Arbeitsschwerpunkte des Referats zur IT-Aufsicht der BaFin 2013/2014

Dr. Josef Kokert, BaFin

Referat „IT-Infrastrukturen bei Banken“

Inhalte

BaFin

I. Regulierung

II. Aktivitäten

III. Einzelfragen

IV. Ausblick SSM

I. Regulierung - EU

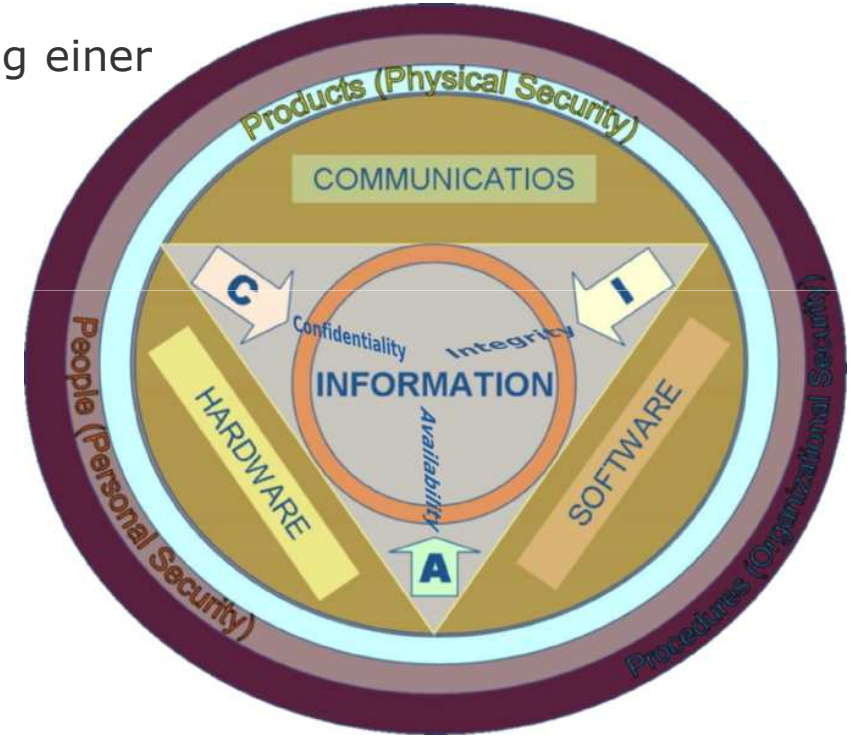
Welche europäischen Regelungen mit IT-Bezug zeichnen sich ab?

- NIS-Richtlinie
- (Datenschutzrichtlinie)
- Zahlungsdiensterichtlinie II
- EBA Guidelines on the Security of Internet Payments

I. Regulierung EU

Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS)

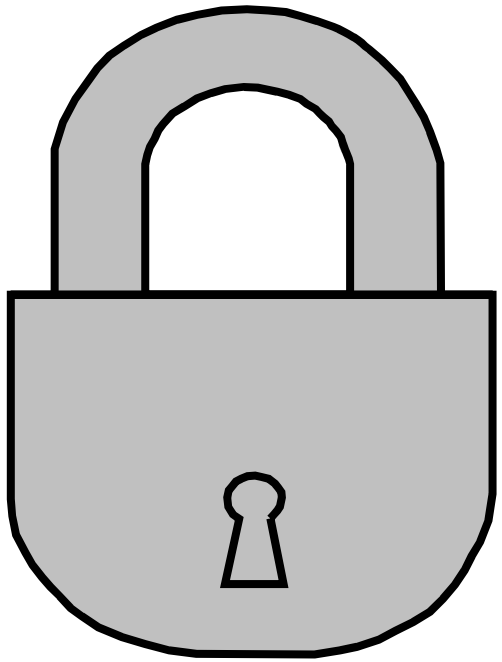
- Art. 14 NIS Marktteilnehmer Maßnahmen
- Stand der Technik
- Risiko – Maßnahmen
- Reaktion auf Sicherheitsvorfälle
- Meldung von Sicherheitsvorfällen



I. Regulierung - EU

Zahlungsdiensterichtlinie II

- Art. 85 manage security risks
- Art. 85 yearly updated assessment
- Art. 85 EBA guidelines
- Art. 86 incident reporting
- Art. 86 provides details to EBA
- Art. 86 EBA guidelines



I. Regulierung - EU

Zahlungsdiensterichtlinie II

- Art. 87 strong customer authentication
- Art. 87a EBA – regulatory technical standards
  - appropriate level of security
  - fair competition
  - technological and business-model neutrality
  - submit draft to the Commission

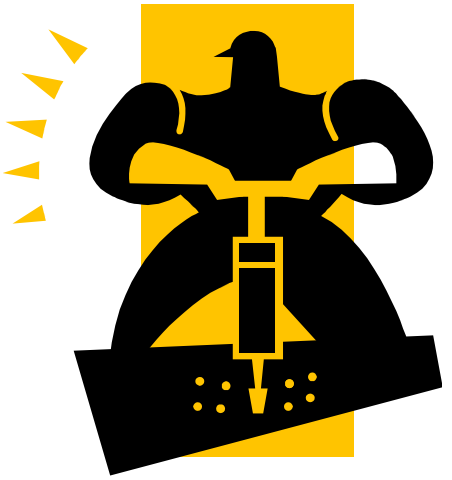
I. Regulierung - EU

EBA - Draft Guidelines on the Security of Internet Payments

- Umsetzung der Empfehlungen des SecuRe Pay Forums vom 01.02.2013
- Konsultation voraussichtlich Ende Oktober 2014
- Konsultation Anpassung an Zahlungsdiensterichtlinie II

I. Regulierung - National

Entwurf IT-Sicherheitsgesetz des BMI



- Umsetzung der NIS
- Ergänzung des BSI-Gesetzes
- Betreiber kritischer Infrastrukturen
- § 8a Einführung einer IT-Aufsicht
- § 8b Meldepflicht für Beeinträchtigungen der IT-Systeme
- Öffnungsklausel

I. Regulierung - National

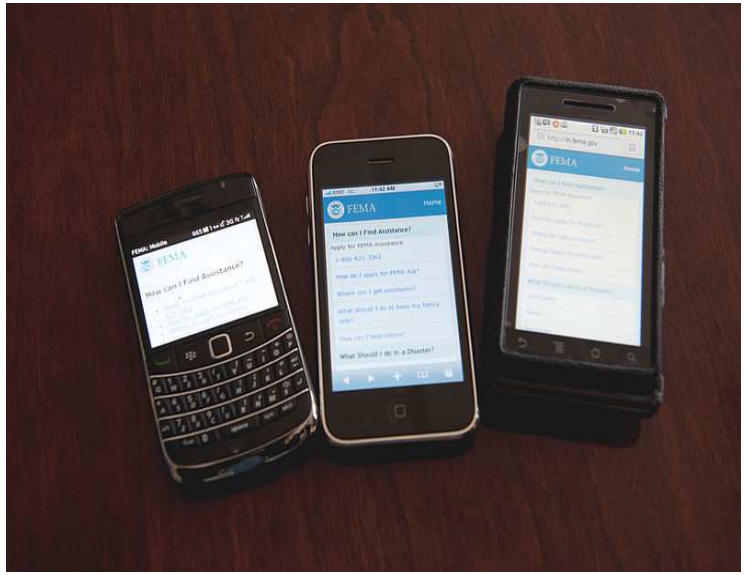
Entwurf IT-Sicherheitsgesetz des BMI

- Vermeidung von Doppelstrukturen
- § 3 Abs. 3 Beraten und Unterstützen
- § 7a Untersuchungsrecht zur IT-Sicherheit

I. Regulierung - National

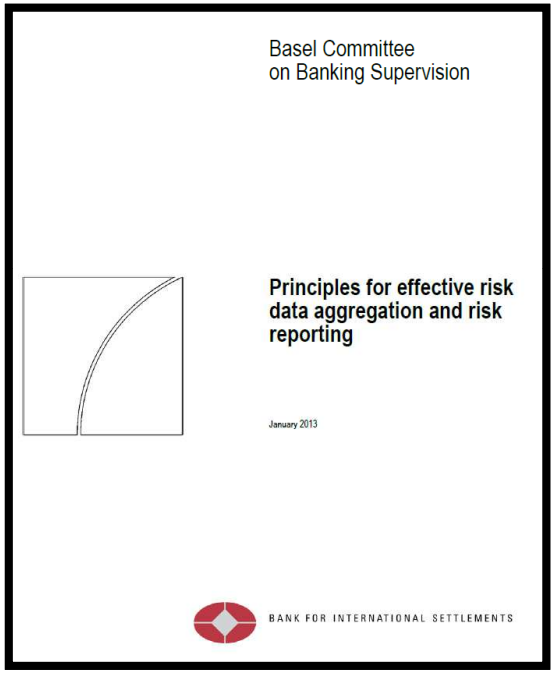
BaFin - Entwurf eines Rundschreiben „Mindestanforderungen an die Sicherheit von Internetzahlungen“

- Eins-zu-eins-Umsetzung der Empfehlungen des SecuRe Pay Forums vom 01.02.2013
- Konsultation steht bevor



I. Regulierung - National

- BaFin – Erarbeitung von Bankaufsichtlichen Anforderungen an die IT (BAIT)
- Umsetzung des Baseler Papiers „Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung“ (BCBS 239 von 2013)



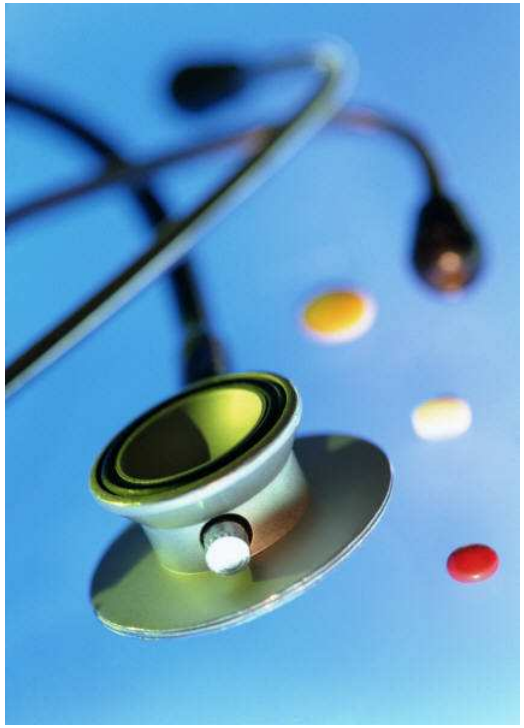
II. Aktivitäten

- IT-Grunderhebung
- Module zur IT-Prüfung
- Umfrage Notstromversorgung
- Gespräche zu Cloudcomputing
- Beobachtung einer Notfallübung

II. Aktivitäten

Heartbleed Bug

- Sichere Software unabdingbar
- Funktionierendes Patchmanagement
- stetige Gewährleistung der IT-Sicherheit



III. Einzelfragen - Rezertifizierung

- AT 4.3.1 Tz. 2 Satz 2 MaRisk
- Überprüfung von IT-Berechtigungen
- Alle Rechte
- Mind. jährlich
- Kritische Berechtigungen: Halbjährlich
- Keine eigene Schutzbedarfskategorie

III. Einzelfragen – „Altfallregelung“

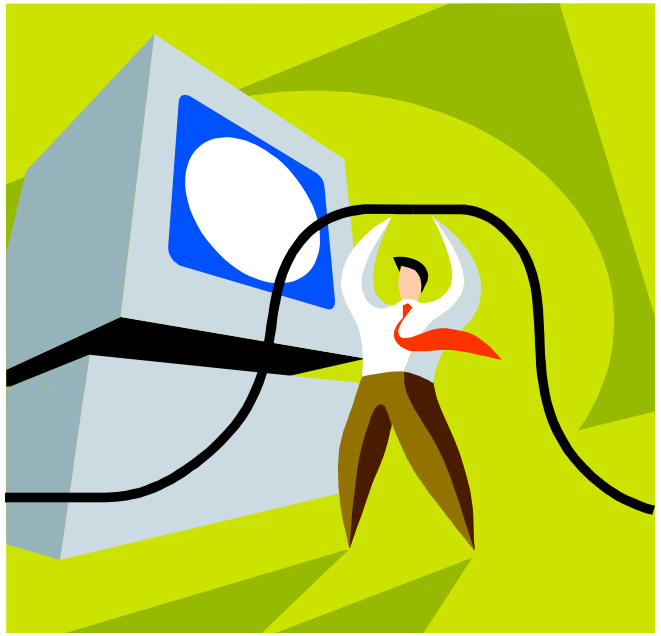
Die sogenannte „Altfallregelung“

im Schreiben vom 30.10.2007, BA 17-K 3106-2007/0010 (Begleitschreiben zur Modernisierung der Outsourcing-Regelungen und Integration in die MaRisk)

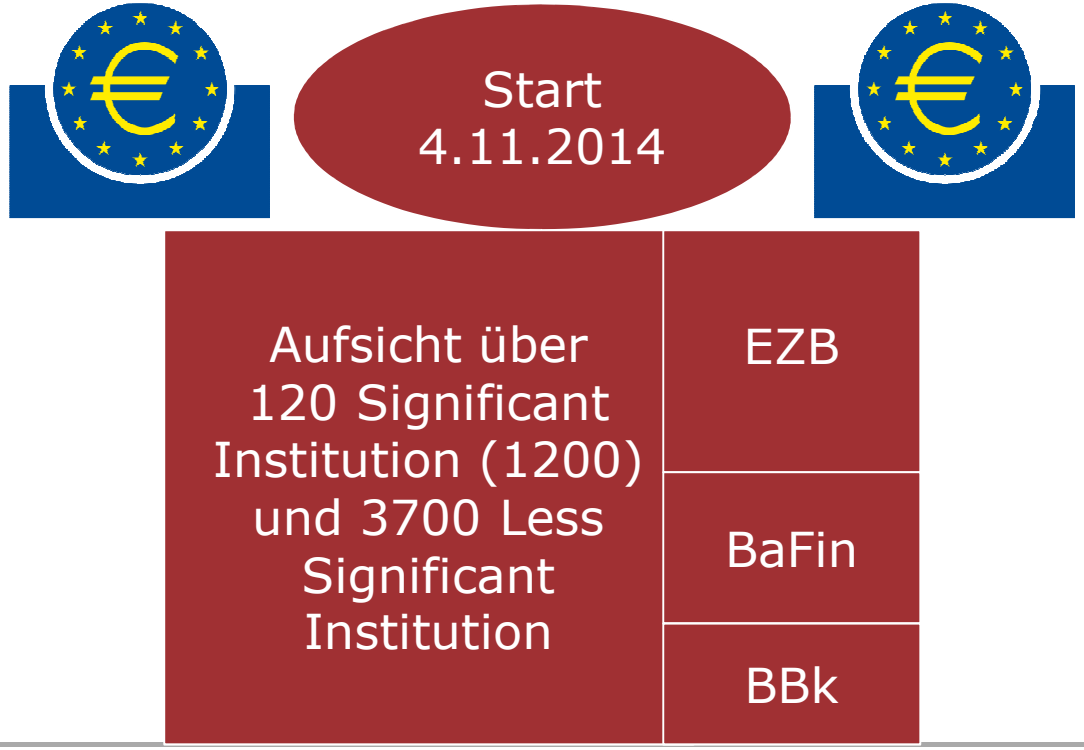
gilt nicht mehr!

III. Einzelfragen – IT-SiB

- Die Funktion des IT-Sicherheitsbeauftragten ist nicht auslagerbar
- Unterstützung durch Externe ist zulässig

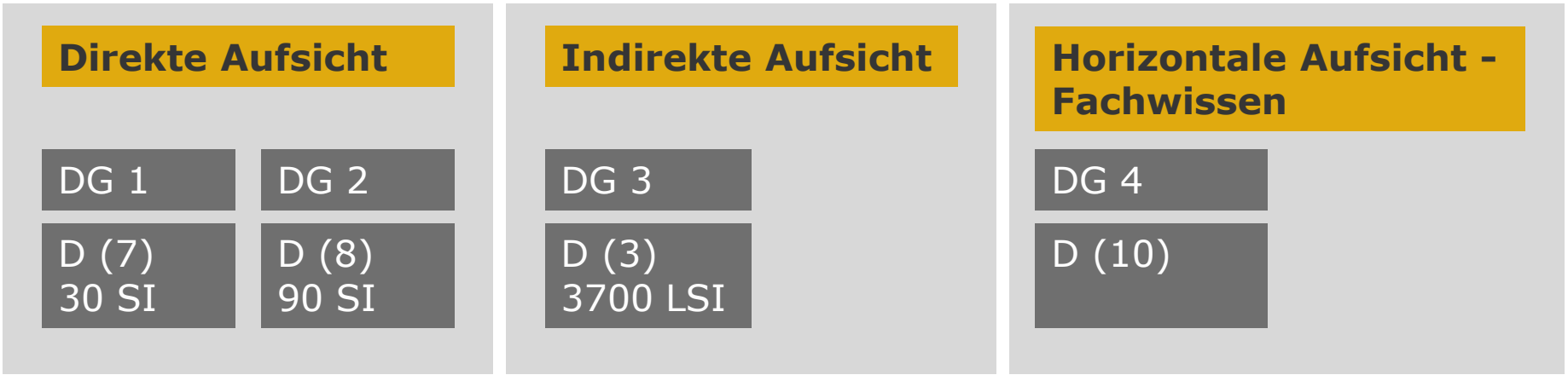


IV. Ausblick SSM



IV. Ausblick SSM - Organisation

Aufsichtsbereiche des SSM in der EZB



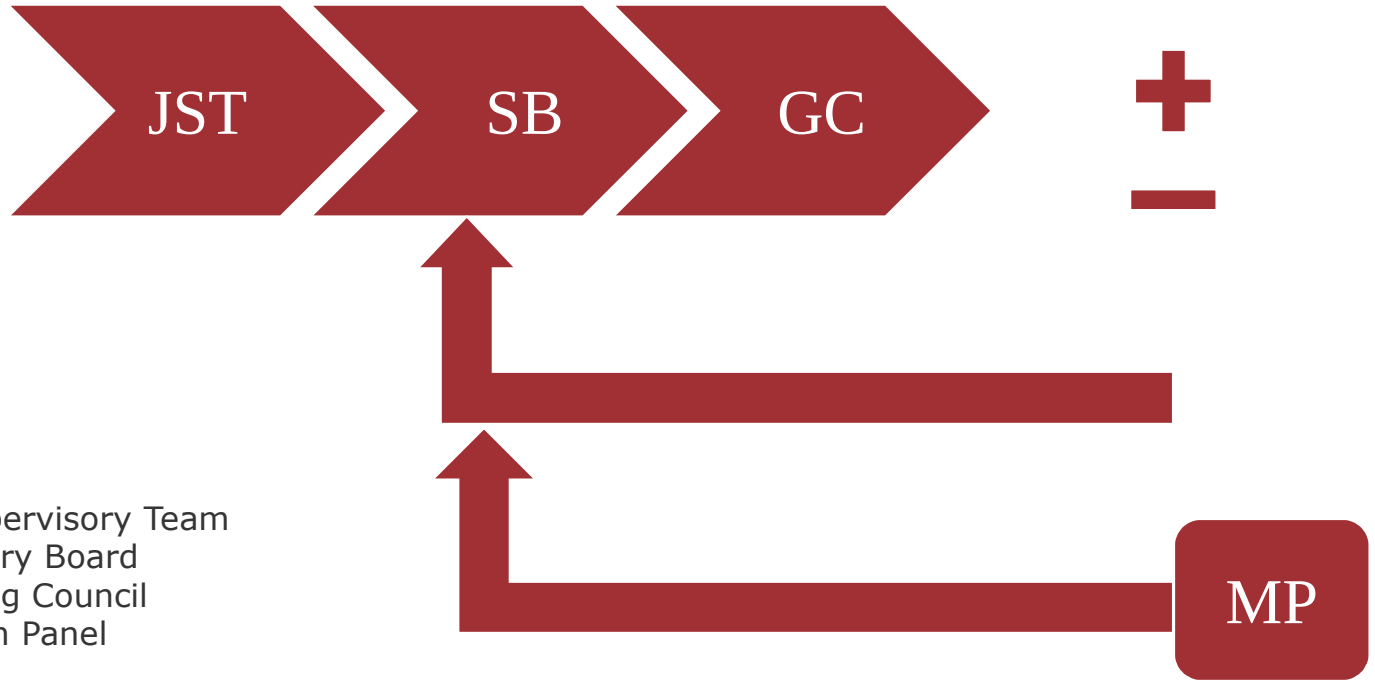
DG=Directorate General
D=Directorate

IV. Ausblick SSM - Entscheidungsprozesse

DG 4

Zulassungsverfahren	Aufsichtsplanung
Vor-Ort-Prüfungen	Aufsichtliche Grundsatzfragen
Krisenmanagement	Aufsichtliche Qualitätssicherung
Durchsetzung und Sanktionen	Risikoanalyse
Methodik u. Entwicklung von Standards	Interne Modelle

IV. Ausblick SSM - Entscheidungsprozesse



JST=Joint Supervisory Team
SB=Supervisory Board
GC= Governing Council
MP= Mediation Panel

IV. Ausblick SSM – Rechtsbehelfe

- Nationales Verfahren
- EZB-Verfahren
- Europäischer Gerichtshof

IV. Ausblick SSM – SSM-Manual

„IT risk is the current or prospective risk to earnings and capital arising from inadequate information technology and processing.“

IV. Ausblick SSM – SSM-Manual

- Verweis auf Cobit, ISO 2700X, ITIL
- Cyberkriminalität, Komplexität, Abhängigkeit
- Warten auf EBA
- Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität, Nutzerberechtigungen, Flexibilität der IT

IV. Ausblick SSM – SSM-Manual

Informations- und Datenqualitätsmanagement

- Accuracy
- Effectiveness
- Efficiency
- Quality

IV. Ausblick SSM – SSM-Manual

- IT-Risiken im Fokus der EZB
- Erfahrungen durch Sonderprüfungen Efficiency

Kontaktdaten

Dr. Josef Kokert

Bundesanstalt für Finanzdienstleistungsaufsicht

Tel. +49 (0)228 / 41 08-1806

josef.kokert@bafin.de