

Praxisseminar

IT-Risk

Regulatorische Anforderungen an die IT von Auslandsbanken

- **Aktuelles aus Sicht der Bankenaufsicht**
Christoph Ruckert | BaFin
 - **IT-Grundschutz bei Banken**
Daniel Gilles | Bundesamt für Sicherheit in der Informationstechnik (BSI)
 - **IT-Outsourcing und Cloud Services**
Dr. Lars Lensdorf | Covington & Burling LLP
 - **Absicherung von „Cyber-Risiken“: versichert = gesichert?**
Christoph Reiland | Berkshire Hathaway Specialty Insurance
 - **GoBD – Praxiserfahrungen bei Auslandsbanken**
Bernd Schmitt | EY
 - **Sicherheitsmaßnahmen im Zahlungsverkehr**
Dr. Mario Reichel | PPI AG
 - **Neue Regulierungen und Aufsichtstrends**
Julian Monschke | Noerr LLP
-

Moderation

Elke Weppner und Andreas Kastl | Verband der Auslandsbanken in Deutschland e.V.

Dienstag, 2. April 2019, 08:30 – ca. 17:30 Uhr

DVFA Conference-Center Frankfurt
Mainzer Landstr. 37-39 | 60329 Frankfurt am Main
(Eingang über François-Mitterrand-Platz)

Zielsetzung:

Das Seminar behandelt verschiedene aktuelle Anforderungspakete zur Abwehr von Cyberrisiken in der Finanzindustrie, die von der Bankenaufsicht als auch anderen Regulierungsbehörden und Standardsetzern erarbeitet wurden. Die Veranstaltung richtet sich unter anderem an Informationssicherheitsbeauftragte in Auslandsbanken sowie weitere Mitarbeiter der Fachbereiche IT, Compliance, Recht und gegebenenfalls die Datenschutzbeauftragten sowie die Geschäftsleitung.

Programm

08:30 bis 08:55 Uhr: Frühstücksempfang

08:55 bis 09:00 Uhr: Begrüßung

09:00 bis 10:00 Uhr

Neue Regulierungen und Aufsichtstrends

Julian Monschke | Noerr LLP

- EU Cybersecurity Act und Zertifizierungsregelungen
- Freier Verkehr nicht personen-bezogener Daten
- ENISA-Bericht zum Einsatz von Cloud Computing im Finanzsektor
- BaFin-Studie „Big Data trifft auf künstliche Intelligenz“

10:00 bis 11:00 Uhr

IT-Outsourcing und Cloud Services

Dr. Lars Lensdorf | Covington & Burling LLP

- Regulatorischer Überblick (KWG, MaRisk, BAIT, DSGVO, GwG usw.)
 - Kriterien zur Abrenzung von Auslagerung und sonstigem Fremdbezug
 - Risikoanalyse
 - Bankinterne Zuständigkeiten und Zusammenarbeit (DSB, Legal, Compliance, IT usw.)
 - RfI-/RfP-Prozess
 - Bedeutung von Zertifikaten, Standards etc. bei der Dienstleisterwahl
- Vertragliche Regelungen – was muss, was kann, was sollte vertraglich geregelt werden?
 - Typische Fallstricke: SLA, Beendigungsleistungen, etc.
- Besonderheiten bei Cloud Services
- Steuerung und Kontrolle – Auslagerungsmanagement und Verantwortlichkeiten

11:00 bis 11:30 Uhr: Kaffeepause



11:30 bis 12:30 Uhr

Aktuelles aus Sicht der Bankenaufsicht

Christoph Ruckert | BaFin

- Aufsichtsschwerpunkte 2019:
 - IT-Aufsicht und
 - IT-Sicherheit
- Überblick über "EBA draft Guidelines on ICT and security risk management"
- Ausblick auf das BAIT-Modul Notfallmanagement
- Cyberresilience Testing

12:30 bis 13:15 Uhr

GoBD – Praxiserfahrungen bei Auslandsbanken

Bernd Schmitt | EY

- Überblick über die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (**GoBD**)
- Anforderungen an ein Internes Kontrollsystem (IKS) im Hinblick auf
 - Zugangs- und Zugriffsberechtigungskontrollen
 - Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten
- IT-Anforderungen: maschinelle Auswertbarkeit, Datenzugriff durch Finanzbehörden und (elektronische) Aufbewahrungspflichten
- Auslagerung von Daten aus dem Produktivsystem und Systemwechsel
- Exkurs: Auslagerung der Buchführung, § 146 AO

13:15 bis 14:15 Uhr: Mittagessen

14:15 bis 15:00 Uhr

Absicherung von „Cyber-Risiken“: versichert = gesichert?

Christoph Reiland | Berkshire Hathaway Speciality Insurance

- Klassische Informationssicherheits-Risiken im Finanzdienstleistungssektor
- Mögliche Auswirkungen von Breaches, Hacks etc.
- Risikomanagement/Vorbereitung auf den Ernstfall
- Versicherbare Risiken/Cyber-Versicherungen
- Individueller Bedarf beim Management von Cyber-Risiken/Versicherungsschutz

15:00 bis 15:30 Uhr: Kaffeepause

15:30 bis 16:30 Uhr

IT-Grundschutz bei Banken

Daniel Gilles | Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Aufbau des IT-Grundschutzkonzepts
 - BSI-Standard 200-1: Managementsystem für Informationssicherheit (ISMS)
 - BSI-Standard 200-2: IT-Grundschutz-Methodik
 - BSI-Standard 200-3: Risikomanagement
 - BSI-Standard 200-4: BCM (Entwurf)
- IT-Grundschutz-Kompodium
- Anwendung durch Banken und andere Finanzdienstleister

16:30 bis 17:30 Uhr

Sicherheitsmaßnahmen im Zahlungsverkehr

Dr. Mario Reichel | PPI AG

- Überblick über aktuelle Sicherheitsmaßnahmen im Zahlungsverkehr mit IT-Bezug:
 - PSD II
 - SWIFT Customer Security Programme (CSP)
 - Risk Management Annex (RMA) gemäß EPC-Rulebooks
 - Anforderungen an kritische und nicht-kritische Teilnehmer an TARGET2

17:30 Uhr: Abschließende Diskussion und Verabschiedung