

Prüfungsbereich IKT Management

Prüfung der IKT Prozesse entsprechend
den aufsichtsrechtlichen Anforderungen
der BAIT und MaRisk 08/2021

Name

Inhaltsverzeichnis

1.0 Managementsummary	4
1.1 Prüfungsurteil	4
1.2 Zusammengefasstes Prüfungsergebnis	5
2.0 Risikoorientierung.....	6
2.0.1 Vorerhebung und dynamisch risikoorientierter Prüfungsansatz.....	6
2.01.1 Prüfungsansatz.....	6
2.01.2 Vorerhebung.....	6
2.0.1.3 Betroffene Risikoarten in der Prüfung.....	6
2.0.1.4 Datenschutzrechtliche Hinweise	6
2.0.1.5 Feststellungen aus der Vorprüfung.....	6
2.1 Prüfungshandlungen zur Risikobeurteilung	7
2.1.1 Aufbauorganisation.....	7
2.1.2 Ablauforganisation	8
2.1.2.1 Betriebsvereinbarungen und Mitbestimmungsrechte	10
2.1.3 Schulungskonzepte	11
2.1.3.1 Schulung der Mitarbeiter ISM und IT	11
2.1.3.2 Schulung aller Bereiche.....	11
2.2 Methoden und Verfahren sowie Kontrollen.....	11
2.2.1 Hinweise zu eingesetzten Methoden und Verfahren	12
2.2.2 Kontrollrahmen für IKT- und Sicherheitsrisiken	12
2.3 Datenschutzmanagement.....	13
2.4 Berichtswesen	13
2.5 Anpassungsprozesse	13
3. Prüfungsurteil zur Aufbauprüfung	13
4. Funktions- und Prozessprüfung zu den Prüfungsfeldern	14
4.1 IT-Strategie.....	14
4.2 IT Governance.....	16
4.3 Informationsrisikomanagement.....	17
4.3.1 Schutzbedarfsanalysen	18
4.3.2 Risikoanalyse	20
4.3.3 Risikobehandlung	20
4.3.4 Controlling der Risiken.....	21
4.3.5 akzeptierte Abweichungen.....	21
4.3.6 Genehmigungsprozesse.....	21
4.3.6 Prozesse in Bezug auf den IT-Dienstleister	21
4.3.7 Berichtswesen	21
4.4. Informationssicherheitsmanagement.....	22
4.4.1 Tätigkeit des Informationssicherheitsbeauftragten	22
4.4.2 ISM-Sitzungen und Berichtswesen	24
4.4.3 Kontroll- und Überwachungsprozesse des ISB	25
4.5 Operative Informationssicherheit	25
4.5.1 Informationssicherheitsvorfälle	26
4.5.2 Security Information Event Management (SIEM).....	27
4.5.3. Securation Operation Center (SOC)	27
4.5.4 CERT.....	27
4.5.4 FRAUD	28
4.5.5 Sicherheitsrichtlinien und Tests zur Informationssicherheit	28
4.6 IT-Projekte und Anwendungsentwicklung.....	29
4.6.1 IKT-Projektmanagement.....	29

4.6.2	Anwendungsentwicklungen	31
4.6.3	Test- und Freigabe erstellter Software.....	31
4.6.4	Implementierungstests erworbener Software	32
4.6.4	Patchversorgung/Bündelwartung/Updates	32
4.6.4.1	Releasewechsel Bankanwendungsverfahren	33
4.6.4.2	Updates weiterer Softwaresysteme	33
4.6.4.3	Bündelwartungen/Patches	33
4.6.5	Datenanalysen IDA Reporting	33
4.7	IT-Betrieb.....	34
4.7.1	IT- Infrastruktur	34
4.7.2	Change-Management	36
4.7.3	Abweichungen vom Regelbetrieb	36
4.7.4	Incident- und Problemmanagement.....	37
4.7.5	Leistungs- und Kapazitätsbedarf	38
4.7.6	Datensicherungen	38
4.7.7	Netzwerksicherheit	38
4.8	Auslagerungen und sonstiger Fremdbezug	38
4.9	Bewertung der IKT Risikopositionen.....	39
5.	Ausgewählte IT-Themen.....	39
5.1	Administratorentätigkeiten	40
5.2	Cybersicherheit.....	41
5.3	Mobile Datenträger	41
5.4	Internet, E-Mail und social media	41
5.4.1	Social media	42
5.4.2	Internetauftritt	42
5.5	Smartphones und Tablets.....	42
5.6	Mobile Arbeitsplätze	43
5.7	Kritische Infrastrukturen.....	43
6.	IT-Infrastruktur außerhalb des IT-Dienstleisters	43
7.	Erkenntnisse zum genutzten IT Standard.....	44
8.	Ergebnis der Funktions- und Prozessprüfung.....	44
9.	Qualitätsbeurteilung der gesamten Prüfung	44
10.	Ursachenanalyse.....	45
11.	Erklärung zur Prüfung.....	45
12.	Disclaimer	45
13.	Auftragsgrundlagen der Internen Revision	46