

## Hybrides Seminar

---

# Gap-Analyse BAIT/DORA für Auslandsbanken und ausländische Wertpapierinstitute

---

- IKT-Risikomanagement in Finanzinstituten  
Christian Moerler | Severn Consultancy GmbH
  - Informationssicherheit im Rahmen des IKT-Risikomanagements  
Norman Nehls | Severn Consultancy GmbH
  - Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle  
Jan Pohle | DLA Piper UK LLP
  - Testen der digitalen operationalen Resilienz (TLPT)  
Christoph Edinger | EY
  - Management des IKT-Drittparteienrisikos  
Dr. Jens H. Kunz und Julian Monschke | Noerr Partnerschaftsgesellschaft mbB
  - Regelungen zum Informationsaustausch, weitere regulatorische Änderungen und Fortbestand der BAIT  
Andreas Kastl | Verband der Auslandsbanken in Deutschland e.V.
- 

### Referent

Weitere Informationen zu unseren Referenten haben wir [hier](#) für Sie bereitgestellt.

### Moderation

Andreas Kastl | Verband der Auslandsbanken in Deutschland e.V.

---

**Mittwoch, 29. März 2023, 9:00 – 16:00 Uhr**

Mövenpick Hotel Frankfurt City  
Den Haager Str. 5 | 60327 Frankfurt

Den Online-Teilnehmern werden die Einwahldaten  
am Veranstaltungstag 30 Minuten vor Beginn zugesandt.

---

---

## Zielsetzung

Zu den [Risiken im Fokus der BaFin 2023](#) gehören unter anderem Risiken aus Cyberattacken mit gravierenden Auswirkungen, und hierin erkennt die BaFin darüber hinaus ein erhöhtes Risiko durch Auslagerungen. Daher sind die BaFin-beaufsichtigten Auslandsbanken und ausländischen Wertpapier- und Finanzinstitute in Deutschland gefordert, ihre Fähigkeiten zur Bewältigung von IKT-Risiken zu stärken und sich auf **DORA**, die am 17. Januar 2025 in Kraft tretende [Verordnung \(EU\) 2022/2554](#) über die digitale operationale Resilienz im Finanzsektor, bestmöglich vorzubereiten.

Die Veranstaltung richtet sich insbesondere an die Informationssicherheitsbeauftragten in den Auslandsbanken sowie an weitere Mitarbeiter der Fachbereiche IT, Compliance, Recht, und gegebenenfalls auch an die Datenschutzbeauftragten sowie an Geschäftsleitungsmitglieder.

---

## Anmeldung

Die Anmeldung ist über die [Homepage](#) des Verbands möglich.

**Anmeldefrist für Präsenz-Teilnehmer: 22.03.2023**

**Anmeldefrist für Online-Teilnehmer: 27.03.2023**

---

## Teilnahmebedingungen

### Online

Der Seminarpreis beträgt:

**EUR 490** zzgl. MwSt. [für [Mitglieder](#)]

**EUR 590** zzgl. MwSt. [für Nichtmitglieder]

Darin enthalten ist die Online-Teilnahme am Veranstaltungstag. Der Online-Zugriff auf die elektronischen Tagungsunterlagen werden den Teilnehmern am Tag vor dem Seminar zur Verfügung gestellt. Der Online-Zugriff nach der Veranstaltung besteht einen Monat lang.

Nach Eingang der Anmeldung erfolgt eine Bestätigung. Bei Stornierung bis 14 Tage vor Veranstaltungstermin wird eine Bearbeitungsgebühr in Höhe von EUR 119 zzgl. MwSt. berechnet. Bei Nichtteilnahme am Online-Seminar wird die gesamte Teilnahmegebühr erhoben. Eine Vertretung des angemeldeten Teilnehmers ist ohne zusätzliche Kosten bis 24 Stunden vor Seminarbeginn möglich. Grundsätzlich sind nur die gesamte Veranstaltung und nicht einzelne Veranstaltungsteile buchbar. Programmänderungen sind vorbehalten.

### Präsenz

Der Seminarpreis beträgt:

**EUR 790** zzgl. MwSt. [für [Mitglieder](#)]

**EUR 990** zzgl. MwSt. [für Nichtmitglieder]

Darin enthalten sind Pausenbewirtung mit Erfrischungsgetränken sowie der Online-Zugriff auf die elektronischen Tagungsunterlagen am Tag vor dem Seminar. Der Online-Zugriff nach der Veranstaltung besteht einen Monat lang. Anmeldungen werden der Reihenfolge nach berücksichtigt.

Nach Eingang der Anmeldung erfolgt eine Bestätigung. Bei Stornierung bis 14 Tage vor Veranstaltungstermin wird eine Bearbeitungsgebühr in Höhe von EUR 119 zzgl. MwSt. berechnet. Bei Rücktritt oder bei Nichterscheinen am Seminartag wird die gesamte Teilnahmegebühr erhoben. Eine Vertretung des angemeldeten Teilnehmers ist ohne zusätzliche Kosten bis 24 Stunden vor Seminarbeginn möglich. Eine Änderung der Präsenz-Teilnahme auf eine Online-Teilnahme ist bis 7 Tage vor Veranstaltungstermin kostenfrei möglich. Grundsätzlich sind nur die gesamte Veranstaltung und nicht einzelne Veranstaltungsteile buchbar. Programmänderungen sind vorbehalten.

---

## Programm

### 08:30 Uhr bis 08:55 Uhr: Frühstücksempfang/Digitales Onboarding

### 08:55 Uhr bis 09:00 Uhr: Begrüßung

09:00 Uhr bis 09:45 Uhr

#### **Management des IKT-Drittparteirisikos**

Dr. Jens H. Kunz und Julian Monschke | Noerr Partnerschaftsgesellschaft mbB

- Management des IKT-Drittparteirisikos (Kapitel V DORA)
  - Schlüsselprinzipien für ein solides Management des IKT-Drittparteirisikos: Allgemeine Prinzipien (Art. 28) und Grundsatz der Verhältnismäßigkeit (Art. 4 Abs. 2)
  - Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene (Art. 29)
  - Wesentliche Vertragsbestimmungen (Art. 30)
  - Überwachungsrahmen für kritische IKT-Drittdienstleister, insb. Einstufung kritischer IKT-Drittdienstleister (Art. 31) und Auswirkungen für auf Auslandsbanken und ausländische Finanzinstitute in Deutschland und deren Gruppen
  - Ausblick auf die künftige Regulierungsstandards

### 09:45 Uhr bis 10:00 Uhr: Kurze Pause

10:00 Uhr bis 10:45 Uhr

#### **Testen der digitalen operationalen Resilienz (TLPT)**

Christoph Edinger | EY

- Die Entwicklung von Cyberrisiken und regulatorischer Anforderungen
- Digital Operational Resilience Act (DORA)
- Testen der digitalen operationalen Resilienz (Kapitel IV DORA)
  - DORA-Anforderungen bzgl. des Testen der digitalen operationalen Resilienz (Kapitel IV. Art. 24, Art. 25, Art. 26 & Art. 27)
  - Fokusthema: Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT (Art. 26)
  - TIBER-EU als Rahmenwerk zur Erfüllung der DORA-Anforderungen
- Ausblick: Weiterentwicklung von DORA in den kommenden Jahren

### 10:45 Uhr bis 11:00 Uhr: Kurze Pause

11:00 Uhr bis 11:45 Uhr

### **IKT-Risikomanagement in Finanzinstituten**

Christian Moerler | Severn Consultancy GmbH

- Anforderungen an das IKT-Risikomanagement (Kapitel II DORA)
  - **Verantwortung und Aufgabenbereiche der Geschäftsleitungen/Leitungsorgane** der Finanzunternehmen im Rahmen von Governance und Organisation (Art. 5) im Vergleich zur IT-Strategie und IT-Governance (Kapitel 1 und 2 BAIT)
  - IKT-Risikomanagementrahmen Art. 6), Grundsatz der Verhältnismäßigkeit (Art. 4 Abs. 1 und 3), im Vergleich mit dem Informationsrisikomanagement nach Kapitel 3 BAIT
  - Anforderungen an IKT-Systeme, -Protokolle und -Tools (Art. 7),
  - Identifizierung (Art. 8) der IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten, die Informations- und IKT-Assets, die diese Funktionen unterstützen, sowie deren Rollen und Abhängigkeiten hinsichtlich der IKT-Risiken, im Vergleich zum Informationsverbund und Schutzbedarf (BAIT)
- Fokusthema **Risikomanagement auf Gruppenebene** (Taxonomie, KPI, ) und Auswirkungen auf Auslandsbanken und ausländische Finanzinstitute in Deutschland
- Ausblick auf die künftige Regulierungsstandards

**11:45 Uhr bis 12:00 Uhr: kurze Pause**

12:00 Uhr bis 12:45 Uhr

### **Informationssicherheit im Rahmen des IKT-Risikomanagements**

Norman Nehls | Severn Consultancy GmbH

- Informationssicherheit im Rahmen des IKT-Risikomanagements (Kapitel II DORA)
  - Schutz und Prävention (Art. 9) im Vergleich mit Informationssicherheitsmanagement nach Kapitel 4 BAIT: Informationssicherheitsleitlinie und IKT-Sicherheitsrichtlinien
  - **Die Zukunft des Informationssicherheitsbeauftragten (BAIT)**
  - Erkennung anomaler Aktivitäten (Art. 10) im Vergleich zum Erkennen von Gefährdungen des Informationsverbundes gemäß der operativen Informationssicherheit gemäß Kapitel 5 BAIT
  - **Reaktion und Wiederherstellung** (Art. 11): IKT-Geschäftsfortführungsleitlinie und Business-Impact-Analyse (BIA), Richtlinie und Verfahren zum Backup (Datensicherung) sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung (Art. 12) und Vergleich mit (IT-)Notfallmanagement nach MaRisk/BAIT
  - Anforderungen an die Kommunikation (Art. 14)

**12:45 Uhr bis 14:00 Uhr: Mittagspause**

14:00 Uhr bis 14:45 Uhr

## **Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle**

Jan Pohle | DLA Piper UK LLP

- Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III DORA)
  - Grundsatz der Verhältnismäßigkeit (Art. 4 Abs. 2),
  - Prozess für die Behandlung IKT-bezogener Vorfälle (Art. 17)
  - Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen (Art. 18)
  - Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen (Art. 19), Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen (Art. 23) und Vergleich mit BaFin- Rundschreiben 03/2022 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle gemäß § 54 Abs. 1 ZAG
  - Harmonisierung von Inhalt und Vorlagen von Meldungen (Art. 20), Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle (Art. 21)
- Vergleich mit § 54 ZAG über zahlungsbezogene Vorfälle und mit § 24 KWG über auslagerungsbezogene Vorfälle (FISG; [BaFin-Template](#) zur Meldung über schwerwiegende Vorfälle)
- Ausblick auf die künftige Regulierungsstandards

### **14:45 Uhr bis 15:00 Uhr: kurze Pause**

15:00 Uhr bis 15:45 Uhr

## **Regelungen zum Informationsaustausch, weitere regulatorische Änderungen und Fortbestand der BAIT**

Andreas Kastl | Verband der Auslandsbanken in Deutschland e.V.

- Vereinbarungen über den Austausch von Informationen (Kapitel VI DORA),
  - Austausch von Erkenntnissen zu Cyberbedrohungen (Art. 45)
  - Gruppeninterner Austausch vs. externer Austausch
- Auswirkungen der Änderungsrichtlinie (EU) 2022/2556 vom 14. Dezember 2022 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor
  - SREP und DORA,
  - PSD2- Anpassungen,
  - Auswirkungen für Wertpapierfirmen
- Interaktionen von DORA mit NIS2, CER, CRA
- Fortbestand der BAIT, insbesondere IT-Projekte und Anwendungsentwicklung und IT-Betrieb

### **15:45 Uhr: abschließender Bericht aus der Verbandsarbeit des VAB**

### **16:00 Uhr: Abschließende Diskussion und Verabschiedung**