DEUTSCHE BUNDESBANK EUROSYSTEM

BaFin

Konkretisierung der MaRisk durch ein Rundschreiben zu Bankaufsichtlichen Anforderungen an die IT (BAIT)

Informationsveranstaltung IT-Aufsicht bei Banken

Renate Essler, BaFin
Dr. Michael Paust, Deutsche Bundesbank

Inhaltsverzeichnis

Ausgangslage

BaFin

*… dass **bei Ausfall der IT innerhalb weniger Stunden enorme Schäden entstehen** und bereits eine Ausfallzeit im Tagesbereich ausreichen kann, um **das Überleben von Organisationen zu gefährden**."*

Hochverfügbarkeitskompendium, BSI, Version 1.6, 2013,
Band G, Kapitel 1: Einführung, S. 5

IT-Strategie (AT 4.2 MaRisk), IT-Berichtswesen, **Datenqualität (u.a. AT 4.3.2 Tz. 2 und AT 7.2 Tz. 2 MaRisk)**

IT-Revision (AT 4.4.3, BT 2)

IT-Organisation, **IT-Auslagerung (AT 9 MaRisk)**

IT-Notfallmanagement (AT 7.3 MaRisk)

Informations-risikomanagement (AT 4.3.2 i.V.m. BTR 4 MaRisk),

Benutzerberechtigungen (AT 7.2 Tz. 2 i. V. m. AT 4.3.1 Tz. 2 MaRisk)

Anwendungsentwicklung (AT 7.2 Tz. 2 bis 4 MaRisk)

Systembetrieb

*„… für die einzelne Bank bringt die **Digitalisierung** neue **Risiken**. … Denn die Zahl der **schützens-werten Güter** ist gewachsen: Neben **Geldvermögen** sind inzwischen auch **persönliche Daten** und damit der Zugang zu **Dienstleistungen** im "**Cyberspace**" gespeichert."*

Eröffnungs-Vortrag beim Bundesbank Symposium "Bankenaufsicht im Dialog", Frankfurt am Main | 08.07.2015
Dr. Andreas Dombret, Mitglied des Vorstands der Deutschen Bundesbank

*…Denn was heute als sicher gilt, kann morgen schon **Einfallstor für Cyberangriffe** sein. Wir fordern diese **Sicherheit** ein und verlangen von den Unternehmen, diese Sicherheit auch von ihren **IT-Dienstleistern** und **Zulieferern** einzufordern.*

Rede von Felix Hufeld – BaFin-Präsident zum Neujahrsempfang am 10.1.2017

* Quelle: BaFin Informationsveranstaltung IT-Aufsicht bei Banken, Prüfungspraxis und Prüfungsergebnisse der Deutschen Bundesbank, Kai Kreische

Zielsetzung

- Mit BAIT wird ein **flexibler und praxisnaher Rahmen** insbesondere für das Management der IT-Ressourcen und das IT-Risikomanagement geschaffen.
- 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**.

Vorgehensmodell

- Die von BaFin und Bundesbank erarbeiteten Entwürfe für 8 BAIT-Themenbereiche wurden insbesondere mit Vertretern von Industrie sowie Verbänden in 3 Sitzungen des Fachgremiums IT (20.05., 14.10., 15./16.12.2016) diskutiert.
  Link zu den Fachgremiumsprotokollen:
  https://www.bafin.de/DE/Aufsicht/BankenFinanzdienstleister/Fachgremien/IT/informationstechnologie_artikel.html
  http://www.bundesbank.de/Redaktion/DE/Dossier/Aufgaben/arbeitskreis_bankenaufsicht.html?notFirst=true&docId=382214#chap
- Das BAIT-Gesamtdokument wurde am 25.1.2017 an das Fachgremium IT zur Kommentierung geschickt.
- Die Anmerkungen des Fachgremiums IT wurden geprüft und in das BAIT-Gesamtdokument eingearbeitet.

Grundprinzipien der BAIT

§ 25a Abs. 1 KWG, § 25b KWG

präzisiert

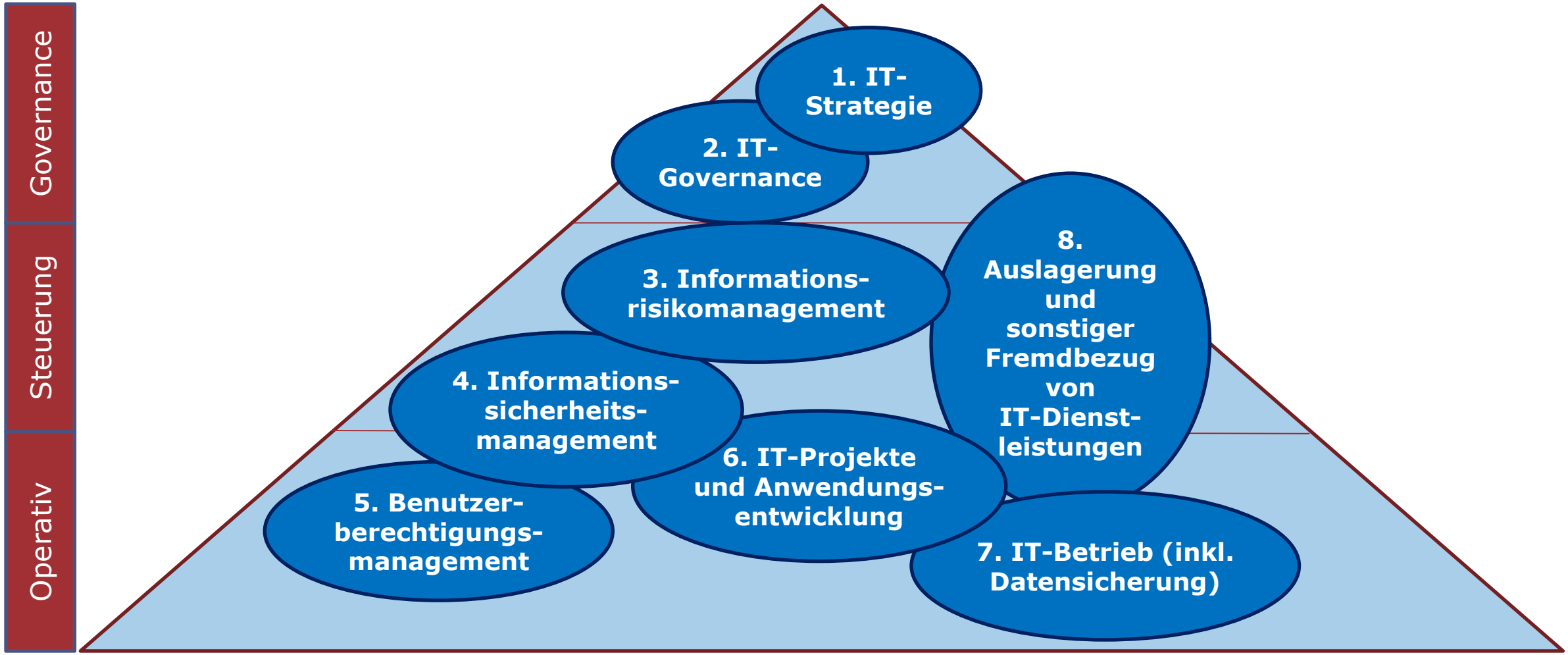
- Die BAIT sind ein **Rundschreiben** der BaFin.
- Die BAIT **präzisieren** § 25a Abs. 1 KWG und § 25b KWG.
- Die BAIT **konkretisieren** die MaRisk.
- Die BAIT sind **prinzipienorientiert** ausgestaltet, damit das **Proportionalitätsprinzip** gewahrt bleiben kann.
- Der **Aufbau** der BAIT ist **analog** dem der **MaRisk**.
- Die BAIT beinhalten **Verweise** auf die Tz. in den MaRisk.
- Die in den MaRisk enthaltenen Anforderungen bleiben unberührt.
- Die **Verpflichtung** des Instituts, **gängige Standards** zu beachten (AT 7.2 Tz. 2 MaRisk) bleibt erhalten.

BAIT

konkretisiert

MaRisk

Überblick der BAIT-Themen



Aufbau der BAIT

BaFin

I. Vorbemerkung

II. Anforderungen

Themenbereiche als Kapitel (1-8)

Leitsätze mit Verweis auf die Textziffern in den MaRisk

Textziffern

Erläuterungen

Aufbau der BAIT – Beispiel

BaFin

1. IT-Strategie

1. Die IT-Strategie hat die Anforderungen nach AT 4.2 der MaRisk zu erfüllen. Dies beinhaltet insbesondere, dass die Geschäftsleitung eine nachhaltige IT-Strategie festlegt, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden.

2. Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen. Mindestinhalte der IT-Strategie sind:

- **a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation sowie der dazugehörigen IT-Prozesse des Instituts sowie der IT-Auslagerungsstrategie**
- **b) Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT**
- **c) Eckpunkte der Informationssicherheits-organisation**
- **d) Strategische Entwicklung der IT-Architektur**
- **e) Aussagen zum Notfallmanagement**
- **f) Aussagen zu den in den Fachbereichen selbst betrieben bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten)**

Zu a): Beschreibung der Rolle, der Positionierung und des Selbstverständnis der IT im Hinblick auf Personaleinsatz, Budget und Wirtschaftlichkeit der IT-Aufbau- und IT-Ablauforganisation sowie der dazugehörigen IT-Prozesse sowie die Darstellung des Dienstleistungsportfolios mit IT-Bezug

Zu b): Auswahl der gängigen Standards und Umsetzung auf die IT-Prozesse des Instituts sowie die Darstellung des Zielbilds im Hinblick auf den Erfüllungsgrad

Zu c): Beschreibung der Bedeutung der IT-Sicherheit im Institut sowie der Einbettung der IT-Sicherheit in die Fachbereiche und in das jeweilige Zusammenarbeitsmodell mit den IT-Dienstleistern

Zu d): Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die Anwendungslandschaft

Darstellung ausgewählter Anforderungen – IT-Strategie

- Die Geschäftsleitung hat eine mit der Geschäftsstrategie **konsistente IT-Strategie** festzulegen, zu überprüfen und regelmäßig anzupassen.
- Mindestinhalte der IT-Strategie sind:
  - ✓ Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation sowie der dazugehörigen IT-Prozesse des Instituts sowie der **IT-Auslagerungsstrategie**
  - ✓ Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT
  - ✓ Eckpunkte der **Informationssicherheitsorganisation**
  - ✓ Strategische Entwicklung der IT-Architektur
  - ✓ Aussagen zum Notfallmanagement
  - ✓ Aussagen zu den **in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen** (Hardware- und Software-Komponenten)

Darstellung ausgewählter Anforderungen – IT-Governance

- Die IT-Governance ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie.
- Die **Geschäftsleitung** ist dafür **verantwortlich**, dass die Regelungen zur IT-Governance wirksam umgesetzt werden.
- Das Institut hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb sowie die Anwendungsentwicklung quantitativ und qualitativ **angemessen mit Personal auszustatten**.
- Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau und IT-Ablauforganisation sind zu vermeiden.

Darstellung ausgewählter Anforderungen – Informationsrisikomanagement

- Aktueller Überblick über die **Bestandteile des Informationsverbundes** sowie deren **Abhängigkeiten und Schnittstellen**
- Methodik zur Ermittlung des **Schutzbedarfs** (insbesondere im Hinblick auf die Schutzziele „Integrität", „Verfügbarkeit", „Vertraulichkeit" und "Authentizität")
- Festlegung von **Soll-Anforderungen** des Instituts zur Umsetzung der Schutzziele in den Schutzbedarfskategorien (Referenzmaßnahmenkatalog)
- Durchführung der **Risikoanalyse** (Schadenspotenzial und Schadenshäufigkeit) auf Grundlage eines Vergleichs der Referenzmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen
- Überführung der **Restrisiken** in den Prozess des Managements der operationellen Risiken
- **Information der Geschäftsleitung** über die Ergebnisse sowie Veränderungen an der Risikosituation

Darstellung ausgewählter Anforderungen – Informationssicherheitsmanagement (1/4)

- Auf Basis der Informationssicherheitsrichtlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitskonzepte und **Informationssicherheitsprozesse** hinsichtlich der Dimensionen **Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung** zu definieren.
- **Erläuterung:** Informationssicherheitsprozesse dienen u.a. der Vorbeugung und Identifikation von Informationssicherheitsvorfällen sowie der angemessenen Reaktion und Kommunikation im Falle ihrer Materialisierung.

Darstellung ausgewählter Anforderungen – Informationssicherheitsmanagement (2/4)

- Das Institut hat die **Funktion des Informationssicherheitsbeauftragten** einzurichten.
- Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsrichtlinie und den Informationssicherheitskonzepten des Instituts niedergelegten Ziele und Maßnahmen sowohl intern als auch gegenüber Dritten transparent gemacht und deren **Einhaltung überprüft** und **überwacht** werden.
- **Erläuterungen** zu den **Aufgaben** des Informationssicherheitsbeauftragten:
  - die Informationssicherheitskonzepte zu erstellen und fortzuschreiben
  - die Informationssicherheitsprozesse im Institut zu steuern und zu koordinieren
  - die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen
  - Informationssicherheitsvorfälle zu untersuchen und diesbezüglich an die Geschäftsleitung zu berichten

Darstellung ausgewählter Anforderungen – Informationssicherheitsmanagement (3/4)

- Die Funktion des Informationssicherheitsbeauftragten ist **organisatorisch und prozessual unabhängig** auszugestalten, um mögliche Interessenskonflikte zu vermeiden.
- **Erläuterungen** zur Vermeidung von **Interessenskonflikten**:
  - Die Funktion des Informationssicherheitsbeauftragten wird aufbauorganisatorisch von den Bereichen getrennt, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind.
  - Verpflichtung der Beschäftigten des Instituts sowie der IT-Dienstleister zur sofortigen und umfassenden Unterrichtung des Informationssicherheitsbeauftragten über alle bekannt gewordenen IT-sicherheitsrelevanten Sachverhalte, die das Institut betreffen.
  - Der Informationssicherheitsbeauftragte nimmt keinesfalls Aufgaben der Internen Revision wahr.

Darstellung ausgewählter Anforderungen – Informationssicherheitsmanagement (4/4)

- Jedes Institut hat die Funktion des **Informationssicherheitsbeauftragten grundsätzlich im eigenen Haus** vorzuhalten.
- **Erläuterungen** zu der **Auslagerbarkeit** des Informationssicherheitsbeauftragten:
  - Regional tätige (insbesondere **verbundangehörige**) Institute sowie kleine (insbesondere gruppenangehörige) Institute **ohne wesentliche eigenbetriebene IT** mit einem **gleichgerichteten Geschäftsmodell** und **gemeinsamen IT-Dienstleistern** können einen gemeinsamen Informationssicherheitsbeauftragten bestellen.
  - Der gemeinsame Informationssicherheitsbeauftragte muss die Wahrnehmung der einschlägigen Aufgaben der Funktion in allen betreffenden Instituten **jederzeit gewährleisten** können. In jedem Institut ist eine zuständige **Ansprechperson** für den Informationssicherheitsbeauftragten zu benennen.
  - Kleine Institute können die Funktion des Informationssicherheitsbeauftragten grundsätzlich mit anderen Funktionen im Institut **kombinieren**.
  - Die Möglichkeit, sich externer Unterstützung per Servicevertrag zu bedienen, bleibt für die Institute unberührt.

Darstellung ausgewählter Anforderungen – Benutzerberechtigungsmanagement

- Das **IT-Berechtigungskonzept** legt den Umfang und die Nutzungsbedingungen der IT-Berechtigungen für die IT-Systeme konsistent zum ermittelten Schutzbedarf […] fest. Die IT-Berechtigungskonzepte haben die Vergabe von IT-Berechtigungen an Benutzer nach dem **Prinzip der minimalen Rechtevergabe** sicherzustellen und die **Funktionstrennung** zu wahren. Darüber hinaus sind **miteinander unvereinbare Tätigkeiten** und **Interessenskonflikte** des Personals zu vermeiden.
- Die Verfahren zur **Einrichtung, Änderung, Deaktivierung oder Löschung von IT-Berechtigungen** […] haben durch Genehmigungs- und Kontrollprozesse sicherzustellen, dass die Vorgaben des IT-Berechtigungskonzepts eingehalten werden. Dabei ist die **fachlich verantwortliche Stelle** angemessen einzubinden.
- Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur **Protokollierung** einzurichten, die sicherstellen, dass die IT-Berechtigungen nur wie vorgesehen eingesetzt werden.

Darstellung ausgewählter Anforderungen – IT-Projekte, Anwendungsentwicklung (1/2)

- **IT-Projekte** sind angemessen zu steuern, insbesondere unter Berücksichtigung der Risiken im Hinblick auf die Dauer, den Ressourcenverbrauch und die Qualität von IT-Projekten. Hierfür sind **Vorgehensmodelle** festzulegen, deren Einhaltung zu überwachen ist.
- Das **Portfolio der IT-Projekte** ist angemessen zu überwachen und zu steuern. Dabei ist zu berücksichtigen, dass auch aus Abhängigkeiten verschiedener Projekte voneinander Risiken resultieren können.
- **Wesentliche IT-Projekte und IT-Projektrisiken** sind der Geschäftsleitung regelmäßig und anlassbezogen zu **berichten**.
- Für die **Anwendungsentwicklung** sind **angemessene Prozesse** festzulegen, die Vorgaben zur Anforderungsermittlung, zum Entwicklungsziel, zur (technischen) Umsetzung (einschließlich Programmierrichtlinien), zur Qualitätssicherung, sowie zu Test, Abnahme und Freigabe enthalten.
  - Anwendungsentwicklung umfasst die auch die vom Endbenutzer in den Fachbereichen selbst entwickelten Anwendungen (z.B. Individuelle Datenverarbeitung – **IDV**).

Darstellung ausgewählter Anforderungen – IT-Projekte, Anwendungsentwicklung (2/2)

- Jede neu entwickelte bzw. veränderte Anwendung ist **vor Produktivsetzung** angemessen zu testen. Die **Tests** haben in ihrem Umfang die Funktionalität der Anwendung, die Sicherheitskontrollen und die Systemleistung unter verschiedenen Stressbelastungsszenarien einzubeziehen.
- Die Durchführung von **fachlichen Abnahmetests** verantwortet der für die Anwendung zuständige Fachbereich. **Testumgebungen** zur Durchführung der Abnahmetests haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.
- Ein angemessenes **Verfahren für die Klassifizierung / Kategorisierung** (Schutzbedarfsklasse) und den **Umgang** mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen (**IDV**) ist festzulegen.
- Die Vorgaben zur Identifizierung aller von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess der Berechtigungen sind innerhalb einer Arbeitsanweisung (z.B. **IDV-Richtlinie**) zu regeln.

Darstellung ausgewählter Anforderungen – IT-Betrieb

- Die **Komponenten der IT-Systeme** sowie deren Beziehungen zueinander sind in geeigneter Weise zu **verwalten** und die erfassten Bestandsangaben regelmäßig sowie anlassbezogen zu aktualisieren.
- Das **Portfolio** aus IT-Systemen ist angemessen zu **steuern**. Hierbei werden auch die Risiken aus veralteten IT-Systemen berücksichtigt (Lebens-Zyklus Management).
- Die **Prozesse zur Änderung von IT-Systemen** sind abhängig von Art, Umfang, Komplexität und Risikogehalt auszugestalten und umzusetzen. Dies gilt ebenso für **Neu- bzw. Ersatzbeschaffungen** von IT-Systemen sowie für **sicherheitsrelevante Nachbesserungen** (Sicherheitspatches).
- Die Meldungen über **ungeplante Abweichungen vom Regelbetrieb** (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und ggf. zu eskalieren.

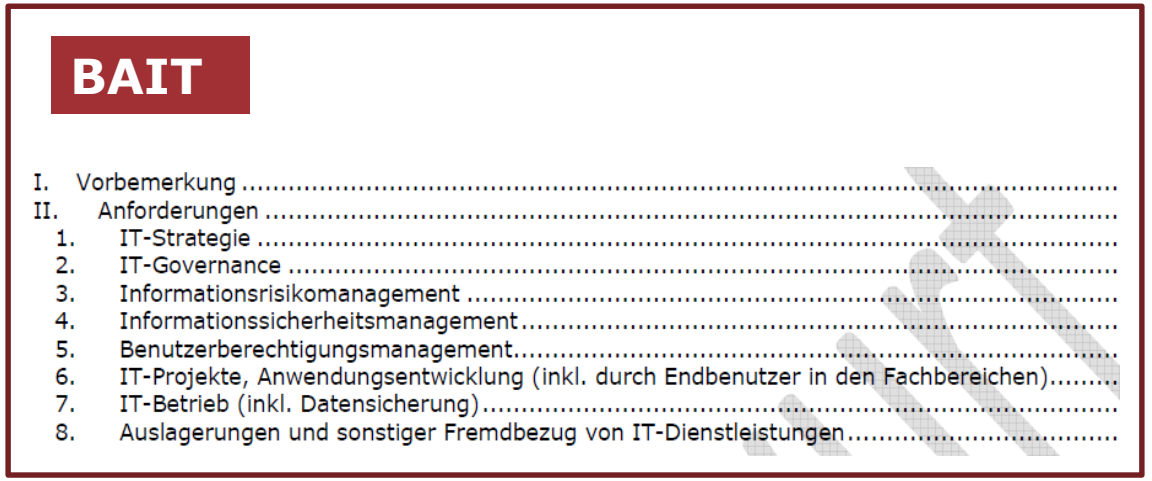
Darstellung ausgewählter Anforderungen – Auslagerungen und Sonstiger Fremdbezug von IT-Dienstleistungen

BaFin

- Die **Verträge** betreffend den sonstigen Fremdbezug von IT-Dienstleistungen sind **strategisch** analog den IT-Auslagerungsverträgen zu **steuern**.
- Für jeden sonstigen Fremdbezug von IT-Dienstleistungen ist eine **Risikobewertung** durchzuführen.
- Für den sonstigen Fremdbezug von IT-Dienstleistungen wird eine **Vertragsevidenz** im Einklang mit den Vorgaben der IT-Strategie des Instituts vorgehalten.
- Die **Risikobewertungen** in Bezug auf den sonstigen Fremdbezug von IT-Dienstleistungen sind regelmäßig und anlassbezogen zu **überprüfen** und ggf. inkl. der Vertragsinhalte **anzupassen**.
- Die Leistungserbringung im Rahmen des sonstigen Fremdbezugs von IT-Dienstleistungen ist angemessen zu überwachen.

Weiteres Vorgehen

- Der Beginn der öffentlichen **Konsultation** des Rundschreibens zu den BAIT ist für Ende März 2017 geplant.
- Die **Veröffentlichung** des Rundscheibens zu den BAIT ist für Mitte 2017 geplant.



Ansprechpartner

Dr. Michael Paust

Tel. +49 (0)69 / 9566-3746

michael.paust@bundesbank.de

Zentralbereich Banken- und Finanzaufsicht
Bankgeschäftliche Prüfungen und Umsetzung internationaler Standards

Renate Essler

Tel. +49 (0)228 / 4108-2440

renate.essler@bafin.de

Bankenaufsicht
Kompetenzcenter IT-Sicherheit