BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

# Bankaufsichtliche Anforderungen an die IT (BAIT)

3. BDL-Forum Digitalisierung,
02.10.2018

BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

# Bankaufsichtliche Anforderungen an die IT (BAIT)

Christoph Ruckert, Referat GIT 3, Gruppe IT-Aufsicht
Grundsatz IT-Aufsicht und Prüfungswesen

Der Referent gibt seine persönliche Ansicht wieder

# Inhalt

# Ausgangslage

„In einer globalisierten Finanzwelt, in der immer mehr Menschen digital bezahlen beziehungsweise Geld transferieren und in der viele Anleger ihre Geldanlage online bestreiten, haben IT-Governance und Informationssicherheit für die Aufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Institute mit Kapital und Liquidität."

Exekutivdirektor Raimund Röseler, 2017

# Zielsetzung

- BAIT stellen einen flexiblen und praxisnahen Rahmen insbesondere für das Management der IT-Ressourcen sowie das Informationsrisikomanagement und das Informationssicherheitsmanagement dar.
- BAIT tragen dazu bei, das unternehmensweite IT-Risikobewusstsein im Institut und gegenüber den Auslagerungsunternehmen zu erhöhen.
- Die Erwartungshaltung der Aufsicht an die Institute wird durch BAIT transparenter.

# Vorgehen

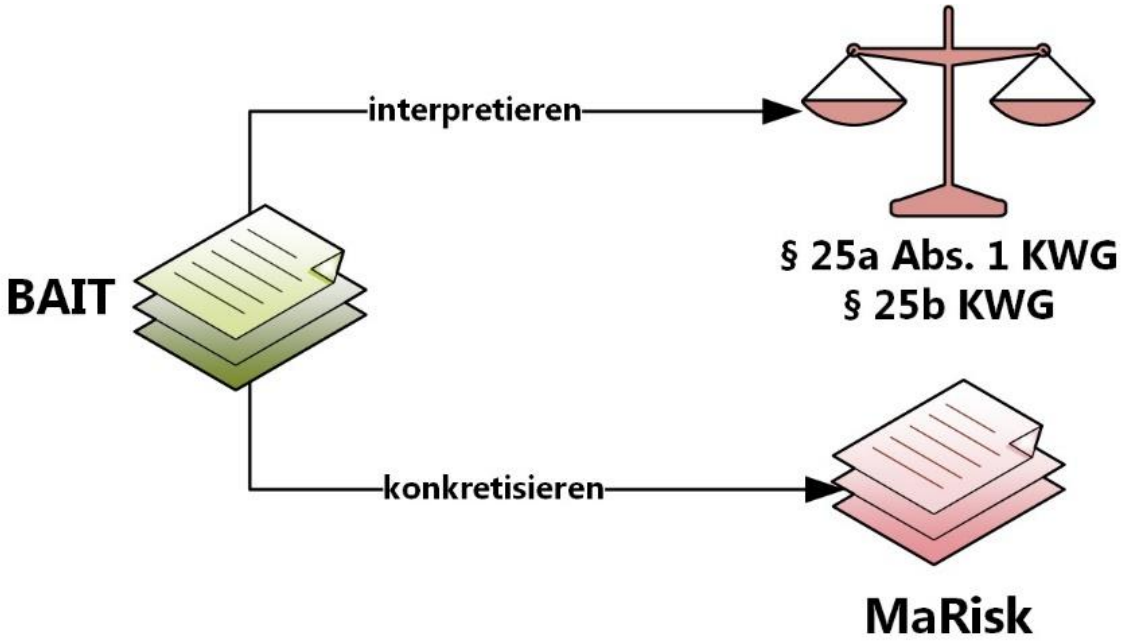
- Erarbeitung
- Erläuterung im Fachgremium-IT
  - Verbände
  - kleine und große Banken
  - IT-Dienstleister
- Öffentliche Konsultation (Stellungnahmen)
- Abstimmung innerhalb der Aufsicht
- Veröffentlichung am 06.11.2017
  - Keine Übergangsfristen
  - Ergänzung um KRITIS-Modul am 14.09.2018

**Englische Übersetzung**

- Circular 10/2017 (BA): Supervisory Requirements for IT in Financial Institutions
- Bereitgestellt am 05.02.2018

# Grundprinzipien

- Prinzipienorientiert
- Proportionalitätsprinzip bleibt gewahrt
- Aufbau der Module analog zu MaRisk
- MaRisk-Anforderungen bleiben unberührt
- Gängige Standards sind weiterhin zu beachten



# I. Vorbemerkungen

- Zentrale Bedeutung von IT für die Finanzwirtschaft
  - in den Instituten
  - bei IT-Dienstleistern
- IT wird weiter an Bedeutung gewinnen
- Themen der BAIT nicht abschließend
- Institut bleibt verpflichtet auf gängige Standards abzustellen
- Prinzip der doppelten Proportionalität

# II. Anforderungen

1. IT-Strategie
2. IT-Governance
3. Informationsrisikomanagement
4. Informationssicherheitsmanagement
5. Benutzerberechtigungsmanagement
6. IT-Projekte, Anwendungsentwicklung, IDV
7. IT-Betrieb
8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
9. Kritische Infrastrukturen

# 1. IT-Strategie

- Geschäftsführung legt fest, überprüft und passt an
- Konsistent zur Geschäftsstrategie
- Inhalte der IT-Strategie sind mindestens:
  - Entwicklung der IT-Aufbau- und IT-Ablauforganisation
  - Entwicklung der Auslagerungen von IT-Dienstleistungen
  - Zuordnung der gängigen Standards
  - Einbindung der Informationssicherheit in die Organisation
  - Entwicklung der IT-Architektur
  - Notfallmanagement
  - In den Fachbereichen betriebene IT-Systeme

# 2. IT-Governance

- Struktur zur Steuerung und Überwachung
  - des Betriebs und der Weiterentwicklung der IT-Systeme
  - der dazugehörigen IT-Prozesse
- Geschäftsführung für wirksame Umsetzung verantwortlich
- Quantitativ und qualitativ angemessene Personalausstattung
  - Informationsrisikomanagement
  - Informationssicherheitsmanagement
  - IT-Betrieb
  - Anwendungsentwicklung
- Interessenkonflikte und unvereinbare Tätigkeiten vermeiden

# 3. Informationsrisikomanagement

- Bestandteile des Informationsverbundes, inkl. deren
  - Abhängigkeiten
  - Schnittstellen
- Ermittlung des Schutzbedarfs im Hinblick auf die Schutzziele
- Anforderungen ermitteln → Sollmaßnahmenkatalog
- Risikoanalyse: Sollmaßnahmen vs. umgesetzte Maßnahmen
- Genehmigung und Management der operationellen Risiken
- Information der Geschäftsführung (mind. vierteljährlich)
  - Ergebnisse
  - Veränderungen der Risikosituation

# 4. Informationssicherheitsmanagement Informationssicherheitsprozess

- Informationssicherheitsleitlinie
- Informationssicherheitsrichtlinien
- Informationssicherheitskonzepte
- Teilprozesse, z. B. für
  - Identifizierung, Schutz
  - Entdeckung
  - Reaktion und Wiederherstellung
- Funktion Informationssicherheitsbeauftragte(n) einzurichten

**Rahmenbedingungen:**
- Organisatorisch/prozessual unabhängig
- Getrennt von Bereichen für Betrieb/ Weiterentwicklung der IT-Systeme
- Grundsätzlich im eigenen Haus, bei Ausnahmen (gemäß Erläuterung Tz. 20)

# 5. Benutzerberechtigungsmanagement

**Rahmenbedingungen**

- Genehmigungsprozess und Kontrollprozess
  - binden fachlich verantwortliche Stellen angemessen ein
  - stellen Einhaltung der Berechtigungskonzepte sicher
- Protokollierung gemäß Schutzbedarf und Sollanforderungen
- Für personalisierte, nicht personalisierte & technische Benutzer

**Berechtigungskonzepte**

- Sind konsistent zum ermittelten Schutzbedarf
- Legen fest
  - Umfang der Berechtigungen
  - Nutzungsbedingungen
- Stellen Sparsamkeitsgrundsatz sicher
- Wahren der Funktionstrennung
- Vermeiden von Interessenkonflikten

# 6. IT-Projekte, Anwendungsentwicklung

- Prozesse enthalten Vorgaben über
  - Anforderungsermittlung
  - Technischen Umsetzung (Programmierrichtlinien)
  - Qualitätssicherung
  - Tests (Aspekte der Produktionsumgebung)
  - Freigabe
- Betreffen auch individuelle Datenverarbeitung; außerdem:
  - Identifizierung
  - Dokumentation
  - Verfahren zur Klassifizierung und für Umgang festzulegen

**IT-Projekte:**
- Aspekte der angemessenen Steuerung
  - Dauer, Ressourcen, Qualität
  - Regelmäßig/anlassbezogen berichten
- Portfolio der IT-Projekte überwachen und steuern

# 7. IT-Betrieb (inkl. Datensicherung)

- Bestandsangaben verwalten über
  - Komponenten der IT-Systeme und
  - ihre Beziehungen zueinander
- Portfolio der IT-Systeme steuern (Lebenszyklus)
- Prozesse auszugestalten und umzusetzen
  - Neu- und Ersatzbeschaffung
  - Änderung von IT-Systemen
  - Sicherheitsrelevante Nachbesserungen
  - Störungen (und ihre Ursachen) priorisieren und eskalieren

# 8. Auslagerungen, sonstiger Fremdbezug von IT-Dienstleistungen

**Für sonstigen Fremdbezug von IT-Dienstleistungen gilt**

- Verträge analog zu IT-Auslagerungsverträgen zu steuern
- Maßnahmen bei Vertragsgestaltung berücksichtigen
- Risikobewertung durchzuführen
  - unter Proportionalitätsgesichtspunkten
  - regelmäßig/anlassbezogen zu überprüfen
  - ggf. Vertragsinhalte anzupassen
- Geschuldete Leistungen sind zu überwachen

# 9. Kritische Infrastrukturen

- Freiwillig anwendbar für Betreiber Kritischer Infrastrukturen
- Möglichkeit der Nachweiserbringung nach § 8a BSIG im Rahmen der Jahresabschlussprüfung
- Bedingungen und Voraussetzungen:
  - Aufsichtliche Anforderungen werden eingehalten
  - Kritische Dienstleistungen sind zu überwachen
  - Konzepte der Hochverfügbarkeit
  - Notfallvorsorgemaßnahmen werden regelmäßig getestet
  - KRITIS-Komponenten werden kenntlich gemacht (Tz. 10)
  - KRITIS-Schutzziel wird vollständig berücksichtigt

  *Namentlich: im IRM (Modul 3) und im ISM (Modul 4)*

BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

# Vielen Dank für Ihre Aufmerksamkeit!

Für Ihre Fragen steht zur Verfügung

Christoph Ruckert
Telefon: 0228 4108-2480
E-Mail: Christoph.Ruckert@bafin.de