21. Oktober 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

Alexander Rothländer
Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank
Frankfurt/Main

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

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 (in Echtzeit) und Implementierung von Systemen zur Bedrohungserkennung
- Notwendiger Anpassungs- und Umsetzungsbedarf in den Instituten – Häufig identifizierte 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
- Besondere Anforderungen an die Funktion der Notfallbeauftragten/BCM-/ITSCM-Beauftragten

Alexander Rothländer, Bundesbank · 12:45–14:45 Uhr

Konkrete DORA-Anforderungen an das IKT-Geschäftsfortführungsmanagement

- Geschäftsfortführungsmanagement und Berücksichtigung des Business Continuity Management nach DORA
- Von der Übersicht über die Funktionen bis zur Auswertung von Testergebnissen: Übersicht über die Prozesse im IKT-Geschäftsfortführungsmanagement
- Notwendigkeit aussagekräftiger und wirksamer Konzepte für das Geschäftsfortführungsmanagement: IKT-Geschäftsfortführungs-, IKT-Reaktions- und Wiederherstellungspläne
- Tipps zur technischen Umsetzung von IKT-Reaktions- und Wiederanlaufplänen und Tests
- Aufsichtliche Anforderungen an Datensicherung- und Datenwiedergewinnung
- Anforderungen an Kontrollen und Umgang mit Geschäftsfortführung bei IKT-Drittbezügen (inkl. Cloud-Services)
- Prüfungshandlungen & häufige Feststellungen im IKT-Geschäftsfortführungsmanagement

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

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

- Anforderungen an die Notfallprozesse sowie Verantwortlichkeiten und Zuständigkeiten für das Notfall- und Krisenmanagement
- Praxis-Anforderung an die 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 – Ableitung entsprechender Handlungsfelder
- Prüfung des Ineinandergreifens u. a. von Notfallplänen, Notfallprozessen, Wiederanlaufplänen und dem Notfallhandbuch entlang einer Prozesskette
- Risikoorientierte Einbindung von (IKT-)Drittdienstleistern in die Notfallplanung und das Notfallmanagement – Handlungsempfehlungen
- Prüfung, Begleitung und Auswertung (Maßnahmen!) von Notfallübungen und Notfallsimulationen in der Praxis
- Berücksichtigung der Anforderungen von übergreifender Notfallszenarien (bspw. erheblicher Ausfall der Kommunikationsinfrastruktur) auf Basis von Erkenntnissen aus dem KVP-Prozess
- Stärkung der Cyber-Resilienz durch Verzahnung von Informationssicherheit, BCM und Krisenmanagement; Alarmierungsverfahren zum IT-Notfallmanagement
- Häufige Schwachstellen bei der Umsetzung von Notfallkonzepten und Notfalltests
- Ermittlung und Berichterstattung von Kontinuitätsrisiken (BCM und ITSCM) an die Geschäftsleitung – Handlungsfelder in der Praxis

Seminarziel

Die neuen DORA-Vorgaben und MaRisk fordern eine deutliche Verbesserung des IKT-Notfallmanagements, der IT-Notfallkonzepte sowie des Business Continuity Managements (BCM) und IT Service Continuity Managements (ITSCM) bei Instituten und Dienstleistern(!), um Risiken frühzeitig zu erkennen und Gegenmaßnahmen umzusetzen.

Schwerwiegendere Feststellungen im Auslagerungs- und Notfallmanagement sowie die Zunahme von Cyber-Risiken haben zu erweiterten aufsichtsrechtlichen Vorgaben geführt.

Zuständigkeiten von Notfallbeauftragten und Krisenstäben sowie Notfallmaßnahmen müssen klar definiert, dokumentiert und intern kommuniziert werden. Die Aufsicht verlangt häufigere (Gesamt-)Notfalltests und die Einbindung von Dienstleistern in Übungen und Konzepte. Änderungen in Bedrohungslage und Wirksamkeit der Notfallkonzepte sind im Risikomanagement zu erfassen und im Notfallplan zu berücksichtigen. Das BCM muss so gestaltet sein, dass die Resilienz zeitkritischer Prozesse gestärkt, auf Vorfälle adäquat reagiert (SIEM) und der Geschäftsbetrieb schnell wieder aufgenommen werden kann. Eine ganzheitliche Betrachtung bleibt zentral.

Das Seminar beantwortet aktuelle Prüfungs- und Praxisfragen zu DORA und liefert praxisnahe Empfehlungen und Tipps.

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.

Alexander Rothländer
Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank, Frankfurt/Main

Alexander Rothländer arbeitet als Bankgeschäftlicher Prüfer für die Deutsche Bundesbank. In dieser Funktion prüft er die Risikomanagementprozesse von Banken »vor Ort«. Die Prüfungen erstrecken sich auf bedeutende und weniger bedeutende Kreditinstitute im nationalen und internationalen Umfeld. Zuvor hat er als Entwickler und IT-Projektleiter Erfahrungen in den Bereichen Entwicklung, Betrieb und Ablösung von IDV-Anwendungen gesammelt

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 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.

DORA-konforme Dienstleister-Steuerung bei Weiterverlagerungen & DL-Konzentrationen
23. Juli 2025, Online-Veranstaltung

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

Abstimmung Notfall-Konzepte und BCM-Prozesse mit dem (IKT-)Dienstleister
16. September 2025, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen
18. September 2025, Online-Veranstaltung

Praxis-Umsetzung aktueller DORA- und Aufsichts-Anforderungen in der DL-Steuerung
22. September 2025, Online-Veranstaltung

Risikomanagement im Fokus der Aufsicht
23. September 2025, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement
23./24. September 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

Dienstag, 21. Oktober 2025
9:30–17:00 Uhr
Online-Zugang ab 9:15 Uhr

Seminar-Nr. 25 10 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.

05.25 / 25 10 BA038

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