802.11-a, b, d, e, g, h, i, j. IEEE 802.11-2012 basiert auf IEEE 802.11-2007 und integriert weitere erfolgte Änderungen bzw. Ergänzungen.

**G****Gefahrenmeldeanlage (GMA)**

Gefahrenmeldeanlagen (GMA) dienen dazu, Gefahren für Personen und Sachen durch Einbruch, Überfall, Feuer und Wasser zu erkennen und zu melden.

**Geschäftskritische Unterlagen** – Vital Records

„Lebenswichtige“, d. h. geschäftskritische Unterlagen und Aufzeichnungen (vital records) sind für den Geschäftsbetrieb unverzichtbar und müssen daher – auch im Notfall – verfügbar sein und erhalten bleiben. Beispiele hierfür können geheime Produktionsverfahren und –formeln, Fahrzeugbriefe, Informationen über und Verträge mit Kunden, Lieferanten, Dienstleistern, Versicherungen und Mitarbeitern, Vollmachtenregelungen, etc. sein.

**Governance**

Unter Governance ist die gute und verantwortliche Unternehmensführung zu verstehen, die sich u. a. an relevanten gesetzlichen Vorschriften und vergleichbaren Vorgaben zur Leitung und Überwachung von Unternehmen sowie diesbezüglichen international und national anerkannten Standards orientieren sollte. Dies beinhaltet den wirtschaftlichen Einsatz von Ressourcen, das Risikomanagement und die angemessene Berücksichtigung aller Bezugsgruppen.

**GRC**

Governance, Risk & Compliance

**H****Hacker**

Unter einem Hacker versteht man einen technisch sehr versierten Angreifer, dessen Angriffe darauf abzielen, Schwachstellen in IKT-Systemen aufzudecken. Primäres Ziel ist es dabei üblicherweise jedoch nicht, sich persönlich wirtschaftliche Vorteile zu verschaffen und Dritten einen direkten wirtschaftlichen Schaden zuzufügen, sondern auf Schwachstellen hinzuweisen.

**Home Banking Computer Interface (HBCI)**

Das Home Banking Computer Interface (HBCI) ist ein Element der Financial Transaction Services (FinTS), eines Standards des Zentralen Kreditausschusses (ZKA).

**I****IKT – ICT** (information and communication technology)

Informations- und Kommunikationstechnologie

**IKTSiPyr** – ICTSaSePyr

IKT-Sicherheitspyramide

**Informationslebenszyklusmanagement (ILM)** – Information Lifecycle Management (ILM)

Informationslebenszyklusmanagement bezeichnet die Kosten-Nutzen-optimierte Steuerung, Verfolgung, Speicherung und Verwaltung von Informationen jeglicher Art und jeglichen Typs während ihres Lebenszyklus von der Erstellung über die Aufnahme, Speicherung, Archivierung, Auffindung, Nutzung und Aussonderung bis hin zur Vernichtung. Ziel ist es, Informationen entsprechend ihrer geschäftlichen Bedeutung und ihren Sicherheitsanforderungen sowie ihrer Zugriffs- und Änderungshäufigkeit zu minimalen Kosten rechtzeitig am richtigen Ort verfügbar zu haben. Dies erfordert eine kontinuierliche Optimierung der Architektur aus Prozessen und Verfahren sowie Ressourcen und Technologien.

**Institut der Wirtschaftsprüfer (IDW)**

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) ist ein eingetragener Verein, der Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften Deutschlands auf freiwilliger Basis vereint.

**Integrität – Integrity**

s. Unverfälschtheit

**International Engineering Consortium (IEC)**

Das International Engineering Consortium (IEC) ist eine Non-Profit-Organisation mit dem Ziel, den weltweiten technologischen und wirtschaftlichen Fortschritt im Bereich hochtechnisierter Industrien und universitärer Gemeinschaften zu katalysieren.

**International Organization for Standardization (ISO)**

Die International Organization for Standardization (ISO) ist ein Netz nationaler Standardisierungsinstitute. In ihr sind mehr als 160 Länder vertreten, jedes durch ein Mitglied. Das Zentralsekretariat der ISO hat seinen Sitz in Genf und koordiniert das Gesamtsystem.

Die ISO ist keine staatliche Organisation. Ihre Mitglieder sind daher keine Delegationen nationaler Regierungen.

Manch einer mag sich schon gefragt haben, warum die Abkürzung ISO heißt, wo die englischen Anfangsbuchstaben doch „IOS“ und die französischen „OIN“ (Organisation Internationale de Normalisation) ergäben. Dies rührt daher, dass zu Beginn entschieden wurde, das Wort aus dem griechischen „isos“ (ἴσος: gleich) abzuleiten.

Die ISO verwendet folgende Abkürzungen für den Status Ihrer Normen:

- AWI= Approved Work Item
- CD= Committee Draft
- FCD= Final Committee Draft
- DIS= Draft International Standard (Normentwurf)
- FDIS= Final Draft International Standard
- ISO/TR= ISO Technical Report
- ISO/TS= ISO Technical Specification
- NP= New Work Item Proposal
- PRF= Proof of a new International Standard
- WD= Working Draft

**ISiPyr – ISiPyr (Information Safety/Security Pyramid)**

IT- bzw. IKT-Sicherheitspyramide

**IT-Governance**

Unter IT- bzw. IKT-Governance ist die an der Geschäftstätigkeit, der Unternehmensstrategie und den Unternehmenszielen ausgerichtete gute und verantwortliche Leitung der IT bzw. IKT zu verstehen. Sie sollte sich u. a. orientieren an relevanten gesetzlichen, aufsichtsbehördlichen und vergleichbaren Vorgaben und Standards zur Leitung, Steuerung und Überwachung der IT bzw. IKT, an diesbezüglichen international und national anerkannten Normen und Standards, an Good und Best Practices, an De-facto-Standards sowie an vertraglichen Vereinbarungen. Dies beinhaltet den wirtschaftlichen Einsatz von Ressourcen, das Risikomanagement mit der Optimierung und zielgerichteten Steuerung von Risiken und die angemessene Berücksichtigung aller Bezugsgruppen.

Eine ähnliche, aber weniger detaillierte Definition wählt das IT Governance Institute® in COBIT® 4.0, indem es – frei übersetzt – IT-Governance als Verantwortlichkeit der Führungskräfte und -gremien bezeichnet, durch Führung, Organisationsstruktur und Prozesse dafür zu sorgen, dass die IT die Strategien und Ziele des Unternehmens bzw. der Organisation trägt und ausweitet.

**K****Kerberos™ – Kerberos™**

Kerberos™ ist ein ticket-basiertes Authentisierungsverfahren, das vom MIT entwickelt wurde. Es ist benannt nach dem Höllenhund Kerberos, dem Sohn des Typhon und der Echidna, der in der griechischen Mythologie den Eingang zum Hades, der Unterwelt, benannt nach dem Gott Hades, bewachte. Er ließ keinen der Eingetretenen mehr heraus. Nur Orpheus und Herakles bezwangen ihn.

**Key-Logger**

Key-Logger protokollieren die Tastatureingaben des Nutzers. Es existieren sowohl Software- als auch Hardware-Key-Logger. Software-Key-Logger kommen einerseits als ordnungsgemäße Software-Programme zum Einsatz, werden andererseits aber auch von Angreifern über Trojaner verbreitet.

Hardware-Key-Logger lassen sich zwischen Tastatur und Rechner stecken, z. B. an der USB-Schnittstelle. Es gibt Hardware-Key-Logger, die 2 Mio. Tastatureingaben aufzeichnen können oder die aufgezeichneten Tastatureingaben automatisch per E-Mail über einen vorhandenen Funkzugangspunkt (Wireless Access Point) übermitteln. Im Gegensatz zu Software-Key-Loggern verbleiben nach der Entfernung der Komponente keine verräterischen Datenspuren auf dem überwachten Computer.

**Kommunales Netz – Metropolitan Area Network (MAN)**

Ein MAN dient der Zusammenschaltung von Systemen und Netzen in Ballungsräumen.

**Kontrollelement – Control**

Ein Kontrollelement bzw. eine Kontrollaktivität (Control Activity) dient dazu, die Erreichung eines Kontrollziels nachzuweisen, indem es dieses überwacht und seine Erfüllung sicherstellt. Ein Kontrollelement für den Zutritt bzw. Zugang nur berechtigter Personen erfordert beispielsweise ein Rechtekonzept und einen dokumentierten Berechtigungsvergabeprozess mit ordnungsgemäß unterzeichneten Berechtigungsanträgen und dementsprechend eingerichteten Berechtigungen. Kontrollelemente für den Durchsatz von Prozessen, Systemen und Anlagen sind beispielsweise geeignete Mess- und Überwachungstools, die beim Erreichen vorgegebener Warnschwellen so frühzeitig alarmieren, dass Maßnahmen zur Einhaltung der Kontrollziele noch möglich sind. Darüber hinaus ermöglichen regelmäßige Trendanalysen eine proaktive Vermeidung von Engpässen.

**Kontrollziel – Control Objective**

Kontrollziele leiten sich aus den internen und externen Anforderungen sowie SLAs ab. Kontrollziele können beispielsweise sein, dass der Zutritt zum Serverraum und der Zugang zu einer Anwendung nur berechtigten Personen möglich ist, oder dass ein IKT-System oder eine Anlage eine vereinbarte Verfügbarkeit oder einen vereinbarten Durchsatz aufweist.

**Kritikalität – Criticality**

Kritikalität bezeichnet, wie kritisch bzw. wichtig beispielsweise ein Prozess oder eine Ressource für ein Unternehmen ist.

**Kritische Infrastrukturen (KRITIS)**

Als Kritische IT-Infrastrukturen (KRITIS) versteht das Bundesministerium des Innern „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere drama-

tische Folgen eintreten würden.“ [Bundesministerium des Innern, Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden, Mai 2011]

Zu den kritischen Infrastruktursektoren gehören u. a. Transport und Verkehr, Energie, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Wasser, Ernährung, Gesundheit, Staat und Verwaltung sowie Medien.

[www.kritis.bund.de, Glossar, Kritische Infrastrukturen (KRITIS), eingesehen am 08.01.2015]

## L

### **Layer of Protection Analysis (LOPA)**

Die Layer of Protection Analysis (LOPA), d. h. die Analyse des Schutzniveaus, ist eine Methode zur Gefahrenabschätzung und Risikobewertung. Sie liegt zwischen stärker qualitativ orientierten Bewertungen, wie z. B. HAZOP, und stärker quantitativ orientierten Bewertungen, die sich beispielsweise in der Fehlerbaumanalyse (Fault Tree Analysis) zeigen.

### **Lokales Netz – Local Area Network (LAN)**

Lokale Netze dienen dem internen Hochgeschwindigkeits-Datenaustausch und befinden sich im privaten Besitz des Betreibers. Sie sind beispielsweise in Büros und auf Firmengeländen anzutreffen.

## M

### **MAC**

1. Mandatory Access Control – erzwungene Zugriffskontrolle
2. Medium Access Control – medienpezifisches Zugangsprotokoll
3. Message Authentication Code – Nachrichtenauthentisierung

## N

### **Nacharbeit**

Nacharbeit wird in der Regel dann erforderlich, wenn durch den Übergang zum oder vom Notbetrieb sowie im Notbetrieb selbst Leistungen nicht oder nur eingeschränkt erbracht werden konnten. Die liegen gebliebenen Arbeiten müssen nachgearbeitet werden.

### **Network Address Translation (NAT)**

Durch Network Address Translation können IP-Adressen eines (meist internen) Netzes auf die IP-Adressen eines (meist öffentlichen) Netzes übersetzt werden. Hierdurch lassen sich z. B. die internen IP-Adressen gegenüber dem öffentlichen Netz verbergen. Die Umsetzung kann statisch (stets dieselbe Zuordnung) oder dynamisch (Zuordnung erfolgt nach bestimmten Kriterien während der Laufzeit) erfolgen.

### **Network Attached Storage (NAS)**

NAS stellt ein Speichersystem dar, das als (zentraler) Datei-Server dient, und an ein LAN oder WAN angeschlossen ist.

### **Netzersatzanlage (NEA)**

Eine Netzersatzanlage ist eine Stromversorgung in Form eines Notstromaggregats, z. B. Notstromdiesel, mit dem ein längerfristiger Stromausfall überbrückt werden kann.

### **NIST**

National Institute of Standards and Technology

**Notbetrieb**

Unter Notbetrieb wird der vom regulären Betrieb abweichende und in der Regel eingeschränkte Betrieb nach einem Notfall oder einer Katastrophe bezeichnet.

**O****OpenPGP**

OpenPGP, dessen Message Format in RFC 4880 spezifiziert ist, stellt Dienste zur digitalen Signatur und zur Verschlüsselung von Nachrichten, z. B. E-Mails, und Dateien zur Verfügung. OpenPGP basiert auf einer Software-Familie, die von Philip R. Zimmermann entwickelt wurde. Zum Schutz der Vertraulichkeit nutzt OpenPGP die symmetrische Verschlüsselung in Verbindung mit der Verschlüsselung mit einem öffentlichen Schlüssel (public key).

Zum Verschlüsseln und Signieren von E-Mails unter Windows® kann z. B. Gpg4win (GNU Privacy Guard for Windows®) genutzt werden. Gpg4win unterstützt sowohl OpenPGP als auch S/MIME. Bitte beachten Sie, dass es sich bei dieser Tool-Angabe um eine unbewertete Momentaufnahme handelt.

**Open Systems Interconnection-Referenzmodell (OSI-Referenzmodell)**

Das Open Systems Interconnection (OSI)-Referenzmodell der International Organization for Standardization (ISO) wurde als Grundlage für die Bildung von Kommunikationsstandards geschaffen und besteht aus 7 Schichten.

**Organisierte Kriminalität (OK) – Organized Crime**

Organisierte Kriminalität ist in den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV, Stand 2008), Anlage E wie folgt definiert: „Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder auf unbestimmte Dauer arbeitsteilig a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, b) unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder c) unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken. Der Begriff umfasst nicht Straftaten des Terrorismus.“

**Organization for the Advancement of Structured Information Standards (OASIS®)**

Die Organization for the Advancement of Structured Information Standards (OASIS®, [www.oasis-open.org](http://www.oasis-open.org)) ist eine globale Non-Profit-Organisation, die die Entwicklung, Konvergenz und Anpassung von E-Business-Standards vorantreibt. Sie wurde 1993 unter dem Namen SGML Open als Konsortium von Anbietern und Nutzern gegründet, um Richtlinien für die Interoperabilität zwischen jenen Produkten zu entwickeln, welche die Standard Generalized Markup Language (SGML) unterstützen. 1998 erfolgte die Umbenennung in OASIS®, um damit das erweiterte Aufgabengebiet zu unterstreichen, das z. B. die Extensible Markup Language (XML) und andere diesbezügliche Standards umfasst.

**P****Public Available Specification (PAS)**

Bei dringendem Marktbedarf nach einem standardisierenden Dokument kann ein technisches Komitee der ISO sich für eine kurzfristige Veröffentlichung als Public Available Specification (PAS) oder Technische Spezifikation (TS) entscheiden.



**Phishing**

Phishing ist ein Kunstwort aus „Password fishing“. Es beschreibt eine kriminelle Handlung, bei der Datendiebe versuchen, durch gefälschte E-Mails in den Besitz vertraulicher Daten, wie z. B. PINs, Passwörter, Konto- oder Kreditkartennummern zu gelangen, d. h. vertrauliche Daten „abzufischen“. Die E-Mails sehen Original-Nachrichten von Unternehmen, z. B. Banken, sehr ähnlich. Betätigt der Empfänger den dortigen Link, so gelangt er auf eine gefälschte Webseite, auf der er aufgefordert wird, vertrauliche Daten einzugeben. Um die Attraktivität derartiger Betrügereien einzudämmen, können z. B. Überweisungsmittele limitieren dienen. Die Anzeige der zuletzt getätigten Transaktion ermöglicht das Erkennen einer Manipulation beim nächsten Einloggen. Geeignete Challenge-Response-Verfahren mit Einmalpasswörtern können je nach Gegebenheit den Nutzen des Abfischens weiter reduzieren.

**PIN – PIN**

Persönliche Identifikationsnummer – Personal Identification Number

**PROSim**

Das Akronym PROSim steht für die zweite Dimension der Sicherheitspyramide V und repräsentiert die Prozesse, Ressourcen und Organisation für das Sicherheitsmanagement. Je nach Themenstellung lautet das Akronym z. B. bei Arbeitsschutzmanagement PROArm, bei BCM PROBCM, bei Kontinuitätsmanagement PROKom, bei Projektmanagement PROProm, bei Qualitätsmanagement PROQuam, bei Risikomanagement PRORim, bei Servicemanagement PROSem, bei Sourcing-Management PROSom, bei Testmanagement PROTem.

**Protokollauswertung**

Die Protokollauswertung dient der Überprüfung (z. B. durch die Revision) von Protokolldateien, die bei der Protokollierung entstehen.

**Protokollierung – logging**

Die Protokollierung dient der Aufzeichnung sicherheitsrelevanter Ereignisse, wie z. B. des Zugangs zu Netzen und Systemen oder des Zugriffs auf Daten.

**ProTOPSi**

Das Akronym ProTOPSi, das die zweite Dimension der Sicherheitspyramide III repräsentiert, steht für Prozesse, Technologie, Organisation und Personal für Sicherheit. Der Begriff Technologie wurde hierbei sehr weit gefasst und bezieht sich u. a. auf Verfahren, Methoden, Werkzeuge und Technik im Sinne von Hardware und Software sowie Infrastruktur, wie z. B. Gebäude. Die Sicherheitspyramide IV fasst die Begriffe Technologie und Personal aus Gründen der Systematik zum umfassenden und verständlicheren Begriff Ressource zusammen.

**Public Key Infrastructure (PKI)**

Die Public Key Infrastructure (PKI) umfasst Software, Verschlüsselungstechnologien und Dienste. Sie unterstützt den Einsatz von Verschlüsselungs- und Signaturdiensten, indem sie die Erstellung, Verteilung, Verwaltung, Prüfung und Rücknahme von Zertifikaten und Schlüsseln regelt.

**R****RAM**

1. Ein Random Access Memory (RAM) ist ein Halbleiterspeicher mit kurzen Zugriffszeiten, dessen gespeicherte Informationen bei Abschalten der Betriebsspannung verloren gehen.
2. Reliability, Availability, Maintainability (RAM)

### **Records Management**

Records Management lässt sich im Deutschen mit dem etwas altertümlich anmutenden Begriff Schriftgutverwaltung übersetzen. Records Management dient der Kennzeichnung, Steuerung, Verfolgung und Verwaltung geschäftsrelevanter Unterlagen in Form von physischen und elektronischen Informationen, Dokumenten, Aufzeichnungen und Nachweisen von deren Erstellung über die Aufnahme, Aufbewahrung, Auffindung, Nutzung und Aussonderung bis hin zur Vernichtung.

Records Management begleitet die Prozesse einer Organisation während ihres gesamten Lebenszyklus. Es beinhaltet u. a. Vorgaben für das Ordnungs- und Ablagesystem, Namenskonventionen für die Identifizierung und Sicherheitsklassifizierung sowie Standards für die Versionierung und Datierung, beginnend mit der Erst- und später dem Änderungsdatum, über das jeweilige Freigabedatum bis hin zum Aussonderungsdatum. Prozess- und Strukturorganisation mit Zuständigkeiten und Verantwortlichkeiten sind ebenso zu regeln wie Zutritts- und Zugriffs- sowie Bearbeitungsrechte. Die Normenreihe ISO 15489 behandelt das Records Management, das in der deutschen Fassung mit Schriftgutverwaltung übersetzt ist. MoReq2, die Model Requirements for the Management of Electronic Records, Stand: 2008, der europäischen Kommission beschreiben auf über 200 Seiten vorrangig funktionale Anforderungen an Electronic Records Management Systeme (ERMS). Kapitel 4 von MoReq2 geht auf sicherheitsrelevante Anforderungen ein, beispielsweise hinsichtlich Zugangs- und Zugriffsschutz, Protokollierung, Datensicherung und -wiederherstellung sowie geschäftskritische Unterlagen (Vital Records). Als „gute Praxis“ existiert das Good Electronic Records Management (GERM).

### **Resilience**

(Fault oder Failure) Resilience, d. h. Fehlerelastizität bzw. Fehlertoleranz, bezeichnet die Eigenschaft eines Unternehmens, eines Prozesses, einer Ressource, eines Produktes oder einer Dienstleistung, sich trotz einer begrenzten Anzahl von Fehlern weiterhin anforderungs- bzw. spezifikationsgerecht zu verhalten, eventuell auf einem akzeptierten reduziertem Leistungsniveau.

### **Return on Safety, Security and Continuity Investment (RoSSCI)**

Als Return on Safety, Security and Continuity Investment (RoSSCI) bezeichne ich den Ertrag und den vermiedenen Schaden, den ein Unternehmen aufgrund von Investitionen hat, welche es in die Betriebs- und Angriffssicherheit sowie die Kontinuität getätigt hat.

### **Return on Security Investment (RoSI)**

Return on Security Investment (RoSI) bezeichnet den Ertrag und den vermiedenen Schaden, den ein Unternehmen aufgrund einer in die Sicherheit getätigten Investition hat.

### **Risiko – Risk**

Risiko bezeichnet das Potenzial, dass eine Bedrohung aufgrund einer Schwachstelle einen Schaden anrichtet.

### **Risikoanalyse – Risk Analysis**

Risikoanalyse ist der Prozess zur Ermittlung, Analyse und Bewertung des Schadenspotenzials und des Bedrohungspotenzials sowie des Schwachstellenpotenzials aufgrund von Sicherheits- und Kontinuitätsdefiziten sowie zur Identifikation zusätzlich erforderlicher Sicherheits- und Kontinuitätsmaßnahmen.

**S****Schadsoftware** – Malware

Schadsoftware umfasst z. B. Viren, Würmer und trojanische Pferde.

**Schwachstelle** – Weakness

Eine Schwachstelle stellt eine Sicherheitslücke oder ein Sicherheitsdefizit dar.

**Sensibilisierung**

Sensibilisierungsmaßnahmen für die Themen Sicherheit, Kontinuität und Risiko dienen dazu, bei Mitarbeitern Bewusstsein für Sicherheits- und Kontinuitätsanforderungen, Bedrohungen, Schwachstellen und Risiken sowie Sicherheits- und Kontinuitätsmaßnahmen zu schaffen.

**Service-Level-Vereinbarung (SLV)** – Service Level Agreement (SLA)

Eine Service-Level-Vereinbarung (Service Level Agreement (SLA)) beinhaltet die Festlegung der zwischen Service-Geber und Service-Nehmer vereinbarten messbaren Qualität (Servicegüte) der Leistungen.

**Sicherheitshandbuch (SIHA)**

Das Österreichische Informationssicherheitshandbuch (SIHA) beschäftigt sich mit dem Informationssicherheitsmanagement und Maßnahmen zur Informationssicherheit.

**Sicherheitskonzept** – Safety/Security Specification

Ein Sicherheitskonzept legt fest, welche Maßnahmen zur Erhöhung der Sicherheit für ein spezifisches Thema oder Schutzobjekt, z. B. eine Anlage, ein IKT-System, ein Netz, eine Anwendung, ein Produkt oder eine Leistung, ergriffen werden sollen.

**Sicherheitsleitlinien** – Safety/Security Policies

Sicherheitsleitlinien geben einen Orientierungsrahmen für die Sicherheit im Unternehmen.

**Sicherheitsmaßnahme** – Safeguard bzw. Safety/Security Measure

Maßnahme, Mechanismus, Prozess oder Schutzsubjekt zur Vermeidung, Verringerung oder Verlagerung eines Risikos bzw. zur Steigerung des Sicherheitsniveaus.

**Sicherheitsniveau** – Safety/Security Level

Das Sicherheitsniveau beschreibt das Maß an Sicherheit.

**Sicherheitsphilosophie** – Safety/Security Philosophy

Die Sicherheitsphilosophie legt in schriftlicher überblicksartiger Form fest, welche Bedeutung und Ausprägung das Thema Sicherheit haben soll.

**Sicherheitspyramide** – Occupational Health, Safety, Security, Continuity and Risk (Management) Pyramid

Die Sicherheits(management)pyramide<sup>Dr.-Ing. Müller</sup> stellt ein anschauliches, strategisches, systematisches und ganzheitliches Vorgehensmodell zum schrittweisen Aufbau und zur Weiterentwicklung des Sicherheitsmanagements dar. Die Sicherheitspyramide enthält das Sicherheits-, Kontinuitäts- und Risikomanagement. Ich bezeichne sie daher auch als RiSiKo-Pyramide bzw. RiSiKo-Managementpyramide. Sie ist hierarchisch aufgebaut und berücksichtigt den Lebenszyklus von Prozessen und Ressourcen, wie z. B. (IKT-) Systemen, der Organisation sowie Produkten und Dienstleistungen hinsichtlich der Themenfelder Prozesse, Ressourcen und Organisation und im Hinblick auf das Sicherheitsmanagement (PROSim).

Der Begriff Prozess umfasst hierbei Geschäfts-, Support- und Begleitprozesse. Hinter dem Begriff Ressource verbergen sich alle materiellen und immateriellen Ressourcen vom Gebäude mit seinen Räumlichkeiten und der haustechnischen Infrastruktur über Fertigungsstraßen, Produktionsanlagen, Maschinen, Informations- und Kommunikationssysteme, Arbeitsmittel, Materialien, finanzielle Mittel, Methoden, Daten, Know-how, Image und Services bis hin zu Personal. Die Organisation umfasst die Linien-

organisation, wie sie beispielsweise im Organigramm mit Geschäfts-, Bereichs-, Abteilungs- und Gruppenleitung sowie Stabsabteilungen dargestellt ist, sowie Rollen, wie z. B. Projektmanager und Projektleiter.

**Sicherheitsrichtlinien** – Occupational Health, Safety, Security and Continuity Guidelines

Sicherheitsrichtlinien geben einen einzuhaltenden Rahmen z. B. bei der Entwicklung von Konzepten vor.

**Sicherheitsstandards** – Occupational Health, Safety, Security and Continuity Standards

Sicherheitsstandards geben – wie auch Sicherheitsrichtlinien – einen einzuhaltenden Rahmen vor

**Sicherheitsstrategie** – Occupational Health, Safety, Security and Continuity Strategy

Die Sicherheitsstrategie legt fest, welches Maßnahmenbündel von der Prävention über das Monitoring, die Detektion und Meldung bzw. Alarmierung sowie der Reaktion und der Evaluation des Schadens bis hin zur Wiederherstellung, der Nacharbeit (Postvention) und der Verbesserung (Emendation) zur Vermeidung, Verringerung oder Verlagerung eines Risikos in welchem Umfang ergriffen werden sollte.

**Sicherheitsstudie** – Occupational Health, Safety, Security and Continuity Assessment

Eine Sicherheitsstudie beinhaltet den Prozess zur Ermittlung, Analyse und Bewertung von Risiken sowie zur Identifikation zusätzlich empfohlener oder erforderlicher Sicherheitsmaßnahmen. Sie kann für unterschiedliche Schutzobjekte und mit unterschiedlichem Fokus durchgeführt werden, z. B. im Hinblick auf betrieblichen Gesundheits- bzw. Arbeitsschutz, auf Betriebs- und Angriffssicherheit, auf Kontinuität sowie für ausgewählte Sicherheitskriterien.

**Sicherheitsziele** – Occupational Health, Safety, Security and Continuity Objectives

Sicherheitsziele leiten sich aus der Sicherheits-, Kontinuitäts- und Risikopolitik ab und werden im Rahmen einer Schutzbedarfsanalyse bzw. Business Impact Analysis anhand angenommener Sicherheitsverletzungen und deren Konsequenzen je Sicherheitskriterium ermittelt.

**Single Point of Failure**

Ein „Single Point of Failure“ (Einzelfehler) ist eine Stelle, an der ein einzelner Fehler zu einem Ausfall führt. Derartige Situationen ergeben sich bei nicht konsequent redundanter Auslegung von Ressourcen.

**Single Sign-on** – Single Sign-on

Das Single Sign-on dient dazu, mit nur einem Identifikations- und Authentisierungsvorgang Zugang zu verschiedenen Systemen zu erhalten. Dies gilt in entsprechender Form für den Zutritt zu verschiedenen Gebäuden oder Räumlichkeiten.

**Skript Kiddie**

Die Bezeichnung Skript Kiddie kennzeichnet Internet-Nutzer, die Angriffe unter Nutzung vorgefertigter Schadprogramme durchführen. Daher reichen für ihre Angriffe bescheidene technische Kenntnisse aus. Ihre Attacken erfolgen meist wahllos und nicht zwangsläufig zur vorsätzlichen Schädigung der Angegriffenen, sondern entspringen teilweise der Neugier z. B. jugendlicher Internet-Nutzer.

**Sniffer**

Ein Sniffer ist ein Programm, das Datenpakete, die über ein Netz übertragen werden, heimlich mitliest.

**Social Engineering**

Beim Social Engineering bringt ein Angreifer sein Opfer dazu, Dinge zu tun, die der Angreifer will. So gibt sich ein Angreifer z. B. als Netzadministrator oder Sicherheits-

manager aus und erschleicht sich unter einem Vorwand Passwörter. Meist erfolgen diese Angriffe per Telefon, da es so schwieriger ist, des Täters habhaft zu werden. Aber auch entsprechendes Auftreten kann zum unberechtigten Zutritts- und Zugangserfolg führen, genauso wie der Auftritt als vermeintlicher Repräsentant eines Herstellers und „bewaffnet“ mit entsprechender Hardware. Phishing ist ebenfalls ein Beispiel für Social Engineering.

#### **Spionagesoftware – Spyware**

Spionagesoftware sind Programme, die mit oder ohne das Wissen des Nutzers auf seinem Computer installiert werden, Informationen sammeln und weiterleiten. Sie können damit die Privatsphäre beeinträchtigen. Spyware kann z. B. in kostenloser Software enthalten sein oder beim Besuch von Webseiten heruntergeladen werden. Spionagesoftware verlangsamt den Rechner.

#### **Sprachalarmanlage (SAA)**

Eine Sprachalarmanlage ist eine elektroakustische Anlage zur Alarmierung von Personen.

## **T**

#### **Taschenauthentifikator – Token**

Der Taschenauthentifikator besteht häufig aus einer Anzeige sowie einem Eingabefeld und verfügt über einen geheimen Schlüssel sowie gegebenenfalls eine interne Uhr. Er dient dazu, ein Einmal-Passwort zu erzeugen.

#### **Trojanisches Pferd – Trojan Horse**

Ein trojanisches Pferd in der IKT ist – in Analogie zur List des Odysseus im Kampf um Troja – Programmcode, der etwas Nützliches zu tun vorgibt, während er tatsächlich etwas Unerwünschtes ausführt. Beispielsweise kann es Programmcode sein, der die Login-Maske darstellt und Benutzererkennung und Passwort dann an Unbefugte weiterleitet.

## **U**

#### **Überfallmeldeanlage (ÜMA)**

Eine Überfallmeldeanlage (ÜMA) ermöglicht mittels Überfallmeldern, z. B. Hand- oder Fußmeldern, die Meldung und damit Erkennung von Überfällen, um anschließend geeignete Maßnahmen einleiten zu können.

#### **Unterbrechungsfreie Stromversorgung (USV) – Uninterruptable Power Supply (UPS)**

Eine USV ist eine Stromversorgung, mit der sich ein kurzzeitiger Stromausfall überbrücken lässt. Die IEC 62040-3 (s. a. DIN EN 62040-3) nennt folgende 10 Netzstörungen: 1. Netzausfälle, 2. Spannungsschwankungen, 3. Spannungsspitzen, 4. Unterspannungen, 5. Überspannungen, 6. Blitzeinwirkung, 7. Spannungsstöße, 8. Frequenzschwankungen, 9. Spannungsverzerrungen, 10. Spannungsüberschwingungen. Die IEC 62040-3 unterscheidet folgende USV-Klassen:

- Voltage and Frequency Independent (VFI) from mains supply. Dieser USV-Typ ist vergleichbar mit der Online-USV mit Dauerwandler. Bei VFI-USVs sind Spannung und Frequenz am USV-Ausgang unabhängig vom Eingangsnetz. VFI-USVs bieten Schutz gegen alle 10 Netzstörungsarten. Bei einer VFI-USV läuft die Stromversorgung der angeschlossenen Geräte, z. B. Computer, stets über die USV.
- Voltage Independent (VI) from mains supply. Diese USV-Klasse ist vergleichbar mit Line-Interactive-USVs. Bei VI-USVs ist die Spannung am USV-Ausgang unabhängig vom Eingangsnetz. Störungen der Netzfrequenz gelangen ungefiltert zur Last. VI-USVs bieten Schutz gegen die Netzstörungsarten 1 – 5. Sie überbrücken

Stromausfall und können Spitzen und Unebenheiten in der Stromversorgung glätten.

- Voltage and Frequency Dependent (VFD) from mains supply. VFD-USVs sind vergleichbar mit Offline-USVs. Eine VFD-USV befindet sich solange im „standby“-Modus wie das Netz die Last im regulären Betrieb direkt versorgt. Erst im Falle einer Störung der Stromversorgung erfolgt die Umschaltung auf den Batteriebetrieb. VFD-USVs bieten Schutz gegen die Netzstörungenarten 1 – 3.

Unter Kontinuitätsaspekten ist zu berücksichtigen, dass die USV einen SpoF darstellen kann. Sie sollte daher in geeigneter Form redundant ausgelegt sein.

**Unverfälschtheit (Integrität) – Integrity**

Eigenschaft eines Objekts, unverfälscht und vollständig, d. h. nicht unzulässig oder unbefugt verändert oder gelöscht worden zu sein.

## V

**Validierung – Validation**

Die Validierung prüft die Übereinstimmung des erzeugten Produktes bzw. der erbrachten Leistung mit den Anforderungen der Auftraggeber. Dies beinhaltet die Überprüfung der Sicherheitsanforderungen. Ein Beispiel ist die Überprüfung, dass ein Software-Produkt die Anforderungen der Benutzer erfüllt.

**VdS**

Verband der Sachversicherer

**Verbindlichkeit (Nichtabstreitbarkeit) – (Non Repudiation)**

Eigenschaft eines Objekts, z. B. einer Transaktion, verbindlich, d. h. nicht abstreitbar zu sein.

**Verfügbarkeit – Availability**

Eigenschaft eines Objekts, wie z. B. eines Prozesses oder einer Ressource (Gebäude, Räumlichkeiten, Anlagen, Betriebsmittel, Computer, Netze, Programme, Daten, Rollen, Funktionen, ...), in einem bestimmten Umfang bereit zu stehen, zugreifbar und nutzbar zu sein. Verfügbarkeitsanforderungen beziehen sich üblicherweise auf die zugesicherten Betriebszeiten einer Ressource.

**Verfügbarkeitsklassen – Availability Environment Classification (AEC)**

Die Harvard Research Group hat Verfügbarkeit in 5 Klassen von 0 bis 4 definiert (Availability Environment Classification {AEC}) [86]. Diese orientieren sich an den Auswirkungen eines Ausfalls auf die Geschäftsaktivitäten und auf die Kunden. Die höchste Klasse AE4 kennzeichnet den Betrieb an 24 h/Tag x 7 Tage/Woche, d. h. den Rund-um-die-Uhr-Betrieb, während die niedrigste Stufe AE0 für den Betrieb mit Unterbrechungen steht, bei denen die Verfügbarkeit der Daten nicht wesentlich ist

**Verifikation – Verification**

Die Verifikation prüft, ob das Ergebnis einer Lebenszyklusphase die zu Beginn der Phase gestellten Anforderungen erfüllt. Dies beinhaltet die Überprüfung der Sicherheitsanforderungen.

**Verteilter DoS-Angriff – Distributed Denial of Service (DDoS) Attack**

Großflächiger Angriff, bei dem eine Vielzahl von Systemen ein Zielsystem oder -Netzwerk lahm legen.

**Vertrag auf Gegenseitigkeit – Reciprocal Agreement**

Bei einem Vertrag auf Gegenseitigkeit vereinbaren zwei oder mehrere Parteien, z. B. Unternehmen, Unternehmenstöchter oder Organisationseinheiten, die prinzipiell

gleichartige Schutzobjekte nutzen, dass sie beispielsweise im Notfall Schutzobjekte des Vertragspartners nutzen können, um dort den Notbetrieb durchzuführen.

**Vertraulichkeit** – Confidentiality

Eigenschaft eines Objekts bzw. einer Information, nur Befugten (Personen, Prozessen oder Ressourcen) bekannt bzw. zugänglich zu sein.

**Verwundbarkeit** – Vulnerability

Eigenschaft eines Objektes, z. B. eines Informationssystems oder eines Rechenzentrums, gegenüber bestimmten Ereignissen, z. B. Stromausfall oder Hacker-Angriffen, ungeschützt zu sein.

**Virtuelles privates Netz (VPN)** – Virtual Private Network (VPN)

Ein VPN stellt eine gesicherte Verbindung über ein öffentliches Netz dar.

**Vishing**

Vishing ist ein Kunstwort für „Voice over IP Phishing“. Hierbei nutzen Angreifer die niedrigen Kosten und die weltweite Verfügbarkeit der Internettelefonie für meist automatisierte Anrufe. Ein Dialer ruft eine Vielzahl von VoIP-Adressen an. Im Telefonat täuscht eine Stimme von Band vor, der Anruf käme von einer vertrauenswürdigen Instanz, z. B. einem Finanzinstitut. Die Stimme veranlasst das potenzielle Opfer, vertrauliche Daten, insbesondere Kreditkartennummer, Kontonummer, PIN und TAN preiszugeben, so dass der Angreifer an die Finanzen des Opfers gelangen kann. Ebenfalls abgefragt werden können Geburtstag, Sozialversicherungsnummer und Passnummer, um Identitätsdiebstahl begehen zu können. Die Auswertung der Anrufe kann auf Seiten des Anrufers ebenfalls automatisiert erfolgen. Hierzu wandelt ein System entweder die per Tastatur eingegebenen Ziffern um, indem es die Töne der Ziffern in digitale Zeichen umsetzt oder es verwendet die Spracherkennung. Anstelle des automatisierten Anrufs kann der Angreifer zuvor eine E-Mail oder eine SMS einer scheinbar vertrauenswürdigen Instanz an das Opfer schicken, die es dazu veranlasst, die vom Angreifer vorgegebene Telefonnummer anzurufen.

**VIVA**

Abkürzung für Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität

## W

**Wassermeldeanlage (WMA)**

Wassermeldeanlagen (WMA) gehören zu den Gefahrenmeldeanlagen. Sie dienen dazu, Flächen, Räume, Rohrleitungen und andere Einrichtungen auf den Austritt leitender Flüssigkeiten, wie z. B. Wasser, zu überwachen.

**Weitverkehrsnetz** – Wide Area Network (WAN)

Ein Weitverkehrsnetz ist ein nicht lokales Verbindungsnetz, das einen größeren geographischen Bereich abdeckt und von einem eigenständigen Betreiber angeboten wird.

**Z**

**Zentrale Rechtsteuerung und –verwaltung** – Single Point of Security Control and Administration (SPSCA)

Die zentrale Rechtsteuerung und –verwaltung umfasst die Eingabe, Pflege, Sperrung, Freigabe und Löschung von Rechten und die darauf aufbauende Steuerung von Berechtigungsanfragen.

**Zentrale Rechteverwaltung** – Single Point of Security Administration (SPSA)

Zentrale Rechteverwaltung ist die Stelle, an der die Rechte für z. B. IKT-Systeme verwaltet, d. h. administriert werden.

**Zuverlässigkeit** – Reliability

Zuverlässigkeit beschreibt die Eigenschaft eines Prozesses, einer Ressource, eines Produktes oder einer Dienstleistung innerhalb eines betrachteten Zeitraums die an ihn/sie gestellten Anforderungen zu erfüllen. Kenngrößen sind die Lebensdauer und die Ausfallwahrscheinlichkeit.



## 29 Sachwortverzeichnis

---

3

3D-RiSiKo-Pyramide..... 24  
 3D-Sicherheitspyramide ..... 24

---

4

4Vs ..... 133, 210

---

A

Abfahrtskontrolle ..... 333, 371  
 Abgabenordnung ..... 42, 299, 541  
 Abgangskontrolle ..... 333, 369  
 Abhören ..... 368  
 Abhörschutz ..... 368  
 ABMS ..... 550  
 Abschottung  
   - Kabeldurchführung..... 342  
   - Rohrdurchführung ..... 342  
 Abseilvorrichtung..... 344  
 Absendekontrolle ..... 333, 367  
 Abstand..... 237  
 Abwehrrechner ..... 405  
 Abweichungsanalyse ..... 505  
 AC..... 398  
 Accessmanagement ..... 352  
 ACM  
   - Pyramide..... 304  
 Actor Analysis  
   - Functional ..... 489  
   - Technical ..... 494  
 ADV..... 51, 438  
 AEC ..... 588  
 AES..... 362  
 AGG ..... 541  
 Agreement  
   - Reciprocal ..... 588  
   - Service Level..... 585  
 AICPA ..... 114

AIHA ..... 573  
 Aktenvernichter ..... 366  
 AktG ..... 41, 541  
 Aktiengesetz ..... 41  
   - Pflichtverletzung ..... 37  
 Alarm..... 573  
 Alarmanlage ..... 56  
   - DIN EN 50130 Beiblatt 1 ..... 553  
 Alarmierung ..... 334, 371  
 Alert ..... 573  
 Algorithmushandel ..... 74  
 AMG ..... 90, 541  
 AMS ..... 563  
   - BAuA ..... 60  
   - LASI ..... 61  
   - OHRIS, 2010..... 61  
 AMWHV ..... 90, 541  
 Änderungsmanagement ..... 289  
 Anforderungsarchitektur ..... 204  
 Anforderungsprofil ..... 383  
 Angriffssicherheit ..... 126, 203, 240, 242  
 Anomalie  
   - Erkennung..... 406  
   - statistische ..... 406  
 ANSI ..... 573  
   - Z10-2012 ..... 107  
 Anti-Korruptionsmanagement  
   - BS 10500, 2011 ..... 550  
 Antrags- und Genehmigungsverfahren  
   - Zufahrt..... 463  
   - Zugang ..... 463  
   - Zugriff..... 463  
   - Zutritt..... 463  
 Anwendungssicherheit  
   - ISO/IEC 27034 ..... 561  
 AO..... 541  
 Appliance..... 378, 400, 573  
 Application Level Gateway ..... 404  
 Application security  
   - ISO/IEC 27034 ..... 561  
 Application Whitelisting  
   - NIST SP 800-167, DRAFT ..... 565  
 Arbeitsschutz..... 82

- Gesetz.....53
- Management .....254
- Managementsystem ..... 165, 563
  - Leitfaden.....107
- Pyramide .....256
- Arbeitssicherheit .....203
  - Gesetz.....53
  - Pyramide .....256
- Arbeitsstätte
  - Technische Regeln (ASR) .....60
- Arbeitsstättenverordnung..... 53, 55, 298
- ArbIG.....62
- ArbSchG .....53, 541
- ArbStättV ..... 53, 55, 541
- ArbVG .....62
- Architecture
  - Pattern.....485
  - Requirements.....204
- Architektur
  - Anforderungs- .....204
  - Bedrohungen.....207
  - Beschreibung
    - ISO/IEC 42010, 2011.....563
  - Management .....374
    - Richtlinie.....475
  - Schadenspotenzial.....266
  - Schwachstellen.....267
  - Sicherheitszone.....228
  - TOGAF .....566
- Archivierung
  - Strategie .....392
- ArG .....62, 543
- Arzneimittelgesetz .....90
- AschG .....62
- ASiG.....53, 541
- ASP .....274
- ASR .....60
- ASSE .....573
- Assessment
  - IT Security .....502
  - IT Security, NIST SP 800-53A.....564
  - Privacy, NIST SP 800-53A .....564
  - Risk, ISO 31010, 2009 .....563
- Asset .....106
  - Intangible.....119
- Asset Management
  - ISO 55001 ..... 563
  - ISO 55002 ..... 563
  - Software, ISO/IEC 19770..... 556
- AStV ..... 62
- ASVG ..... 62
- Atemschutz
  - Haube ..... 344
  - Kissen ..... 344
- Attacke
  - Before-Zero-Day ..... 409
  - Brute-Force ..... 574
  - Zero-Day ..... 409
- Audit
  - FFIEC..... 89
- Auftragsdatenverarbeitung ..... 438
- Ausfall
  - Dauer.....214, 444
    - maximal tolerierbare ..... 445
  - Kosten .....21, 307
  - Stromversorgung
    - SAIDI..... 5
  - Ursachen..... 21
  - Zeitraum
    - maximal tolerierbarer ..... 445
- Auslagerung..... 324
  - BaFin.....74, 79, 85
  - Banken..... 275
  - Strategie ..... 326
  - Unternehmen ..... 427
- Auslöser ..... 573
- Authentifizierung ..... 573
- Authentisierung ..... 573
  - Einfaktor
    - Besitz..... 345
    - Merkmal ..... 345
    - Verhalten.....345, 346
    - Wissen ..... 345
  - Zweifaktor ..... 345
    - Besitz und Merkmal .....345, 346
    - Merkmal und Wissen .....345, 346
    - Wissen und Besitz.....345, 346
- Autorisierung..... 573
- Availability..... 588
  - Environment Classification ..... 588

awareness ..... 385  
 AWI ..... 579

---

**B**

Backup ..... 402  
 Balanced Pyramid Scorecard® ..... 509  
 Balanced Scorecard ..... 509  
 Band ..... 393  
 - Archiv ..... 342  
 - Bibliothek ..... 401  
 - Roboter ..... 394  
 Banken  
 - Algorithmushandel ..... 74  
 - Gefährdungen ..... 75  
 - interne Kontrolle ..... 543  
 - Notfallkonzept ..... 75  
 - Operationelles Risiko ..... 543  
 - Outsourcing ..... 74, 543  
 - Schutzbedarf ..... 75  
 - Zweifaktor-Authentisierung ..... 75  
 BankG ..... 87, 543  
 BankV ..... 87, 543  
 Basel II ..... 42, 81, 548  
 Basel III ..... 548  
 Bastion Host ..... 405  
 - entmilitarisierte Zone ..... 405  
 - kaskadiert ..... 405  
 - Secure Server Network ..... 405  
 BAuA ..... 60  
 BCM ..... 129, 298, 303  
 - Datenbank ..... 455  
 - Framework ..... 310  
 - holistic ..... 302  
 - ISO 22301 ..... 557  
 - ISO 22313 ..... 557  
 - pyramid ..... 304  
 - Pyramide ..... 304  
 - Rahmenwerk ..... 310  
 BCP ..... 573  
 BDSG ..... 47, 48, 541  
 Bedrohung ..... 3, 204, 573  
 - Architektur ..... 207, 267  
 - Landkarte ..... 206  
 - Potenzialanalyse ..... 267  
 - potenzielle ..... 207  
 - prinzipielle ..... 204

- Profil ..... 207  
 Before-Zero-Day-Attacke ..... 409  
 Befugnisgrenze ..... 491  
 Begleitprozess ..... 242  
 - Änderungsmanagement ..... 289  
 - Arbeitsschutzmanagement ..... 254  
 - Architekturmanagement ..... 374  
 - Compliance Management ..... 251  
 - Datenschutzmanagement ..... 256  
 - Ereignismanagement ..... 282  
 - Finanzmanagement ..... 280  
 - Innovationsmanagement ..... 376  
 - Kapazitätsmanagement ..... 295  
 - Konfigurationsmanagement ..... 292  
 - Konformitätsmanagement ..... 251  
 - Kontinuitätsmanagement ..... 300, 301  
 - Leistungsmanagement ..... 273  
 - Lizenzmanagement ..... 293  
 - Performancemanagement ..... 295  
 - Personalmanagement ..... 383  
 - Problemmanagement ..... 288  
 - Projektmanagement ..... 281  
 - Qualitätsmanagement ..... 281  
 - Releasemanagement ..... 291  
 - Risikomanagement ..... 263  
 - Securitymanagement ..... 328  
 - Service Level Management ..... 273  
 - Überblick ..... 249  
 - Wartungsmanagement ..... 297  
 Begrenzungsrouter ..... 405  
 BEHG ..... 543  
 Beinahekrise ..... 314  
 Beinahenotfall ..... 314  
 Belastbarkeit  
 - ISO 22316, CD ..... 557  
 Belastbarkeit, Organisation ..... 108  
 Benchmark, Occ. Health Safety Security  
 Continuity Risk ..... 518  
 Benutzerdokumentation  
 - ISO/IEC/IEEE 26511ff. ..... 559  
 Benutzerfreundlichkeit ..... 383  
 Benutzerkonto ..... 467  
 - gesperrtes ..... 466, 469  
 - verwaist ..... 353, 513  
 Benutzerservice ..... 247, 282  
 Berechtigungskubus ..... 336  
 Berechtigungsmanagement  
 - ISO 22600, 2014 ..... 558

- Berechtigungswürfel .....336
- Berichtswesen
- Anforderungen.....505
  - Continuity .....505
  - Occupational Health.....505
  - Safety.....505
  - Security .....505
  - Sicherheit.....505, 507
- Betrieb
- regulär.....311
  - Rückkehr .....301
- Betriebseinflussanalyse ..... 179, 573
- Beispiel.....183
- Betriebssanitäter .....58
- Betriebsicherheit ..... 126, 203, 240, 242
- BetrSichV .....53
- Beweissicherung.....371
- BGB ..... 39, 64, 541
- BIA ..... 129, 176
- BImSchG.....541
- BImSchV 12, 2013..... 311, 541
- Biometrie .....346
- ISO 19092, 2008 .....556
  - ISO/IEC 19792, 2009 .....556
  - ISO/IEC 24745, 2011 .....558
  - ISO/IEC 24761, 2009 .....558
  - Sicherheit
    - Rahmenwerk .....556
- BJR.....37, 495
- Blacklist .....408
- Bluetooth
- IT Security .....565
- BMA..... 319, 343, 573
- DIN VDE 0833-2 .....551
  - VdS 2095, 2010 .....567
- BMAS.....60
- BMIS .....111
- Bodyscanner .....358
- Bombendrohung
- Formblatt .....459
- BPS .....509
- Brand
- Abschnitt .....342
  - Begrenzung .....342
  - Bekämpfung.....343
  - Datensicherung ..... 552
  - Erkennung ..... 343
  - Folgen..... 343
  - Meldeanlage .....319, 343, 573
  - Melder .....56, 343
  - Posten..... 341
  - Vermeidung ..... 340
  - Wache..... 341
- Brandgasmelder ..... 343
- Brandschutz .....56, 340
- Kissen ..... 342
  - Leitfaden, VdS 2000, 2010..... 566
  - Ordnung
    - DIN 14096, 2014..... 552
  - Richtlinie..... 458
  - Zeichen..... 341
- Brute-Force-Attacke ..... 574
- Brutto-Risiko ..... 131
- BS 10012, 2009 ..... 550
- BS 10500, 2011 ..... 550
- BS 11000-1, 2010..... 550
- BS 11000-2, 2011..... 550
- BS 11200, 2014 ..... 550
- BS 65000, 2014 ..... 550
- BS PAS 99, 2012..... 550
- BSC ..... 509
- prozessbasiert..... 509
  - pyramidenbasiert..... 509
- BSI.....100, 574
- Bausteinatalog..... 98
  - Standard 100-1 .....98, 551
  - Standard 100-2 .....98, 551
  - Standard 100-3 .....98, 551
  - Standard 100-3, Ergänzung ..... 551
  - Standard 100-4 .....98, 551
  - TR-03109 ..... 551
- BSIG..... 541
- Buchführung
- Mangel ..... 44
  - ordnungsmäßige..... 42
- Bunch of Disks
- JBOD..... 400
  - MBOD ..... 400
  - SBOD ..... 400
- Bundesimmissionsschutzverordnung 311

Bürgerliches Gesetzbuch .....	39, 64
Business Activity Monitoring .....	244
Business Continuity	
- FFIEC .....	89
- ISO 22301, 2012.....	557
- ISO 22313, 2012.....	557
- ISO/IEC 27031, 2011.....	560
- Joint Forum.....	83, 550
- Management.....	111
- Plan .....	317
- Planning	
-- FFIEC .....	546
Business Continuity Management .....	111, 129, 298, 303, 314, 457
- ganzheitlich .....	302
- holistic .....	302
- human aspects.....	551
- KMU .....	551
- PD 25111, 2010.....	551
- PD 25222, 2011.....	551
- PD 25666, 2010.....	551
- PD 25888, 2011.....	551
- recovery.....	551
- supply chain .....	551
- testing .....	551
Business Impact Analysis .....	129, 176
Business Judgement Rule .....	37, 495
Business Performance Management ..	244
Business Process Management .....	244
BWG .....	542
BYOD .....	412

---

**C**

CBCO .....	416, 530
CC .....	551
CCO.....	416, 530, 574
CCTV	
- DIN EN 50132.....	553
CD.....	579
CD-ROM.....	393
CEM.....	551
CEO .....	39
CERT® .....	574
Certified in Risk and Information Systems Control™.....	574

Certified in the Governance of Enterprise IT® .....	574
Certified Information Security Auditor™ .....	574
Certified Information Security Manager® .....	574
CESO .....	416, 530
CFO.....	39
CFR .....	91
- 16 CFR Part 312 .....	546
- 21 CFR Part 11 .....	546
- 21 CFR Part 110 .....	546
- 21 CFR Part 211 .....	546
- 21 CFR Part 58 .....	546
- 21 CFR Part 820 .....	546
CFSO.....	416, 530
CGEIT® .....	574
cGLP	
- OECD.....	565
CGMP .....	546
Challenge-Response-Verfahren .....	349
Change	
- History .....	289
- Management .....	289
- Request .....	289
Check-out-check-in.....	290
ChemG .....	89, 542
Chief Business Continuity Officer .....	416
Chief Compliance Officer .....	416, 574
Chief Enterprise Security Officer .....	416
Chief ICT Continuity Officer.....	416
Chief ICT Service Continuity Officer ..	416
Chief Information Risk Officer.....	416
Chief Information Security Officer .....	416
Chief Risk Officer.....	416, 574
Chiffprat .....	362
Chiffrierung.....	361
Chinese Wall.....	80
CHSO.....	416, 530
CIA.....	574
CIA² .....	574
CICO.....	416, 530
CIFS .....	399
CIM.....	401
circle of trust.....	351
Circuit Level Gateway.....	404
CIRO.....	416, 530
CISA® .....	574

- CISCO ..... 416  
 CISM® ..... 574  
 CISO ..... 416, 530  
 Clear Desk Policy ..... 219  
 Closed-Shop-Betrieb ..... 227  
 Cloud  
   - Datenschutz ..... 560  
 Cloud Computing  
   - Architektur, ISO 17789, 2014 ..... 555  
   - Definition ..... 565  
   - NIST SP 800-144 ..... 565  
   - NIST SP 800-145 ..... 565  
 Cloud Services ..... 381  
   - ISO/IEC 20000-9, TR ..... 556  
   - ISO/IEC 27017, DIS ..... 560  
   - ISO/IEC 27036-4, WD ..... 561  
 Cluster-System ..... 320  
 CMDB ..... 286  
 CMM® ..... 551  
 CMMI® ..... 551  
 COBIT® 5 ..... 111  
   - Domänen ..... 113  
   - Prozessdomänen ..... 112  
   - Prozessmodell ..... 112  
   - Reifegradmodell ..... 114  
   - Zielkaskade ..... 112  
 COBIT® ..... 94, 166, 551  
 Code of Federal Regulations ..... 91  
 Commodity ..... 352  
 Common Criteria ..... 551  
 Compliance ..... 72, 251, 301, 550  
   - Beauftragter ..... 416  
   - Funktion ..... 80  
   - IAM ..... 353  
   - IDW PS 980 ..... 548  
   - IKT ..... 251  
   - IT ..... 251  
   - Management ..... 251  
   - Officer ..... 72, 416  
     -- Garantspflicht ..... 40  
   - Risiko ..... 88  
   - Social ..... 108, 251  
   - Wertpapierhandelsgesetz ..... 69  
 Computer  
   - Emergency Response Team ..... 574  
   - Security Emergency Team ..... 285  
   - Security Incident Response Team ..... 285, 416  
 Computerforensik ..... 373  
 Computervirens Scanner ..... 408  
 Computervirus ..... 575  
 Configuration Management  
   - ISO 10007, 2003 ..... 554  
 Content-Security-System ..... 407, 575  
 Continuity ..... 203, 240, 242  
   - Incident Response ..... 285  
   - Management ..... 300  
     -- Business ..... 129  
   - Plan ..... 310  
 Control ..... 580  
   - Objective ..... 580  
 Controls  
   - Compliance ..... 253  
   - **Continuity** ..... 259, 327  
   - Maturity ..... 526  
   - Policy ..... 157  
 COPPA ..... 546  
 Copyleft ..... 294  
 Corporate Governance ..... 565  
   - deutsch ..... 65  
   - FINMA ..... 87  
   - OECD ..... 66  
   - Schweiz ..... 65  
   - Versicherer ..... 543  
 COSO ..... 92, 546  
 CP ..... 310  
 CR ..... 289  
 Cracker ..... 575  
 CRISC™ ..... 574  
 Criticality ..... 580  
 CRO ..... 416, 530, 574  
 CSIRT ..... 285, 416  
 CSPP-OS ..... 551  
 CTI ..... 286  
 Cybersecurity  
   - ISO/IEC 27032, 2012 ..... 561

**D**

DAS ..... 398, 399

## Data

- Leakage ..... 376
  - Prevention ..... 409
  - Protection ..... 409
- Loss
  - Prevention ..... 409
  - Protection ..... 409

## Data Center

- Best Practices ..... 549
- TIA 942-A-2012 ..... 549

Data Striping ..... 396

## Database

- Firewall ..... 404
- Security Gateway ..... 404

Datenabfluss ..... 376

Datendiebstahl ..... 583

## Datenlöschung

- NIST SP 800-88, Rev. 1 ..... 564

## Datenschutz

- Architektur
  - ISO/IEC 29101, 2013 ..... 562
- Auftragsdatenverarbeitung ..... 438
- Beauftragter ..... 416
  - Bestellung ..... 437
- Bewertung
  - ISO/IEC 29190, PRF ..... 563
- BS 10012, 2009 ..... 550
- Cloud ..... 560
- Deutschland
  - BDSG ..... 47
  - LDSG ..... 47
  - SGB X ..... 47
  - Sozialdaten, SGB X ..... 50
  - TKG ..... 47
  - TMG ..... 47
- E-Mail-Übertragung ..... 257
- EU ..... 52
  - Datenschutzrichtlinie ..... 51
- ISO 22307, 2008 ..... 557
- Management ..... 256
- Österreich
  - DSGVO 2000 ..... 51
- Rahmenwerk
  - ISO/IEC 29100, 2011 ..... 562
- Richtlinie, Europa ..... 544

- Schweiz

-- DSGVO ..... 51

- USA ..... 52

-- Privacy Act ..... 53

-- Privacy Protection Act

--- Children (COPPA) ..... 53

--- Drivers (DPPA) ..... 53

--- Family Educational (FERPA) 53

- Verletzung

-- Kosten ..... 22

Datenschutzbeauftragter ..... 49

Datensicherung ..... 322

- Archiv ..... 326

- Aufbewahrung ..... 450

- Auslagerungsverfahren ..... 326

- Aussonderungsfrist ..... 450

- Beispielskonzepte ..... 100

- Container ..... 552

- differenziell ..... 322

- Dokumentationsvorlage ..... 480

- Generationen ..... 324

- Generationenprinzip ..... 450

- inkrementell ..... 323

- komplett ..... 322

- Medien ..... 450

- Methoden ..... 323

- Namenskonventionen ..... 449

- Plan ..... 450

- Prozess ..... 241

- Räume ..... 552

- Ressourcen ..... 241

- Richtlinie ..... 449

- Schränke ..... 552

- selektiv ..... 323

- Sicherheitszeitpunkt ..... 324

- Strategie ..... 392

- Verantwortlichkeit ..... 241

- Verfahren ..... 450

- zeitgleich ..... 325

- zeitnah ..... 325

- zeitversetzt ..... 325

## Datenträger

- Archiv ..... 319

- Kataster ..... 450

- Vernichtung ..... 367

-- chemisch ..... 367

-- DIN 66399 ..... 554

-- mechanisch ..... 367

-- thermisch .....	367	DIN EN 1627, 2011 .....	552
Datenverarbeitung im Auftrag .....	48, 438	DIN EN 179, 2014 .....	551
Datenverlust		DIN EN 3-7 .....	551
- maximal tolerierbarer .....	445	DIN EN 50126, 2000 .....	553
- Recovery Point Objective .....	445	DIN EN 50128, 2012 .....	553
Datenvernichtung .....	367	DIN EN 50129, 2003 .....	553
DDoS .....	588	DIN EN 50130 Beiblatt 1 .....	553
Dechiffrierung .....	362	DIN EN 50131 .....	553
Deckenschott .....	342	DIN EN 50132 .....	553
Deduplizierung .....	297, 402	DIN EN 50133 .....	553
De-Gausser .....	367	DIN EN 50134 .....	553
Demilitarized Zone .....	576	DIN EN 50600 .....	553
Denial of Service .....	575	DIN EN 60812, 2006 .....	554
Deny-All-Prinzip .....	223	DIN EN 62040-3, 2011 .....	554
DES .....	362	DIN EN 80001-1, 2011 .....	554
Design Pattern .....	485	DIN EN ISO 9001 .....	175
Detection System		DIN EN ISO 9001, 2008 .....	552
- Explosive .....	360	DIN ISO 23601, 2010 .....	553
Development and Acquisition		DIN ISO 9735-9 .....	552
- FFIEC .....	547	DIN VDE 0833 .....	551
DGUV .....	53	Direct Attached Storage .....	398, 399
- Grundsätze .....	53	DIS .....	579
- Information .....	53	Disaster Recovery .....	111
- Regel .....	53	- Plan .....	317
- Vorschrift .....	53	Disk	
- Vorschrift 1 .....	57, 58	- Solid State .....	393
- Vorschrift 2 .....	59	Diskette .....	393
- Vorschrift 3 .....	59	Distanzanforderung .....	236
Dienstleistungssicherheit		Distanzprinzip .....	236
- lebenszyklusimmanent .....	147	DLM .....	575
Digital Evidence		DLP .....	409
- ISO/IEC 27042, DIS .....	561	- Systeme .....	409
Digitales Wasserzeichen .....	575	DLT .....	396
DIN 14096, 2014 .....	552	DMTF® .....	401
DIN 16557-4, 2002 .....	552	DMZ .....	576
DIN 16560-15, 2003 .....	552	DNS .....	575
DIN 16602-30-02, 2014 .....	552	Dokumentation	
DIN 18095-2 .....	553	- Definition .....	389
DIN 25424 .....	553	- ISO/IEC/IEEE 26511ff. ....	559
DIN 40041 .....	553	- Management .....	381
DIN 4102 .....	552	- Prozess .....	244
DIN EN 1125 .....	552	Dokumentenlebenszyklusmanagement	
DIN EN 12251 .....	552	.....	575
DIN EN 12600 .....	552	Dokumentenmanagementsystem .....	321
DIN EN 15975 .....	552	Domain Name Services .....	575



Doppelsprinkler.....	344
DoS .....	575
DPPA.....	546
Drei-Säulen-Modell.....	87
Drohanruf	
- Formblatt.....	459
Drucker-Richtlinie .....	431
Druckjob	
- Ausgabe .....	378
Druckknopfmelder.....	343
Druckstraße .....	342
DS .....	398
DSB.....	416
DSG .....	51, 543
DSG 2000 .....	51, 542
DTDS .....	237, 398
DTDS+ .....	237, 398
DVD.....	393
DViA .....	51

---

**E**

ebXML.....	555
ECPA .....	546
EDIFACT .....	552
EDS.....	360
EEPROM.....	393
EFF .....	373
EFTA .....	110
EHS.....	109
Eigenmittel	
- FINMA .....	87, 543
Einbruchhemmung	
- DIN EN 1627, 2011.....	552
Einbruchmeldeanlage .....	332, 340, 575
Eindringling .....	373
Einmalpasswort .....	347
Einscheibensicherheitsglas .....	339
Ein-Schlüssel-Verfahren .....	362
Eintrittswahrscheinlichkeit .....	575
Einwegfunktion .....	364
ELA.....	576
Electronic Discovery	
- ISO/IEC 27050.....	562
Elektronische Lautsprecheranlage .....	576
EMA .....	332, 340, 575
- DIN EN 50131.....	553

- DIN VDE 0833-3 .....	551
- VdS 2170, 2010 .....	567
- VdS 2311, 2010 .....	567
- VdS 3172, 2013 .....	568
Emergency Preparedness.....	107
EN 1047 .....	552
Endpoint Security .....	410
Energiegesetz.....	66
Energieversorger	
- ISO/IEC 27019, TR, 2013 .....	560
Energiewirtschaftsgesetz .....	66
EnG .....	66
Engineering	
- Health, Safety and Security.....	122
- Health, Safety, Security and	
Continuity .....	122
- Health, Safety, Security, Continuity	
and Risk.....	122
Entfernung.....	237
entmilitarisierte Zone .....	405, 576
Environment Analysis.....	489
EnWG .....	66
Ereignis, sicherheitsrelevant.....	372
Ereignismanagement.....	282
Erhaltungssatz.....	235
Erlaubnisschein .....	341
Erste Hilfe .....	58
Ersthelfer.....	58
Escrow-Agentur .....	380
ESG .....	339
ESSCMS.....	117
Etagenverteiler .....	319
Ethernet.....	399
- Gigabit .....	399
EU-Datenschutzrichtlinie .....	51
Europa	
- Entscheidungen .....	544
- Richtlinien.....	544
European Free Trade Association.....	110
EuroSOX.....	39
Evakuierung	
- ISO 22315, 2014.....	557
EVU	
- Deutschland	
-- EnWG.....	66
- Schweiz	
-- EnG.....	66
Exploit .....	576

Explosive Detection System.....360  
 Explosive Trace Detection System .....360

---

## F

Fabrics.....399  
 Facility Management ..... 18, 244  
 Fahrtroutenverfolgung.....370  
 FAIT 1 .....44  
 FAIT 2 .....44  
 FAIT 3 .....44  
 Falsch negativ .....576  
 Falsch positiv .....576  
 Fälschungsschutz.....378  
 False Acceptance Rate ..... 346, 364, 576  
 False negative .....576  
 False positive .....576  
 False Rejection Rate ..... 346, 364, 576  
 FAR ..... 346, 364, 576  
 FATF .....70  
 Fault Tree Analysis ..... 500, 581  
 Fax-Richtlinie.....430  
 FC .....576  
 FCA .....87  
 FC-AL .....399  
 FCD .....579  
 FCIP .....401  
 FCM .....303  
   - Pyramide .....304  
 FDA.....91  
 FDIC  
   - Managing Multiple Service Providers  
     .....546  
   - Selecting a Service Provider .....546  
 FDIS .....579  
 Federal Data Protection Act.....47  
 Fehlerbaumanalyse ..... 500, 553, 581  
 fehlertoleranter Rechner.....320  
 Fenster .....339  
 Fernmeldegeheimnis .....47  
 FERPA .....546  
 Festplatte .....393  
 Feuerarbeiten .....341  
 Feuerlöscheinrichtung.....56  
 Feuerwiderstandsklasse .....342

FFIEC ..... 89  
   - Business Continuity Planning..... 546  
   - Development and Acquisition ..... 547  
   - Information Security ..... 547  
   - IT Risk Management ..... 547  
   - Operations ..... 547  
   - Outsourcing..... 547  
   - Supervision of Technology Service  
     Providers..... 547  
 Fibre Channel..... 576  
   - Arbitrated Loop ..... 399  
 Financial Conduct Authority ..... 87  
 Financial Services  
   - ISO 22307, 2008 ..... 557  
 Financial Transaction Services..... 576  
 Finanzdienstleistungen  
   - Information Security  
     -- ISO 13569, TR, 2005..... 554  
     -- ISO/IEC 27015, TR, 2012..... 560  
 Finanzmanagement..... 280  
 Fingerabdrucknehmen ..... 577  
   - aktiv ..... 577  
   - passiv..... 577  
 Fingerabdruck-Sensor..... 377  
 fingerprinting..... 577  
 FINMA ..... 86  
   - Corporate Governance..... 87  
   - Eigenmittel .....87, 543  
   - Interne Revision ..... 87  
   - Internes Kontrollsystem..... 87  
   - Outsourcing..... 87  
   - Risikomanagement..... 87  
 FINMAG..... 86  
 FinTS .....554, 576  
   - HBCI..... 576  
   - PIN/TAN..... 576  
 Firewall .....402, 577  
   - Appliance..... 405  
   - Application Level Gateway ..... 404  
   - Bastion Host ..... 405  
   - Begrenzungsrouter ..... 405  
   - Circuit Level Gateway ..... 404  
   - Database..... 404  
   - Dual-Home ..... 405

- Guidelines	
-- NIST SP 800-41, Rev. 1.....	564
- Multi-Home.....	405
- Paketfilter.....	403
- Policy	
-- NIST SP 800-41, Rev. 1.....	564
- Web Application.....	404
- XML.....	404
FIRST.....	577
FISMA.....	547
FkSolV.....	69
Flash Drive.....	393
Flash-EEPROM.....	393
Flucht- und Rettungsplan.....	299
- DIN ISO 23601, 2010.....	460, 553
- VdS 2037EF, 2013.....	567
Flucht- und Rettungswege.....	460
Fluchtweg.....	56, 444
- Länge.....	60
- Mindestbreite.....	60
Flugausfall.....	262
FMEA	
- DIN 16602-30-02, 2014.....	552
- DIN EN 60812, 2006.....	554
- ONR 49002-2.....	106
FMECA	
- DIN 16602-30-02, 2014.....	552
FoIA.....	544
Food and Drug Administration.....	91
Food safety	
- ISO-22000-Familie.....	557
forensische Codes.....	373
forensische Computeranalyse.....	373
forensische Informatik.....	373, 577
forensische Psychologie.....	384
forensischer Informatiker.....	373
forensischer Sachverständiger.....	373
FOSS.....	294
Freie Software.....	294
FRR.....	346, 364, 576
FTA.....	500
Funk-LAN.....	577
Funktionstrennung.....	220
Funkwanze.....	368

---

**G**

GAMP® 5.....	111
- Backup und Restore.....	111
- BCM.....	111
- Business Continuity Management.....	111
- Security Management.....	111
Ganzkörperscanner.....	358
Garantenpflicht.....	40
Gebäude.....	318
GeBüV.....	543
Gefahrenmeldeanlage.....	551, 577
- VdS 2463, 2007.....	567
Geldfälscher.....	373
Geldwäschegesetz	
- Finanzdienstleistungsinstitute.....	69
- Immobilienmakler.....	69
- Kapitalverwaltungsgesellschaften.....	69
- Kreditinstitute.....	69
- Spielbanken.....	69
- Versicherungsunternehmen.....	69
Geldwäscherei.....	87, 543
Generische Sicherheitskonzepte.....	143
GERM.....	554, 584
Geschäftsbücherverordnung.....	543
Geschäftsdiskontinuität.....	300
Geschäftseinflussanalyse.....	129, 176
Geschäftsfortführungsplan.....	444
Geschäftskontinuität.....	129, 444
- Planung.....	444
Geschäftskritikalität.....	172
Geschäftsunterbrechung.....	300
- Notfallplan.....	83
Gesetze	
- Deutschland.....	541
- Großbritannien.....	544
- Österreich.....	542
- Schweiz.....	543
- USA.....	546
Gesundheitsschutz.....	82
Gesundheitswesen	
- Berechtigungsmanagement	
-- ISO 22600, 2014.....	558
- ISO 18307, TR, 2001.....	556
- ISO 18308, 2011.....	556
- ISO 20514, TR, 2005.....	557
- ISO 21091, 2013.....	557
- ISO 21298, TS, 2008.....	557

- ISO 22600, 2014 .....	558	GSK	
- ISO 27789, 2013 .....	562	- IT .....	563
- ISO 27799, 2008 .....	562	Gute Laborpraxis .....	565
- TIA 1179-2010 .....	549	GwG .....	542, 543
GLBA .....	547	- Schweiz .....	87
GLP .....	89	GwV	
- IT-Anforderungen .....	109	- FINMA 1 .....	543
- OECD .....	565	- Schweiz .....	87
GMA .....	551, 577	GxP .....	246
- VdS 2463, 2007 .....	567	- PIC/S .....	110
- VdS 2833, 2003 .....	567		
GmbHG .....	542		
GMP .....	91, 110	<hr/>	
- PIC/S .....	110	<b>H</b>	
GoB .....	548	Hacker .....	578
GoBD .....	361, 548	Hafen	
GoDV .....	548	- sicherer .....	52
Governance .....	578	Haftung	
- Corporate .....	65, 66, 565	- Arbeitnehmer .....	39
- IKT .....	579	- Geschäftsführer .....	36, 151
- Information Security .....	94	- Geschäftsherr .....	38
-- ISO/IEC 27014, 2013 .....	560	- persönliche .....	38
- Informationssicherheit .....	120, 166	- Unternehmen .....	40
- IT .....	579	- Vorstand .....	37, 151
-- ISO/IEC 38500, 2008 .....	563	Handbuch	
- Principles .....	550	- Katastrophenvorsorge .....	451
GPG .....	111	- Krisenvorsorge .....	451
GPS-Sender .....	370, 377	- Notfallvorsorge .....	451
GRC .....	578	Handelsgesetzbuch .....	41, 42, 299
Grenzenzenarien .....	160, 445	Handfeuerlöscher .....	344
Grob- und Feintechnikzone .....	227	Hash-Algorithmus .....	366, 474
Großbritannien		Hash-Funktion .....	364
- Gesetze .....	544	Haus zur Sicherheit .....	192
Grundsätze		Hazard and Operability Analysis .....	501
- Corporate Governance .....	565	HAZOP .....	501
- DGUV .....	53	- ONR 49002-2 .....	106
- GoB .....	42, 299, 548	HBCI .....	578
- GoBD .....	299, 548	hBCM .....	302
- GoDV .....	42, 548	Health .....	203
- Gute Laborpraxis .....	565	Health Informatics	
- ordnungsmäßige Buchführung .....	548	- Data Warehouse, ISO 22221, TR, 2006 .....	557
- Prävention .....	57	- ISO 17090 .....	555
- sicherer Hafen .....	52, 544	- ISO 18307, TR, 2001 .....	556
Grundwerte der IS .....	128	- ISO 18308, 2011 .....	556
		- ISO 20514, TR, 2005 .....	557

- ISO 21091, 2013.....	557
- ISO 21298, TS, 2008.....	557
- ISO 22600, 2014.....	558
- ISO 27789, 2013.....	562
- ISO 27799, 2008.....	562
Health, Safety and Security Engineering .....	122
Health, Safety, Security and Continuity Engineering.....	122
Health, Safety, Security and Continuity Function Deployment.....	193
Health, Safety, Security, Continuity and Risk Engineering.....	122
HGB.....	41, 542
HHSSC.....	192
HI.....	308, 417
HIDS.....	407
Hinweispflicht.....	29, 305
HIPAA.....	547
HITECH Act.....	547
HIVI.....	417
HMAC.....	348, 365
HMTA.....	547
Home Banking Computer Interface....	578
hot fixes.....	290
hot pluggable.....	320
hot space.....	397
hot spare.....	397
hot swap.....	397
hot swappable.....	321
HOTP.....	348
House of Health, Safety, Security and Continuity.....	192
HSW.....	63, 544
HVAC.....	111

**I**

IAGAP.....	311
IAM.....	352
IAO.....	60
ICS - Stuxnet.....	11
IDEA™.....	362
Identitätsmanagement.....	352, 378
- föderiert.....	351
- Liberty Alliance.....	351

Identitäts-Provider.....	351
Identity - Life Cycle.....	352
- maintaining.....	352
- Management.....	352
-- ISO/IEC 24760.....	558
- provisioning.....	352
- terminating.....	352
Identity Management - Federated.....	351
IdM.....	352
IDPS - ISO/IEC 27039, 2015.....	561
- NIST SP 800-94, Rev. 1, DRAFT....	564
IDS.....	407
IDW.....	44, 115, 165, 251, 578
- PS 330.....	548
- PS 340.....	42
- PS 525.....	548
- PS 880.....	548
- PS 951.....	115, 176, 548
- PS 980.....	548
- RS FAIT 1.....	548
- RS FAIT 2.....	548
- RS FAIT 3.....	548
- RS FAIT 4.....	549
IEC.....	579
IEC 62040-3, 2011.....	554
iFCP.....	401
IKS.....	39, 43, 71, 269
- Prüfung -- IDW PS 951.....	548
IKT.....	578
- Sicherheitsmanagement.....	120
IKTSiPyr.....	578
IKT-Systemsicherheit - lebenszyklusimmanent.....	147
ILM.....	578
ILO.....	60, 107
- OSH.....	107
IMAC.....	274
Impact Analysis - Business.....	176
- Operational.....	179
Impact Architecture - Business.....	266
- Resource.....	266
IMS.....	115

- In-Band-Virtualisierung .....400
- Incident
- Detection, Conformity .....284
  - Detection, Continuity.....284
  - Detection, Privacy .....284
  - Detection, Security .....284
  - Management
    - ISO/IEC 27035, 2011.....561
  - Response.....285
- Inertgas.....344
- Information
- DGUV .....53
- Information Security Officer.....416
- Informations- und Kommunikationssysteme
- Vorgaben .....319
- Informationslebenszyklus
- Management .....578
- Informationssicherheit
- FFIEC .....89, 547
  - Governance .....94, 120, 166
  - Handbuch
    - NIST SP 800-100.....564
  - ISO/IEC-27000-Familie .....94, 559
  - Managementsystem .....118
  - Politik
    - nach ISO/IEC 27003 .....124
- Informationstechnologie
- Anforderungen.....72, 85
- InfoSiG.....92, 543
- InfoSiV .....92, 543
- Infrastruktur .....414
- Gebäude.....318
  - Räumlichkeiten.....319
- ingenieurmäßige Sicherheit .....121, 122
- Inhaltskontrolle .....354, 358
- Innovationsmanagement .....376
- Instanz .....127
- Intangible Asset.....119
- Integriertes Managementsystem
- OHRIS.....61
- Integrität.....579, 588
- persönliche .....384
  - Test.....384
- Interdependenz
- Baum .....455
  - horizontal.....308, 417
  - Netz .....31, 309, 417, 418, 455
  - Plan.....455
  - vertikal.....308, 417
- International Engineering Consortium579
- International Organization for Standardization .....579
- Interne Revision
- Versicherer.....543
- Interner Alarm- und Gefahrenabwehrplan.....311
- Internes Kontrollsystem .....10, 39, 43, 546, 548
- Prüfung
    - IDW PS 951 .....548
  - Versicherer.....543
- Internet
- iFCP .....401
  - iSCSI .....401
- Intruder.....373
- Intrusion
- Detection
    - ISO/IEC 27039, 2015.....561
    - NIST SP 800-94, Rev. 1, DRAFT .....564
  - Detection-System.....406
    - hostbasiert.....407
    - netzbasiert.....406
  - Prevention .....407
  - Protection.....407
  - Response-System .....407
  - Signature.....406
- Investmentgesellschaften
- InvMaRisk .....78, 549
  - Notfallkonzept .....79
  - Outsourcing.....79
- InvMaRisk .....78, 549
- IP-Adresse .....575
- IPS.....407
- IP-Stack .....577
- IRS .....407
- ISACA® .....111
- ISAE 3402.....114

iSCSI .....	401	ISO 28004-2, 2014 .....	562
ISiPyr .....	579	ISO 28004-3, 2014 .....	562
ISMS .....	93, 98, 118, 529, 530	ISO 28004-4, 2014 .....	562
- ISO/IEC 27001 .....	95	ISO 28005-2, 2011 .....	562
- ISO/IEC 27007, 2011 .....	560	ISO 29119, 2013 .....	562
- ISO/IEC-27000-Familie .....	94	ISO 31000, 2009 .....	563
ISO .....	416, 579	ISO 31010, 2009 .....	563
- PDCA-Zyklus .....	107	ISO 45001, CD .....	563
ISO 10007, 2003 .....	554	ISO 55001, 2014 .....	563
ISO 14001, 2004 .....	554	ISO 55002, 2014 .....	563
ISO 14971, 2007 .....	554	ISO/IEC 29100, 2011 .....	562
ISO 15000, TS .....	555	ISO/IEC 12207, 2008 .....	554
ISO 15489-1, 2001 .....	555	ISO/IEC 13335 .....	175
ISO 15489-2, TR, 2001 .....	555	ISO/IEC 13569, 2005 .....	554
ISO 16085, 2006 .....	555	ISO/IEC 15408 .....	555
ISO 17090 .....	555	ISO/IEC 15443, TR .....	555
ISO 18307, TR, 2001 .....	556	ISO/IEC 15446, TR, 2009 .....	555
ISO 18308, 2011 .....	556	ISO/IEC 15504 .....	555
ISO 19092, 2008 .....	556	ISO/IEC 18028 .....	555
ISO 19600, 2014 .....	556	ISO/IEC 18028-4 .....	166
ISO 20514, TR, 2005 .....	557	ISO/IEC 18045, 2008 .....	555
ISO 21091, 2013 .....	557	ISO/IEC 19770 .....	556
ISO 21298, TS, 2008 .....	557	ISO/IEC 19792, 2009 .....	556
ISO 22221, TR, 2006 .....	557	ISO/IEC 20000 .....	93, 166, 175, 556
ISO 22300, 2012 .....	557	ISO/IEC 20004, TR, 2012 .....	556
ISO 22301 .....	299	ISO/IEC 20006-1, 2014 .....	556
ISO 22301, 2012 .....	557	ISO/IEC 21000-5 .....	557
ISO 22307, 2008 .....	557	ISO/IEC 21827, 2008 .....	557
ISO 22311, 2012 .....	557	ISO/IEC 2382-8, 1998 .....	554
ISO 22312, TR, 2011 .....	557	ISO/IEC 24745, 2011 .....	558
ISO 22313, 2012 .....	557	ISO/IEC 24759, 2014 .....	558
ISO 22315, 2014 .....	557	ISO/IEC 24760-1, 2011 .....	558
ISO 22316, CD .....	557	ISO/IEC 24760-2, FDIS .....	558
ISO 22320, 2011 .....	557	ISO/IEC 24760-3, CD .....	558
ISO 22322, PRF .....	558	ISO/IEC 24761, 2009 .....	558
ISO 22324, DIS .....	558	ISO/IEC 24763, TR, 2011 .....	558
ISO 22398, 2013 .....	558	ISO/IEC 24764, 2010 .....	558
ISO 22600, 2014 .....	558	ISO/IEC 24775, 2014 .....	400, 558
ISO 26000, 2010 .....	559	ISO/IEC 25000, 2014 .....	558
ISO 26262, 2011 .....	559	ISO/IEC 25001, 2014 .....	559
ISO 27040, 2015 .....	561	ISO/IEC 25010, 2011 .....	559
ISO 27789, 2013 .....	562	ISO/IEC 25012, 2008 .....	559
ISO 27799, 2008 .....	562	ISO/IEC 25020, 2007 .....	559
ISO 28000 Familie .....	562	ISO/IEC 25030, 2007 .....	559
ISO 28001, 2007 .....	562	ISO/IEC 25040, 2011 .....	559
ISO 28002, 2011 .....	562	ISO/IEC 25041, 2012 .....	559
ISO 28003, 2007 .....	562	ISO/IEC 25045, 2010 .....	559
ISO 28004 .....	562	ISO/IEC 25060, TR, 2010 .....	559

ISO/IEC 27000, 2014.....	559	IT Governance Institute® .....	94, 120, 166
ISO/IEC 27001, 2013.....	95	IT Network Security	
ISO/IEC 27001, 2013, Cor. 1, 2014.....	559	- ISO/IEC 18028 .....	555
ISO/IEC 27002.....	175	- ISO/IEC 27033 .....	561
ISO/IEC 27002, 2013.....	560	IT Risk Management	
ISO/IEC 27003, 2010.....	560	- FFIEC.....	547
ISO/IEC 27004, 2009.....	560	- ISO/IEC 27005, 2012.....	560
ISO/IEC 27005, 2012.....	560	IT Security	
ISO/IEC 27006, 2011.....	560	- Assessment .....	502
ISO/IEC 27007, 2011.....	560	- Bluetooth.....	565
ISO/IEC 27008, TR, 2011.....	560	- Cloud Computing.....	565
ISO/IEC 27009, CD .....	560	- Configuration Management.....	565
ISO/IEC 27010, 2012.....	560	- Continuous Monitoring.....	565
ISO/IEC 27011, 2008.....	560	- Engineering Principles.....	564
ISO/IEC 27013, 2012.....	560	- Evaluation	
ISO/IEC 27014, 2013.....	560	-- ISO/IEC 18045, 2008.....	555
ISO/IEC 27015, TR, 2012.....	560	- Firewall Guidelines and Policy.....	564
ISO/IEC 27016, TR, 2014.....	560	- Glossary .....	563
ISO/IEC 27017, DIS .....	560	- IDPS.....	564
ISO/IEC 27018, 2014.....	560	- Incident Handling .....	564
ISO/IEC 27019, TR, 2013.....	560	- ISO/IEC 15443-1,2, TR.....	555
ISO/IEC 27031, 2011.....	560	- ISO/IEC 15446, TR .....	555
ISO/IEC 27032, 2012.....	561	- IT-GSK.....	563
ISO/IEC 27033.....	561	- Media Sanitization.....	564
ISO/IEC 27035, 2011.....	561	- Mobile Devices.....	565
ISO/IEC 27036.....	561	- Mobile Devices, DRAFT .....	565
ISO/IEC 27037, 2012.....	561	- Performance Measurement .....	564
ISO/IEC 27038, 2014.....	561	- Product Selection Guide .....	564
ISO/IEC 27039, 2015.....	561	- Server .....	565
ISO/IEC 27041, FDIS .....	561	- Testing.....	564
ISO/IEC 27042, DIS .....	561	- Training Requirements .....	564
ISO/IEC 27043, 2015.....	561	- Virtualization .....	565
ISO/IEC 27044, WD.....	562	- Web Services .....	564
ISO/IEC 27050.....	562	- WLAN Guidelines.....	565
ISO/IEC 28004-1, 2012.....	562	IT Securitymanagement	
ISO/IEC 28005-1, 2013.....	562	- ISO/IEC 27001, 2013.....	95
ISO/IEC 29125, TR, 2010.....	563	IT Service Continuity	
ISO/IEC 29190, PRF.....	563	- ISO/IEC 27031, 2011.....	560
ISO/IEC 29361, 2008.....	563	IT Service Management	
ISO/IEC 29362, 2008.....	563	- COBIT®.....	551
ISO/IEC 29363, 2008.....	563	- ISO/IEC 20000-1, 2011 .....	556
ISO/IEC 38500, 2008.....	563	- ISO/IEC 20000-10, TR, 2013 .....	556
ISO/IEC-27000-Familie .....	93	- ISO/IEC 20000-11, PDTR.....	556
ISPE.....	111	- ISO/IEC 20000-2, 2012 .....	556
ISSCRMMM.....	520	- ISO/IEC 20000-3, 2012 .....	556



- ISO/IEC 20000-4, TR, 2010 .....	556
- ISO/IEC 20000-5, TR, 2013 .....	556
- ISO/IEC 20000-6, WD .....	556
- ISO/IEC 20000-8, WD .....	556
- ISO/IEC 20000-9, TR .....	556
- ISO/IEC 90006, TR, 2013.....	563
- ITIL® .....	563
ITAF .....	111
IT-Governance .....	579
IT-Grundschutzhandbuch.....	98, 99
IT-Grundschutzkataloge.....	98, 166, 563
IT-GSHB.....	98, 99
IT-GSK .....	98, 99, 563
ITIL® .....	166, 175, 563
ITSCM.....	133, 303
- Pyramid.....	304
- Pyramide.....	304
ITSEC .....	563

---

## J

JBOD.....	400
Joint Forum	
- Business Continuity.....	83, 550
- Outsourcing.....	550
Just a Bunch of Disks.....	400

---

## K

Kabelführungszone .....	227
KAG.....	543
KAGB .....	69, 542
Kapazitätsmanagement .....	295
Kapitalanlagegesellschaften	
- Notfallkonzept .....	79
- Outsourcing.....	79
Kapitalanlagegesetzbuch.....	69
Katastrophe .....	443
Katastrophenvorsorge .....	451
- Handbuch .....	451
KAVerOV .....	542
KDC.....	350
Kennzahl.....	273
Kerberos™.....	350, 580
Kernprozess.....	242, 243
Key Distribution Center.....	350

Key Performance Indicator.....	510
Key-Logger .....	368, 580
Klassen-Maßnahmen-Matrix.....	197
KMM .....	197
KMU .....	IX
- Sicherheitsmanagement .....	35
Knowledgeware .....	145
Kollisionsresistenz .....	365
Kommunales Netz .....	580
Konfigurationscluster.....	293
Konfigurationsdatenbank.....	292
Konfigurationselement .....	292
Konfigurationsmanagement.....	292
- ISO 10007, 2003.....	554
- NIST SP 800-128, 2011.....	565
Konformität .....	72, 251
Konformitätsmanagement.....	251
Konsolidierung	
- Arbeitsmittel .....	232
- Dataware .....	231
- Daten.....	232
- Hardware .....	231
- Hilfsmittel .....	232
- Interface.....	231
- Knowledgeware .....	231
- Komponenten .....	232
- Materialien .....	232
- Middleware.....	231
- Organisation .....	233
- Orgware.....	231
- Processware .....	231
- Produkt.....	233
- Prodware .....	231
- Prozess.....	231
- Schnittstellen.....	232
- Service.....	233
- Servware.....	231
- Software.....	231
- Technologie.....	232
- Wissen .....	232
Kontinuität	
- Anforderungen.....	92, 115
- Architektur	
-- unternehmensspezifisch.....	202
- dienstleistungsimmanent.....	231
- lebenszyklusimmanent.....	230
- Management .....	300, 301, 314
-- Handbuch.....	438

-- ISO 22301, 2012 .....	557
-- ISO 22313, 2012 .....	557
-- Portal .....	438
-- Prozess .....	313
-- Pyramide .....	303
-- Regelkreis .....	313
- organisationsimmanent .....	230
- pervasiv .....	231
- Planung .....	83
- Politik .....	141, 152, 304
- produktimmanent .....	231
- prozessimmanent .....	230
- Pyramide .....	303
- ressourcenimmanent .....	230
- Strategie .....	208
- ubiquitär .....	231
KonTraG .....	41, 262, 542
Kontrollaktivität .....	580
Kontrolle	
- Abgang .....	258
- Absende .....	258
- Auftrag .....	259
- Eingabe .....	259
- Empfänger .....	259
- Lese .....	258
- Quellen .....	259
- Transport .....	258
- Übertragung .....	258
- Verfügbarkeit .....	259
- Wiederaufbereitung .....	258
- Zugang .....	258
- Zugriff .....	258
- Zutritt .....	258
- Zweck .....	259
Kontrollelement .....	580
Kontrollen	
- Konformitätsmanagement .....	253
- Kontinuitätsmanagement .....	259, 327
- Politik .....	157
- Reifegrad .....	526
Kontrollsystem	
- internes .....	71, 91
Kontrollziel .....	580
Körperscanner .....	358
Korrekturmaßnahmen .....	505

Kosten	
- Datenschutzverletzung .....	22
- Sicherheitsverletzung .....	22
KPI .....	510, 513
Kreditwesengesetz .....	67
Kriminalität	
- organisierte .....	582
Krise .....	442
Krisenmanagement	
- BS 11200, 2014 .....	550
- DIN EN 15975-1 .....	552
Krisenmanager .....	453
Krisenstab .....	416, 453
Krisenvorsorge .....	451
- Handbuch .....	451
Kritikalität .....	580
- Klassen .....	177
KRITIS .....	580
Kryptografie .....	361
- ISO/IEC 24759, 2014 .....	558
Krypto-Tool .....	364
KWG .....	67, 542

---

## L

Lagebericht .....	41
- Informationssicherheit .....	19
LAN .....	581
- virtuell .....	228
Landkarte	
- Bedrohung .....	206
LASI .....	61
LASI LV 58 .....	563
Layer of Protection Analysis .....	581
Least Privileges .....	224
Lebenderkennung .....	346
Lebenszyklus .....	141, 484
- Produkt .....	484
- Prozess .....	484, 486
- Ressource .....	486
- System .....	484
lebenszyklusimmanent	
- Dienstleistungssicherheit .....	147
- IKT-Systemsicherheit .....	147
- Produktsicherheit .....	147

- Sicherheit .....	146
- Sourcing .....	279
- Systemsicherheit .....	147
Leistungsmanagement.....	273
Leistungsvereinbarung .....	273
Leitlinie .....	125
Liberty Alliance .....	351
Lieferproblem.....	262
Limit.....	491
Lizenzmanagement .....	293
- Freie Software.....	294
Local Area Network .....	581
logging .....	371, 583
Lokales Netz.....	581
LOPA.....	581
Löschanlage.....	344
- Wassernebel.....	344
Löschdecke.....	344
Löscheinrichtung	
- Handfeuerlöscher .....	344
- Löschdecke .....	344
- Wandhydrant .....	344
Löschtools.....	367
Löschverfahren	
- BSI.....	367
- DoD 5220.22-M.....	367
- DoD 5220.22-M ECE .....	367
- Gutmann .....	367
Löschvorgang.....	367
Lötarbeiten .....	341
Luftverkehr .....	262
LV 58 .....	61, 563

---

**M**

MAC.....	581
MaComp.....	80, 549
MaIuK .....	91, 549
Malware.....	408, 585
MAN .....	580
Managed Objects .....	245
Managed Services.....	380
Management by	
- Objectives.....	385
- walking around.....	385
Management Review .....	107
Managementdisziplin .....	242

- Änderungen.....	289
- Arbeitsschutz.....	254
- Architektur.....	374
- Change.....	289
- Compliance .....	251
- Datenschutz .....	256
- Ereignisse .....	282
- Finanzen.....	280
- Innovation.....	376
- Kapazität .....	295
- Konfiguration .....	292
- Konformität.....	251
- Kontinuität.....	300, 301
- Leistungen.....	273
- Lizenzen .....	293
- Performance.....	295
- Personal .....	383
- Probleme .....	288
- Projekte.....	281
- Qualität.....	281
- Release .....	291
- Risiko .....	263
- Security .....	328
- Service Level.....	273
- Überblick.....	249
- Wartung .....	297
Managementsystem.....	25
- Anti-Korruptionsmanagement.....	550
- Arbeitsschutz	
-- BS OHSAS 18001 .....	107, 550
-- BS OHSAS 18002 .....	550
-- ISO 45001, CD .....	563
-- LASI LV 58 .....	61, 563
-- OHRIS, 2010 .....	61
- Asset Management	
-- ISO 55001, 2014 .....	563
-- ISO 55002, 2014 .....	563
- BCM	
-- ISO 22301, 2012 .....	557
- Business Continuity	
-- bsi PD 25... ..	551
- Compliance .....	548, 556
- Datenschutz .....	550
- Food safety	
-- ISO-22000-Familie .....	557
- Informationssicherheit .....	551
-- ISO-27000-Familie .....	559

- integriert	
-- OHRIS .....	61
- ISM	
-- ISO-27000-Familie.....	94
- Rahmenwerk.....	550
- Risiko .....	261
- Risikomanagement	
-- ISO 31000, 2009 .....	563
- Social Compliance	
-- SA8000®.....	566
- Sozialschutz	
-- SA8000®.....	566
Mandatory Access Control .....	581
MAO .....	273, 445
MaRisk	
- BA.....	549
- Banken .....	71
- Investmentgesellschaften .....	78
- Notfallkonzept.....	299
- Notfallplanung .....	299
- Notfalltests .....	299
- VA .....	84, 549
-- Notfallplanung.....	85
- Versicherungen.....	84
Maschinenrichtlinie .....	64
Maschinenrichtlinie, Europa .....	545
Massenevakuierung	
- ISO 22315, 2014 .....	557
Maßnahmen-Klassen-Matrix.....	197
Materialvereinzelung	
- videobasiert.....	377
Maturity Model .....	520
Maximal tolerierbare Ausfalldauer .....	445
Maximalabstand.....	237
Maximale Wiederanlaufzeit .....	445
Maximum Acceptable Outage.....	273, 445
Maximum Tolerable Downtime.....	445
Maximum Tolerable Period of Disruption	
.....	445
MBCO .....	445
MBOD.....	400
MD5 .....	366
MDM .....	411
Medium Access Control.....	581
Message Authentication Code .....	581
Metropolitan Area Network .....	580
Mindestanforderungen	
- Compliance-Funktion .....	80
- Datenschutzbeauftragter .....	49
- IuK.....	91
- MaRisk .....	71
- MaRisk BA.....	165
- Risikomanagement.....	78
- Versicherungen.....	84
Mindestgeschäftsbetrieb.....	18, 178, 445
Mindestszenarien .....	155, 160, 446
Minimalabstand.....	237
Minimum Business Continuity Objective	
.....	445
Minimum Privileges .....	224
Minimum Services .....	225
Mini-Spion.....	368
mirroring .....	397, 400
- host based .....	446
- storage based.....	446
MISRA C®.....	563
MISRA® C++.....	563
mission criticality .....	172
MKM.....	197
Mobile Device Management .....	411
Mobile Devices Security	
- NIST SP 800-124, Rev. 1 .....	565
- NIST SP 800-164, DRAFT.....	565
MOF .....	401
Momentaufnahme .....	500
MTA .....	273, 445
MTBF.....	445
MTBSI .....	445
MTD .....	445
MTPD.....	273, 445
MTTA.....	445
MTTR .....	445
Multi-Provider-Management.....	280
Mustererkennung.....	406
<hr/>	
N	
N+1-Redundanz.....	218
N+x-Redundanz .....	218
Nacharbeit.....	301, 446, 581

- Nachvollziehbarkeit ..... 225
- Namenskonvention ..... 292
- narrensicherer Mechanismus ..... 215
- NAS ..... 399, 402, 581
- Nassanlage ..... 344
- NAT ..... 581
- NEA ..... 217, 318, 581
- near miss ..... 256, 314
- Need-to-know-Prinzip ..... 80
- Nessus ..... 503
- Netto-Risiko ..... 131
- Network Address Translation ..... 581
- Network Attached Storage ..... 399, 581
- network centric ..... 399
- Netzersatzanlage ..... 217, 318, 581
- Netzidentität
- föderierte ..... 351
- Netzsegment ..... 227, 228
- NEWS 2011
- BS 10500, 2011 ..... 550
  - DIN EN 80001-1 ..... 554
  - GAMP® 5 GPG
    - GxP Process Control Systems.. 111
  - ISO 18308 ..... 556
  - ISO 22002-3 ..... 557
  - ISO 22312, TR ..... 557
  - ISO 22320 ..... 557
  - ISO 26262-1...9 ..... 559
  - ISO 28002 ..... 562
  - ISO 28005-2 ..... 562
  - ISO 29100 ..... 562
  - ISO/IEC 24745 ..... 558
  - ISO/IEC 24760-1 ..... 558
  - ISO/IEC 24763 ..... 558
  - ISO/IEC 25010 ..... 559
  - ISO/IEC 25040 ..... 559
  - ISO/IEC 27006 ..... 560
  - ISO/IEC 27007 ..... 560
  - ISO/IEC 27008, TR ..... 560
  - ISO/IEC 27031 ..... 560
  - ISO/IEC 27035 ..... 561
  - ISO/IEC/IEEE 26511 ..... 559
  - ISO/IEC/IEEE 42010 ..... 563
  - NIST SP 800-125 ..... 565
  - NIST SP 800-128 ..... 565
  - NIST SP 800-137 ..... 565
  - NIST SP 800-144 ..... 565
  - NIST SP 800-145 ..... 565
  - Rechenzentrum, Best Practices ..... 549
  - Risk Management Principles ..... 550
- NEWS 2012
- 15443-1 ..... 555
  - 15443-2 ..... 555
  - ANSI/AIHA/ASSE Z10-2012 ..... 107
  - Bankenaufsicht
    - Grundsätze ..... 83
  - BS PAS 99 ..... 550
  - CC ..... 551
  - CEM ..... 551
  - CIM 3.0.0 ..... 401
  - COBIT® 5 ..... 111
  - DIN 66399-1 ..... 554
  - DIN 66399-2 ..... 554
  - DIN EN 50128 ..... 553
  - FFIEC
    - AUD ..... 89
    - TSP ..... 89
  - GAMP® 5 GPG
    - GxP Compliance ..... 111
    - Test von GxP-Systemen ..... 111
  - IDW
    - RS FAIT 4 ..... 549
  - IEEE 802.11-2012 ..... 577
  - ISO 19770-1 ..... 556
  - ISO 20004, TR ..... 556
  - ISO 22300 ..... 557
  - ISO 22301 ..... 557
  - ISO 22311 ..... 557
  - ISO 22313 ..... 557
  - ISO 26262-10 ..... 559
  - ISO/IEC 20000-2 ..... 556
  - ISO/IEC 20000-3 ..... 556
  - ISO/IEC 25041 ..... 559
  - ISO/IEC 27005 ..... 560
  - ISO/IEC 27010 ..... 560
  - ISO/IEC 27013 ..... 560
  - ISO/IEC 27015, TR ..... 560
  - ISO/IEC 27032 ..... 561
  - ISO/IEC 27033-2 ..... 561
  - ISO/IEC 27037 ..... 561
  - MaRisk ..... 71
  - NIST SP 800-121 Rev 1 ..... 565
  - NIST SP 800-153 ..... 565
  - NIST SP 800-164, DRAFT ..... 565
  - NIST SP 800-30, Rev 1 ..... 564
  - NIST SP 800-61, Rev 2 ..... 564

- NIST SP 800-94, Rev. 1, DRAFT.....	564	NEWS 2014	
NEWS 2013		- BS 11200 .....	550
- COSO		- BS 65000 .....	550
-- Framework .....	92	- cGLP, DRAFT.....	565
- DIN 66399-3 .....	554	- Corporate Governance	
- DIN EN 15975-2.....	552	-- Kodex.....	65
- DIN EN 50600-1.....	553	-- OECD.....	565
- DIN EN 50600-2-3.....	553	- DIN 14096.....	552
- FISMA.....	547	- DIN 16602-30-02.....	552
- IDW PS 951.....	115, 548	- DIN EN 1125 .....	552
- ISO 17090-1.....	555	- DIN EN 50600-2-1.....	553
- ISO 19770-5.....	556	- DIN EN 50600-2-2.....	553
- ISO 21091 .....	557	- DIN EN 50600-2-4.....	553
- ISO 22002-2.....	557	- DIN EN 50600-2-5.....	553
- ISO 22398 .....	558	- DIN EN 50600-2-6.....	553
- ISO 27789 .....	562	- DIN VDE 0833-1 .....	551
- ISO 28005-1.....	562	- DIN VDE 0833-4 .....	551
- ISO 29119-1/2/3 .....	562	- GoBD.....	43, 548
- ISO/IEC 20000-10.....	556	- ISO 17090-4.....	555
- ISO/IEC 20000-5.....	556	- ISO 17789 .....	555
- ISO/IEC 24761 .....	558	- ISO 19600 .....	556
- ISO/IEC 27001 .....	95, 559	- ISO 20006-1 .....	556
- ISO/IEC 27014 .....	560	- ISO 22004 .....	557
- ISO/IEC 27019, TR.....	560	- ISO 22315 .....	557
- ISO/IEC 27033-5.....	561	- ISO 22600 .....	558
- ISO/IEC 27036-3.....	561	- ISO 28004-2 .....	562
- ISO/IEC 29101 .....	562	- ISO 28004-3 .....	562
- ISO/IEC 90006, TR.....	563	- ISO 28004-4 .....	562
- ISO/TR 31004.....	563	- ISO 55001 .....	563
- KAGB.....	542	- ISO 55002 .....	563
- KAVerOV .....	542	- ISO/IEC 24759 .....	558
- NIST IR 7298 Rev 2.....	563	- ISO/IEC 24764 .....	558
- NIST SP 800-124, Rev. 1.....	565	- ISO/IEC 24775 .....	558
- NIST SP 800-53, Rev. 4.....	564	- ISO/IEC 25000 .....	558
- PCI DSS, Version 3.0 .....	566	- ISO/IEC 25001 .....	559
- Risikomanagement		- ISO/IEC 27000 .....	559
-- Datenaggregation .....	550	- ISO/IEC 27002 .....	560
- Risk data aggregation.....	263, 374	- ISO/IEC 27016, TR .....	560
- VdS 2037EF .....	567	- ISO/IEC 27018 .....	560
- VdS 2263 .....	567	- ISO/IEC 27033-4 .....	561
- VdS 2366 .....	567	- ISO/IEC 27034-1 .....	561
- VdS 3172 .....	568	- ISO/IEC 27036-1 .....	561
- VdS 3426 .....	568	- ISO/IEC 27036-2 .....	561
- VdS 3534 .....	568	- ISO/IEC 27038 .....	561
COSO, Internal Control .....	546		

- Kosten	
- Datenschutzverletzung.....	22
- Sicherheitsverletzung.....	22
- MaComp .....	80
- NIST SP 800-161, 2nd DRAFT .....	565
- NIST SP 800-167, DRAFT.....	565
- NIST SP 800-53A, Rev. 4 .....	564
- NIST SP 800-88, Rev. 1 .....	564
- ONR 49000.....	566
- ONR 49001.....	566
- ONR 49002.....	566
- ONR 49003.....	566
- PIC/S GMP.....	110
- Review of Risk Management	
Principles .....	550
- SA8000®.....	566
- SERA.....	566
- Sicherheitsstudie <kes> .....	19
- SMI-5 1.6.0 .....	400
- Swiss Code.....	65
- VdS 2333.....	567
NEWS 2015	
- Business Continuity Planning, FFIEC	
.....	546
- ISO 27040 .....	561
- ISO/IEC 27039.....	561
- VDI 7000.....	566
NFS.....	399
Nichtraucherschutz.....	56
NIDS.....	406
NIST .....	581
- Bluetooth Security .....	565
- Cloud Computing	
-- Definition .....	565
-- Security.....	565
- Firewall Guidelines and Policy ....	564
- IDPS.....	564
- Information Security	
-- Handbook .....	564
- IT Security Engineering Principles	564
- Media Sanitization.....	564
- Mobile Devices Security.....	565
- Risk Management .....	564
- Secure Web Services.....	564
- Securing WLANs.....	565
- Security	
-- Continuous Monitoring.....	565
-- in Mobile Devices, DRAFT .....	565
-- Performance Measurement .....	564
-- Virtualization Technologies .....	565
- Security Assessment .....	564
- Security Controls.....	564
- Security Incident Handling.....	564
- Security Testing.....	564
- Security-Focused Configuration	
Management .....	565
- Selecting IT Security Products.....	564
- Server Security.....	565
- Supply Chain Risk Management	
Practices, 2nd DRAFT.....	565
- Training Requirements.....	564
NNIDS.....	407
Notausgang .....	56, 446
Notausgänge.....	460
Notbetrieb.....	44, 299, 301, 446, 582
- Nacharbeit.....	301
- Postvention .....	301
- Rückkehr .....	301
- Übergang.....	301, 311
Notfall.....	442
- Konzept	
-- BaFin .....	79
-- Investmentgesellschaften .....	79
-- Kapitalanlagegesellschaften.....	79
Notfall-, Krisen- und	
Katastrophenvorsorge	
- Plan .....	317
- Planung .....	457
Notfallkonzept .....	71
- Outsourcing .....	79
Notfallplan.....	83
- Geschäftsunterbrechung .....	83
Notfallplanung.....	85
- Tool .....	455
Notfalltest .....	74
Notfallvorsorge .....	107, 451
- Handbuch.....	451
- Investitionen .....	22
NP .....	579
<hr/>	
O	
OASIS® .....	582
Objektorientierung .....	214
Objektschutz.....	332

- äußerer .....	332	OpenAM.....	353
- innerer.....	332	OpenPGP.....	582
Occupational Health.....	203	OpenVAS.....	294, 503
Occupational Health and Risk		Operational Impact Analysis .....	179, 573
Management System .....	61	- Beispiel.....	183
Occupational Health and Safety		Operational Level Agreement .....	273, 379
Assessment Series.....	107	Operational Risk.....	81
Occupational Health, Safety, Security and		Operationelles Risiko.....	81
Continuity Management.....	119	- Banken.....	543
Occupational Health, Safety, Security,		- Schweiz .....	543
Continuity and Risk Management		Operations	
Maturity Model.....	520	- FFIEC.....	547
Occupational Safety and Health Act .....	64	Opferlamm.....	405
Occupational Safety and Health		Optical Character Recognition (OCR)	354
Management Systems		Ordnungsmäßigkeit .....	126
- Guidelines .....	107	Organisation.....	145
OCR .....	354	- Belastbarkeit, ISO 22316, CD.....	557
OCTAVE® .....	106	Organisatorische Belastbarkeit.....	108
OENORM		Organisierte Kriminalität (OK).....	582
- S 2400 .....	300, 566	Organization for the Advancement of	
- S 2401 .....	566	Structured Information Standards..	582
- S 2402 .....	566	Organized Crime.....	582
- S 2403 .....	566	Ö-SGMS .....	62
Öffentlichkeitsbeteiligung.....	566	OSH.....	60
OHRIS, 2010.....	61, 566	- ILO.....	107
OHSAS .....	107, 165, 550	OSH Act.....	64, 547
- 18001 .....	107, 550	OSI-Referenzmodell.....	582
- 18002 .....	107, 550	Österreich	
OHSMS.....	107, 165	- Gesetze.....	542
OHSSCE .....	122	- Verordnungen.....	542
OHSSCEPRE.....	122	OTP .....	347
OHSSCRE.....	122	- HOTP .....	348
OHSSCRMMM.....	520	- TOTP .....	348
OIA.....	179, 573	Out-of-Band-Virtualisierung .....	400
OK .....	582	Outsourcing .....	71
OLA .....	273, 379	- Anforderungen, Joint Forum .....	77
One Time Password (OTP).....	347	- BaFin.....	74, 79, 85
ONR 49000, 2014 .....	566	- Banken.....	74, 543
ONR 49001, 2014 .....	566	- FFIEC.....	89, 547
ONR 49002-1, 2014 .....	566	- FINMA .....	87
ONR 49002-2, 2014 .....	566	- Information Security	
ONR 49002-3, 2014 .....	566	-- ISO/IEC 27036.....	561
ONR 49003, 2014 .....	566	- Investmentgesellschaften.....	79
ONR-49000-Familie.....	105	- Joint Forum.....	77, 550
Open Door Policy.....	385	- Kapitalanlagegesellschaften.....	79



- Notfallkonzept .....	79	- White-Box- .....	502
<hr/>		Pepper .....	365
<b>P</b>		Performancemanagement .....	295
Paketfilter .....	403	Perimeterschutz .....	339
- mit Zustandstabelle .....	403	- VdS 3143, 2012 .....	567
Pandemie		Period of Disruption .....	307, 445
- Vorsorgeplanung .....	461	Personal .....	145
Paperware .....	292	- Beschaffung .....	384
Papierkorb		- Betreuung .....	385
- selbstlöschend .....	341	- Einarbeitung .....	384
Papierlager .....	342	- Management .....	383
PAS .....	582	- Planung .....	384
password		- Prozess .....	383
- cracking .....	347	- Recruiting .....	384
- guessing .....	347	- Trennung .....	388
- social hacking .....	347	- Weiterentwicklung .....	385
Passwort		Personal Identification Number (PIN)	345
- Eigenschaften .....	472	Personen-Hilferufanlagen	
- ermitteln .....	347	- DIN EN 50134 .....	553
- erraten .....	347	Personenvereinzelnung	
- Gebote .....	471	- videobasiert .....	377
- probieren .....	347	Perspektive	
- Regeln .....	471	- finanziell .....	509
- Vielfalt .....	349	- Kunden .....	510
Patchmanagement .....	290	- Prozesse .....	513
PatG .....	542	pervasiv	
Pattern		- RiSiKo-Management .....	231
- Architecture .....	485	pervasive	
- Design .....	485	- Continuity .....	231
pBSC .....	509	- Safety .....	231
PCAOB .....	91	- Security .....	231
PCI DSS .....	566	Pfadanalyse .....	221
PCM .....	303	Pfandbriefgesetz (PfandBG) .....	68, 542
- Pyramide .....	304	PfG .....	543
PD 25111 .....	551	Pflichten	
PD 25222 .....	551	- Anweisungspflicht .....	38
PD 25666 .....	551	- Hinweispflicht .....	38
PD 25888 .....	551	- Kontrollpflicht .....	38
PDA .....	15, 364	- Personalauswahlpflicht .....	38
PDCA-Zyklus .....	530	- Unterrichtspflicht .....	38
- Kontinuitätsmanagement .....	313	Pflichtverletzung .....	37
- Qualitätsmanagement .....	270	PH 9.330.1 .....	44
- Risikomanagement .....	270	PH 9.330.2 .....	44
Penetrationstest .....	370, 502	PH 9.330.3 .....	44
- Black-Box- .....	502	PHA .....	501
- Grey-Box- .....	502	Phishing .....	583
		Physical Content Security .....	354, 358
		PIA .....	257

- PIC..... 110  
 PIC/S ..... 110  
   - PE 009-11, Annexes ..... 546  
   - PI 011-2 ..... 546  
 PIMS ..... 550  
 PIN ..... 345, 583  
 Pit ..... 393  
 PKI ..... 583  
 Plagiat ..... 378  
 Plan-Ist-Vergleich..... 504  
 Plant Management ..... 244  
 Planungshorizont..... 18, 155  
 Plattenspiegelung..... 397  
 Plausibilitätsprüfung ..... 215  
 PMBOK® ..... 112  
 Poka-Yoke ..... 215  
 Politik..... 125  
 Portscanning ..... 406  
 Posteingangsschutz ..... 359  
 Postvention ..... 301  
 Powermanagement ..... 342  
 Practices  
   - USA ..... 546  
 Präventivmaßnahme ..... 316  
 Preliminary Hazard Analysis ..... 501  
 PRF ..... 579  
 Primärspeicher ..... 392, 396  
 Prinzip  
   - Abstraktion ..... 213  
   - Abwesenheitssperre..... 219  
   - Aktiv-Passiv-Differenzierung..... 238  
   - aufgeräumter Arbeitsplatz..... 219  
   - Ausschließlichkeit ..... 223  
   - Clear Screen Policy ..... 219  
   - deny all ..... 223  
   - Funktionstrennung ..... 220  
   - generelles Verbot..... 223  
   - grundsätzliches Verbot..... 223  
   - Klassenbildung ..... 214  
   - Konsistenz ..... 235  
   - Konsolidierung ..... 231  
   - minimale Dienste ..... 225  
   - minimale Nutzung ..... 225  
   - minimale Rechte ..... 224  
   - minimaler Bedarf..... 224  
   - Namenskonvention ..... 216  
   - Need-to-Know ..... 224  
   - Need-to-Use ..... 224  
   - Plausibilisierung ..... 234  
   - Poka-Yoke..... 215  
   - Redundanz ..... 216  
   - Sicherheitsschalen..... 221  
   - Standardisierung ..... 233  
   - Subjekt-Objekt-Differenzierung.... 238  
   - Vererbung ..... 237  
   - Vier-Augen-..... 220  
   - Wirtschaftlichkeit ..... 212  
 Privacy  
   - Assessment  
     -- ISO/IEC 29190, PRF..... 563  
   - ISO 22307, 2008 ..... 557  
   - ISO/IEC 29101, 2013..... 562  
 PROArm ..... 255, 583  
 Problemmanagement..... 288  
 Processware..... 292  
 PROCom..... 303  
 ProdHaftG ..... 40, 542  
 ProdSG..... 542  
 Produktevaluation ..... 455  
 Produktsicherheit  
   - lebenszyklusimmanent ..... 147  
 Projektmanagement ..... 281  
 PROKom..... 303, 583  
 promiscuous mode..... 407  
 PROMSim ..... 141  
 PROProm..... 583  
 PROQuam ..... 583  
 PRORim ..... 264, 269, 583  
 PROSem..... 583  
 PROSim ..... 140, 145, 202, 583  
 PROSom ..... 583  
 PROSoM ..... 279  
 PROTem ..... 583  
 Protokollauswertung ..... 334, 583  
 Protokollierung..... 334, 371, 583  
 ProTOPSi ..... 141, 583  
 Provider  
   - Management..... 273, 279  
     -- Multi- ..... 280  
   - Managing, FDIC ..... 546

- Selecting, FDIC.....	546
Proxy .....	404
- Reverse.....	404
Prozess .....	145, 308, 417
- Architektur .....	173, 243
- IKT-Betrieb .....	245
- Landschaft .....	173
prozessimmanent	
- Sicherheit .....	146
PRP-Maßnahmen.....	301
Prüfvorschriften	
- USA.....	546
PS 330 .....	44
PS 525 .....	548
PS 850 .....	44
PS 880 .....	44, 548
PS 951 .....	548
PS 980 .....	548
Psychologie	
- forensisch.....	384
Public Available Specification .....	582
Public Key Infrastructure .....	583
Public-Key-Verfahren .....	363
PVC-haltige Bodenbeläge.....	343
PVC-Kabel .....	343
Pyramide	
- ACM .....	304
- Arbeitsschutz.....	25, 256
- Arbeitssicherheit.....	25, 256
- Architektur .....	25, 374
- BCM .....	25, 304
- FCM .....	304
- Governance.....	25
- IKT .....	25
- ISM.....	25
- IT .....	25
- ITSCM .....	304
- IT-Sicherheit .....	25
- IuK .....	25
- Kontinuität .....	25, 304
- Management.....	25
- Modell .....	24, 28
- PCM.....	304
- Projekt .....	25
- Qualität .....	25
- Risiko.....	25
- RiSiKo.....	25, 160
- SCM .....	304

- Service.....	25
- Sicherheit.....	25
- Sourcing.....	25, 275
- Sozialschutz .....	25
- Test.....	25
- Umweltschutz.....	25
- Unternehmen.....	25
- Unternehmenssicherheit .....	25
Pyramidenmodell® .....	24, 28
- Arbeitsschutzpyramide.....	25
- Arbeitssicherheitspyramide.....	25
- Architekturmanagementpyramide.....	374
- BCM-Pyramide .....	25
- ISM-Pyramide .....	25
- Kontinuitätspyramide .....	24, 25
- Managementsystem.....	374
- Projektpyramide .....	25
- Qualitätspyramide.....	25
- Risikopyramide.....	24
- RiSiKo-Pyramide .....	24
- Servicepyramide .....	25
- Sicherheitspyramide.....	24
- Sourcingpyramide .....	25
- Testpyramide .....	25
- Umweltschutzpyramide.....	25
- Unternehmenspyramide .....	25
- USM-Pyramide .....	25

---

## Q

Qualifikationsarchitektur.....	415
Qualifikationsprofil .....	415
Qualitätsmanagement .....	281

---

## R

RAID.....	396
- EDAP .....	397
- fehlerresistent .....	397
- fehlertolerant .....	397
- katastrophentolerant.....	397
- Level.....	396
- Neue Kriterien .....	397
RAM .....	393, 583
RAMS .....	553
- DIN EN 50126, 2000 .....	553

Rauchmelder.....	343	- Kontrollen.....	526
Räumlichkeiten .....	319	Relay .....	368
RC5™.....	362	Releasemanagement .....	291
Rechenzentrum .....	319, 342	Reliability .....	590
- Best Practices.....	549	remote	
- DIN EN 50600 .....	553	- access, ISO/IEC 18028-4 .....	555
- TIA 942-A-2012.....	549	- lock .....	411
Rechteverwaltung .....	332	- wipe.....	411
Records Management.....	584	Replay .....	476
recovery.....	446, 454	Report	
Recovery.....	311	- Continuity.....	507
- Disaster .....	111	- Risk.....	507
- Plan .....	317	- Safety.....	507
- Point Objective.....	178, 273, 445	- Security .....	507
- Time Objective .....	445	Reporting	
- Verfahren.....	457	- Continuity.....	505
Redundant Array of		- Safety.....	505
- Independent Disks .....	396	- Security .....	505
- Inexpensive Disks.....	396	Requirements Architecture .....	204
Redundanz.....	216	Resilience.....	584
- aktive.....	218	Ressource.....	145
- Geschwindigkeit.....	218	restauration .....	447
- heiße.....	218	Restore .....	402
- kalte.....	218	Rettungsleiter.....	344
- Latenz .....	218	Rettungsweg .....	446
- N+1 .....	218	Return on Safety, Security and	
- N+x .....	218	Continuity Investment .....	584
- passive .....	218	Return on Security Investment.....	584
- Qualität.....	218	Reverse Proxy .....	404
- Quantität.....	217	Revision.....	146
- semiaktiv .....	218	Richtlinie.....	125
- strukturell.....	217	- Architekturmanagement .....	475
- vollständig.....	217	- Ausdrücke .....	431
- warme.....	218	- Benutzerkennung .....	470
Redundanzgrad.....	217	- Berichtswesen	
Regel		Kontinuitätsmanagement.....	463
- 70/30.....	490	- Computerviren-Schutz .....	473
- 80/20 von Pareto .....	490	- Datensicherung.....	449
- DGVU .....	53	- Drucker .....	431
Regeneration.....	301	- E-Mail-Nutzung.....	433
regulärer Betrieb		- Faxgerät .....	430
- Rückkehr .....	262	- Fax-Nutzung .....	430
Reifegrad		- IKT-Benutzerordnung.....	431
- RiSiKo-Management.....	526	- Internet-Nutzung.....	435
Reifegradmodell.....	520	- Kapazitätsmanagement .....	440

- Leseschutz..... 473
- mobile Geräte ..... 411
- Passwort..... 471
- Protokollierung ..... 474
- Räumlichkeiten ..... 447
- Sourcing ..... 427
- Umgang mit Schlüsseln und Zutrittskarten ..... 467
- Vorbeugender Brandschutz..... 458
- Zufahrtsschutz ..... 464
- Zutrittskontrollsystem ..... 476
- Zutrittsschutz ..... 467
- Richtlinien
  - Europa..... 544
  - Schweiz ..... 543
- RIPEMD-160..... 366
- Risiko..... 584
  - Adressenausfall..... 273
  - Aggregation..... 269
  - Analyse..... 106, 269, 584
    - SERA..... 566
  - Architektur ..... 268
    - brutto ..... 268
  - Assessment ..... 107
    - ISO 31010, 2009..... 563
    - NIST SP 800-30 ..... 564
  - Bewertung..... 107
    - NIST SP 800-30 ..... 564
  - brutto ..... 131
  - Controlling..... 269
  - Definition ..... 131
  - Diversifikation..... 269
  - Dreiklang ..... 131
  - finanziell ..... 273
  - Forschung ..... 272
  - Früherkennungssystem ..... 42
  - Grenzwert..... 160
  - Identifikation ..... 268
  - Inventar..... 268
  - Inventur..... 133, 268
  - Kapital..... 81
  - Kategorie..... 266, 267
  - Kommunikation..... 270
    - lebenszyklusimmanent..... 271
  - Lagerung ..... 272
  - Landkarte..... 160, 439
  - Liquidität ..... 273
  - Management..... 71, 133, 261, 263
  - Aktiengesetz..... 41
  - Audit ..... 269
  - Basel II..... 81
  - COSO ..... 546
  - Datenaggregation ..... 550
  - Handbuch..... 438
  - Handelsgesetzbuch ..... 41
  - IDW PS 340..... 42
  - IDW PS 525..... 548
  - ISO 14971, 2007 ..... 554
  - ISO 16085, 2006 ..... 555
  - ISO 31000, 2009 ..... 563
  - ISO 31004, TR, 2013 ..... 563
  - ISO Guide 73, 2009 ..... 554
  - ISO/IEC 27005, 2012 ..... 560
  - KonTraG ..... 41
  - lebenszyklusimmanent..... 82
  - MaRisk ..... 71
  - MaRisk BA..... 165
  - MaRisk VA ..... 84
  - Methoden ..... 41
  - NIST 800-30, Rev. 1 ..... 564
  - NIST SP 800-39..... 564
  - OHRIS..... 566
  - ONR 49000..... 165, 566
  - ONR-49000-Familie..... 105
  - Policy..... 263
  - Portal..... 438
  - Prinzipien ..... 550
  - Prinzipien, eBanking..... 549
  - Prinzipien, Review ..... 550
  - Prozess ..... 270
  - Pyramide ..... 264
  - Qualität ..... 110
  - Stress Testing Practices ..... 550
  - System..... 68
  - Versicherer ..... 543
  - Versicherungen..... 84
  - V-Quadrupel ..... 133, 210
  - Ziele..... 41
- Manager ..... 106, 566
- netto ..... 131
- Non-Compliance ..... 273
- operationelles..... 81
- Personal..... 272
- Politik..... 141, 152, 263, 264
- Portfolio..... 160, 420, 439
- Produkt..... 272

- Produktion .....	272	- DIN VDE 0833-4 .....	551
- Projekt .....	272	sachverständiger Dritter .....	244
- Prozess .....	272	Sacrificial Host .....	405
- Pyramide .....	264	Safety .....	203, 240, 242
- Recht .....	273	Safety and Security Engineering .....	122
- Strategie .....	208, 210, 265	Safety-Security-Continuity	
- Streuung .....	269	- Audit .....	148
- Transport .....	272	- Benchmark .....	518
- unerkannt .....	262	Safety-Security-Continuity-Risk	
RiSiKo .....	134	- Report .....	507
- Analyse .....	499	- Reporting .....	428
- Anforderungen .....	526	SAIDI .....	5
- Architektur .....	526	SAINT .....	503
- Controls .....	526	Salt .....	365
- Klassen .....	154, 177, 530	SAN .....	399
- Management .....	3, 498	- Fibre-Channel .....	399
-- Handbuch .....	438	Sanktion .....	433
-- pervasiv .....	231	Sarbanes-Oxley Act .....	39, 91
-- Prozess .....	530	SAS 70 .....	114
-- Reifegrad .....	526	SBOD .....	400
-- System .....	530	SCADA	
-- ubiquitär .....	231	- Stuxnet .....	11
- Politik .....	151, 152, 158, 530	SCAMPI .....	566
- Pyramide .....	160	Scanner .....	503
Risikomanagement		Schadenersatzrisiko .....	9
- DIN EN 15975-2 .....	552	Schadenspotenzialarchitektur .....	266
Risk		Schadenspotenzialklasse .....	266
- Asset Liability Mismatch .....	272	Schadensszenarien	
- Map .....	160	- Tabelle .....	181
Risk IT .....	111	Schadsoftware .....	585
risk optimized security .....	IX	Schadstoffbelastung .....	343
Roboterraum .....	342	Schalenmodell .....	221
Rolle		Scheduling .....	245
- Hausverwalter .....	465	Schlüssel	
RoSI .....	584	- öffentlicher .....	363
RoSSCI .....	584	- privater .....	363
RPO .....	273, 445	Schneidarbeiten .....	341
RSA .....	363	Schredder .....	366, 367
RTO .....	445	Schulung	
RWA .....	344	- ISO/IEC 20006 .....	556
		- ISO/IEC 24763, TR, 2011 .....	558
		Schutzbedarfsanalyse .....	129, 176
		- Prozesse, Beispiel .....	183
		Schutzbedarfsklassen .....	171, 188
		Schutzeinrichtung .....	127
<b>S</b>			
SA8000® .....	566		
SAA .....	587		

- Schutzobjekt ..... 127, 173  
 - Klasse..... 127
- Schutzsubjekt ..... 127  
 - Klasse..... 127
- Schwachstelle ..... 585
- Schwachstellen  
 - Analyse  
 -- ISO/IEC 20004, TR, 2012 ..... 556  
 - Architektur ..... 267  
 - Potenzialanalyse ..... 267
- Schwan, schwarz ..... 262
- Schweißarbeiten..... 341
- Schweiz  
 - Gesetze ..... 543  
 - Outsourcing..... 543  
 - Richtlinien..... 543  
 - Verordnungen..... 543
- SCM  
 - Pyramide..... 304
- Security ..... 203, 240, 242  
 - Appliance..... 409  
 - Assessment ..... 564  
 - Controls..... 564  
 - Gateway  
 -- Database ..... 404  
 - Incident  
 -- ISO/IEC 27035, 2011 ..... 561  
 -- ISO/IEC 27041, FDIS ..... 561  
 -- ISO/IEC 27043, 2015 ..... 561  
 -- ISO/IEC 27044, WD ..... 562  
 - Incident Response ..... 285  
 - Management..... 111, 328  
 -- Supply chain, ISO-28000-Reihe 562  
 - Scanner  
 -- Nessus..... 503  
 -- OpenVAS ..... 294, 503  
 -- SAINT ..... 503  
 - Storage..... 561
- Sekundärspeicher ..... 392, 394
- Self Service..... 352
- Sensibilisierung..... 385, 585
- SERA ..... 566
- Server Security  
 - NIST SP 800-123 ..... 565
- Serverraum..... 319
- Service  
 - Catalogue ..... 273  
 - Desk..... 247, 282  
 - Geber..... 318  
 - Level..... 585  
 -- Agreement..... 273, 318  
 -- Framework ..... 273  
 -- Management ..... 273  
 -- Requirement..... 273  
 -- Vereinbarung ..... 585  
 - Parameter ..... 273  
 - Ticket ..... 350  
 - Vereinbarung..... 278
- Service Oriented Architecture..... 232
- Service Provider ..... 351  
 - Managing, FDIC..... 546  
 - Selecting, FDIC ..... 546
- SGB ..... 542
- SGB IV ..... 542
- SGB VII..... 53, 54, 542
- SGB X..... 277, 542
- SGML..... 582
- SGMS..... 62
- SHA ..... 366
- sicherer Hafen ..... 52, 544
- Sicherheit  
 - dienstleistungsimmanent..... 231  
 - Ereignis  
 -- ISO/IEC 27035, 2011 ..... 561  
 -- ISO/IEC 27041, FDIS..... 561  
 -- ISO/IEC 27043, 2015 ..... 561  
 -- ISO/IEC 27044, WD ..... 562  
 - Hash-Algorithmus ..... 366  
 - ingenieurmäßig ..... 122  
 - Kontrollelemente..... 564  
 - lebenszyklusimmanent... 146, 230, 318  
 - leistungsimmanent..... 318  
 - organisationsimmanent..... 230  
 - pervasiv ..... 231  
 - produktimmanent..... 231, 318  
 - prozessimmanent..... 146, 230, 318  
 - ressourcenimmanent ..... 230, 318  
 - risikooptimiert..... IX  
 - Speicher, ISO 27040, 2015 ..... 561  
 - Trinkwasser  
 -- DIN EN 15975 ..... 552  
 - ubiquitär..... 231
- Sicherheits-, Kontinuitäts- und Risikomanagementprozess ..... 529
- Sicherheits-, Kontinuitäts- und Risikopolitik ..... 158

- Sicherheitsanalyse ..... 499
- Sicherheitsanforderungen ..... 92, 115, 142
- prinzipielle ..... 203
  - Transformation ..... 193
- Sicherheitsarchitektur ..... 143
- unternehmensspezifisch ..... 202
- Sicherheitsauditor ..... 148
- Sicherheitsbewusstsein ..... 385
- Sicherheitscontrolling ..... 503
- Sicherheitsdreiklang ..... 129
- Sicherheitselement ..... 241
- Kategorien ..... 202
- Sicherheitsglas ..... 339
- Einscheiben ..... 339
  - Verbund ..... 339
- Sicherheitshandbuch
- Österreich ..... 585
- Sicherheitsklasse ..... 177, 355
- Sicherheitskonzept ..... 585
- generisch ..... 143
  - spezifisch ..... 144, 479
- Sicherheitskriterien ..... 128, 176
- Grundwerte der IS ..... 128
  - primär ..... 203
  - sekundär ..... 204
- Sicherheitsleitlinie ..... 124, 585
- Sicherheitsmanagement ..... 119
- Handbuch ..... 438
  - ISO-28000-Familie ..... 562
  - Portal ..... 438
  - Prozess ..... 529
- Sicherheitsmaßnahme ..... 145, 482, 585
- Sicherheitsmerkmal ..... 193
- Abbildung ..... 195
- Sicherheitsmodell
- negativ ..... 408
- Sicherheitsniveau ..... 143, 500, 585
- Sicherheitsphilosophie ..... 585
- Sicherheitspolitik ..... 124, 141, 152
- gemäß Sicherheitspyramide ..... 124
  - Leitsatz ..... 154
  - nach ISO/IEC 27003 ..... 124
- Sicherheitspolitische Leitlinien ..... 167
- Sicherheitsprinzipien ..... 208
- Sicherheitsprozess ..... 529
- Sicherheitspyramide ..... VI, 122, 138, 585
- dreidimensional ..... VI
  - Unternehmen ..... VII
- Sicherheitsregelkreis ..... 148
- Sicherheitsrichtlinien ..... 143, 586
- Sicherheitssschalen ..... 221
- Modell ..... 330
- Sicherheitssschirm ..... 330
- Sicherheitsstandards ..... 143, 586
- Sicherheitsstrategie ..... 208, 211, 586
- Sicherheitsstudie ..... 499, 586
- <kes> ..... 19
- Sicherheitsstufe ..... 214
- Sicherheitsziele ..... 142, 178, 586
- Sicherheitszone ..... 226, 227, 235, 355
- Anwendung ..... 228
  - architekturell ..... 228
  - Closed Shop ..... 227
  - Grob- und Feintechnik ..... 227
  - Kabelführung ..... 227
  - logisch ..... 226
  - Netz ..... 228
  - räumlich ..... 226
  - Speicherbereich ..... 228
  - zeitlich ..... 226, 229
  - Zutritt ..... 227
- SIEM
- ISO/IEC 27044, WD ..... 562
- SigG ..... 542
- SigV ..... 542
- Single Point of
- Contact ..... 247, 282
  - Failure ..... 217, 300, 586
  - Security Administration ..... 590
  - Security Control and Administration ..... 339, 590
- Single Sign-on ..... 349, 378, 586
- föderiert ..... 351
  - Kerberos™ ..... 350
  - Passwort-Synchronisation ..... 350
  - Ticket-basiert ..... 350
- Single-Author-Konzept ..... 290
- SiRiKo ..... 134
- Skalierbarkeit ..... 218
- Skill Profile ..... 415



Skript Kiddie .....	586	- Maßnahmen .....	279
SLA .....	273, 585	- Politik.....	276
- Framework .....	273	- PROSoM.....	279
SLM .....	273	- Prozess.....	279
SLR .....	273	- prozessimmanent .....	279
Smart Meter Gateway .....	551	- Pyramide .....	275
Smartphones .....	15	- ressourcenimmanent .....	279
SMI-S .....	400	- Richtlinie .....	278, 427
Snapshot .....	500	- Strategie.....	278
- Copy .....	400	- Ziele .....	276
Sniffer .....	368, 586	SOX .....	39, 547
- Interface .....	406	- Section 302.....	39
SOA .....	232	- Section 404.....	91
SOC 1® .....	114, 549	- Section 409.....	91, 282
SOC 2® .....	114, 549	Sozialdaten	
- Report .....	114, 176	- SGB X.....	50
SOC 3 <sup>SM</sup> .....	114, 549	Sozialdatenschutz .....	277
Social Compliance .....	108	Soziale Verantwortung	
Social Engineering.....	586	- ISO 26000, 2010.....	559
Social Hacking .....	347	- SA8000® .....	566
Social responsibility		Sozialgesetzbuch.....	54
- ISO 26000, 2010.....	559	Sozialschutzmanagement .....	108
Software Asset Management, ISO/IEC		Spam-Mail.....	407
19770 .....	556	Speicher.....	396
Software Engineering		- Bereich .....	227
- Architecture Description		- Deduplizierung .....	297
-- ISO/IEC 42010, 2011 .....	563	- Hierarchie.....	392
- Risk Management		- Management .....	392
-- ISO 16085, 2006.....	555	-- ISO/IEC 24775 .....	558
- SQuaRE		- Medien.....	394
-- ISO/IEC-25000-Familie .....	558	-- Lebensdauer .....	395
- Web Site		- Netz.....	399
-- ISO/IEC 23026, 2006.....	558	- nichtflüchtig.....	393
-- ISO/IEC/IEEE 23026, FDIS .....	558	- Pool .....	400
Software Test, ISO 29119 .....	562	- Sicherheit	
Solid State Disk .....	393	-- Best Practices.....	402
Solvabilität.....	68	- Sicherheit, ISO 27040, 2015.....	561
Solvabilität II.....	23	- Topologie .....	398
- Richtlinie, Europa .....	545	- Virtualisierung .....	400
Solvabilitätsverordnung .....	68	SPICE.....	566
Solvency II .....	23, 87	Spionagesoftware.....	587
SolvV .....	68, 542	Splitterschutz.....	339
SOP .....	90, 110, 389	SPoC .....	282
Sourcing		Sprachalarmanlage .....	587
- Anforderungen .....	276	Sprinkler.....	343
- Architektur .....	277	- Anlage.....	343
- Konzepte .....	279	-- Nassanlage .....	344
- lebenszyklusimmanent .....	279	-- Trockenanlage.....	344



TOTP .....	348
TR .....	579
Transformation .....	143
Transformationsvorgang .....	193
Transparenz- und Publizitätsgesetz.....	65
Transportrückstau .....	262
Transportsicherung .....	334, 370
T-Ray .....	358
Trennschleifarbeiten.....	341
Treuhänder.....	380
Triple DES .....	362
Trockenanlage.....	344
Trojanisches Pferd (Trojan Horse).....	587
Trust-Center .....	363
TS.....	579
TSCA .....	548
Two-Phase-Commit .....	325

---

**U**

Überfallmeldeanlage.....	587
Übertragungssicherung.....	333, 368
Überwachungssystem.....	42
ubiquitär	
- RiSiKo-Management .....	231
ubiquitous	
- Continuity .....	231
- Safety .....	231
- Security.....	231
Übung .....	315, 446
- Art.....	198, 454
- Dokumentation .....	198
- Intervall.....	198, 454
- Objekt .....	454
- Prozess .....	454
- Umfang .....	315
- unangekündigt.....	314
- vorbereitet.....	314
- Ziel.....	454
UC.....	273, 379
ÜMA.....	587
- DIN EN 50131.....	553
- DIN VDE 0833-3.....	551
- VdS 3172, 2013.....	568
UMAG.....	37, 542
UmweltHG.....	40, 542
Underpinning Contract .....	273, 379

Unfall	
- Beinahe .....	256
Unified Threat Management .....	378, 409
Uninterruptable Power Supply (UPS). 587	
Unterbrechungsfreie Stromversorgung (USV).....	318, 587
Unterlagen	
- geschäftskritisch .....	578, 584
Unternehmenspyramide.....	175
Unternehmenssicherheitspyramide ... VII, 138	
Unterstützungsprozess .....	243
Unverfälschtheit.....	588
UPS .....	587
Urheberrechtsgesetz (UrhG) .....	65
UrhG.....	65, 542
URL.....	575
USA	
- Gesetze .....	546
- Practices.....	546
- Prüfvorschriften .....	546
USB	
- Festplatte .....	377
-- AES-verschlüsselt .....	376
-- Biometrie .....	376
- Memory Stick.....	364, 377, 393
- Token .....	347
User Help Desk (UHD) .....	247, 282
USMS.....	117, 529, 530
USV .....	318, 587
- Anlage.....	342
- Line-Interactive .....	587
- Offline .....	587
- Online .....	587
- VFD .....	587
- VFI.....	448, 587
- VI.....	587
UTM.....	378, 409
UVG.....	63, 543
UVV Kassen.....	59, 165

---

**V**

VAG.....	84, 87, 543
- Deutschland .....	542
- Österreich .....	543
- Schweiz.....	543

Val IT .....	111	Verordnungen	
Validierung .....	588	- Österreich .....	542
VDI 7000, 2015 .....	566	- Schweiz .....	543
VdS .....	588	Verschlüsselung .....	361, 378
VdS 2000, 2010 .....	566	- AES .....	362
VdS 2007, 2004 .....	566	- asymmetrisch .....	363
VdS 2008, 2009 .....	567	- DES .....	362
VdS 2036, 2009 .....	567	- IDEA™ .....	362
VdS 2037EF, 2013 .....	567	- RC5™ .....	362
VdS 2095, 2010 .....	567	- RSA .....	363
VdS 2170, 2010 .....	567	- symmetrisch .....	362
VdS 2247 .....	567	- Triple DES .....	362
VdS 2263, 2013 .....	567	Versicherer	
VdS 2311, 2010 .....	567	- Corporate Governance .....	543
VdS 2333, 2014 .....	567	- Interne Revision .....	543
VdS 2366, 2013 .....	567	- Internes Kontrollsystem .....	543
VdS 2367, 2004 .....	567	- Risikomanagement .....	543
VdS 2463, 2007 .....	567	Versicherung	
VdS 2465 .....	567	- Betriebshaftpflicht .....	327
VdS 2472, 2007 .....	567	- Betriebsunterbrechung .....	327
VdS 2493, 2004 .....	567	- Computermissbrauch .....	327
VdS 2833, 2003 .....	567	- Cyber .....	327
VdS 3143, 2012 .....	567	- Datenmissbrauch .....	327
VdS 3436, 2005 .....	568	- Maschinenbetriebsunterbrechung .....	327
VdS 3534, 2013 .....	568	- Sach .....	327
VDSG .....	543	- Transport .....	327
Verbindlichkeit .....	588	- Vermögensschaden .....	327
Verbotssprinzip .....	223	Versicherungsaufsichtsgesetz .....	84
Verbund sicherheitsglas .....	339	Versicherungsunternehmen	
Vereinbarung		- Compliance-Funktion .....	88
- auf Gegenseitigkeit .....	446	- Geschäftsorganisation .....	84
Vereinzelung		- Governance .....	88
- Material .....	377	- interne Kontrolle .....	88
- Personen .....	377	- interne Revision .....	84, 88
- videobasiert .....	377	- MaRisk VA .....	84
Verfügbarkeit .....	588	- Notfallplanung .....	85
- Klassen .....	214, 588	- Risikomanagement .....	84, 88
Verifikation .....	588	- Risikostrategie .....	84
Verkabelung .....	319	- Risikotragfähigkeit .....	84
- TIA 942-A-2012 .....	549	- Solvency II .....	87
Verkehrswege .....	56	- VAG .....	84
Vernichtung		Versorgung .....	318
- Daten .....	367	- Topologie .....	414
- Datenträger .....	367	Vertrag	
		- auf Gegenseitigkeit .....	588

- Vertrauenszirkel ..... 351  
 Vertraulichkeit ..... 589  
 Vertraulichkeitsbereich..... 80, 227  
 Vertraulichkeitsstufe..... 214  
 Verwundbarkeit..... 589  
 VFD ..... 587  
 VFI ..... 448, 587  
 VI (vertikale Interdependenz)..... 308, 417  
 VI (Voltage Independent)..... 587  
 Videoüberwachung  
   - ISO 22311, 2012..... 557  
 Vier-Augen-Prinzip..... 220  
 Virenkennung ..... 408  
 Virenschanner ..... 408  
 Virensignatur ..... 409  
 Virtual LAN ..... 228  
 Virtual Tape Library..... 401  
 Virtuelle Bandbibliothek ..... 401  
 Virtuelles LAN..... 228  
 Virtuelles Privates Netz..... 589  
 Virus, s. Computervirus ..... 575  
 Vishing..... 589  
 Vital Records..... 321, 578, 584  
 VIVA ..... 589  
 VLAN..... 228  
 Voice over IP ..... 377  
 VoIP..... 377  
 Vorgehensmodell ..... 25  
 Vorschrift  
   - DGUV ..... 53  
 VPN ..... 589  
 V-Quadrupel ..... 133, 210  
 VSG..... 339  
 VSITR ..... 568  
 VTL..... 401  
 VÜA  
   - Betriebsbuch  
   -- VdS 3425, 2008 ..... 568  
   - VdS 2366, 2013..... 567  
   - VdS 3425, 2008..... 568  
   - VdS 3426, 2013..... 568  
 Vulnerability  
   - Analysis  
   -- ISO/IEC 20004, TR, 2012..... 556  
   - Architecture..... 267  
   - Assessment ..... 267  
 VUV..... 63, 543
- 
- W  
 Wachpersonal..... 356  
 WAF..... 404  
 WAN..... 589  
 Wandhydrant ..... 344  
 Wandschott..... 342  
 WarDriver ..... 368  
 Wareneingangsschutz ..... 359  
 Wartung ..... 298  
   - präventiv ..... 298  
 Wartungsmanagement..... 297  
 Wassermeldeanlage ..... 319  
 Wassermeldeanlage (WMA) ..... 589  
 Wassernebel..... 344  
 WBEM ..... 401  
 WD..... 579  
 Weakness ..... 585  
 Web Application Firewall (WAF)..... 404  
 Web Services  
   - NIST SP 800-95 ..... 564  
 Web Site  
   - Software Engineering  
   -- ISO/IEC 23026, 2006 ..... 558  
   -- ISO/IEC/IEEE 23026, FDIS..... 558  
 WebShield..... 404  
 Weitverkehrsnetz..... 589  
 Wertpapierhandelsgesetz  
   - Compliance ..... 69  
 Wertpapierhandelsgesetz (WpHG)..... 69  
 Werttransport ..... 371  
 Whitelist ..... 408  
 Wide Area Network (WAN) ..... 589  
 Widerstandsfähigkeit  
   - BS 65000..... 550  
 Widerstandsklasse  
   - Einbruchhemmung ..... 214  
   - Feuer ..... 214  
 Wiederanlauf..... 311, 446  
   - maximale Dauer ..... 445  
   - maximale Zeit ..... 445  
   - maximaler Zeitraum ..... 445  
 Wiederanlaufplan ..... 74  
 Wiederaufbereitung ..... 333, 366  
 Wiederherstellung ..... 301, 447  
   - Dauer ..... 447  
 Wi-Fi® ..... 577  
 WiMAX ..... 368

Wirtschaftskriminalität .....9  
 WLAN .....577  
   - NIST SP 800-153, 2012.....565  
 WMA .....319, 589  
 Workaround .....282  
 Workflow .....463  
 WORM.....393  
 WpHG .....69, 542  
 Write XOR Execute .....228

---

## X

XML .....582  
   - Firewall.....404  
   - Gateway.....404

---

## Z

Z10-2012 .....107  
 ZAG .....542  
 Zahlungsdiensterichtlinie, Europa .....545  
 Zentraler Kreditausschuss .....576  
 Zero-Day-Attacke .....409  
 Zielvereinbarungsprozess.....504

ZKA (Zentraler Kreditausschuss) ..... 576  
 ZKA (Zutrittskontrollanlage) ..... 355  
 ZKS (Zutrittskontrollsystem).....332, 355  
 Zufahrtskontrolle, automatische ..... 354  
 Zufahrtsschutz-Richtlinie..... 464  
 Zugangsschutz..... 332  
 Zugriffsschutz..... 332  
 Zugriffszeit..... 394  
 Zutrittskontrollanlage (ZKA) ..... 355  
   - Betriebsbuch, VdS 3436, 2005..... 568  
   - DIN EN 50133 ..... 553  
   - Richtlinie..... 476  
   - VdS 2367, 2004..... 567  
   - VdS 2493, 2004..... 567  
 Zutrittskontrollsystem (ZKS).....332, 355  
   - DIN EN 50133 ..... 553  
   - Richtlinie..... 476  
 Zutrittsschutz.....57, 332, 355  
   -- Richtlinie..... 467  
 Zutrittszone.....227, 342  
 Zuverlässigkeit ..... 590  
 Zuwachssicherung ..... 323  
 Zweifaktor-Authentisierung..... 345

## 30 Über den Autor

**Dr.-Ing. Klaus-Rainer Müller** studierte und promovierte in Karlsruhe. Danach war er als Gruppenleiter der Software-Entwicklung bei einem Hersteller frei programmierbarer Steuerungen tätig, wo er Software spezialisierte und entwickelte sowie Software-Engineering-Methoden einführte.

Als Senior Software Engineer wechselte er zur deutschen Tochter eines internationalen System- und Softwarehauses. Hier war er u. a. als Team- und Projektleiter großer, teilweise kritischer Entwicklungsprojekte sowie als Berater tätig und nahm die Positionen Stv. Abteilungsleiter und Key Account Manager wahr.

Bei der ACG Automation Consulting Group GmbH, einer Unternehmensberatung für Organisation und Informationsverarbeitung in Frankfurt ([www.acg-gmbh.de](http://www.acg-gmbh.de)), startete er als Senior Berater und Projektmanager. Er leitete den Bereich „Sicherheits- und Qualitätsmanagement“ sowie das Fach-Competence-Center (FCC) Unternehmensentwicklung und beriet in diesen Themenfeldern. Heute verantwortet er das FCC ISM, ITSCM, ITSM.

Er befasst sich mit dem Unternehmenssicherheitsmanagement (USM), dem Business und Service Continuity Management (BCM, SCM), dem IT-Sicherheits-, -Kontinuitäts-, -Risiko-, -Qualitäts-, -Test-, -Service-Level- und -Projektmanagement sowie den betriebswirtschaftlichen Themen Führungssysteme, Prozess- und Strukturorganisation einschließlich Sourcing sowie Organisationsentwicklung. Als Senior Management Consultant berät und unterstützt er Kunden beim Aufbau des effizienten und durchgängigen Sicherheits-, Business-Continuity-, IT Service Continuity- und IT-Risikomanagements, bei der Entwicklung von Notfall-, Krisen- und Katastrophenvorsorgekonzepten sowie bei der Planung und Durchführung von Notfalltests und -übungen

Er führt er u. a. Schutzbedarfsanalysen, Sicherheitsstudien, Reviews und Audits durch, berät und coacht Sicherheits- und Kontinuitätsverantwortliche und moderiert Workshops mit teils stark kontroversen Meinungen. Als Sonderthema gestaltete er im Jahr 1999 den Jahr-2000-Wechsel des IT-Bereichs einer Großbank und begleitete ihn erfolgreich. Er beriet und unterstützte Unternehmen erfolgreich bei der Beseitigung von BaFin-Moniten. Darüber hinaus berät er in der breiten Palette der oben genannten Themenbereiche. Zu seinen bisherigen Kunden gehören renommierte Unternehmen u. a. aus den Branchen Banken, Versicherungen einschließlich Sozialversicherungen und Automobil sowie IT-Dienstleister aus den Branchen Banken, Versicherungen und Chemie. Die Projekte sind je nach Themenstellung national, europäisch oder international ausgerichtet.

Er ist Architekt des Pyramidenmodell®, das wegweisend und dreidimensional ist, sowie seiner dreidimensionalen Sicherheits(management)pyramide und der RiSiKo-(Management)Pyramide. Den Begriff „Sicherheitspyramide“ prägte er erstmals Mitte der 1990er Jahre und veröffentlichte ihn damals zusammen mit ihrer Darstellung in Artikeln und auf Veranstaltungen. Naturgemäß haben sich ihre Inhalte parallel zu den technologischen, gesetzlichen, regulatorischen und normativen Veränderungen in dieser Zeit weiter entwickelt. Darüber hinaus konzipierte und füllte er das auf seinen Ideen basierende zielgruppenorientierte und hoch flexible ISM-, BCM-, ITSCM- und ITRM-Tool der ACG GmbH. Dem technologischen Fortschritt folgend ist das ACG-Tool inzwischen neu entwickelt worden.

Zusätzlich zum Begriff „Sicherheits(management)pyramide“, „RiSiKo-(Management-)Pyramide“, „Pyramidenmodell®“ und weiteren „...pyramiden“ wie der „Sicherheits- und Risikopyramide“, der „ISM-Pyramide“, der „ITSCM-Pyramide“, der „BCM-Pyramide“, der „ITSM-Pyramide“ und der „Architekturpyramide“ etc. schuf bzw. prägte er weitere Begriffe, Methoden und Hilfsmittel, wie z. B. Balanced Pyramid Scorecard®, Distanzprinzip, Eskalationsschritte, etc.

lationstrichter, Haus zur Sicherheit, Haus zur Kontinuität, House of Safety, Security and Continuity, Interdependenznetz bzw. -plan, Prinzip der Immanenz, Prinzip der Subjekt-Objekt- bzw. Aktiv-Passiv-Differenzierung, PROBCM, PROPyR, PRORim, PROSim und weitere PRO..., RiSiKo, Risikodreiklang, Safety, Security and Continuity Function Deployment (SSCFD), Sicherheitsdreiklang, Sicherheitshierarchie und V-Quadrupel.

Ende Juli 2003 erschien die erste Auflage seines erfolgreichen Buchs „IT-Sicherheit mit System“, der im August 2005 die zweite, im Oktober 2007 die dritte, im Mai 2011 die vierte und im März 2014 die fünfte Auflage folgte. Sicherheitshierarchie und Lebenszyklus sowie Prozesse, Ressourcen und Organisation sind ebenso wie Kennzahlen seit der 1. Auflage integrative Kernelemente, ebenso wie Muster-Richtlinien u. a. zur E-Mail-Nutzung, zum Computervirenschutz, zur Datensicherung und zur Notfallvorsorge.

Im Oktober 2005 veröffentlichte er als Trendsetter für das Zusammenwachsen von IT- und Unternehmenssicherheit sowie von Sicherheits-, Kontinuitäts- und Risikomanagement das „Handbuch Unternehmenssicherheit“ in der ersten Auflage, der im Jahr 2010 die zweite Auflage folgte und das hiermit in der 3. Auflage vorliegt.

Im April 2008 publizierte er das Buch „IT für Manager“, dem er den Untertitel „Mit geschäftszentrierter IT zu Innovation, Transparenz und Effizienz“ gab.

Bisher veröffentlichte der Autor Artikel zur systematischen Pflichtenhefterstellung, zum Software-Engineering, zur Sicherheitspyramide, zum Sicherheits- und Qualitätsmanagement, zur Sicherheit im Software-Lebenszyklus, zum Architekturtrichter, zur prozessorientierten Abnahmeorganisation, zur lebenszyklus- und prozessimmanenten IT-Sicherheit, zum Sourcing mit System, zum Security Engineering, zum Sicherheits- und Risikomanagement, zur genormten Sicherheit, zur Biometrie, zu Notfallübungen, zur elektronischen Gesundheitskarte sowie zur Information Security als unternehmerische Aufgabe. Außerdem schrieb er die Studie der ACG GmbH zu Biometrie und Smart Cards. Weiterhin veröffentlichte er prägnante Überblicksartikel zu verschiedenen nationalen und internationalen Normen und weitere Fachartikel.

Darüber hinaus hielt er auf Kongressen, Seminaren, Foren und Veranstaltungen Vorträge und Präsentationen zu obigen Themenbereichen. Diese behandelten z. B. das Sicherheitsmanagement, Notfalltests und -übungen, das Business Continuity Management, sicherheits- und kontinuitätsrelevante Aufgaben und Anforderungen des Service Desk, Biometrie, SOA Security und BCM, Führungstraining für IT-Sicherheitsexperten, die unternehmensweite Sicherheits- und Risikopolitik als Basis für ein unternehmensweites Sicherheits- und Risikomanagement, das Thema „Business – immer und überall“ mit den Aspekten Mobility, Cloud Services, BYOD, Bedrohungen und Risiken sowie Leit- und Richtlinien sowie das Thema Informationssicherheitsmanagement und der Weg zum integrierten Managementsystem.