ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK EUROSYSTEM

IT-Risiko/IT-Sicherheit im Fokus der Bankenaufsicht

Wien, 12.Oktober 2017

Aufsicht im europäischen Kontext: FMA/OeNB, EZB und EBA

- Direkte Beaufsichtigung der **bedeutendsten Kreditinstitute** (sog. „SI“) durch die EZB
  - seit November 2014
  - „Bankenunion“: SSM und SRM
- Aufsicht der **weniger bedeutenden Kreditinstitute** („LSI“) verbleibt in nationaler Zuständigkeit (FMA und OeNB)
- Europäische Bankenaufsicht (EBA)
  - Teil des Europäischen Systems der Finanzaufsicht (ESFS)
  - Gewährleistung eines wirksamen und kohärenten Maßes an Regulierung und Beaufsichtigung im europäischen Bankensektor
  - Erstellen von technischen Standards, Leitlinien etc.

Aufsicht im europäischen Kontext: SREP

- SREP: aufsichtlicher Überprüfungs- und Bewertungsprozess
- Die Aufsicht hat demnach in regelmäßigen Abständen die folgenden Bereiche zu bewerten:
  - **Geschäftsmodell**
  - Interne Governance
  - **Kapitalrisiken**
  - Liquidität
- Ergebnis des SREP: Vorschreibung einer SREP-Gesamtkapitalquote
- Relevant im Hinblick auf IT-Risiken: EBA-Guidelines ICT risk assessment under the SREP:
  - Module Geschäftsmodell und Kapitalrisiken (operationelles Risiko)

IT-Risiko: Rechtsgrundlagen

- National:
  - § 69 Abs 2 BWG: Beaufsichtigung von operationellen Risiken
  - § 39 BWG: allgemeine Sorgfaltspflichten
  - Kreditinstitute-Risikomanagementverordnung (KI-RMV)
- Europäisch/International:
  - **Guidelines on ICT risk assessment under the SREP**
  - **Cyber Incident Reporting Framework der EZB**
  - **EBA-Recommendation on Outsourcing to Cloud Service Providers**
  - BCBS 239
  - EBA-Guideline on Incident Reporting (PSD II)
  - Richtlinie für Netzwerk- und Informationssicherheit (NIS-RL)
  - Datenschutz-Grundverordnung

Laufende Aufsicht (Off-Site)

- Öffentlich verfügbare Information
- Austausch mit Aufsichtsbehörden (Neue Bedrohungsszenarien etc.)
- Security Incident Reporting
- Questionnaires (SREP Fragebogen)
- Managementgespräche
- Informationen zur Behebung von Mängeln, die in Vor-Ort-Prüfungen festgestellt wurden

Vor-Ort-Prüfung (On-Site)

- Die laufende Aufsicht wird durch Vor-Ort-Prüfungen ergänzt
- Möglich sind Routine- und Ad-Hoc-Prüfungen; Prüfplanung erfolgt im Zusammenspiel von FMA, OeNB und (im Falle der SIs) der EZB
- Ein bestimmter Risikoaspekt wird als Prüffokus gewählt
- Themen bei Prüfungen des IT-Risikos können u.a. umfassen:
  - Datenqualitätsmanagement
  - IT-Sicherheit
  - Softwareentwicklung, Projektmanagement, Qualitätssicherung
  - IT-Outsourcing
  - IT-Risikomanagement und IT-Governance
- Prüfmethoden sind grundsätzlich standard- und technologieneutral, aber an internationalen Standards orientiert
- Für Prüfungen im Rahmen des SSM: SSM Supervisory Manual

Durchführung einer Vor-Ort-Prüfung

- Abstimmung des Prüfumfangs mit dem Auftraggeber (FMA/JST)
- Prüfvorbereitung (Verständigung, Unterlagenanforderung, Logistik)

- Formelles Eröffnungsgespräch
- Laufende Prüfung:
  - Durchsicht der bankinternen Dokumentationen
  - Gespräche mit Management und Mitarbeitern
  - Datenabzüge, Testfallanalyse/Stichproben etc.
  - Protokoll der Erkenntnisse
- Besprechung der Prüfergebnisse
- Erstellung des Prüfberichtes, Qualitätssicherung
- Schlussgespräch

- Verfolgung der Feststellungen durch die laufende Aufsicht

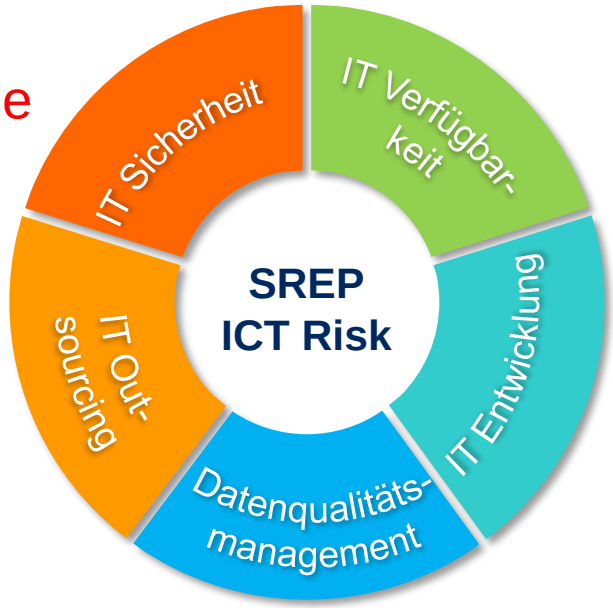
EBA GL on ICT Risk Assessment (SREP)

ICT Security Risks
- Unbefugte Zugriffe auf Daten/Systeme von innen / außen
- Inklusive physische Sicherheit (z.B. Rechenzentrums-Standorte)

Cyberresilience

ICT Availability and Continuity Risks
- IT-Betrieb
- Business Continuity Management, Ausfallsicherheit, Datensicherung

Cybercrime



ICT Outsourcing Risks
- Risiken durch inadäquate Systeme und Verfahren beim Outsourcing Dienstleister

Cloud Computing

ICT Change Risks
- Risiken durch fehlerhafte / instabile Systeme
- Projektrisiken, v.a. bei Großvorhaben

BCBS 239

ICT Data Integrity Risks
- Vollständigkeit, Richtigkeit und Konsistenz
- Primärdatenqualität (Daten in den Geschäftssystemen), Zusammenführung von Daten

Großprojekte im Bankenbereich

FinTech

Weitere Themen:
- Datenschutz
- Konsumentenschutz
- Zahlungsverkehr

PSD 2

EBA GL on ICT Risk Assessment – ICT Security Risk

- Klare Rollen und Verantwortung für das Management der IT-Sicherheit
- Angemessene Unabhängigkeit der IT Security Funktion
- Policies basierend auf international anerkannten IT Security Standards und Prinzipien
- Prozesse zur Definition, Identifikation, Implementierung und Überwachung von Sicherheitsanforderungen
- Regelmäßige und proaktive Threat Assessments
- Security Incident Management Prozesse (inkl. Eskalationsprozedere)
- Logging Mechanismen für User und Administrationsaktivitäten
- Awareness und Informationskampagnen
- Physische Sicherheitsmaßnahmen
- Spezifische Cyber Security Kontrollen (z.B. Inventory, IDS, IPS, Maßnahmen, Hardening Procedures, IT Security Testing Programm inkl. Berichterstattung an Vorstand)

IT-Risiko/IT-Sicherheit im Fokus der Bankenaufsicht