ZAIT Novelle 2021 Aufbau und Inhalt auf einen Blick
IT-Anforderungen an Zahlungs- und E-Geld-Institute

Strategie & Governance

IT-Strategie

- Zuordnung Standards auf Informationssicherheit
- Berücksichtigung externer Dienstleister und externe Abhängigkeiten in IT-Auf- und Ablauforganisation
- Anwendung des Grundsatzes der Proportionalität

IT-Governance

- Angemessene qualitative und quantitative Ressourcenausstattung
- Vermeidung von Interessenskonflikten
- Standard zur Ausgestaltung der IT-Systeme (BSI, ISO270xx, PCI-DSS)

Steuerung

Informationsrisikomanagement

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

Informationssicherheitsmanagement

- Aufbau eines ISMS und Erstellung von Informationssicherheitsleitlinie und –Richtlinie
- Etablierung eines unabhängigen ISB
- Zeitnahe Analyse und Nachbearbeitung von Security Incidents

Notfallmanagement

- Festlegung eines Notfallmanagementprozesses
- Notfallkonzepte für alle IT-Systeme und ausgelagerte Dienste
- Regelmäßige Notfalltests aller Systeme

IT-Projekte und Anwendungsentwicklung

- Angemessene Prozesse und Projektstrukturen für die Anwendungsentwicklung
- Berücksichtigung der Informationssicherheit
- Hohe Dokumentationsanforderungen an die Entwicklung

Auslagerung und sonstiger Fremdbezug

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

Management der Beziehungen mit Zahlungsdienstnutzern

- Angemessene Prozesse zu Reduzierung von Risiken, insbesondere von Betrugsrisiken

Operativ

IT-Betrieb

- Verwaltung der IT-Komponenten und deren Beziehungen untereinander
- Life Cycle Management
- Änderungen von IT-Systemen sind in geordneter Art und Weise aufzunehmen und zu dokumentieren.
- Standardisierte IT-Prozesse

Identitäts- und Rechtemanagement

- Standardisierte Berechtigungs-prozesse für alle Bestandteile des Informationsverbundes
- Berücksichtigung von Zugangs- und Zutrittsrechten
- Turnusmäßige und anlassbezogene Rezertifizierung

Operative Informationssicherheit

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

Kritische Infrastrukturen

- Erhöhte Anforderungen für KRITIS-Betreiber (§ 7 BSI-Kritisverordnung)
- Nachweiserbringung bezüglich Einhaltung der Anforderungen

Ampelsystem bewertet Kritikalität auf Grundlage von msg GillardonBSM-Erfahrungen