

IKT-Risikomanagement KOMPAKT

Neue Anforderungen an Informationssicherheit, IT-Sicherheit und BCM



Banken-Praxis-Seminar · 14 CPE-Punkte

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

- 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)

Referent



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

Programm Tag 1 · 19. November 2024

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

Einführung in das IKT-Risikomanagement

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

Gesetzlich und regulatorische Anforderungen an das IKT-Risikomanagement

- Erweiterte MaRisk-/DORA-Anforderungen an IT-Sec 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 gemäß DORA
- Berichterstattung und Dokumentationsanforderungen
- Identifikation von Restrisiken; Umgang mit Risikoakzeptanz (Kompetenzregelungen für IKT-Risiken)
- Monetäre Bewertung der IKT-Risiken im OpRisk-Mgmt.
- 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 · 20. November 2024

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

IKT-Risikomanagement im Outsourcing

- Arten der Dienstleistungsbeziehung, Cloud-Grundlagen
- Cyber-Governance: Umgang mit Cyberrisiken bei Auslagerungen und deren Verzahnung mit dem NFR
- Beurteilung von IT- und Informationssicherheits-Risiken im Rahmen des Auslagerungsprozesses
- Besondere Herausforderungen bei Cloud-Dienstleistungen
- Regelung der Informationssicherheit in Auslagerungsverträgen und SLAs; Risikoanalyse bei Dienstleistungen

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

- Definition Notfallvorsorge/Krisenmanagement; 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 »IKT-Risikomanagement KOMPAKT« vermittelt fundierte Kenntnisse über die wesentlichen Aspekte des Informations- und Kommunikationstechnologie-Risikomanagements, wobei der Fokus auf der Identifikation, Bewertung und Steuerung von Risiken liegt. Dabei werden gesetzliche und regulatorische Anforderungen an das IKT-Risikomanagement 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. Ebenfalls werden die spezifischen Herausforderungen des IKT-Risikomanagements im Outsourcing beleuchtet und praxisorientierte Lösungsansätze erarbeitet.

Die Teilnehmenden werden zudem in die Grundlagen der operativen Informationssicherheit sowie der Implementierung eines Identitäts- und Rechte-managements (IAM) eingeführt

Abschließend wird das Thema des BCM behandelt, um sicherzustellen, dass Organisationen auch in Krisensituationen handlungsfähig bleiben. Den Teilnehmenden wird ein umfassendes Verständnis für das IKT-Risikomanagement vermittelt, das sie unmittelbar in ihren beruflichen Kontexten anwenden können.

Wissenswertes

Aus der Praxis für die Praxis!

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
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

Nutzung von Clouds und Software as a Service (SaaS) in der Praxis
23. September 2024, Online-Veranstaltung

Abgrenzung & Steuerung von (IT-)Auslagerungen & (IKT-)Drittdienstleistungen
24. September 2024, Online-Veranstaltung

IKT und DORA im Fokus:
Informationssicherheit & IKT-Risikomanagement
25. September 2024, Online-Veranstaltung

Neue DORA- & Aufsichts-Anforderungen an (IT-)Notfallmanagement & BCM
7. Oktober 2024, Online-Veranstaltung

OpRisk SPEZIAL: IKT-Risiken im Fokus der Aufsicht
7. Oktober 2024, Online-Veranstaltung

Prüfung & Begleitung von IT-Projekten im Fokus der Aufsicht
8. Oktober 2024, Online-Veranstaltung

Prüfung der IKT-Anforderungen vor dem Hintergrund neuer DORA-Vorgaben
28. Oktober 2024, Online-Veranstaltung

Fachtag IT-Aufsicht
18. November 2024, 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

IKT-Risikomanagement KOMPAKT

Name _____

Vorname _____

Position _____

Firma _____

Straße _____

PLZ / Ort _____

Tel./Fax _____

E-Mail _____

Name der Assistenz _____

Datum Unterschrift _____

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

Termin + Seminarzeiten

Dienstag/Mittwoch
19./20. November 2024
09:00 – 17:00 Uhr (an beiden Tagen)
Online-Zugang jeweils ab 08:45 Uhr
Seminar-Nr. 24 11 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.

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
www.akademie-heidelberg.de

