

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



Banken-Aufsicht-Seminar · 8 CPE-Punkte

Konkrete Praxis-
Berichte, Handlungs-
empfehlungen und
Umsetzungshinweise!

- **Erweiterte DORA-/MaRisk-Anforderungen an das (IKT-)Notfallmanagement und die (IT-)Notfallkonzepte**
- **Häufig identifizierte Schwachstellen und Prozess-Schwächen**
- **Neue Pflichten der Mitglieder des Notfall-/Krisen-Managements**
- **DORA-konforme Aufbau- und Ablauforganisation des BCM/ITSCM**
- **Risikoorientierte Einbindung von IKT-Drittdienstleistern**
- **Prüfung, Begleitung und Auswertung (Maßnahmen!) von Notfallübungen und Notfallsimulationen in der Praxis**

20 Jahre
**AKADEMIE
HEIDELBERG**

Referenten



Dr. Jens Gampe
ehem. BaFin-Referent im
Bereich Grundsatz IT-Aufsicht,
Überwachung IT-MMDL und
Krisenprävention



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



Torsten Zacher
Business Continuity Manager
Certified Lead Auditor ISO 22301
RSM Ebner Stolz

Programm

Dr. Jens Gampe, ehem. BaFin · 9:30–12:00 Uhr

Notfallmanagement und BCM/ITSCM: Aufsichtliche Erwartungen und Anforderungen aus DORA, MaRisk, BAIT & EBA-Leitlinien

- Erweiterte DORA-Anforderungen an die Angemessenheit der Notfallkonzepte in Bezug auf die (Neu-)Erstellung und regelmäßige Aktualisierung, insb. kontinuierliche Überwachung der IKT-Systeme und Implementierung von Systemen zur Echtzeitüberwachung und Bedrohungserkennung.
- Notwendiger Anpassungs- und Umsetzungsbedarf in den Instituten – Häufig identifizierte Schwachstellen und Prozess-Schwächen
- Erwartungen der Aufsicht an die Durchführung von Business Impact Analysen (BIA) und die Überführung der Ergebnisse in das Risikomanagement
- Erwartungen an die Durchführung regelmäßiger (GESAMT-)Notfalltests und die Einbindung der Dienstleister in Notfallübungen und Notfallkonzepte
- Besondere Anforderungen an die Funktion des Notfallbeauftragten/BCM-/ITSCM-Beauftragten
- Umsetzungshinweise und Praxistipps

Torsten Zacher, Ebner Stolz · 12:45–14:45 Uhr

Aufbau- und Ablauforganisation im Sinne des BCM/ITSCM – Ausblick auf mögliche Veränderungen aus der DORA

- BSI 200-4, MaRisk und DORA – Kurze Gegenüberstellung der Anforderungen ausgewählter Prüfungsschwerpunkte
- Personalkapazitäten für das Notfallmanagement
 - Sicherstellung durchgehend ausreichender Personalressourcen, insbesondere für das präventive BCM
- Prozesslandkarte
 - Vollständige Prozesslandkarte als Grundlage für die Durchführung der BIA
 - Praxisprobleme bei der Erhebung, Darstellung und Granularität der Einzelprozesse und der Notfallrelevanz
 - Besonderheiten und Abstimmungsbedarf von Prozessketten für das Notfall-(Prozess-)Management

- Schriftlich fixierte Ordnung (SfO) und Anweisungswesen/zentrales Notfallhandbuch
 - Verankerung der BCM-/ITSCM-Anforderungen im Notfallhandbuch und der SfO
 - Benennung von Ansprechpartnern für die Notfallsituation – Zusammensetzung des Krisenstabs
 - Berücksichtigung von Stress-Faktoren
 - Festlegung von Verantwortlichen für die akute Notfall- und Krisenbekämpfung sowie die Krisenkommunikation
- Identifikation von (kritischen) internen & externen Schnittstellen und Vermeidung von Silodenken

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

Überprüfung und Beurteilung der Prozesse im (IT-)Notfallmanagement & BCM/ITSCM (u. a. Notfallplanung, Wiederanlaufplanung, Notfallkonzepte, Notfalltests, SIEM)

- (Neue) Anforderung an Geschäftsfortführungs-, Notbetriebs- und Wiederherstellungspläne – Anforderung der DORA angemessen berücksichtigen.
- Praxis-Check neuer BSI-Standard 200-4
- Auswirkung und Umgang mit Kennzahlen des BCM – Umsetzung der Erhebung von Recovery Time Objective (RTO), Recovery Point Objective (RPO) und Maximum tolerable Period of Disruption (MTPD)
- Vorgehensweise bei der Risikoanalyse interner Notfallkonzepte – Identifizierung von Risiken und Lücken – Ableitung entsprechender Handlungsfelder
- Risikoorientierte Einbindung von (IKT-)Drittdienstleistern in die Notfallplanung und das Notfallmanagement
- Prüfung, Begleitung und Auswertung (Maßnahmen!) von Notfallübungen und Notfallsimulationen in der Praxis
- Ermittlung und Berichterstattung von Kontinuitätsrisiken an die Geschäftsleitung – Handlungsfelder in der Praxis
- Häufige Schwachstellen bei der Umsetzung von Notfallkonzepten und Notfalltests
- Stärkung der Cyber-Resilienz durch Verzahnung von Informationssicherheit, BCM und Krisenmanagement; Alarmierungsverfahren zum IT-Notfallmanagement

Seminarziel

Die neuen DORA-Vorgaben in Verbindung mit den MaRisk fordern eine deutliche Verbesserung des IKT-Notfallmanagements und der Notfallkonzepte sowie des Business Continuity Managements (BCM) und des IT Service Continuity Management (ITSCM) der Institute und Dienstleister(!), um gravierende Risiken und Bedrohungen frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren.

Verantwortlichkeiten der Notfallbeauftragten und des Krisenstabs sowie Maßnahmen und Vorgehensweisen im Notfall müssen genauer festgelegt, dokumentiert und ggü. den Mitarbeitern kommuniziert werden.

Zudem erwartet die Aufsicht regelmäßige (GESAMT-)Notfalltests und die Einbindung der Dienstleister in Notfallübungen und Notfallkonzepte. Veränderungen in der Bedrohungslage sowie in der Wirksamkeit des Notfallkonzeptes müssen umgehend im Risikomanagement erfasst und im Notfallplan ergänzt werden.

Das BCM muss daher so aufgesetzt sein, dass die Widerstandsfähigkeit der (zeit-)kritischen Geschäftsprozesse ständig verbessert wird, auf Schadensereignisse angemessen reagiert werden kann (SIEM) und die Geschäftstätigkeiten nach einem Notfall so schnell wie möglich wieder aufgenommen werden können. Eine ganzheitliche Betrachtung ist daher ausschlaggebend.

Wissenswertes

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- Notfallmanagement und Business Continuity Management (BCM)
- IT und IT Service Continuity Management (ITSCM)
- IT-Organisation, Informationssicherheit (ISB) und Informationsrisikomanagement
- Interne Revision und IT-Revision, Datenschutz (DSB) und Data Governance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- sowie andere interessierte Fachbereiche bzw. Grundsatzbereiche, externe Prüfer*innen und Bankdienstleister

Unsere Referenten



Dr. Jens Gampe

ehem. BaFin-Referent im Bereich Grundsatz IT-Aufsicht, Überwachung IT-MMDL und Krisenprävention

Nach diversen Stationen in der Fachaufsicht war Dr. Jens Gampe viele Jahre im IT-Grundsatz der BaFin beschäftigt und u. a. maßgeblich an der Erarbeitung und Novellierung der Bankaufsichtlichen Anforderungen an die IT beteiligt. Nach Veröffentlichung der BAIT-Novelle war er u. a. für die operative IT-Mehrmandantendienstleister-Überwachung und die Krisenprävention im Finanzsektor zuständig.



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.



Torsten Zacher

Business Continuity Manager, Certified Lead Auditor ISO 22301
RSM Ebner Stolz

Torsten Zacher ist seit 20 Jahren im Bankaufsichtsrecht tätig und Experte in den Themenfeldern Business Continuity Management, Krisenmanagement und Outsourcing Management. Seit Mai 2023 bei RSM Ebner Stolz als BCM-Manager tätig. Zuvor arbeitete er bei als BCM-Beauftragter für die Börse Stuttgart, bei der Mercedes-Benz Bank AG im Bereich Compliance (BCM, zentrales Auslagerungsmanagement, Organisation) und bei LBBW in den Bereichen Compliance und Risikomanagement (BCM, zentrales Auslagerungsmanagement).

Seminar-Vorschläge

DORA-Umsetzung im Fokus der Aufsicht
2. 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

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

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

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

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

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

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

Mittwoch, 29. Januar 2025
9:30–17:00 Uhr
Online-Zugang ab 9:15 Uhr
Seminar-Nr. 25 01 BA029 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

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.

**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

