

DORA im Fokus von Aufsicht & Prüfern

Erkenntnisse, Prüfungserfahrungen, weitere Umsetzung



Banken-Aufsicht-Seminar · 8 CPE-Punkte

- DORA – aktueller Stand und weitere proportionale Umsetzung (insb. RTS/ITS)
- Identifizierte Fallstricke und bestehende Umsetzungslücken aus aktuellen Aufsichts- und Jahresabschlussprüfungen
- Weitere notwendige Anpassungen im IKT-Risikomanagement
- DORA in der Prüfungs-Praxis: Überprüfung der DORA-Konformität von (IKT-)Dienstleistern und Cloud Service Providern
- Vorfallsmeldungen, TLPT-Tests, Steuerung des IKT-Drittparteirisikos

Referenten

Dr. Jens Gampe
Referatsleiter Bundeswehrverwaltung
Experte für Krisenprävention
im Finanzsektor, Berlin

Mag. Marvin Nadler
IT-Risiko-Aufsicht
über Banken
Finanzmarktaufsicht, Wien

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

Programm

Dr. Jens Gampe, BWV, ehem. BaFin · 09:00 – 12:00 Uhr

DORA – aktueller Stand der Umsetzung: IKT-Risiken als wesentliche Herausforderung für die operative Widerstandsfähigkeit, Leistungsfähigkeit und Stabilität im Finanzsektor

- Der IKT-Risikomanagementrahmen (Kap. II DORA, RTS gem. Art. 15) – inkl. vereinfachtem Rahmen für kleinere Institute (RTS Art. 16 Abs. 3)
- Meldepflichten bei IKT-Vorfällen und IKT-Bedrohungen (Kap. III, RTS Art. 18 Abs. 3); Einheitliche Kriterien zur Klassifizierung und Meldung schwerwiegender IKT-Vorfälle an die Aufsichtsbehörden
- Resilienztests & TLPTs (Kap. IV DORA) Umfang, Methoden und Schwellenwerte für «Threat-Led Penetration Testing» (TLPT) je nach Risikoprofil – Umsetzungshilfen der Aufsicht
- KT-Drittparteienrisiko: Strategien & Registerpflicht (Kap. V, RTS & ITS zu Art. 28) – Anforderungen an Verträge, Risikobewertung und das Informationsregister
- Kritische IKT-Drittdienstleister: Überwachung und Einstufung (Art. 31–44, Delegierte VO 2024/896) und Abgrenzung zu IKT-Dienstleistungen, die kritische oder wichtige Funktionen (kowFs) unterstützen
- Weitere (proportionale) Umsetzung in Deutschland: Verhältnis zur bestehenden MaRisk (u. a. AT 9) sowie den weggefallenen XAIT-Anforderungen – Konfliktpotenziale

Mag. Marvin Nadler, FMA · 12:45 – 14:45 Uhr

Proportionale DORA-Umsetzung bei Instituten und Dienstleistern & Erfahrung aus einem Jahr DORA-Aufsicht

- DORA-Proportionalität: Erwartungen der Bankenaufsicht an eine proportionale Umsetzung und Operationalisierung
- Erfahrungen aus einem Jahr DORA-Aufsicht – Highlights, Herausforderungen & Way Forward
- Governance: Erweiterte Anforderungen an die Abstimmung von Geschäfts-/Risikostrategien und IKT-Risikomanagement; besondere Verantwortung der GL
- IKT-Risikomanagement: Einrichtung und Aufrechterhaltung stabiler IKT-Systeme und IKT-Instrumente

- Meldung IKT-bezogener Vorfälle: Einrichtung instituts-individueller Managementprozess zur Überwachung, Protokollierung und Meldung IKT-bezogener Vorfälle
- Prüfung digitale Betriebsstabilität: nötige Prozessequalität
- Risikobewertung von IKT-Drittanbietern: Beurteilung der vertraglichen Regelungen mit IKT-Dienstleistern
- Informationsaustausch Institute/Dienstleister/Aufsicht: Möglichkeit des Austauschs von Informationen und Erkenntnissen über Cyberbedrohungen
- TLPT-Tests und Steuerung des IKT-Drittparteienrisikos

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

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

- Inwieweit haben die auslagernden Institute bereits alle DORA-Anforderungen in den Dienstleister-Steuerungsprozessen und Arbeitsanweisungen abgebildet?
- ECHTE Cyber-Resilienz auf Banken- und Dienstleisterseite
- Ergebnisse der DORA-Überprüfung der von Dienstleistern betriebenen/gewarteten IKT-Systeme
- Identifizierte Schwachstellen in den Frühwarnsystemen
- Regelbasierte Dienstleistersteuerung – ein Muss nach DORA aus Effektivitäts- und Effizienzüberlegungen
- 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 institutseigener Schwachstellenscans und Penetrationstests
- Behebung aktueller DORA-Schwachstellen im ISM, IRM und (IT-)Notfallmanagement (BCM/ITSCM)
- Prüfungsergebnisse zu Lieferkettenrisiken
- Praxistipps und Prüfungsansätze für die Interne Revision

Seminarziel

Das Seminar «DORA im Fokus von Aufsicht & Prüfern» beleuchtet die aktuellen regulatorischen Anforderungen an die digitale operationelle Resilienz im Finanzsektor und deren praktische Umsetzung aus Sicht von Aufsicht, Prüfung und Instituten. Im Mittelpunkt stehen der IKT-Risikomanagementrahmen, Meldepflichten bei IKT-Vorfällen, Resilienztests einschließlich TLPTs sowie das Management von IKT-Drittparteienrisiken und kritischen Dienstleistern.

Dabei werden auch nationale Besonderheiten und Konfliktpotenziale im Zusammenspiel mit bestehenden Vorgaben adressiert. Auf Basis der Erfahrungen aus einem Jahr DORA-Aufsicht werden Erwartungen an eine proportionale Umsetzung, Governance-Anforderungen und die Verantwortung der Geschäftsleitung ebenso diskutiert wie wirksame Prozesse zur Vorfallobermittlung, Drittanbietersteuerung und zum Informationsaustausch über Cyberbedrohungen.

Ergänzend geben aktuelle Prüfungserkenntnisse aus Jahresabschluss- und Dienstleisterprüfungen Einblick in typische Schwachstellen, häufige Umsetzungsdefizite und konkrete Handlungsbedarfe – von Gap-Analysen über Lieferkettenrisiken bis hin zu Cyber-Resilienz, Notfallmanagement und Internen Revisionsansätzen.

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche:

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

Sowie andere interessierte Fach- bzw. Grundsatzbereiche, externe Prüferinnen und Prüfer sowie Dienstleister/Mehrmandantendienstleister.

Unsere Referenten



Dr. Jens Gampe

Referatsleiter Bundeswehrverwaltung* Berlin, ehem. BaFin*-Referent, Experte für Krisenprävention im Finanzsektor, Berlin

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.



Mag. Marvin Nadler

IT-Risiko-Aufsicht über Banken
Finanzmarktaufsicht*, Wien

Marvin Nadler ist seit 2023 in der FMA tätig und aktuell Teil des Teams IT-Risiko-Aufsicht in der Abteilung Conduct- und IT-Risiko-Aufsicht über Banken. In seiner Rolle verantwortet er die Beaufsichtigung von IKT-Risiken im Bereich der LSIs. Der Referent vertritt seine persönliche Auffassung und nicht diejenige der FMA, 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, Ettlingen

Prof. Dr. Ralf Kühn ist Geschäftsführender Gesellschafter einer mittelständischen Wirtschaftsprüfungs- und Steuerberatungsgesellschaft mit langjähriger nationaler und internationaler Erfahrung in der Betreuung von Prüfungs- und Beratungsmandaten sowie der Steuerung strategischer Großprojekte mit Schwerpunkt IT, IKS, Compliance und Revision in der deutschen und europäischen Kreditwirtschaft.

* 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.

KI-Governance: Aufsichts-Anforderungen
an den Einsatz von Künstlicher Intelligenz
14. April 2026, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an
Notfallmanagement & BCM
20. April 2026, Online-Veranstaltung

Abgrenzung und parallele Steuerung von
Auslagerungen (MaRisk) & IKT-Dienstleistungen (DORA)
28. April 2026, Online-Veranstaltung

Auslagerungen & IKT-Dienstleistungen im Fokus
von Aufsicht, MaRisk & DORA
29. April 2026, Online-Veranstaltung

DORA-Umsetzung bei KVGen
30. April 2026, Online-Veranstaltung

Risikoanalyse von Auslagerungen (MaRisk) & IKT-DL (DORA)
5. Mai 2026, Online-Veranstaltung

Zertifikatslehrgang Auslagerungsmanagement (MaRiks) &
(IKT-)Dienstleistersteuerung (DORA)
15. bis 17. Juli 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 im Fokus von Aufsicht & Prüfern

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

Dienstag, 12. Mai 2026
9:00 – 17:00 Uhr
Online-Zugang ab 8:45 Uhr
Seminar-Nr. 26 05 BA099 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
HEIDELBERG**

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de