Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Arbeitsschwerpunkte zur IT-Aufsicht 2016/ 2017

4. IT-Informationsveranstaltung der BaFin

16. März 2017

Vorstellung Kompetenzreferat IT-Sicherheit (BA 51)

- 2012 Gründung des Referats „IT-Infrastrukturen bei Banken“ im Geschäftsbereich BA
- 2016 **Weiterentwicklung** zu einem im **geschäftsbereichsübergreifenden Kompetenzreferat** für die Themen IT-/ Cybersicherheit im Finanzsektor sowie Zahlungsverkehr. Das Kompetenzreferat IT-Sicherheit (BA 51) ist weiterhin im Geschäftsbereich BA angesiedelt und dort in der Grundsatzabteilung BA 5 „Bankgeschäftliche Risiken“. Zuständiger Abteilungsleiter ist Herr Mattias Güldner.

⇒ **Ziel: Organisatorische Bündelung** der vorhandenen Ressourcen und Kompetenzen und bestmögliche Nutzung des vorhandenen Wissens. Hebung von Synergien und Gewährleistung der Einheitlichkeit des Verwaltungshandelns - soweit sachlich angemessen – auch bei der aufsichtlichen Beurteilung neuer Technologien (bspw. Cloud Computing).

⇒ **Tagesgeschäft** insbesondere **Unterstützung der Fachaufsicht** bspw. Begleitung von IT-Prüfungen, Auswertung entsprechender Prüfungsberichte, Erlaubnisverfahren, Beurteilung von Auslagerungsvorhaben, MaSi Meldungen, Grundsatzfragen mit IT-Bezug, Verbraucherbeschwerden, Durchführung von Schulungen für die Fachaufsicht, Mitarbeit in nationale und Internationale Arbeitsgruppen.

BaFin

MaRisk-Novelle 2016

MaRisk-Novelle 2016

I) Umsetzung Baseler Papier zur Risikodatenaggregation und Risikoberichterstattung (BCBS 239)

II) Konkretisierung von Anforderungen entsprechend der Aufsichts- und Prüfungspraxis u.a.:

- AT 7.2 => Identifizierung, Überwachung und Steuerung von IT-Risiken
- AT 7.2 => Einsatz von durch die Fachbereiche selbst entwickelten Anwendungen (Individuelle Datenverarbeitung - „IDV“)
- AT 9 => Abgrenzung von Auslagerung und Fremdbezug (auch mit Blick auf Software)

  → Neu: Klarstellung in AT 9 Tz. 1, dass zivilrechtliche Ausgestaltungen und Vereinbarungen das Vorliegen einer Auslagerung nicht ausschließen, strikte Einzelfallbetrachtung

- AT 9 => Voraussetzungen für Weiterverlagerungen

Veröffentlichung der Endfassung: voraussichtlich Q 1 2017

BaFin

Bankaufsichtliche Anforderungen an die IT (BAIT)

BAIT - Zielsetzung & Grundprinzipien

- Die BAIT sollen:
  - einen flexiblen und praxisnahen Rahmen insbesondere für das Management der IT-Ressourcen und das IT-Risikomanagement schaffen
  - das IT-Risikobewusstsein im Institut und gegenüber den Auslagerungsunternehmen erhöhen
  - die Erwartungshaltung der Aufsicht für die Institute transparenter gestalten
- Die BAIT sind:
  - eine Konkretisierung aber keine Erweiterung der MaRisk
  - im Grundsatz prinzipienorientiert und erhalten das Proportionalitätsprinzip der MaRisk
  - analog den MaRisk aufgebaut und über konkrete Verweise mit den MaRisk verknüpft
  - auch für „Nicht-IT Experten" verständlich formuliert

BAIT - Stand der Arbeiten und weiteres Vorgehen

- Die BAIT-Themenmodule wurden gemeinsam mit der Bundesbank erarbeitet und im Verlaufe 2016 im Fachgremium IT diskutiert (u.a. mit Vertretern von Industrie, Verbänden).
- Der Beginn der öffentlichen Konsultation ist kurzfristig im Anschluss an die heutige Veranstaltung geplant.
- Die Veröffentlichung eines entsprechenden Rundschreibens nach öffentlicher Konsultation für Mitte 2017 geplant.

BaFin

BSIG-Umsetzung im Finanzsektor

BSIG-Umsetzung im Finanzsektor

- Kritische Infrastrukturen (KRITIS) sind Organisationen/Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen nach sich ziehen würde.

  ➔ spezieller Fokus auf Versorgungssicherheit

  ➔ Finanzsektor einer von 8 kritischen Sektoren neben u.a. Gesundheitswesen, Energiewirtschaft, Telekommunikation, Handel- und Ernährung.

- Betreiber kritischer Infrastrukturen unterliegen künftig grundsätzlich den Vorschriften des BSIG.

BSIG-Umsetzung im Finanzsektor

<u>Verordnung zur Identifizierung der Betreiber Kritischer Infrastrukturen u.a. im Finanzsektor</u>

- In 2016/2017 Erarbeitung der Rechtsverordnung zur Identifizierung der Betreiber Kritischer Infrastrukturen u.a. im Finanzsektor unter Federführung des BMI.
- Inkrafttreten der sogenannten „Kritis"-Verordnung für das 2. Quartal 2017 geplant.
- Selbstidentifizierungsprozess über kritische Dienstleistungsbereiche, Anlagekategorien, Bemessungsgrundlagen, Schwellenwerte.
- Die kritische Dienstleistung im Bankensektor ist der Zahlungsverkehrs (umfasst Bargeldversorgung, bargeldlosen Zahlungsverkehr und konventionellen Zahlungsverkehr.)

Für Institute, welche zugleich Betreiber Kritischer Infrastrukturen nach dem BSIG und Aufsichtsobjekte der BaFin sind, gelten die Vorschriften des BSIG uneingeschränkt neben denjenigen insbesondere des KWG.

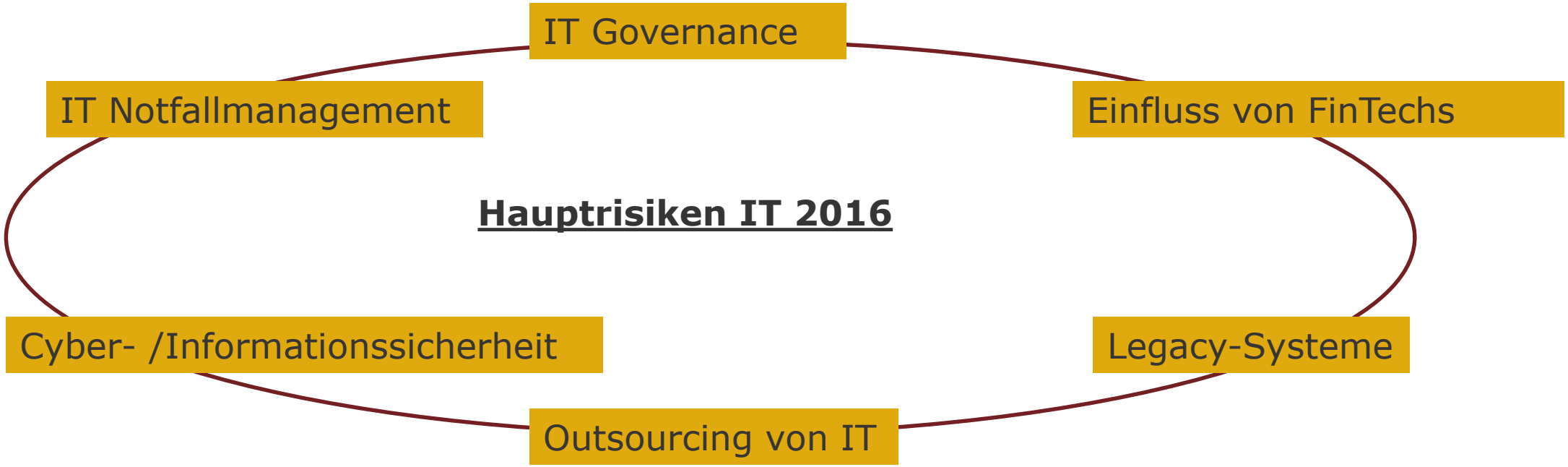
BaFin

Arbeiten der EBA mit IT-Bezug

EBA Task Force on IT Supervision

- EBA Report „**Risk Assessment of the European Banking System**“

  Status: veröffentlicht => enthält Teilreport „Material and emerging IT-risks“ aus Sicht der Aufseher:



EBA Task Force on IT Supervision

- EBA Guidelines on ICT Assessment under the Supervisory Review and Evaluation process (SREP)
  (**Status:** Konsultiert, Veröffentlichung für Q2/2017 geplant)

  Die geplanten Guidelines ergänzen die bestehenden SREP-Guidelines um ein Vorgehensmodell mit expliziten Basisanforderungen zur Analyse und Bewertung von IT-Risiken.

- EBA Recommendations on outsourcing to Cloud Service Providers
  (**Status:** in Bearbeitung, Konsultation für Q3/2017 geplant)

Geplante Themenbereiche u.a.:

- Beurteilung der Wesentlichkeit
- Informationspflichten gegenüber der Aufsicht und Prüfungsrechte für Banken und die Aufsicht
- Physische Zugangsrechte zu den relevanten Geschäftsräumen der Cloud Dienstleister
- Geographische Lage der Daten und der Datenverarbeitung
- Weiterverlagerungen
- Ausstiegsklauseln

EBA Arbeiten zur PSD2

EBA Regulatory Technical Standards (RTS) und Guidelines (GL) zur PSD2 mit Fokus auf IT-Sicherheitsthemen bzw. IT-Technologie:

- EBA Guidelines on Incident Reporting (Ablösung der MaSI-Meldepflichten).

  Status: Konsultation abgeschlossen

- EBA Guidelines on Operational Risk and Security Measures.

  Status: Konsultation geplant 04.2017

- EBA RTS on Strong Customer Authentication and Secure Communication.

  Status: Konsultiert, finaler Entwurf veröffentlicht, Prüfung durch die EU-Kommission

BaFin

G7 Grundelemente zur Cyber-Sicherheit im Finanzsektor

G7 Grundelemente

- Aufgrund der weltweiten Vernetzung unserer Finanzsysteme ist eine strategische Bündelung von Cyber-Sicherheitsaktivitäten auf internationaler Ebene und die Entwicklung von Mindeststandards für die Cyber-Sicherheit in der Finanzdienstleistungsbranche zum Schutz von Verbrauchern, Instituten, Daten und Infrastrukturen wichtig.
- Eine zu diesem Thema eingesetzte G7-Expertengruppe, hat Ende 2016 einen Bericht mit acht Grundelementen ausgearbeitet, die in den G7-Staaten als Basisabsicherung dem Finanzsektor zur Umsetzung und als Basis für die Entwicklung und Implementierung einer Cyber-Strategie anempfohlen werden sollen. Regulatorischen Arbeiten können sie als Leitlinie dienen.
- Veröffentlicht u.a. auf der Homepage des BMF.

G7 Grundelemente

- **8 Grundelemente:**
  - Cybersecurity Strategy (Cyber-Sicherheitsstrategie)
  - Governance (Unternehmensführung)
  - Risk and Control Assessment (Risiko- und Maßnahmenbewertung)
  - Monitoring (Überwachung)
  - Response (Reaktion)
  - Recovery (Wiederherstellung)
  - Information Sharing (Informationsaustausch)
  - Continuous Learning (Kontinuierliches Lernen)
- Zur Umsetzung dieser Elemente in Deutschland tragen unter anderem BSI-G und die geplanten BAIT bei.