31. März 2025 · 9:30–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

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

Lars Ehrenfeld
Abteilungsleiter Prozessmanagement und IT-Governance
Kreissparkasse Heilbronn

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

Programm

Dr. Jens Gampe, ehem. BaFin · 9:30–12:00 Uhr · inkl. 15 Min. Pause

Notfallmanagement und BCM/ITSCM: Aufsichtliche Erwartungen und neue Anforderungen aus DORA

- 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 der Notfallbeauftragten/BCM-/ITSCM-Beauftragten
- Umsetzungshinweise und Praxistipps

Mike Bona-Stecki, DekaBank · 12:45–14:45 Uhr

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

- Anforderungen an die Notfallprozesse sowie die Verantwortlichkeiten und Zuständigkeiten
- BSI-Standard 200-4 zum BCM
- Ausgestaltung von Geschäftsfortführungs-, Notbetriebs- und Wiederherstellungsplänen – Anforderung der DORA angemessen berücksichtigen.
- 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
- Prüfung des Ineinandergreifens u. a. von Notfallplänen, Notfallprozessen, Wiederanlaufplänen und dem Notfallhandbuch
- Risikoorientierte Einbindung von (IKT-)Drittdienstleistern in die Notfallplanung und das Notfallmanagement – Handlungsempfehlungen
- 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

Lars Ehrenfeld, Kreissparkasse Heilbronn · 15:00–17:00 Uhr

Praxisbericht: Einbindung der Bereiche Informationssicherheit und Informationsrisikomanagement in das Business-Continuity Management – Cyber-Security-Anforderungen im BCM

- Erweiterte MaRisk-/DORA-Anforderungen an die Einbindung von Informationssicherheit und IT-Governance in das Notfallmanagement: IT-Risiken & Cyber-Risiken stärker im Fokus der Aufsicht
- BCM-Anforderungen: Änderungen durch DORA – Was müssen nationale Institute jetzt beachten?
- IT-Notfallübungen und IT-Notfall-Simulationen in der Praxis – Testen und prüfen zeitkritischer Prozesse und der Wirksamkeit des Notfallkonzepts
- Häufige Schwachstellen bei der Erstellung und Aktualisierung von Notfallhandbüchern
- Neue Aufgaben und Pflichten der Informationssicherheitsbeauftragten (ISB)
- Cyber-Security-Anforderungen im Notfallmanagement
- Berücksichtigung von Verfügbarkeits- und Integritätsanforderungen bei der Erstellung von Notfallplänen unter Einbindung der (IT-)Dienstleister

Seminarziel

Die neuen DORA-Vorgaben in Verbindung mit den MaRisk fordern eine deutliche Verbesserung des IKT-Notfallmanagements und der IT-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.

Zunehmend schwerwiegendere Feststellungen in den Bereichen Auslagerungsmanagement und Notfallmanagement sowie eine starke Zunahme der Cyber-Risiken haben zu deutlich erweiterten Anforderungen der Aufsicht geführt.

Verantwortlichkeiten der Notfallbeauftragten und des Krisenstabs sowie Maßnahmen und Vorgehensweisen im Notfall müssen genauer festgelegt, dokumentiert und ggü. den Mitarbeitenden kommuniziert werden. Zudem erwartet die Aufsicht regelmäßigere (GESAMT-)Notfalltests und die Einbindung der Dienstleister in Notfallübungen und Notfallkonzepte.

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.

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-Compliance und IKT-Governance
- IT-Organisation, Informationssicherheit (ISB) und Informationsrisikomanagement
- Interne Revision und IT-Revision, Datenschutz (DSB) und Data Governance
- (Zentrales) Auslagerungsmanagement und IKT-Dienstleistersteuerung
- sowie andere interessierte Fach- 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.

Lars Ehrenfeld
Abteilungsleiter Prozessmanagement und IT-Governance
Kreissparkasse Heilbronn, Heilbronn

Lars Ehrenfeld ist bei der Kreissparkasse Heilbronn für die Abteilung Prozessmanagement und IT-Governance verantwortlich. Zu seinen Schwerpunkten gehört u. a. das IT-Aufsichtsrecht. Als Referent aus der Praxis verfügt er über ein breites Wissen und gibt dieses als Dozent an verschiedenen Bildungseinrichtungen weiter.

Prüfung DORA & DORA-Umsetzung
17./18. März 2025, Online-Veranstaltung

DORA-konforme Auslagerungsverträge & SLAs
24. März 2025, Online-Veranstaltung

KI-Governance: Einsatz Künstlicher Intelligenz (KI) & Anforderungen des AI-Act
25. März 2025, Online-Veranstaltung

Aufbau eines aufsichtskonformen & revisionssicheren IKS
27./28. März 2025, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen
1. April 2025, Online-Veranstaltung

Risikoanalyse von Auslagerungen (MaRisk) und IKT-Drittdienstleistungen (DORA)
29. April 2025, Online-Veranstaltung

IKT-Drittpartei-Risiken & Third Party Risk Management (TPRM) im Fokus von Aufsicht und DORA
12. Mai 2025, Online-Veranstaltung

Basis-Seminar Business Continuity Management (BCM)
24. Juni 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

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

Termin + Seminarzeiten

Montag, 31. März 2025
9:30–17:00 Uhr
Online-Zugang ab 9:15 Uhr

Seminar-Nr. 25 03 BA038 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.

02.25 / 25 03 BA038

AKADEMIE HEIDELBERG

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