

# DORA-konformes IKT-Risikomanagement

## Anforderungen an Informationssicherheit, IT-Sicherheit und BCM



### Banken-Praxis-Seminar · 14 CPE-Punkte

- Einführung in das IKT-Risikomanagement
- Gesetzlich und regulatorische Anforderungen (u. a. MaRisk, DORA)
- Informationssicherheits- und Informationsrisikomanagement
- IKT-Risikomanagement im Outsourcing
- IKT-Vorfallsmanagement und Operative Informationssicherheit
- DOR-Testprogramm
- Business Continuity Management (BCM & ITSCM)

#### Referent



Mike Bona-Stecki  
Leiter Informationssicherheit und Business  
Continuity Management, stv. DOR-Beauftragter  
DekaBank Deutsche Girozentrale, Frankfurt/Main

# DORA-konformes IKT-Risikomanagement

Programm – Tag 1 · Mittwoch, 04.02.2026

## Mike Bona-Stecki, DekaBank

### Einführung in das IKT-Risikomanagement

- Ziele und Organisation des IKT-Risikomanagements
- Risikomodelle, Bedrohungsanalyse, BIA, Non-Financial-Risk
- RM-Prozesse nach ISO 31000, ISO 27005, BSI 200-3

### Gesetzliche und regulatorische Anforderungen an das IKT-RM

- Erweiterte MaRisk-/DORA-Anforderungen an IT-Gov. und Informationssicherheit: IT-Risiken/Cyber-Risiken im Fokus
- NIS2-Richtlinie und EBA-Leitlinien zu ESG-Risiken
- BSI-Standards 200-1/-2/-3 und der neue BCM-Standard
- Besondere IKT-Anforderung der DORA

### Resilienz – DOR-Strategie für eine widerstandsfähige Bank

- DOR-Strategie: Anforderungen und Inhalte
- Strategieprozess: Kennzahlen und Mess-Verfahren
- Rollen, Funktionen, Verantwortlichkeiten und Aufgaben des IKT-Risikomanagements

### Informationssicherheit als Basis zur Stärkung der Resilienz

- Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zu Sollmaßnahmenkatalog und höherem Sicherheitsniveau
- Informationsverbund: Identifikation und Gruppierung der IKT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- Ermittlung der kritischen oder wichtigen Funktion und der Kritikalität von Assets und Vererbung der Prozesskritikalität

### IKT-Risikomanagement als Wächter der Resilienz

- IKT-Risikomanagementrahmen
- DORA: Identifikation, Analyse, Bewertung von IKT-Risiken
- Identifikation von Restrisiken; Abgrenzung zum OpRisk
- Best Practices und Standards für ein praxisnahe, effektives und DORA-konformes Informationsrisikomanagement
- Berichterstattung & Dokumentationspflichten zum IKT-RM

Programm – Tag 2 · Donnerstag, 05.02.2026

## Mike Bona-Stecki, DekaBank

### IKT-Vorfallsmanagement

- Identifikation, Behandlung und Meldung von IKT-Vorfällen
- DORA-Anforderungen an operative Informationssicherheit
- Angriffserkennung mit Security Operation Center (SOC) und Security Information and Event Management (SIEM)

### Business Continuity Management

- Abgrenzung Störung, Notfall, Krise; Business Impact Analyse, Geschäftsfortführungspläne, IT-SCM, Test, Übung
- Anforderung an die Ausgestaltung von Geschäftsfortführungs-, Notbetriebs- und Wiederherstellungsplänen
- Kennzahlen des BCM – Umsetzung der Erhebung von Recovery Time Objective (RTO), Recovery Point Objective (RPO) und Maximum tolerable Period of Disruption (MTPD)

### Testprogramm zur Überprüfung der digitalen operat. Resilienz

- DOR-Testprogramm, Verantwortlichkeiten und Rahmenbedingungen, Überblick zu einzelnen Testarten (z. B. TLPT)
- Kontroll- und Überwachungsplan IKT-Risikomanagement
- Prüfung, Begleitung und Auswertung von Notfallübungen

### Identitäts- und Rechtemanagement

- Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen für Benutzer
- Prinzip der minimalen Rechtevergabe (»Need-to-know«, »Need-to-use« und »Least privileges«) & Rezertifizierung

### IKT-Risikomanagement im Outsourcing

- Due Diligence-Verfahren und Sicherstellung der Sorgfaltspflichten für ein angemessenes Sicherheitsniveau
- Vertragliche Anforderungen und Regelung zur Dienstleistersteuerung in Auslagerungsverträgen aus Sicht des IKT-Risikomanagement; Besonderheiten bei Cloud-Services
- BCM im Kontext von Dienstleistungsbeziehungen

## Seminarziel

Das Seminar vermittelt ein fundiertes Verständnis der Anforderungen und Aufgaben im IKT-Risikomanagement. Im Fokus steht der Aufbau eines regelkonformen, resilienten Systems, das strategische, organisatorische und regulatorische Aspekte integriert.

Die Bedeutung des IKT-RM in der DOR-Strategie wird hervorgehoben. BCM, Informationssicherheit, IT-Sicherheits- und Vorfallsmanagement werden praxisnah behandelt.

DORA-Vorgaben zum IKT-Vorfallsmanagement – wie Meldepflichten, Klassifikation schwerwiegender Vorfälle sowie deren Umsetzung mit SOC, SIEM und Frühwarnindikatoren – werden kompakt dargestellt.

Im BCM werden Notfallvorsorge und Wiederanlaufplanung behandelt, etwa Business Impact Analysen, RTO, RPO, MTPD sowie Fortführungspläne. Ergänzend wird das DORA-Testprogramm mit Verfahren wie TLPT.

Identitäts- und Rechtemanagement wird als Sicherheitskernaspekt thematisiert. Abschließend erfolgt eine Analyse der Risiken bei Auslagerungen (z. B. Cloud) inklusive Due-Diligence, Vertragspflichten und BCM-Rolle.

Praxisbeispiele und interaktiver Austausch stärken das Verständnis für wirksames IKT-Risikomanagement.

## Wissenswertes

### Zielgruppe

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

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

### Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu den aktuellen Aufsichtsanforderungen im Bereich IKT-Risikomanagement
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut
- Sie erhalten wertvolle Praxistipps im Erfahrungsaustausch mit dem Referenten
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit anderen Praktiker\*innen

## Unser Referent

---



### Mike Bona-Stecki

Leiter Informationssicherheit und Business Continuity Management  
stv. DOR-Beauftragter, 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.*

# Seminar-Vorschläge

Neue DORA- und Aufsichts-Anforderungen  
an (IKT-)Notfallmanagement & BCM  
28. Januar 2026, Online-Veranstaltung

MaRisk Spezial:  
Risikoberichtswesen & Vorstands-Reporting  
27. Januar 2026, Online-Veranstaltung

Aufsichtskonformes Modell-Risikomanagement  
9. Februar 2026, Online-Veranstaltung

Prozesse zur Steuerung & Überwachung von IKT-Risiken  
23. Februar 2026, Online-Veranstaltung

MaRisk Spezial: Nachhaltigkeit & ESG  
24. Februar 2026, Online-Veranstaltung

Auslagerungsmanagement Spezial:  
Umgang mit „Software as a Service“ (SaaS) & Cloud-Diensten  
4. März 2026, Online-Veranstaltung

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](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

## Anmeldeformular

DORA-konformes IKT-Risikomanagement

|                    |
|--------------------|
| 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](mailto:anmeldung@akademie-heidelberg.de)

### Termin und Seminarzeiten

Mi./Do., 4./5. Februar 2026  
jeweils 9:00–17:00 Uhr  
Online-Zugang ab 8:45 Uhr  
Seminar-Nr. 2602BA178 W

### Teilnahmegebühr

€ 980,– (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](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 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.

 **AKADEMIE**  
**HEIDELBERG**

**AH Akademie für Fortbildung Heidelberg GmbH**  
Maaßstraße 32/1 · 69123 Heidelberg  
Telefon 06221/65033-0  
[info@akademie-heidelberg.de](mailto:info@akademie-heidelberg.de)  
[www.akademie-heidelberg.de](http://www.akademie-heidelberg.de)

