19 Abbildungsverzeichnis

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

20 Tabellenverzeichnis

21 Verzeichnis der Checklisten

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

22 Verzeichnis der Beispiele

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

23 Verzeichnis der Tipps

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

24 Verzeichnis der Informationen

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

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℠ 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.

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

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)

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

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

26.1.2 Österreich: Gesetze, Verordnungen

BWG	Bankwesengesetz (Bundesgesetz über das Bankwesen)
DSG 2000	Datenschutzgesetz 2000

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

26.1.3 Schweiz: Gesetze, Verordnungen, Rundschreiben

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

26.1.4 Großbritannien: Gesetze, Vorschriften

FoIA	Freedom of Information Act (FoIA) 2000
HASAW, HSW, HSWA	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

Entscheidung 2000/520/EG	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
Entscheidung 2002/16/EG	Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG
Richtlinie 89/654/EWG	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)
Richtlinie 95/46/EG	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
Richtlinie 2000/31/EG	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“)
Richtlinie 2001/20/EG	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
Richtlinie 2002/58/EG	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)
Richtlinie 2002/87/EG	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

FFIEC, D&A	IT Examination Handbook, Development and Acquisition, April 2004
FFIEC, IS	IT Examination Handbook, Information Security, Juli 2006
FFIEC, MGT	IT Examination Handbook, Management (IT Risk Management Process), Juni 2004
FFIEC, OPS	IT Examination Handbook, Operations, Juli 2004
FFIEC, OT	IT Examination Handbook, Outsourcing Technology Services, Juni 2004
FFIEC, TSP	IT Examination Handbook, Supervision of Technology Service Providers (TSP), Oktober 2012
FISMA	Federal Information Security Management Act of 2002, der im April 2013 durch The Federal Information Security Amendments Act, H.R. 1163, geändert wurde
GLBA	Gramm-Leach-Bliley Act
HMTA	Hazardous Materials Transportation Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH Act	Health Information Technology for Economic and Clinical Health Act
OSH Act	Occupational Safety and Health Act
	Privacy Act
PCAOB, Auditing Standards	Auditing Standards: • Auditing Standard 1: References in Auditors' Reports to the Standards of the Public Company Accounting Oversight Board • Auditing Standard 3: Audit Documentation • Auditing Standard 4: Reporting on Whether a Previously Reported Material Weakness Continues to Exist • Auditing Standard 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements • Auditing Standard 6: Evaluating Consistency of Financial Statements • Auditing Standard 7: Engagement Quality Review • Auditing Standard 8: Audit Risk • Auditing Standard 9: Audit Planning • Auditing Standard 10: Supervision of the Audit Engagement • Auditing Standard 11: Consideration of Materiality in Planning and Performing an Audit • Auditing Standard 12: Identifying and Assessing Risks of Material Misstatement • Auditing Standard 13: The Auditor's Responses to the Risks of Material Misstatement • Auditing Standard 14: Evaluating Audit Results • Auditing Standard 15: Audit Evidence • Auditing Standard 16: Communications with Audit Committees • Auditing Standard 17: Auditing Supplemental Information Accompanying Audited Financial Statements • Auditing Standard 18: Related Parties
SOX	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

Basel II	Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen
Basel III	A global regulatory framework for more resilient banks and banking systems
DGUV Regelwerk	DGUV-Regelwerk unterscheidet die folgenden vier Kategorien: • DGUV Vorschriften • DGUV Regeln • DGUV Informationen • DGUV Grundsätze
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
GoDV	Grundsätze ordnungsmäßiger Datenverarbeitung [12]
IDW PS 330	Abschlussprüfung bei Einsatz von Informationstechnologie, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 24.09.2002
IDW PS 525	Die Beurteilung des Risikomanagements von Kreditinstituten im Rahmen der Abschlussprüfung, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 26.06.2010
IDW PS 880	Die Prüfung von Softwareprodukten, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 11.03.2010
IDW PS 951	Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 16.10.2013
IDW PS 980	Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 11.03.2011
IDW RS FAIT 1	Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 24.09.2002
IDW RS FAIT 2	Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 24.09.2003
IDW RS FAIT 3	Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 11.07.2006

IDW RS FAIT 4	Anforderung an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 08.08.2012
InvMaRisk	Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk)
MaDSB	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
MaIuK	Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – IuK-Mindestanforderungen
MaRisk BA	Mindestanforderungen an das Risikomanagement (Bankenaufsicht)
MaRisk VA	Aufsichtsrechtliche Mindestanforderungen an das Risikomanagement (Versicherungsaufsicht)
MaComp	Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG
Rundschreiben 6/2013 (BA)	Anforderungen an Systeme und Kontrollen für den Algorithmushandel von Instituten (Bankenaufsicht)

26.3 Standards, Normen, Leitlinien und Rundschreiben

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

BCBS 113, Compliance, April 2005	Compliance and the compliance function in banks, Basel Committee on Banking Supervision
BCBS 155, Stress Testing, Mai 2009	Principles for sound stress testing practices and supervision, Basel Committee on Banking Supervision
BCBS 176, Governance Principles, Oktober 2010	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, Risk Management Principles, Juni 2011	Principles for the Sound Management of Operational Risk, Basel Committee on Banking Supervision
BCBS 239, *Risk Data Aggregation, Januar 2013*	Principles for effective risk data aggregation and risk reporting, Basel Committee on Banking Supervision
BCBS 292, Review of Risk Management Principles, Oktober 2014	Review of the Principles for the Sound Management of Operational Risk, Basel Committee on Banking Supervision
BCBS joint 12, Outsourcing, Februar 2005	Outsourcing in Financial Services, Basel Committee on Banking Supervision, The Joint Forum
BCBS joint 17, Business Continuity, August 2006	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

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

0833-4:2014	• Teil 3: Festlegungen für Einbruch- und Überfallmeldeanlagen • Teil 4: Festlegungen für Anlagen zur Sprachalarmierung im Brandfall
DIN EN 1047-1 1047-2:2013	Wertbehältnisse – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand • Teil 1: Datensicherungsschränke und Disketteneinsätze; Deutsche Fassung der EN 1047-1:2005 • Teil 2: Datensicherungsräume und Datensicherungscontainer; Deutsche Fassung der EN 1047-2:2009+A1:2013
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 • Teil 1: Krisenmanagement; Deutsche Fassung EN 15975-1:2011 • Teil 2: Risikomanagement; Deutsche Fassung EN 15975-2:2013
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 DIN CLC/TS 50134-7:2004-08	Alarmanlagen – Personen-Hilferufanlagen • Teil 1: Systemanforderungen; Deutsche Fassung EN 50134-1:2002 • Teil 2: Auslösegeräte; Deutsche Fassung EN 50134-2:1999 • Teil 3: Örtliche Zentrale und Übertragungsgerät; Deutsche Fassung EN 50134-3:2012 • Teil 5: Verbindungen und Kommunikation; Deutsche Fassung EN 50134-5:2004 • Teil 7: Anwendungsregeln; Deutsche Fassung CLC/TS 50134-7:2003
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 • Teil 1: Allgemeine Konzepte; Deutsche Fassung der EN 50600-1:2012 • Teil 2-1: Gebäudekonstruktion; Deutsche Fassung der EN 50600-2-1:2014 • Teil 2-2: Stromversorgung; Deutsche Fassung der EN 50600-2-2:2014

	• 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	Financial Transaction Services
GAMP® 5	The Good Automated Manufacturing Practice (GAMP®) 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, Stand Februar 2008
GERM	Good Electronic Records Management
ISO Guide 73:2009	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 15408-2:2008 15408-3:2008	Information technology – Security techniques – Evaluation criteria for IT security s. a. Common Criteria • Part 1: Introduction and general model • Part 2: Security functional components • Part 3: Security assurance components
ISO/IEC TR 15443-1:2012 TR 15443-2:2012	Information technology – Security techniques – Security assurance framework • 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, TR 15489-2:2001	Information and documentation: Records management • Part 1: General • Part 2: Guidelines
ISO/IEC 15504-1:2004 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	Information technology – Process assessment • 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 17090-2:2008 17090-3:2008 17090-4:2014	Health informatics – Public key infrastructure • 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

ISO TR 18307:2001	Health informatics – Interoperability and compatibility in messaging and communication standards – Key characteristics
ISO 18308:2011	Health informatics – Requirements for an electronic health record architecture
ISO 19011:2011	Guidelines for auditing management systems
ISO 19092:2008	Financial services – Biometrics – Security framework
ISO 19600:2014	Compliance management systems – Guidelines
ISO/IEC 19770-1:2012 *19770-2:2009* *DIS 19770-3* *19770-5:2013* *AWI 19770-7*	Information technology – Software asset management • Part 1: Processes and tiered assessment of conformance • Part 2: Software identification tag • Part 3: Software entitlement schema • Part 5: Overview and vocabulary • Part 7: Tag management
ISO/IEC 19792:2009	Information technology – Security techniques – Security evaluation of biometrics
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*	Information technology – Service management • Part 1: Service management system requirements • Part 2: Guidance on the application of service management systems • Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1 • Part 4: Process reference model • Part 5: Exemplar implementation plan for ISO/IEC 20000-1 • Part 6: Requirements for bodies providing audit and certification of service management systems • Part 8: Guidance on the application of service management systems for smaller organizations • Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services • Part 10: Concepts and terminology • Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks
ISO/IEC TR 20004:2012	Information technology – Security techniques – Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
ISO/IEC 20006-1:2014 *FDIS 20006-2* *PDTS 20006-3*	Information technology for learning, education and training – Information model for competency • Part 1: Competency general framework and information model • Part 2: Proficiency level information model • Part 3: Guidelines for the aggregation of competency information and data

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® (SSE-CMM®)
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 • Part 1: Food manufacturing • Part 2: Catering • Part 3: Farming
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 • Part 1: Overview and policy management • Part 2: Formal models • Part 3: Implementations
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 • Part 1: Terminology and concepts • Part 2: Reference architecture and requirements • Part 3: Practice
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 • Part 1: Overview • Part 2: Common Architecture • Part 3: Common Profiles • Part 4: Block Devices • Part 5: File systems • Part 6: Fabric • Part 7: Host Elements • Part 8: Media Libraries
ISO/IEC 25000:2014	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE

ISO/IEC 25001:2014	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Planning and management
ISO/IEC 25010:2011	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models
ISO/IEC 25012:2008	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model
ISO/IEC 25020:2007	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Measurement reference model and guide
ISO/IEC 25030:2007	Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Quality requirements
ISO/IEC 25040:2011	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation process
ISO/IEC 25041:2012	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation guide for developers, acquirers and independent evaluators
ISO/IEC 25045:2010	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation module for recoverability
ISO/IEC TR 25060:2010	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
ISO 26000:2010	Guidance on social responsibility
ISO 26262-1:2011 26262-2:2011 26262-3:2011 26262-4:2011 26262-5:2011 26262-6:2011 26262-7:2011 26262-8:2011 26262-9:2011 26262-10:2012	Road vehicles – Functional safety • Part 1: Vocabulary • Part 2: Management of functional safety • Part 3: Concept phase • Part 4: Product development at the system level • Part 5: Product development at the hardware level • Part 6: Product development at the software level • Part 7: Production and operation • Part 8: Supporting processes • Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses • Part 10: Guideline on ISO 26262
ISO/IEC/IEEE 26511:2011	Systems and software engineering – Requirements for managers of user documentation
ISO/IEC 27000:2014	Information technology – Security techniques – Information security management systems – Overview and vocabulary
ISO/IEC 27001:2013, Cor 1:2014	Information technology – Security techniques – Information security management systems – Requirements, Cor 1:2014

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

ISO/IEC 27032:2012	Information technology – Security techniques – Guidelines for cybersecurity
ISO/IEC 27033-1:2009 27033-2:2012 27033-3:2010 27033-4:2014 27033-5:2013 DIS 27033-6	Information technology – Security techniques – Network security • Part 1: Overview and concepts • Part 2: Guidelines for the design and implementation of network security • Part 3: Reference networking scenarios – Threats, design techniques and control issues • Part 4: Securing communications between networks using security gateways • Part 5: Securing communications across networks using Virtual Private Networks (VPNs) • Part 6: Securing wireless IP network access
ISO/IEC 27034-1:2011, Cor 1:2014 DIS 27034-2 NP 27034-3 CD 27034-4 CD 27034-5 NP 27034-5-1 CD 27034-6 NP 27034-7	Information technology – Security techniques – Application security • Part 1: Overview and concepts, Cor 1:2014 • Part 2: Organization normative framework • Part 3: Application security management process • Part 4: Application security validation • Part 5: Protocols and application security controls data structure • Part 5-1: Protocols and application security controls data structure – XML schemas • Part 6: Security guidance for specific applications • Part 7: Application security assurance prediction
ISO/IEC 27035:2011	Information technology – Security techniques – Information security incident management
ISO/IEC 27036-1:2014 27036-2:2014 27036-3:2013 WD 27036-4	Information technology – Security techniques – Information security for supplier relationships • Part 1: Overview and concepts • Part 2: Requirements • Part 3: Guidelines for ICT supply chain security • Part 4: Guidelines for security of cloud services
ISO/IEC 27037:2012	Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038:2014	Information technology – Security techniques – Specification for digital redaction
ISO/IEC 27039:2015	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)
ISO/IEC 27040:2015	Information technology – Security techniques – Storage security
ISO/IEC FDIS 27041	Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigation methods
ISO/IEC DIS 27042	Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043:2015	Information technology – Security techniques – Incident investigation principles and processes

ISO/IEC WD 27044	Information technology – Security techniques – Guidelines for Security Information and Event Management (SIEM)
ISO/IEC CD 27050-1 NP 27050-2 NP 27050-3 NP 27050-4	Information technology – Security techniques – Electronic discovery • Part 1: Overview and concepts • Part 2: Guidance for governance and management of electronic discovery • Part 3: Code of Practice for electronic discovery • Part 4: ICT readiness for electronic discovery
ISO 27789:2013	Health informatics – Audit trails for electronic health records
ISO 27799:2008	Health informatics – Information security management in health using ISO/IEC 27002
ISO 28000:2007	Specification for security management systems for the supply chain
ISO 28001:2007	Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
ISO 28002:2011	Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
ISO 28003:2007	Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems
ISO 28004-1:2007, Cor 1:2012 28004-2:2014 28004-3:2014 28004-4:2014	Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 • Part 1: General principles, Cor 1:2012 • Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations • Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports) • Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective
ISO 28005-1:2013 28005-2:2011	Security management systems for the supply chain – Electronic port clearance (EPC) • Part 1: Message structures • Part 2: Core data elements
ISO/IEC 29100:2011	Information technology – Security techniques – Privacy framework
ISO/IEC 29101:2013	Information technology – Security techniques – Privacy architecture framework
ISO/IEC/IEEE 29119-1:2013 29119-2:2013	Software and systems engineering – Software testing • Part 1: Concepts and definitions • Part 2: Test processes

29119-3:2013 *FDIS 29119-4* *DIS 29119-5*	• Part 3: Test documentation • Part 4: Test techniques • 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 (2nd 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	Guide to Intrusion Detection and Prevention Systems (IDPS), NIST, Februar 2007
Rev 1, DRAFT	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

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

OENORM S 2400:2009	Business Continuity und Corporate Security Management – Benennungen und Definitionen
OENORM S 2401:2009	Business Continuity und Corporate Security Management – Systemaufbau und Business Continuity und Corporate Security Policy
OENORM S 2402:2009	Business Continuity und Corporate Security Management – Business Continuity Management
OENORM S 2403:2009	Business Continuity und Corporate Security Management – Corporate Security Management
OHRIS:2010	Occupational Health and Risk Management System, Bayerisches Staatsministerium für Umwelt, Gesundheit und Verbraucherschutz
ONR 49000:2014	Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen – Umsetzung von ISO 31000 in die Praxis
ONR 49001:2014	Risikomanagement für Organisationen und Systeme – Risikomanagement – Umsetzung von ISO 31000 in die Praxis
ONR 49002-1:2014 *49002-2:2014* *49002-3:2014*	Risikomanagement für Organisationen und Systeme • Teil 1: Leitfaden für die Einbettung des Risikomanagements ins Managementsystem – Umsetzung von ISO 31000 in die Praxis • Teil 2: Leitfaden für die Methoden der Risikobeurteilung – Umsetzung von ISO 31000 in die Praxis • Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement – Umsetzung von ISO 31000 in die Praxis
ONR 49003:2014	Risikomanagement für Organisationen und Systeme – Anforderungen an die Qualifikation des Risikomanagers – Umsetzung von ISO 31000 in die Praxis
PCI DSS Version 3.0, 2013	Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures
SAI SA8000®:2014	Social Accountability 8000, Social Accountability International
SCAMPI℠	Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠) A, Version 1.3: Method Definition Document, Carnegie Mellon University, März 2011
SERA	Introduction to the Security Engineering Risk Analysis (SERA) Framework, Carnegie Mellon University, November 2014
SPICE	Software Process Improvement and Capability dEtermination, s. a. ISO/IEC TR 15504
SSE-CMM®	Information technology – Systems Security Engineering – Capability Maturity Model (ISO/IEC 21827:2008)
TOGAF® 9.1	Enterprise architecture methodology and framework, The Open Group
VDI 7000:2015-01	Frühe Öffentlichkeitsbeteiligung bei Industrie- und Infrastrukturprojekten
VdS 2000:2010-12	Leitfaden für den Brandschutz im Betrieb
VdS 2007:2004-08	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 • Teil 2: Einbruchmeldetechnik • Teil S: Zusatzfragen zur mechanischen Sicherungstechnik
VdS 2263:2013-09	Betriebsbuch für Einbruch- und Überfallmeldeanlagen
VdS 2311:2010-11 *2311-S1:2013-08*	VdS-Richtlinien für Einbruchmeldeanlagen – Planung und Einbau • Ergänzung S1: Korrekturen, Änderungen und Ergänzungen
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 • Ergänzung S1: Korrektur und Anpassung von Satztypen • Ergänzung S2: Protokollerweiterung zur Anschaltung an Netze der Protokollfamilie TCP • Ergänzung S3: Protokollerweiterung zur Anschaltung von Videoüberwachungsanlagen an Gefahrenmeldeanlagen
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

VdS 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.
VdS 3425:2008-07	Betriebsbuch für Videoüberwachungsanlagen
VdS 3426:2013-07	Installationsattest für eine Videoüberwachungsanlage (VÜA)
VdS 3436:2005-08	Betriebsbuch für Zutrittskontrollanlagen
VdS 3534.2013-03	Gefahrenmanagementsysteme für sicherungstechnische Anlagen – Anforderungen und Prüfmethoden
VS-ITR	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

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

[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® 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® 5: A Risk-Based Approach to Compliant GxP Computerized Systems, 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® Continuous Processing® Technology®, 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/dhc-kerberos/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, 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
[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-Grundschutz-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, 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 – Authentification

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.

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

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

CIA²

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 Viruskennung, 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 occurence

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

finierten Bruttorisikos 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®-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" (ισοσ: 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 – ISPyr (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 – medienspezifisches 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) 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. Überweisungslimite 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 Erstell- 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 Österreichisches 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[Dr.-Ing. Müller] 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 Benutzerkennung 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. Spannungsoberschwingungen. 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-USVs 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 Netzstörungsarten 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 Rechtesteuerung und –verwaltung – Single Point of Security Control and Administration (SPSCA)

Die zentrale Rechtesteuerung 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

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

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 spezifizierte 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), 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, Eska-

Klaus-Rainer Müller, *Handbuch Unternehmenssicherheit,*
DOI 10.1007/978-3-658-10151-0, © Springer Fachmedien Wiesbaden 2015

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 Informationssicherheitmanagement und der Weg zum integrierten Managementsystem.