

Inhaltsverzeichnis

Vorwort	5
Einleitung	11
Sofortiges Inkrafttreten	11
Hintergrund der Neufassung	11
Neuerungen im Überblick	12
Historie	12
Risikoorientierte Prüfungsplanung	17
Risikobewusstsein schärfen	17
Risikoorientierte Planung	17
Bewertung einzelner Prüfungsobjekte	18
Themengebiete der IT-Revision	18
Erarbeiten der notwendigen Prüfungstechnik	19
1. IT-Strategie	21
2. IT-Governance	27
Verantwortung der Geschäftsleitung	28
Interessenkonflikte	29
Mögliche Interessenkonflikte aus der Praxis	29
Interne Revision	30
Grundsatz (Definition)	30
Angemessene quantitative und qualitative Personalausstattung	31
Angemessener Umfang und Qualität der technisch-organisatorischen Ausstattung	31
Verantwortung der IT-Governance	32
IT-Kompetenzen	33
IT-relevante Berichte	36
Quantitative und qualitative Kriterien	37
3. Informationsrisikomanagement	41
Schutzbedarfsermittlung	41
Informationsverbund	42
Abhängigkeiten und Schnittstellen	42
Methodik der Klassifizierung	43
Sollmaßnahmenkatalog	43
IT-Risikoanalyse	44
4. Informationssicherheitsmanagement	49
Ziele des Informationssicherheitsmanagements	49
Informationssicherheitsleitlinie	50
Rahmenbedingungen	50

Vorbeugung von Sicherheitsvorfällen.	51
Funktion des Informationssicherheitsbeauftragten	52
Organisatorische prozessuale Unabhängigkeit	53
Vermeidung möglicher Interessenkonflikte.	53
Informationssicherheitsvorfall	55
Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit	56
Vorspann zur allgemeinen Bedrohungslage	56
Exemplarische Inhaltsübersicht der Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit	57
Bedrohungslage und IT-Risikosituation	57
Kategorien von Test- und Überprüfungsobjekten (z.B. das Institut, IT-Systeme, Komponenten)	57
Art, Umfang und Frequenz von Tests und Überprüfungen	58
Zuständigkeiten und Regelungen zur Vermeidung von Interessenkonflikten	60
Sparsamkeitsgrundsatz.	60
Festlegung von Zutritts-, Zugangs- und Zugriffsrechten	60
Sensibilisierungs- und Schulungsprogramm Informationssicherheit	61
Statusbericht Informationssicherheit	62
5. Operative Informationssicherheit	69
Anforderungen an die operative Informationssicherheit	69
Regelbasierte Auswertungen	70
Sicherheitsrelevante Ereignisse	71
Sicherheit der IT-Systeme.	71
6. Identitäts- und Rechte management	75
Need-to-know- und Least-Privilege-Prinzip.	75
IT-Berechtigungsvergabe	75
Prüfung Identitäts- und Berechtigungsmanagement	76
Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen	78
Rezertifizierung von Berechtigungen	78
7. IT-Projekte, Anwendungsentwicklung	85
IT-Aufbau- und Ablauforganisation	85
Steuerung von IT-Projekten auf Portfolioebene	87
Anwendungsentwicklung	88
User Stories und Product Backlog	89
Schutzziele	89
Dokumentation der Anwendung.	90

Versionierung des Quellcodes	90
Testdurchführung	91
Programmierrichtlinien	92
IDV-Anwendungen	92
Zentrales Register der Anwendungen	93
8. IT-Betrieb	101
Steuerung des IT-Portfolios	102
Change-Management	103
Change-Management-Prozesse	104
Risikoarme Konfigurationsänderungen/Parametereinstellungen	104
Identifikation der IT-Risiken	105
Prüfung des Störungsmanagements	105
Datensicherungen	106
Cloud-Anbieter	107
Auslagerungsvereinbarung mit Cloud-Anbietern	107
9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen.	113
Risikobewertung	113
Sonstiger Fremdbezug von IT-Dienstleistungen	114
10. IT-Notfallmanagement	119
IT-Notfallplanung	119
Rahmenbedingungen	119
IT-Notfallpläne	120
IT-Testkonzept	121
Ausfall Rechenzentrum	121
11. Management der Beziehungen mit Zahlungsdienstnutzern	125
12. Kritische Infrastrukturen	131
KRITIS-relevante Prozesse	133
Nachweiserbringung im Rahmen der Jahresabschlussprüfung	134
13. MaRisk AT 7.2: Technisch-organisatorische Ausstattung	139
Informationsverbund	140
Standards zur Ausgestaltung der IT-Systeme	140
Zugriffsrechte	140
Veränderungen an IT-Systemen	140
Abnahme durch die technisch und fachlich zuständigen Mitarbeiter	141
14. MaRisk AT 7.3: Notfallkonzept	145
Zeitkritische Aktivitäten und Prozesse	145
Auswirkungsanalysen	145

Inhaltsverzeichnis

Risikoanalysen	146
Notfallkonzept	146
Notfallszenarien	146
Überprüfungen des Notfallkonzeptes	147
Literaturverzeichnis	149