23./24. September 2025
Online-Veranstaltung

AKADEMIE HEIDELBERG

DORA-konformes IKT-Risikomanagement

(DORA-)Anforderungen an Informationssicherheit, IT-Sicherheit und BCM

Banken-Praxis-Seminar · 14 CPE-Punkte

Neue DORA-Anforderungen an das IKT-Risiko-management!

20 Jahre AKADEMIE HEIDELBERG

- **Einführung in das IKT-Risikomanagement**
- **Gesetzlich und regulatorische Anforderungen (u. a. MaRisk, EBA-GLs, 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
DekaBank Deutsche Girozentrale, Frankfurt

DORA-konformes IKT-Risikomanagement

Programm Tag 1 · 23. September 2025

Mike Bona-Stecki, DekaBank · 9:00–17:00 Uhr

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 praxisnahes, effektives und DORA-konformes Informationsrisikomanagement
- Berichterstattung & Dokumentationspflichten zum IKT-RM

Programm Tag 2 · 24. September 2025

Mike Bona-Stecki, DekaBank · 9:00–17:00 Uhr

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 als wesentlicher Eckpfeiler einer Sicherheitsstrategie

- 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 – inklusive organisatorischer Einbindung und Zuständigkeitsverteilung zwischen Linie, Geschäftsleitung und Aufsicht.

DORA-Vorgaben zum IKT-Vorfalls-management – 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

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- IT und Organisation, Informationssicherheit (ISB) und Informationsrisiko-management (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
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.

Fachtagung IKT-Aufsicht
27./28. Mai 2025, Online-Veranstaltung

DORA Spezial: Informationssicherheit und IKT-Risikomanagement
3. Juni 2025, Online-Veranstaltung

IKT Spezial für Compliance & Governance
25. Juni 2025, Online-Veranstaltung

Prüfung (IT-)Auslagerungen (MaRisk) &
(IKT-)Drittdienstleistungen (DORA)
9. Juli 2025, Online-Veranstaltung

Anforderungen an IT-Infrastruktur & IT-Betrieb unter DORA
10. Juli 2025, Online-Veranstaltung

Zertifizierter Auslagerungs-Manager (MaRisk) &
IKT-Dienstleister-Steuerer (DORA)
16. bis 18. Juli 2025, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)
24. Juli 2025, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse
zur Steuerung & Überwachung von IKT-Risiken
24. Juli 2025, 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

DORA-konformes IKT-Risikomanagement

Name

Vorname

Position

Firma

Straße

PLZ / Ort

Tel./Fax

E-Mail

Name der Assistenz

Datum Unterschrift

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

Termin + Seminarzeiten

Dienstag/Mittwoch
23./24. September 2025
09:00 – 17:00 Uhr (an beiden Tagen)
Online-Zugang jeweils ab 08:45 Uhr

Seminar-Nr. 25 09 BA178 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, wenn gewünscht, 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 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.

04.25 / 25 09 BA178

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 28 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de