

DORA KOMPAKT!

IKT-Notfallmanagement, Kritikalitätsanalyse & DORA-Praxiserfahrungen



Banken-Aufsicht-Seminar · 8 CPE-Punkte

- Notfallmanagement & BCM/ITSCM unter DORA: Erwartungen und neue Anforderungen aus DORA, MaRisk, EBA-Leitlinien
- Erweiterte MaRisk-/ICT-/DORA-Vorgaben zur Bestimmung der IT-Schutzobjekte und Durchführung der Kritikalitätsanalyse
- Schutzbedarfs-/Risikoanalysen sowie IKT-Sicherheitsmaßnahmen nach DORA unter Einbezug von IDV & externen IKT-Dienstleistern
- DORA in der Praxis: Erkenntnisse zur DORA-Umsetzung aus der Jahresabschlussprüfung – Mängel & identifizierte Schwachstellen

Referenten

Dr. Jens Gampe
Referatsleiter Bundeswehrverwaltung
Berlin, ehem. BaFin-Referent, Experte
für Krisenprävention im Finanzsektor

Dirk Mühlhausen
IT-Prüfer und Prüfungsleiter
Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Mainz

Prof. Dr. Ralf Kühn, CIA, CISA
Wirtschaftsprüfer, CPA, Steuerberater
Finance Audit GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft, Ettlingen

Programm

Dr. Jens Gampe · 9:30 –12:00 Uhr

**Notfallmanagement und BCM/ITSCM unter DORA:
Regulatorische Erwartungen und neue Anforderungen aus
DORA, MaRisk, 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, Implementierung von Systemen zur Echtzeitüberwachung und Bedrohungserkennung
- Häufig identifizierte Schwachstellen und Prozess-Schwächen in den Instituten
- 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

Dirk Mühlhausen, Bundesbank · 12:45 –14:45 Uhr

**Erweiterte MaRisk-/ICT-/DORA-Vorgaben zur Bestimmung der
IT-Schutzobjekte und Durchführung der Kritikalitätsanalyse**

- Neue Anforderungen an IKT-Kontrollfunktion, (IT-)Revision, Informationssicherheits-Beauftragte (ISB) und Datenschutz
- Ermittlung von Schadenspotenzialen, Ableitung von Maßnahmen zur Umsetzung der Schutzziele (Sollmaßnahmenkatalog), die Plausibilität sowie eine nachvollziehbare und angemessene Dokumentation
- Überleitung der IT-Restrisiken in das OpRisk-Management
- DORA-Anforderungen bei IKT-DL i.Z.m. IT-Schutzobjekten

**Anforderungen an Schutzbedarfs- und Risikoanalysen sowie
die IKT-Sicherheitsmaßnahmen nach DORA unter Einbezug
von IDV und externen IKT-Dienstleistern**

- Strukturanalyse der IT-Architektur: Identifikation und Gruppierung der IT-Schutzobjekte sowie kritischer und wichtiger Funktionen (kowf)

- Zuordnung geplanter bzw. nachträglich identifizierter IDV-Anwendungen zu einer Schutzbedarfsklasse
- Schutzbedarfsklassifizierung und IKT-Sicherheitsmaßnahmen von IKT-Dienstleistungen
- Durchführung von DORA-Risiko- und Restrisikoanalysen
- DORA-OpRisk-Reporting unter Einbezug externer IKT-DL

Prof. Dr. Ralf Kühn, Finance Audit · 15:00 –17:00 Uhr

**DORA in der Praxis: Aktuelle Erkenntnisse zur
DORA-Umsetzung aus der aktuellen Prüfungs-Praxis –
Häufige Mängel und identifizierte Schwachstellen**

- DORA-Gap-Analyse bei Instituten und (IKT-)Dienstleistern
- Im Fokus: ECHTE Cyber-Resilienz bei Banken und DL
- DORA-Konformität: Ergebnisse der Überprüfung der von Dienstleistern betriebenen/gewarteten IKT-Systeme
- Identifizierte Schwachstellen in den Frühwarnsystemen für IKT-Vorfälle und den angeschlossenen Meldeprozessen
- Regelbasierte Dienstleistersteuerung – ein Muss nach DORA aus Effektivitäts- und Effizienzüberlegungen
- Teilweise mangelhafte Vorgehensweise bei der Identifikation kritischer oder wichtiger Funktionen sowie der DORA-konformen Steuerung kritischer IKT-Drittanbieter und der Bewertung von Konzentrationsrisiken (insb. bei Weiterverlagerungen und Sub-Dienstleistungen)
- Prüfungs-Erkenntnisse bzgl. der Durchführung instituts-eigener Schwachstellenscans und Penetrationstests
- Handlungsbedarf: Behebung der DORA-Schwachstellen im ISM, IRM und (IT-)Notfallmanagement (BCM/ITSCM)
- Prüfungsergebnisse zu Lieferkettenrisiken – auf was geachtet werden muss!
- Prüfungserkenntnisse aus IKT-Dienstleisterprüfungen: Welche DORA-Anforderungen an die Dienstleister bzgl. der Unterstützung ihrer »Kunden-Institute« (u. a. Cyber-Risiko) müssen noch weiter umgesetzt werden?
- Praxistipps und Prüfungsansätze für die Interne Revision

Seminarziel

Die Anforderungen aus DORA, MaRisk und den EBA-Leitlinien stellen Institute vor wachsende Herausforderungen aufgrund unklarer Kritikalitätsanalysen, lückenhafter Notfalltests, Schwächen in der Dienstleistersteuerung und Defiziten bei Frühwarnsystemen.

Externe Prüfungen zeigen, dass viele Häuser die regulatorischen Erwartungen noch nicht ausreichend erfüllen – mit Risiken für Informationssicherheit, Dienstleistersteuerung, IKT-Compliance und tatsächliche Resilienz.

Genau hier setzt das Seminar an: Es zeigt praxisnah, wie Notfallmanagement, BCM/ITSCM sowie Schutzbedarfs- und Risikoanalysen DORA-konform umgesetzt werden.

Teilnehmende erhalten konkrete Lösungsansätze zur Behebung typischer Schwachstellen, zur Integration von IKT-Risiken in das OpRisk-Management und zur wirksamen Steuerung externer Dienstleister.

Ziel ist es, nicht nur regulatorische Vorgaben zu erfüllen, sondern eine belastbare, reversionssichere und tatsächlich wirksame DORA-Resilienz im Institut aufzubauen.

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- Interne Revision, IT-Revision, (IT-)Risikomanagement und Organisation
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- Informationssicherheit (ISB), Informationsrisikomanagement und Compliance

Sowie andere interessierte Fach- bzw. Grundsatzbereiche, externe Prüfer*innen und Dienstleister/Mehrmandantendienstleister.

Unsere Referenten



Dr. Jens Gampe

Referatsleiter Bundeswehrverwaltung* Berlin
Experte für Krisenprävention im Finanzsektor

Dr. Jens Gampe ist seit Mitte 2023 in der Bundeswehrverwaltung tätig. Davor war er nach diversen Stationen in der Fachaufsicht der BaFin viele Jahre im IT-Grundsatz beschäftigt und u. a. maßgeblich an der Erarbeitung und Novellierung der BAIT beteiligt. Des Weiteren war er u. a. für die operative IT-Mehrmandantendienstleister-Überwachung und die Krisenprävention im Finanzsektor zuständig und BaFin-Vertreter im Nationalen Cyberabwehrzentrum.



Dirk Mühlhausen

IT-Prüfer und Prüfungsleiter Bankgeschäftliche Prüfungen
Deutsche Bundesbank*, Mainz

Dirk Mühlhausen besitzt langjährige Erfahrungen als Prüfer und Teamleiter in der Banken- und Finanzaufsicht der Deutschen Bundesbank im Bereich der MaRisk-Prüfungen für Finanzinstitute unterschiedlicher Art und Größe, sowohl national als auch international. Seine Schwerpunkte liegen insbesondere auf Prüfungen des IT-Risikomanagements für bedeutende und weniger bedeutende Institute sowie bei verschiedenen IT-Dienstleistern. Der Referent vertritt seine persönliche Auffassung und nicht diejenige der Deutschen Bundesbank bzw. der Aufsicht und nimmt keine offiziellen Auslegungen zu regulatorischen Vorgaben vor.



Prof. Dr. Ralf Kühn, CIA, CISA

Wirtschaftsprüfer, CPA, Steuerberater, Finance Audit GmbH*
Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft, Ettlingen

Prof. Dr. Ralf Kühn ist Geschäftsführender Gesellschafter einer mittelständischen Wirtschaftsprüfungsgesellschaft mit langjähriger nationaler und internationaler Erfahrung in der Steuerung strategischer Großprojekte mit Schwerpunkt IT, IKS, Compliance und Revision.

* Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht die eines bestimmten Instituts, der Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wieder. Die Referenten nehmen auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.

Anforderungen an IT-Infrastruktur & IT-Betrieb unter DORA

23. Juni 2026, Online-Veranstaltung

TPRM Spezial: DORA-Anforderungen an Software as a Service (SaaS) & Cloud-Dienste

8. Juli 2026, Online-Veranstaltung

DORA- und Praxis-Anforderungen an das Berechtigungsmanagement und die SOD-Matrix

13. Juli 2026, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken

21. Juli 2026, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)

22. Juli 2026, Online-Veranstaltung

Neuer IKT-Risikomanagement-Rahmen nach DORA

11. September 2026, Online-Veranstaltung

DORA-konforme Auslagerungsverträge/SLAs

16. September 2026, 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 KOMPAKT!

Name
Vorname
Position
Firma
Straße/Nr.
PLZ/Ort
Telefon
E-Mail
Name der Assistenz
Datum/Unterschrift

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

Termin und Seminarzeiten

Donnerstag, 10. September 2026

9:30–17:00 Uhr

Online-Zugang ab 9:15 Uhr

Seminar-Nr. 26 09 BA227 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 auf Wunsch 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 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 für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de