24. März 2026 · 9:00–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

# Anforderungen an IT-Infrastruktur und IT-Btrieb unter DORA

## Banken-Aufsicht-Seminar · 8 CPE-Punkte

- **Konkrete Aufsichts-Erwartungen aus MaRisk, DORA & EBA-ICT-GL**
- **Häufige Fragestellungen/identifizierte Schwachstellen in der Praxis**
- **Anforderungen an das (toolunterstützte) Identifizieren und die Behandlung von Schwachstellen**
- **Anforderungen an die Durchführung regelmäßiger PenTests**
- **SIEM-Administration und SIEM-Meldungen innerhalb eines SOC**
- **Anforderungen an das ITSCM/BCM und die Abstimmung mit den IKT-Dienstleistern**

**Referenten**

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, aktuell SAP Systemservices Architektur, Zentrale IT-Plattform-management Drittprodukte, Bundesbank, Düsseldorf

Marcus Schmidt, MBA, CISA, CISM, CGEIT
Leiter IT-Governance
Sparkasse Krefeld

Jan-Philipp Küsters, Referent Operative Informationssicherheit im Bereich IT-Governance, Sparkasse Krefeld

Pasquale Totaro, CISA
Leiter Revision IT
DekaBank, Frankfurt/Main

## Programm

**Alexander Lohr, Bundesbank** · 9:00–12:00 Uhr

Konkrete Erwartungen der Aufsicht an ausgewählte Themen der operativen Informationssicherheit aus MaRisk und DORA

- Konkretisierung der Anforderungen der MaRisk und DORA
- Identifikation, Bewertung und Behandlung von Schwachstellen. Anforderungen an die Nutzung eines Schwachstellenscanners (Netzwerkscan/authentifizierter Scan)
- Umgang mit Schwachstellen im Schwachstellenmanagement, Bündelung und Priorisierung, Reporting und Übertragung in das Risikomanagement
- Notwendigkeit regelmäßiger Penetrationstests: Angriffsszenarien, Root-Cause-Analyse, Bewertung der Ergebnisse
- Einsatz eines SIEM-Systems, notwendige Loganbindungen, Anforderungen an die Qualität der Logs und Speicherfristen, Entwicklung von Use Cases
- Security Operations Center (SOC), 24/7 Überwachung, Reporting von SIEM-Alarmen
- Schutz vor Schadsoftware, Datenabfluss, Verschlüsselung, Vorstellung klassischer Datenabflusskanäle
- Management zulässiger Software und IDV, Entwickler-Clients, administrative Benutzer und Skriptausführung
- IKT-Dienstleister – Prozesstransparenz und Steuerbarkeit
- Identifizierte Schwachstellen aus aktuellen Prüfungen

**Jan-Philipp Küsters & Marcus Schmidt, Sparkasse Krefeld**
13:00–14:45 Uhr

Ganzheitliches Schwachstellenmanagement im IT-Betrieb: Sicherstellung der DORA- Governance und operative Umsetzung in der Infrastrukturpraxis

- Governance: Klare Verantwortlichkeiten zwischen IT-Governance, IT-Betrieb, Informationssicherheitsmanagement (ISM) und Dienstleistern
- Aufbau und Pflege eines IT-Asset- und Servicekatalogs als Fundament für die Priorisierung von Schwachstellen
- End-to-End Vulnerability Management Lifecycle – Integration in bestehende Kontroll- und Meldeprozesse
- CVSS als zentrales Bewertungsinstrument – Nutzung von CVSS für einheitliche technische Risikobewertungen
- Tool- und Scanlandschaft in der Praxis – Zusammenspiel aus Netzwerk-, Endpoint-, Cloud- und Applikationsscannern; Umgang mit proprietären Systemen und fehlender Scanbarkeit in spezialisierten Bankumgebungen
- Risikoorientierte Priorisierung nach DORA-Vorgaben
- Reporting, KPIs & kontinuierliche Verbesserung – Aufbau eines standardisierten Berichtswesens

**Pasquale Totaro, DekaBank** · 15:00–17:00 Uhr

IT-Infrastrukturen und operativer IT-Betrieb in Banken: Herausforderungen, Prüfungsansätze und Erfahrungen aus der Praxis der Internen Revision

- Konkretisierung der Aufsichts-Anforderungen an die IT-Infrastruktur und den operativen IT-Betrieb u. a. in MaRisk, BAIT und IKT-Leitlinien
- Praxiserfahrungen zu den regulatorischen Anforderungen an den IT-Betrieb und dem Umgang mit Auslagerungen
- Prüfung der IT-Infrastruktur durch die (IT-)Revision:
  - Herausforderung: Was gehört zur IT-Infrastruktur einer Bankengruppe?
  - Prüfung der Configuration Management Database und zugehöriger Prozesse
  - Wie können Cloud Anbieter von der Internen Revision berücksichtigt werden?
- Wie können bei Revisionsprüfungen die 1st/2nd line und die Schnittstellen zu ext. DL einbezogen werden?
  - Umgang mit Feststellungen von wesentlichen IT-DL
  - Erkenntnisse aus Prüfungen von Rechenzentren im In- und Ausland bei Auslagerungen und den zugehörigen Subdienstleistern
  - Rolle des Auslagerungsmanagements, ISM und IRM
- Prüfung des operativen IT-Betriebs durch die IT-Revision
- Häufige Prüfungsfeststellungen der Internen Revision, Prüfungsansätze, Erkenntnisse und Praxis-Tipps

## Seminarziel

Die neuen DORA-Anforderungen haben weitreichende Auswirkungen auf den Bereich der operativen Informationssicherheit – insbesondere nach dem Wegfall der BAIT – um die IT-Infrastruktur zu schützen und einen sicheren IT-Betrieb zu gewährleisten. Der Einsatz eines Security Information and Event Management (SIEM)-Systems sowie eines Schwachstellenscanners sind unabdingbar für die Erfüllung eines hohen Schutzbedarfes für sicherheitskritische IT-Systeme. Dementsprechend wachsen auch die aufsichtlichen Anforderungen an die von den Instituten verantworteten IT-Systeme.

Wesentliche Feststellungen in dem Bereich der operativen Informationssicherheit zeigen, dass für viele Institute ein Nachholbedarf bei der Erfüllung der aufsichtlichen Anforderungen haben. Nicht nur die reine Identifikation möglicher Schwachstellen, sondern auch deren Behebung setzt die Informationssicherheit, nicht zuletzt auch aufgrund der stetig wachsenden IT-Landschaft, vor große Herausforderungen, die mit dem Informationsrisikomanagement in Einklang gebracht werden müssen.

Auch eingebundene Dienstleister müssen die Anforderungen einhalten und von der Informationssicherheit überwacht werden. Die (IT-)Revision hat die Einhaltung der in den MaRisk und DORA verankerten Anforderungen entsprechend zu prüfen.

## Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche mit IT-Bezug sowie andere interessierte Fach- bzw. Grundsatzbereiche, Vorstandsmitglieder/ Geschäftsleitung, externe Prüfer*innen sowie Bankdienstleister.

## Unsere Referenten

**Alexander Lohr**
Ehem. Bankgeschäftliche IT-Prüfungen, SAP Systemservices Architektur, Zentrale, IT-Plattformmanagement Drittprodukte, Deutsche Bundesbank*

*Alexander Lohr ist studierter Wirtschaftsinformatiker und arbeitet seit über 12 Jahren bei der Bundesbank. Mehrere Jahre war er als Prüfer im Rahmen von bankgeschäftlichen IT-Prüfungen bei Banken und Sparkassen im Einsatz. Zuvor war er als Programmierer sowie als IT- und Cloud-Architekt für die Bundesbank tätig. Zudem ist er projektbezogen für die Europäische Zentralbank (EZB) tätig.*

**Jan-Philipp Küsters**
Referent Operative Informationssicherheit im Bereich IT-Governance Sparkasse Krefeld*

*Jan-Philipp Küsters ist seit 2024 Referent für Operative Informationssicherheit im Bereich IT-Governance bei der Sparkasse Krefeld. Davor war er als Spezialist IT-Organisator im Bereich IT-Infrastruktur tätig. Als Mitglied im DORA-Projekt hat er die Umsetzung der Themen IKT-Vorfallsmanagement, Protokollierung, Schwachstellen-management, Cyberbedrohungen und Testmanagement verantwortet und ist auch weiterhin für diese Themen verantwortlich.*

**Marcus Schmidt, MBA, CISA, CISM, CGEIT**
Leiter IT-Governance, Sparkasse Krefeld*

*Marcus Schmidt ist Leiter IT-Governance bei der Sparkasse Krefeld. Davor war er in den Bereichen Steuerung, Strategie, Informationssicherheit und Notfallmanagement tätig. Er ist verantwortlich für die Erstellung der IT-Strategie sowie die Überwachung der Einhaltung von KPI und KRI. Als Projektleiter leitete er das Projekt DORA in der Sparkasse Krefeld.*

**Pasquale Totaro, CISA**
Leiter Revision IT, DekaBank*, Frankfurt/Main

*Pasquale Totaro ist Leiter der IT-Revision der DekaBank und besitzt mehr als 20 Jahre Erfahrung im Bereich der Prüfung von IT, IT-Infrastruktur und des IT-Betriebs. Vor seiner Zeit bei der DekaBank war er für eine große Wirtschaftsprüfungsgesellschaft tätig. Datendiebstahl etc.). Zudem berät er Mandanten zur Cyber-Security Prävention (wie aktuell NIS-2) und der Vermeidung bzw. Abwehr von Cybercrime-Attacken.*

**Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht notwendigerweise die eines bestimmten Instituts, der Deutschen Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wider. Die Referenten geben auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte wider.*

DORA-konformes IKT-Risikomanagement
4./5. Februar 2026, Online-Veranstaltung

IKT-Governance im Fokus der Aufsicht
10. Februar 2026, Online-Veranstaltung

DORA-konforme Notfall-Konzepte und BCM-Prozesse unter Einbindung der (IKT-)Drittdienstleister
25. Februar 2026, Online-Veranstaltung

DORA-konformer Umgang mit Eigen-Anwendungen und IDV
2. März 2026, Online-Veranstaltung

TPRM Spezial: Umgang mit „Software as a Service" (SaaS) und Cloud-Diensten unter DORA
4. März 2026, Online-Veranstaltung

Zertifikats-Lehrgang Auslagerungsmanagement (MaRisk) & IKT-Dienstleistersteuerung (DORA)
11. bis 13. März 2026, Online-Zertifikats-Lehrgang

Prüfung DORA & DORA-Umsetzung
16./17. März 2026, Online-Veranstaltung

▶ Diese und weitere Seminar-Angebote finden Sie bei uns online unter *www.akademie-heidelberg.de/online-seminare*

## Zusätzliche Informationen

Fragen zu diesen Schulungen oder unserem gesamten Seminar-Programm beantworte ich Ihnen sehr gerne.

Björn Wehling
Telefon 06221/65033-44
b.wehling@akademie-heidelberg.de

## Anmeldeformular

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA

Name

Vorname

Position

Firma

Straße / Nr.

PLZ / Ort

Telefon

E-Mail

Name der Assistenz

Datum / Unterschrift

Senden Sie Ihre Anmeldung bitte an: **anmeldung@akademie-heidelberg.de**

### Termin und Seminarzeiten

Dienstag, 24. März 2026
9:00–17:00 Uhr
Online-Zugang ab 8:45 Uhr

Seminar-Nr. 26 03 BA 145 W

### Teilnahmegebühr

€ 780,– (zzgl. gesetzl. USt)

Die Gebühr beinhaltet die Teilnahme am Online-Seminar sowie die Präsentation als PDF-Datei.
Im Anschluss an das Seminar erhalten Sie ein Zertifikat, das Ihnen die Teilnahme an der Fortbildung bestätigt.

### Allgemeine Geschäftsbedingungen

Es gelten unsere Allgemeinen Geschäftsbedingungen (Stand: 01.01.2010), die wir Ihnen auf Wunsch gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: www.akademie-heidelberg.de/agb

### Zum Ablauf

- Vor dem Seminartag erhalten Sie von uns eine E-Mail mit einem Link, über den Sie sich direkt in die Online-Veranstaltung einwählen können.
- Für Ihre Teilnahme ist es nicht notwendig, ein Programm herunterzuladen. Sie können am Seminar direkt per *Zoom* im Browser teilnehmen.
- Über Ihr Mikrofon und Ihre Kamera können Sie jederzeit Fragen stellen und mit den Referierenden und weiteren Teilnehmenden diskutieren. Alternativ steht auch ein Chat zur Verfügung.

**AH Akademie für Fortbildung Heidelberg GmbH**
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de

12.25 / 2603BA145