

# DORA Spezial: Informationssicherheit und IKT-Risikomanagement



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

- **Erfahrungsbericht aus einer BaFin-Prüfung mit Fokus Informationssicherheit und IKT-Risikomanagement**
- **DORA: von der Informationssicherheit zum IKT-Risikomanagement**
- **Neue Pflichten des (ISB), Einführung der IKT-Risikokontrollfunktion**
- **Erweiterte Anforderungen (TPRM) an die Nutzung von IKT-Dienstleistern und Cloud-Services**
- **Anforderungen an die Informationssicherheit und das IKT-Risikomanagement beim Einsatz von Künstlicher Intelligenz (KI)**

TOP-Aktuelle  
Praxis-Hinweise und  
Umsetzungs-Tipps!

**20** Jahre  
**AKADEMIE  
HEIDELBERG**

### Referenten



Mike Bona-Stecki  
Leiter Informationssicherheit und  
Business Continuity Management  
DekaBank Deutsche Girozentrale, Frankfurt



Stephan Wirth  
Informationssicherheits- und  
Datenschutzbeauftragter  
NRW.BANK, Düsseldorf

## Programm

**Stephan Wirth, NRW.BANK** · 9:00–10:30 Uhr

Verschärfte Anforderungen aus DORA:  
Informationssicherheit und Informationsrisikomanagement im Spannungsfeld zwischen Regulatorik und Praxis

- Etablierung eines angemessenen IKT-Risikomanagements: IKT-Risiken und Cyber-Risiken stärker im Fokus
- Akzentverschiebung durch DORA: Einführung einer IKT-Risikokontrollfunktion
- Herausforderungen des IKT-Drittpartei-Risikomanagements
- Operative IKT-Sicherheit: Umsetzungsstand und (weiterhin) bestehende Schwachstellen
- Verschärfte Anforderungen an die Datenqualität
- Konkrete Anforderungen an IKT-Projekte und Anwendungsentwicklung/IDV/IT-Inventare, Berechtigungsmanagement und Schutzbedarf
- Hinweis zur DORA-Umsetzung in der Praxis

**Mike Bona-Stecki, DekaBank** · 10:45–12:15 Uhr

Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog und einem höheren Informationssicherheitsniveau

- Ziel und Nutzen der Strukturanalyse, Schutzbedarfsfeststellung, Sollmaßnahmenkataloge und Risikoanalyse
- Gängige Standards: ISO 27.XXX-Reihe, BSI-Standards
- Erhebung des Informationsverbunds: Identifikation und Gruppierung der IT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- Schutzbedarfsfeststellung auf Informations- und Prozessebene
- Erarbeitung des Sollmaßnahmenkatalogs auf Basis der Schutzbedarfsanalyse, Strukturanalyse und gängigen Standards
- Darstellung der Rollen und Zuständigkeiten
- Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog und wie bewerte ich Soll-Ist-Abweichungen?

**Stephan Wirth, NRW.Bank** · 13:15–14:45 Uhr

Neue Pflichten des Informationssicherheitsbeauftragten (ISB) und Einführung der IKT-Risikokontrollfunktion

- Konkretisierung der Verantwortlichkeiten und der Aufgabenbereiche – neue Rechte und Pflichten; inwieweit ist die IKT-Risikokontrollfunktion auslagerbar?
- Wie unterstützen ISB und Risikokontrollfunktion bei der Erstellung von Strategien, Leitlinien und Prozessen zur Erreichung einer angemessenen DORA-Compliance?
- Unterstützung der Fachbereiche bei der DORA-Umsetzung
- Ermittlung von IKT-Risiken und Auswirkungsanalyse
- Best Practices und Standards für ein praxisnahes und effektives IKT-Risikomanagement
- Management von Informationssicherheitsvorfällen: Zeitnahe Analyse der Auswirkungen und Veranlassung angemessener Nachsorgemaßnahmen; verschärfte Meldepflichten aus DORA

**Mike Bona-Stecki, DekaBank** · 15:00–17:00 Uhr

Erweiterte Anforderungen an IT-Auslagerungen (DORA, BAIT, AI-Act), IKT-Drittdienstleistungen (DORA) und Cyber-Security aus dem Blickwinkel der Informationssicherheit

- Abgrenzung DORA- zu MaRisk-Anforderungen
- Umgang mit Cyberrisiken bei Auslagerungen und deren Verzahnung mit dem Non Financial Risk-Management
- Beurteilung von IT- und Informationssicherheits-Risiken im Rahmen des Auslagerungsprozesses
- Umgang mit besonderen Herausforderungen und Risiken bei dem Bezug und der Nutzung von Cloud-Services
- Anforderungen an die vertraglichen Regelungen zur Informationssicherheit bei Auslagerungen
- Business Continuity Management im Kontext von Auslagerungen und Fremdbezug von IT-Dienstleistungen – Aufrechterhaltung der Kontinuität und Qualität der Geschäftstätigkeiten
- Umsetzungshinweise und Praxistipps

## Seminarziel

Gestiegene IT-(Dienstleister-)Risiken, Cyber-Angriffe und Lücken in der Informationssicherheit führen zunehmend häufiger zu Ausfällen kritischer Geschäftsprozesse bei Banken und deren Dienstleistern. Insbesondere Angriffe von außen haben sich hierbei zu einer immanenten Bedrohung entwickelt.

Durch die geplante MaRisk-Novelle 2025 und die neuen DORA-Anforderungen kommen weitreichende zusätzliche Regelungen in den Bereichen Informationssicherheit und Informationsrisikomanagement hinzu, um Ausfälle des Geschäftsbetriebs zu vermeiden.

Die Aufsicht erwartet zusätzliche (Sicherheits-)Maßnahmen der Institute. Damit einher gehen somit auch die erweiterten Aufgaben und Verantwortlichkeiten des Informationssicherheitsbeauftragten (ISB).

Auch Cloud-Dienstleistungen sind aus dem Blickwinkel der Informationssicherheit zu beurteilen – doch wie lassen sich damit verbundene Risiken messen, beurteilen und steuern? Ziel muss es in jedem Fall sein, mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zu einem aussagekräftigen Sollmaßnahmenkatalog zu gelangen und ein höheres Informationssicherheitsniveau zu erreichen.

Das Seminar gibt wertvolle Praxistipps zur Herangehensweise und Umsetzung der aktuellen Anforderungen.

## Wissenswertes

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- DORA-Umsetzung, IT und Organisation
- Informationssicherheit (ISB) und Informationsrisikomanagement (IRM)
- Notfallmanagement und Business Continuity Management (BCM/ITSCM)
- Interne Revision und IT-Revision
- Datenschutz und Data Governance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- IT-Compliance und IT-Governance
- sowie andere interessierte Fach- bzw. Grundsatzbereiche, Geschäftsleiter\*innen/ Vorstandsmitglieder, externe (IT-)Prüferinnen und Prüfer sowie (IKT-)Dienstleister

## Unsere Referenten



### Mike Bona-Stecki

Leiter Informationssicherheit und Business Continuity Management  
DekaBank Deutsche Girozentrale, Frankfurt

*Mike Bona-Stecki ist seit 2018 als Leiter Informationssicherheit und Business Continuity Management bei der DekaBank Deutsche Girozentrale für das Informationssicherheits-, IT-Risiko- und Business Continuity Management verantwortlich. Er leitet ein Team von Sicherheitsexperten und beschäftigt sich schwerpunktmäßig mit der Umsetzung der aufsichtsrechtlichen Anforderungen an das IT-/Informationssicherheits- und Business Continuity Management. Mike Bona-Stecki ist seit über 20 Jahren im Bereich der Informationssicherheit im Bereich des Bundes und im Finanzsektor u. a. als Informationssicherheitsbeauftragter tätig sowie Lehrbeauftragter für den Bereich IT-Sicherheit an der Berufsakademie Rhein-Main. Mike Bona-Stecki veröffentlicht als freier Autor regelmäßig praxisorientierte Beiträge und Fachbücher zu den Themen Informationssicherheit, Business Continuity Management und Outsourcing und ist zudem gefragter Referent in diesen Themengebieten.*



### Stephan Wirth

Informationssicherheits- und Datenschutzbeauftragter  
NRW.BANK, Düsseldorf

*Seit über 20 Jahren ist Herr Wirth in den Bereichen Informationssicherheit, Datenschutz und Notfallplanung in verantwortlicher Position tätig. Bei der NRW.BANK hat er seit 2018 die Funktionen des Informationssicherheits- und des Datenschutzbeauftragten inne. Die Etablierung angemessener Prozesse und Verfahren zur nachhaltigen Sicherstellung der Einhaltung der aufsichtsrechtlichen Anforderungen gehört dabei zu seinen Hauptaufgaben.*

# Seminar-Vorschläge

**IKT Spezial: Identity & Access Management**  
10. Dezember 2024, Online-Veranstaltung

**DORA-Umsetzung im Fokus der Aufsicht**  
20. Januar 2025, Online-Veranstaltung

**Überprüfung der DORA-Konformität von IKT-Dienstleistern & Cloud-Service-Providern**  
21. Januar 2025, Online-Veranstaltung

**Praxis-Umsetzung der aktuellen DORA-Anforderungen im ZAM**  
28. Januar 2025, Online-Veranstaltung

**Neue DORA-Anforderungen an (IKT-)Notfallmanagement & BCM**  
29. Januar 2025, Online-Veranstaltung

**Abgrenzung Auslagerungsregister/Informationsregister**  
3. Februar 2025, Online-Veranstaltung

**DORA-konformes IKT-Risikomanagement**  
5./6. Februar 2025, Online-Veranstaltung

**Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken**  
17. Februar 2025, Online-Veranstaltung

► Diese und weitere Seminar-Angebote finden Sie bei uns online unter [www.akademie-heidelberg.de/online-seminare](http://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](mailto:b.wehling@akademie-heidelberg.de)

## Anmeldeformular

DORA Spezial: Informationssicherheit und IKT-Risikomanagement

Name \_\_\_\_\_

Vorname \_\_\_\_\_

Position \_\_\_\_\_

Firma \_\_\_\_\_

Straße \_\_\_\_\_

PLZ / Ort \_\_\_\_\_

Tel./Fax \_\_\_\_\_

E-Mail \_\_\_\_\_

Name der Assistenz \_\_\_\_\_

Datum Unterschrift \_\_\_\_\_

An [anmeldung@akademie-heidelberg.de](mailto:anmeldung@akademie-heidelberg.de) oder per Fax an: **06221/65033-29**

### Termin + Seminarzeiten

Donnerstag, 23. Januar 2025  
9:00 – 17:00 Uhr  
Online-Zugang ab 8:45 Uhr  
Seminar-Nr. 25 01 BA011 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, wenn gewünscht, gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: [www.akademie-heidelberg.de/agb](http://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 Internet-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**  
**HEIDELBERG**

**AH Akademie für Fortbildung Heidelberg GmbH**  
Maaßstraße 28 · 69123 Heidelberg  
Telefon 06221/65033-0 · Fax 06221/65033-69  
[info@akademie-heidelberg.de](mailto:info@akademie-heidelberg.de)  
[www.akademie-heidelberg.de](http://www.akademie-heidelberg.de)

