5./6. Februar 2025
Online-Veranstaltung

AKADEMIE HEIDELBERG

DORA-konformes IKT-Risikomanagement

Anforderungen an Informationssicherheit, IT-Sicherheit und BCM

Banken-Praxis-Seminar · 14 CPE-Punkte

Neue DORA-Anforderungen an den Umgang mit IKT-Risiken

- **Einführung in das IKT-Risikomanagement**
- **Gesetzlich und regulatorische Anforderungen (u. a. MaRisk, EBA-GLs, DORA)**
- **Informationssicherheitsmanagement**
- **Informationsrisikomanagement**
- **IKT-Risikomanagement im Outsourcing**
- **Operative Informationssicherheit**
- **Business Continuity Management (BCM)**

20 Jahre AKADEMIE HEIDELBERG

Referent

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

DORA-konformes IKT-Risikomanagement

Programm Tag 1 · 5. Februar 2025

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

Einführung in das IKT-Risikomanagement

- Risikobegriff, ISM, IT-Sec, BCM, Schutzziele
- Ziele und Organisation des IKT-Risikomanagement
- Risikomodelle, Bedrohungsanalyse, BIA, Non-Financial-Risk
- RM-Prozesse nach ISO 31000, ISO 27005, BSI 200-3

Gesetzlich und regulatorische Anforderungen an das IKT-Risikomanagement

- Erweiterte MaRisk-/DORA-Anforderungen an Informationssicherheit und IT-Governance: IT-Risiken und Cyber-Risiken stärker im Fokus
- BSI-Standards 200-1/-2/-3 und der neue BCM-Standard
- Überblick zur Anforderung der DORA

IKT-Risikomanagement

- Verantwortlichkeiten und Aufgaben des IKT-RM
- Identifikation, Analyse und Bewertung von IKT-Risiken
- Berichterstattung und Dokumentationsanforderungen IKT
- Identifikation von Restrisiken; Umgang mit Risikoakzeptanz; Kompetenzreglungen zur Akzeptanz von IKT-Risiken
- Schnittstellen zum OpRisk-Management
- Best Practices und Standards für ein praxisnahes, effektives und DORA-konformes Informationsrisikomanagement

Anforderung an die Informationssicherheit

- Informationssicherheitsziele im Rahmen der DOR-Strategie
- Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zu Sollmaßnahmenkatalog und höherem IS–Niveau
- Informationsverbund: Identifikation und Gruppierung der IKT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- SB-Vererbung auf Informations- und Prozessebene
- Ermittlung der kritischen oder wichtigen Funktion
- Schutzmaßnahmen zur Stärkung der DOR

Programm Tag 2 · 6. Februar 2025

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

IKT-Risikomanagement im Outsourcing

- Arten der Dienstleistungsbeziehung, Cloud-Grundlagen
- Risikoanalyse bei Dienstleistungen, Vertragsanforderungen
- Cyber-Governance: Umgang mit Cyberrisken bei Auslagerungen und Verzahnung mit NFR-Management
- Beurteilung von IT- und Informationssicherheits-Risiken im Rahmen des Auslagerungsprozesses
- Besondere Herausforderungen bei Cloud-Dienstleistungen
- Informationssicherheits-Regelung im Auslagerungsvertrag
- BCM im Kontext von Auslagerungen und Fremdbezug

Operative Informationssicherheit

- Anforderungen zur operativen Informationssicherheit
- SIEM-Prozess, Anforderungen an die Aufbau- und Ablauforganisation, Schnittstellen zwischen 2nd & 1st LoD

Identitäts- und Rechtemanagement

- Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen für Benutzer
- Minimale Rechtevergabe, 4-Augen-Prinzip, SoD
- Rezertifizierung unter Beteiligung der Fachbereiche
- Angriffserkennung mit Security Information and Event Management (SIEM) und Security Operation Center (SOC)

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)
- Prüfung, Begleitung und Auswertung von Notfallübungen und Notfallsimulationen in der Praxis

Seminarziel

Das Seminar »DORA-konformes IKT-Risikomanagement« vermittelt eine umfassende Einführung in das IKT-Risikomanagement, wobei der Fokus auf der Identifikation, Bewertung und Steuerung von Risiken liegt. Dabei werden gesetzliche und regulatorische Anforderungen an das IKT-Risiko-management umfassend behandelt – inklusive der neuen DORA-Vorgaben!

Ein zentraler Bestandteil des Seminars ist die Vertiefung in die Themen Informationssicherheitsmanagement und Informationsrisikomanagement, um praxisrelevante Strategien zur Sicherung von Informationen und zur effektiven Risikobewältigung zu entwickeln. Es werden ebenfalls die spezifischen Herausforderungen des IKT-Risikomanagements im Outsourcing beleuchtet und praxisorientierte Lösungsansätze erarbeitet.

Die Teilnehmer werden zudem in die Grundlagen der operativen Informa-tionssicherheit und der Implementierung eines Identitäts- und Rechtemanagements (IAM) eingeführt.

Abschließend wir das wichtige Thema des Business Continuity Managements behandelt, um sicherzustellen, dass Organisationen auch in Krisensituationen handlungsfähig bleiben.

Durch praxisnahe Fallbeispiele und interaktiven Erfahrungsaustausch erhalten die Teilnehmernden ein umfassendes Verständnis für das 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.

IKT-Risikomanagement KOMPAKT
19./20. November 2024, Online-Veranstaltung

DORA-Umsetzung im Fokus der Aufsicht
2. Dezember 2024, Online-Veranstaltung

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

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

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

DORA Spezial: Informationssicherheit & IKT-Risikomanagement
23. Januar 2025, Online-Veranstaltung

Praxis-Umsetzung der aktuellen DORA- und Aufsichts-Anforderungen im Auslagerungsmanagement
28. Januar 2025, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM
29. Januar 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

An **anmeldung@akademie-heidelberg.de** oder per Fax an: **06221/65033-29**

Name

Vorname

Position

Firma

Straße

PLZ / Ort

Tel./Fax

E-Mail

Name der Assistenz

Datum Unterschrift

Termin + Seminarzeiten

Mittwoch/Donnerstag
5./6. Februar 2025
09:00 – 17:00 Uhr (an beiden Tagen)
Online-Zugang jeweils ab 08:45 Uhr

Seminar-Nr. 25 02 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.

10 24 / 25 02 BA178

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 28 · 69123 Heidelberg
Telefon 06221/65033-0 · Fax 06221/65033-69
info@akademie-heidelberg.de
www.akademie-heidelberg.de