BAIT Novelle 2021 Aufbau und Inhalt auf einen Blick
Neue Themen, neue Verschärfungen

Strategie & Governance

IT-Strategie

- Zuordnung Standards auf Informationssicherheit
- Berücksichtigung externer Dienstleister und externe Abhängigkeiten in IT-Auf- und Ablauforganisation

IT-Governance

- Angemessene qualitative und quantitative Ressourcen-ausstattung der IT und der Informationssicherheit

Steuerung

Informationsrisikomanagement

- Informationsverbund muss Schnittstellen und Abhängigkeiten zu Dritten berücksichtigen
- SBF ist durch das Risikomanagement zu überprüfen
- Kontinuierliche Überprüfung der externen und internen Bedrohungslage des Informationsverbundes

Informationssicherheitsmanagement

- Richtlinie zur Überprüfung und Testen von IS-Sicherheitsmaßnahmen
- Sensibilisierungs- und Schulungsprogramme
- Erstellung IS-Richtlinie für physische Sicherheit

IT-Notfallmanagement

- Festlegung eines Notfallmanagementprozesses (siehe MaRisk AT 7.3)
- Notfallkonzepte für alle IT-Systeme und ausgelagerte Dienste
- Regelmäßige Notfalltests aller Systeme

IT-Projekte und Anwendungsentwicklung

- Der Schutzbedarf der zum Test verwendeten Daten ist zu berücksichtigen
- Formulierungen von Akzeptanz- und Testkriterien

Auslagerung und sonstiger Fremdbezug

- Befugnis der Leistungserbringung des Auslagerungsunternehmens
- Vertragliche Vorgaben zum IT-Betrieb mit Dritten auf Grundlage einer Risikobewertung

Management der Beziehungen mit Zahlungsdienstnutzern

- Angemessene Prozesse zur Reduzierung von Risiken, insbesondere von Betrugsrisiken

Operativ

IT-Betrieb

- Vorgaben zum Emergency Change Management
- Erhebung und Planung des Leistungs- und Kapazitätsbedarfs

Identitäts- und Rechtemanagement

- Standardisierte Berechtigungs-prozesse für alle Bestandteile des Informationsverbunds
- Berücksichtigung von Zugangs- und Zutrittsrechten

Operative Informationssicherheit

- Schutzmaßnahmen State-of-the-Art
- Zeitnahe, regelbasierte und zentrale Auswertung von sicherheitsrelevanten Informationen (SIEM)
- Regelmäßige Überprüfung der IT-Systeme
- Schwachstellenmanagement

Kritische Infrastrukturen

- Keine Änderungen

Neue Kapitel

Ampelsystem bewertet Kritikalität auf Grundlage von msg GillardonBSM-Erfahrungen