Grafik Quelle: BaFinJournal

DEUTSCHE BUNDESBANK
EUROSYSTEM

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Bankaufsichtliche Anforderungen an die IT (BAIT)

Dr. Michael Paust,
Deutsche Bundesbank

Renate Essler,
BaFin

Inhalt

Veröffentlichung

- Veröffentlichung der BAIT als „Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT (BAIT)“ erfolgte am 06.11.2017
- die englische Übersetzung „Circular 10/2017 (BA) - Supervisory Requirements for IT in Financial Institutions“ ist auf der Internetseite der BaFin und Deutschen Bundesbank abrufbar

Zielsetzung

- Die Erwartungshaltung der Aufsicht an die Institute wird durch BAIT transparenter
- Erhöhung des unternehmensweiten IT-Risikobewusstsein im Institut und gegenüber den Auslagerungsunternehmen

Zielgruppe – Geschäftsführung:
- zeigt Risikobewusstsein
- legt Strategie fest
- stellt angemessene Ressourcen bereit
- nimmt Steuerungsaufgaben wahr

Grundprinzipien

- Interpretation der Anforderungen an eine ordnungsgemäße Geschäftsorganisation (§ 25a Abs. 1 KWG)
- Interpretation der Anforderungen an Auslagerung von Aktivitäten und Prozessen (§ 25b KWG)
- Konkretisierung der MaRisk
  - knüpft an Textstellen der MaRisk an
  - prinzipienorientiert und flexibel
  - Proportionalitätsprinzip bleibt gewahrt
  - Anforderungen zu Sicherheitszielen in den MaRisk
- Anforderungen der BAIT sind nicht abschließend

Hinweis:
Prinzipien und Ziele gelten gleichermaßen für Auslagerungen

Rückmeldungen der Finanzwirtschaft

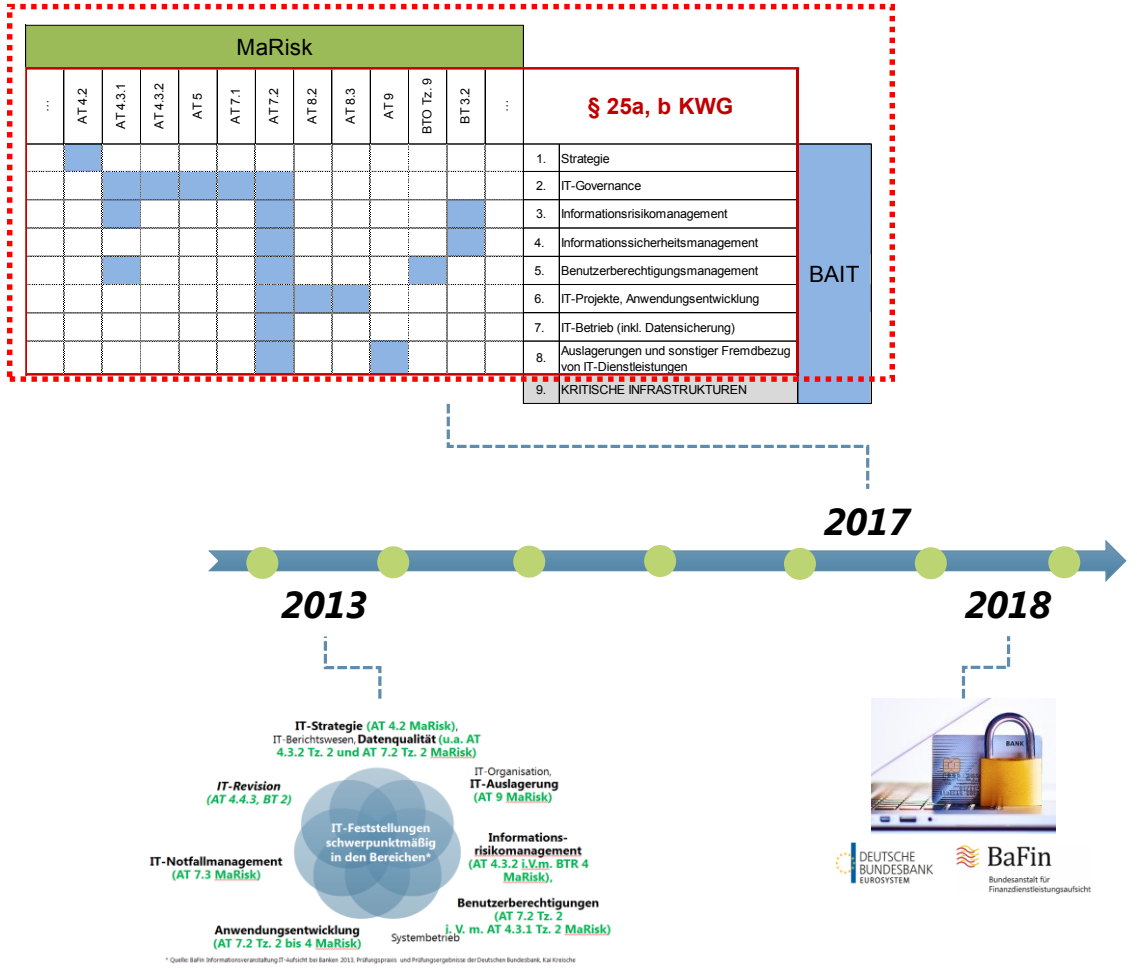
- Hoher Diskussions- und Kommunikationsbedarf mit der Aufsicht
- BAIT Vorträge durch Mitarbeiter der BaFin und Bundesbank
- viele **Fragen während der Vorträge** und im Anschluss zu den Themen
  - Informationssicherheitsbeauftragter
  - sonstigen Fremdbezug von IT-Dienstleistungen
- vereinzelte **Auslegungsfragen** zu den Themen
  - Informationssicherheitsbeauftragter
  - Auslagerungen an Cloud Service Provider
- weiterer Austausch mit Vertretern von Industrie sowie Verbänden
- Teilnahme in verschiedenen Fachgruppen

Inhalt

MaRisk/BAIT Prüfungspraxis - Erste Eindrücke

- MaRisk Anpassung am 27.10.2017
- Veröffentlichung der BAIT am 6.11.2017
- vorlaufend: Erörterung der BAIT-Themen im Fachgremium IT März 2016

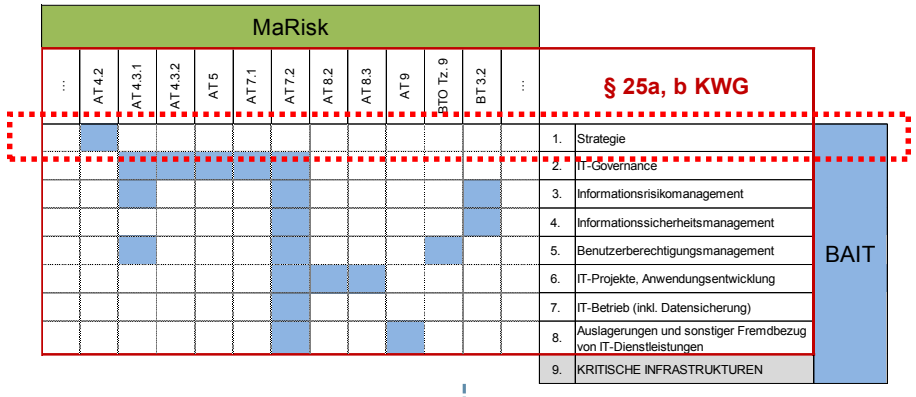
- Awareness
- Transparenz
- Evaluierung
- Projekte

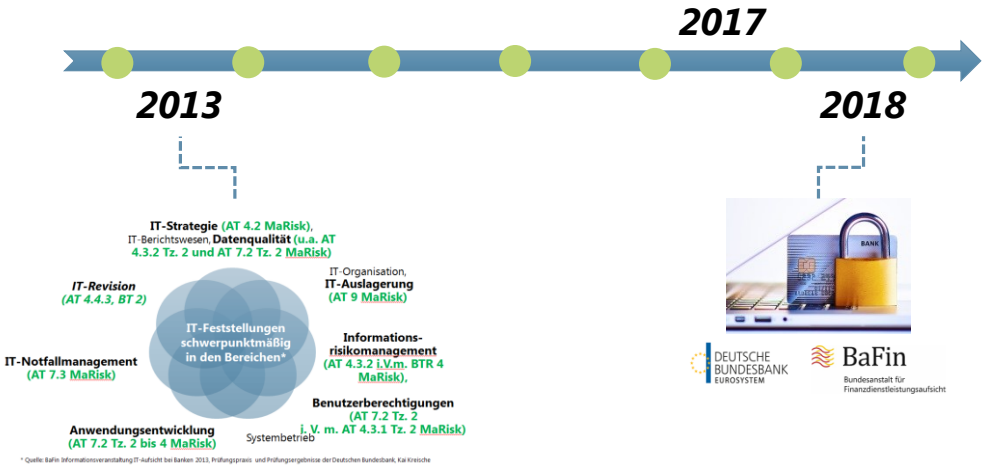


MaRisk/BAIT Prüfungspraxis - Beispiel IT-Strategie

- Strategieprozess
- Konsistenz
- Mindestinhalte
- Überprüfbarkeit der Zielerreichung /

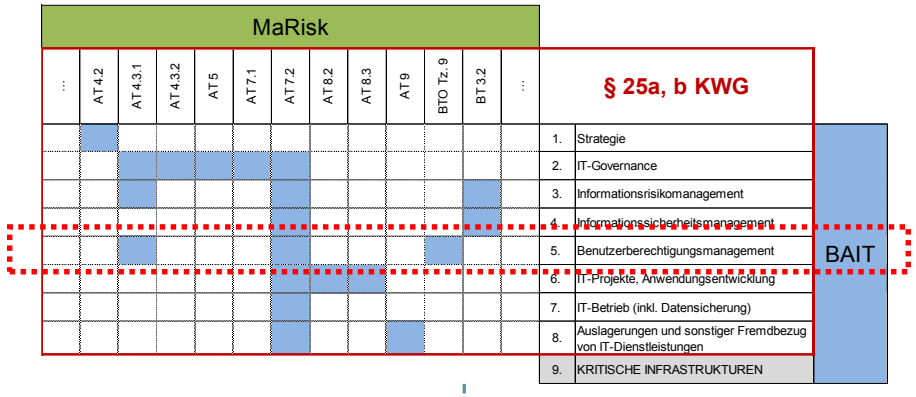
  Überführbarkeit in die operative Unternehmensplanung
- Strategieberichterstattung
- Erörterung Aufsichtsrat

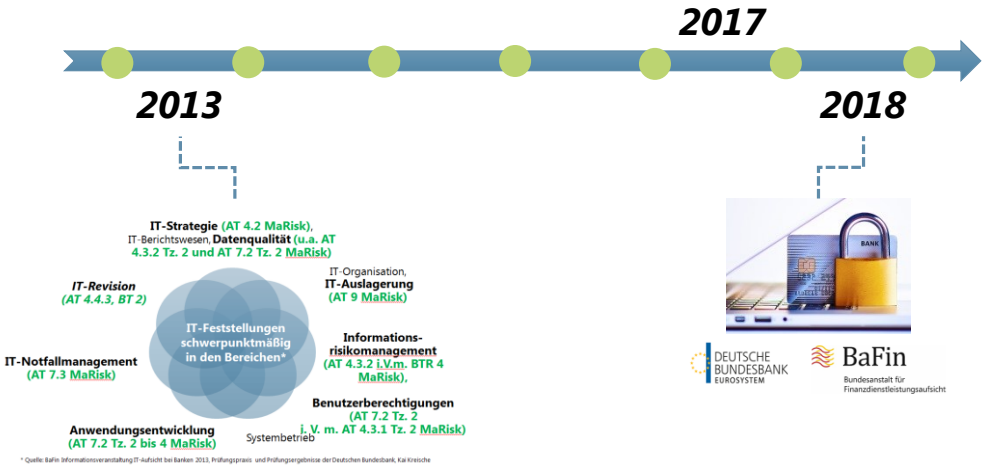




MaRisk/BAIT Prüfungspraxis - Beispiel Benutzerrechte

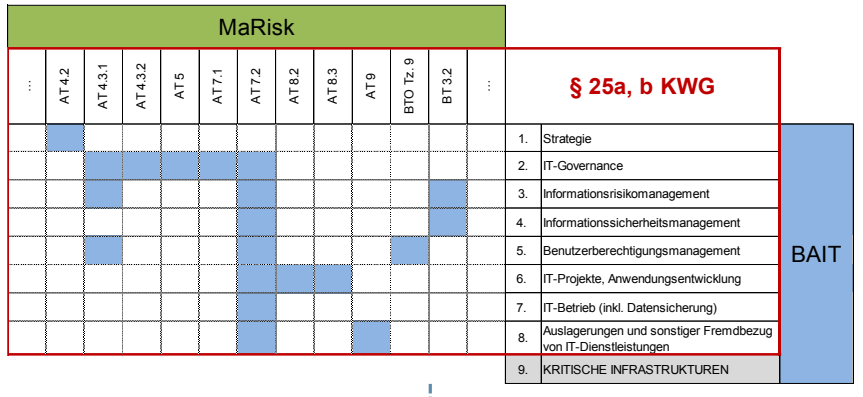
- Minimale Berechtigung / Auslagerung
- SoD, Rechtematrizen, Sonderberechtigungen
- Einbindung aller relevanter Stellen bei Vergabe
- Berechtigungskonzepte
- kritische Berechtigungen
- Rezertifizierung: Zuständigkeiten, Turnus/Rückstände, Soll/Ist, Rechteentzug
- Austauschlaufwerke

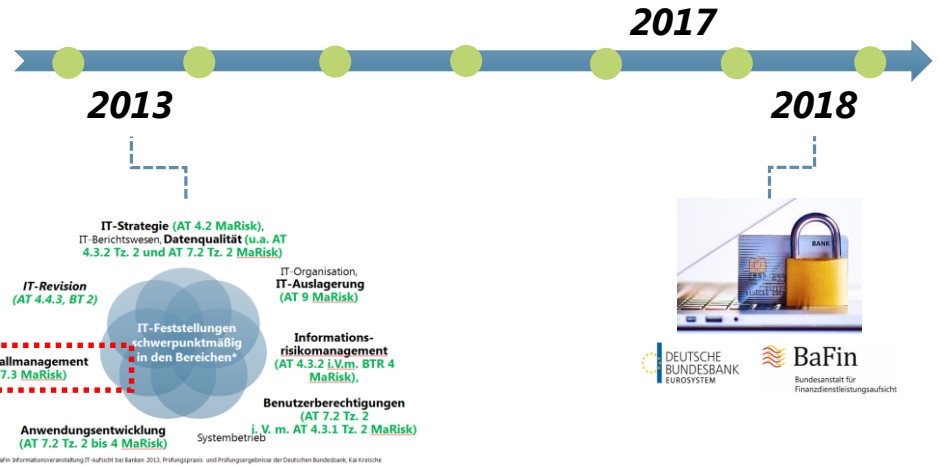




MaRisk/BAIT Prüfungspraxis - Beispiel Notfallvorsorge

- Business Impact Analyse
- Notfallkonzepte
- Testen zeitkritischer Prozesse sowie Komponenten bzgl. identifizierter Szenarien
- Dokumentation
  - Prozess zur Erstellung der BIA
  - Notfalltestplanung / Mehrjahresplanung
  - Wiederherstellung IT-Services
  - Tests

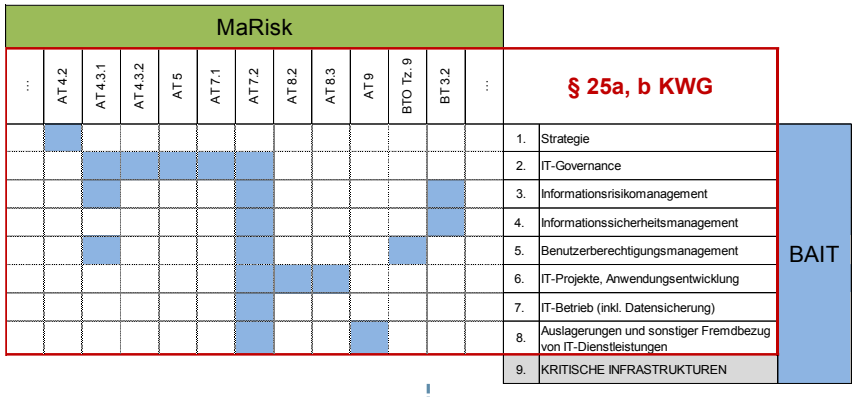


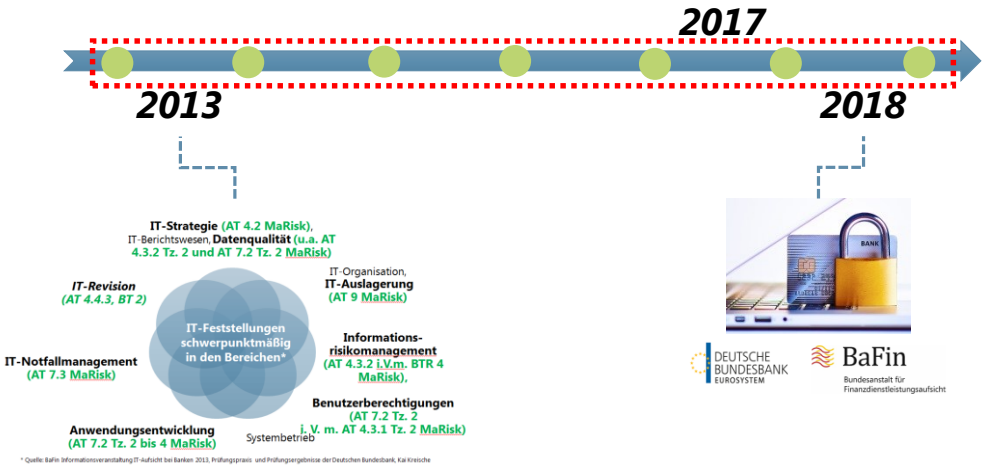


MaRisk/BAIT Prüfungspraxis - Trends

- Bankfachliche MaRisk-Prüfungen
- IT-Prüfungen / Technisch-organisatorische Ausstattung

- Erstaufnahme der IT-Prozesse
- Nachschauprüfungen

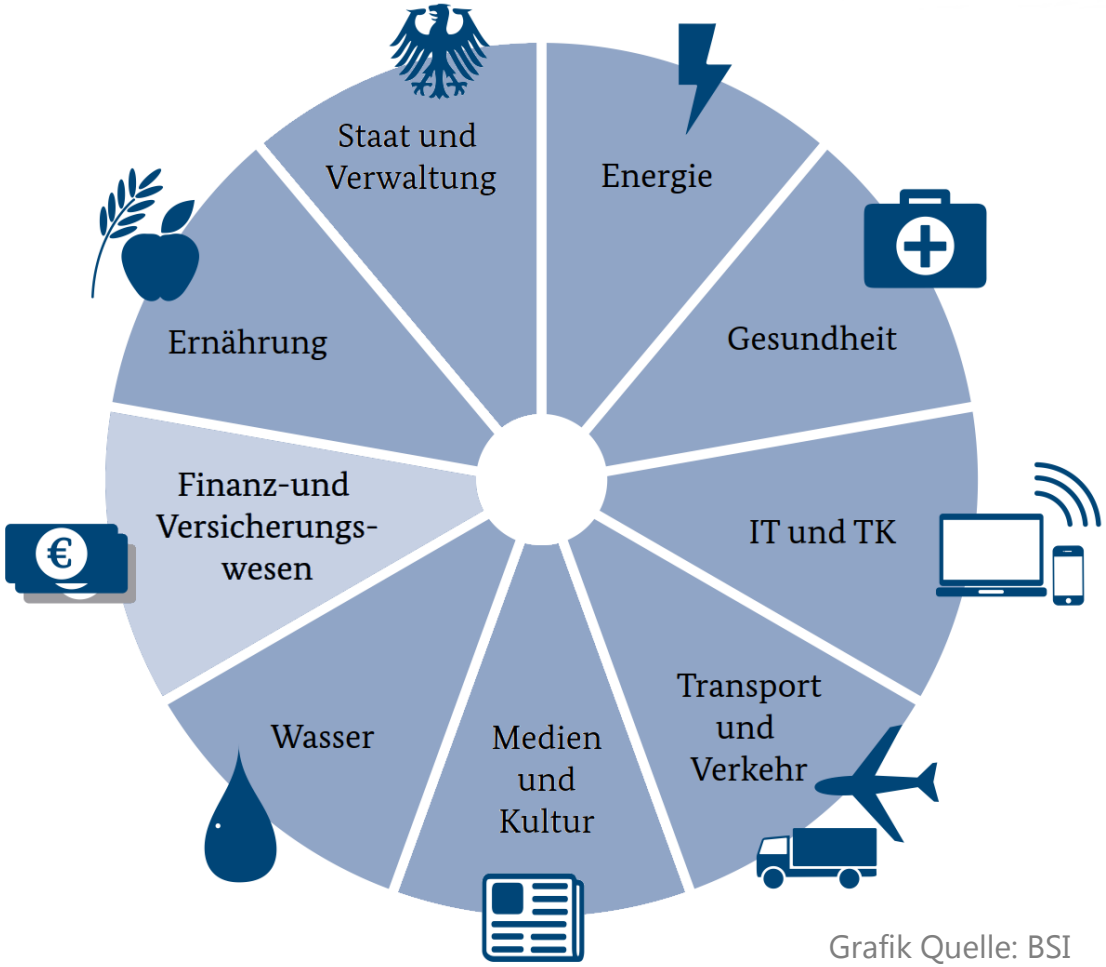




Inhalt

Anwendung der BAIT für Betreiber kritischer Infrastrukturen

- Ergänzung der BAIT (RS 10/2017) am 14.9.2018 um das Kapitel 9. „Kritische Infrastrukturen“
- Optional für die Erbringung des Nachweises gem. § 8a Absatz 3 BSIG
- Erarbeitung in Abstimmung zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- zusätzliche Anforderungen für KRITIS-Betreiber zur Überwachung der kritischen Dienstleistungen



Grafik Quelle: BSI

Anwendung der BAIT für Betreiber kritischer Infrastrukturen

- Anwendung der BAIT-Anforderungen auf alle Komponenten und Bereiche der kritischen Dienstleistung
- Bewertung der Auswirkungen von Sicherheitsvorfällen auf die kritischen Dienstleistungen
- Umsetzung von Maßnahmen zur Risikominderung oder –vermeidung für die kritischen Dienstleistungen (z.B. Anwendung von Konzepten der Hochverfügbarkeit)
- Implementierung und regelmäßiges Testen von Notfallvorsorgemaßnahmen
- Überprüfung und Bestätigung durch den Jahresabschlussprüfer
- Meldepflicht ist unverändert gegenüber dem BSI einzuhalten

Ergänzung um IT-Notfallmanagement

- Erweiterung der BAIT um Anforderungen an ein Notfallmanagement unter Berücksichtigung der IT-Belange geplant
  - Konkretisierung des AT 7.3 der MaRisk in der BAIT
  - Konkretisierung der Test- und Wiederherstellungsverfahren für IT-Systeme und die zugehörigen IT-Prozesse

BAIT im Zusammenhang europäischer Anforderungen

- European Banking Authority (EBA) erarbeitet derzeit ihre Erwartungshaltung an das Management der IT-Risiken in den Instituten mit dem Arbeitstitel „ICT Risk Management Guidelines“
- Europäische Zentralbank (EZB) wird ihre Erwartungshaltung an das Management der IT-Risiken im Rahmen des einheitlichen Aufsichtsmechanismus SSM ebenfalls umsetzen
- Einbeziehung der EBA Guideline 2017/17 „Leitlinien zu Sicherheitsmaßnahmen bzgl. der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)“

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, Gruppe IT-Aufsicht
IT-Prüfungen und Prüfungs-/ Aufsichtsunterstützung