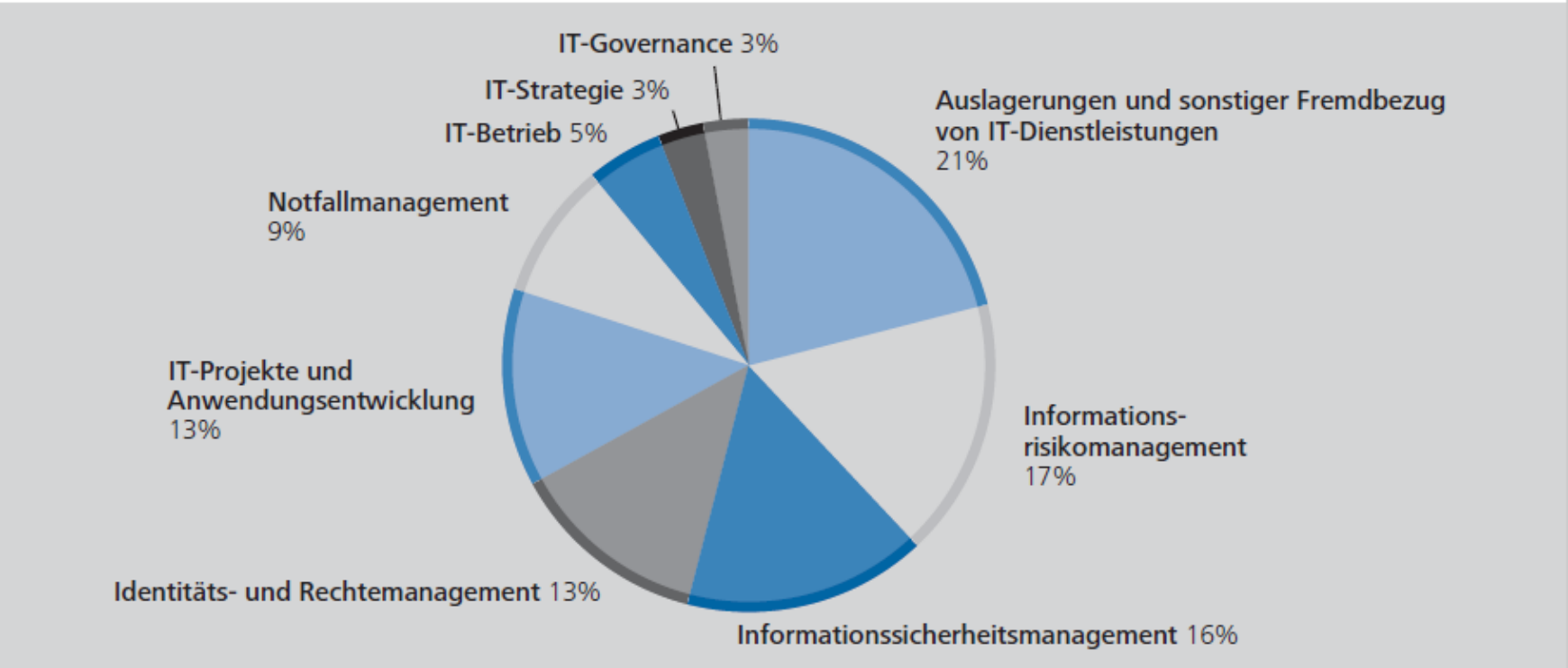
DEUTSCHE BUNDESBANK
EUROSYSTEM

Veranstaltung „IT-Aufsicht bei Banken“

IT-Prüfungen im Lichte der MaRisk-BAIT-Novelle

Rainer Englisch, Deutsche Bundesbank, Hauptverwaltung in Bayern

Wesentliche Mängel aus IT-Prüfungen der letzten 10 Jahre



Quelle: Deutsche Bundesbank, Monatsbericht – Juli 2021, S. 64

Informationsrisikomanagement

- Schwächen im Informationsrisikomanagement führen zu fehlender Transparenz über Informationsrisiken, womit deren angemessene Steuerung nicht möglich ist
- Fehlender Gesamtüberblick über maßgebliche IT-Komponenten und deren Abhängigkeiten voneinander
- Unvollständige und inkonsistente Bewertung der Schutzbedarfe der Schutzobjekte
- Unvollständige und inkonsistente Sollmaßnahmen
- Schwächen beim Soll-Ist-Abgleich bezüglich Durchführung, Nachvollziehbarkeit und Detailliertheit
- Unvollständige und unspezifische Risikoerfassung, unzureichende Nachvollziehbarkeit der Risikobewertungen und unzureichende Risikoakzeptanz-Regelungen
- Mangelhafte Überwachung sonstiger risikomindernder Maßnahmen
- Mangelhafte Berücksichtigung von Informationsrisiken im OpRisk-Management

Informationsrisikomanagement und Auslagerungen

- Informationsrisiken ausgelagerter Prozesse sind ebenfalls zu managen
- Unzureichende Vereinbarung von Sollmaßnahmen beim Leistungsbezug von Dritten
- Im Falle der Durchführung des Soll-Ist-Abgleichs durch eine unabhängige Kontrolleinheit des Dienstleisters: Fehlende vertragliche Vereinbarung bzw. mangelhafte Steuerung
- Unzureichende Maßnahmen der Informationssicherheitsorganisation zur Sicherstellung der Angemessenheit des durch den Dienstleister durchgeführten Soll-Ist-Abgleichs

Informationssicherheitsmanagement

- Schwächen im Informationssicherheitsmanagement verhindern ein angemessenes und durchgängiges Schutzniveau
- Mangelnde Interessenkonfliktfreiheit der Informationssicherheitsorganisation
- Unzulässige Auslagerung des Informationssicherheitsbeauftragten
- Keine ausreichende Berücksichtigung der IT-Strategie-Ziele in der Informationssicherheitsleitlinie
- Implementierte Schutzmaßnahmen entsprechen nicht den Vorgaben gängiger Standards bzw. nicht dem Stand der Technik, die Wirksamkeit wird nicht ausreichend überprüft und die nachhaltige Abstellung aufgedeckter Mängel ist nicht sichergestellt
- Unzureichende Information der Informationssicherheitsorganisation bei potenziellen Informationssicherheitsvorfällen
- Nichteinbindung der Informationssicherheitsorganisation in Prozesse, die informationssicherheitsrelevant sind

Informationssicherheitsmanagement und Auslagerungen

- Unzulässige Auslagerung des Informationssicherheitsbeauftragten
- Nicht ausreichende Steuerung im Falle einer zulässigen Auslagerung des Informationssicherheitsbeauftragten
- Mangelhafte Berücksichtigung der mit Auslagerungen verbundenen Informationssicherheitsrisiken

Identitäts- & Rechtemanagement

- Schwächen im Identitäts- & Rechtemanagement führen zu unberechtigten oder missbräuchlichen Zugriffen und damit zur Gefährdung der Informationssicherheit
- Nicht ausreichend detaillierte anwendungs- und systemspezifische Berechtigungskonzepte, die nicht angemessen überprüft und ggf. aktualisiert werden
- Nicht ausreichende übergreifende Berechtigungsregelungen
- Zuordnung der Nutzung unpersönlicher Benutzerkennungen zu handelnden oder verantwortlichen Personen nicht möglich, nicht ausreichende Überprüfung von Tätigkeiten, die mit unpersönlichen Benutzerkennungen mit privilegierten Berechtigungen erfolgen
- Nicht ausreichend qualitätsgesicherte Datengrundlage für Rezertifizierung und Soll-Ist-Abgleich, nicht ausreichende Tiefe des Soll-Ist-Abgleichs
- Ineffektive Überwachung der Verwendung eingeräumter Berechtigungen

Identitäts- & Rechtemanagement und Auslagerungen

- Anforderungen an die Verfahren zum Zugriffsmanagement müssen auch im Rahmen von Auslagerungen beachtet werden
- Regelung der Verfahren, durch die Mitarbeiter des Dienstleisters Zugriffsrechte auf IT-Systeme der Bank haben, nicht bekannt oder nicht ausreichend
- Nicht ausreichende Überwachung der Dienstleisterzugriffe auf die Informationen des Instituts, die auf den IT-Systemen des Dienstleisters verarbeitet werden
- Keine Sicherstellung ausreichenden Schutzes vor unberechtigten, mandantenübergreifenden Zugriffen bei Mehrmandantendienstleistern
- Keine oder nicht ausreichende Behandlung der Risiken, die durch die Nichterfüllung bankaufsichtlicher Anforderungen im Identitäts- & Rechtemanagement im Zusammenhang mit Auslagerungen bestehen