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

AKADEMIE HEIDELBERG

DORA-UpDate! – Aktueller Stand!

Banken-Aufsicht-Seminar · 8 CPE-Punkte

- **DORA – Aktueller Stand und weitere proportionale Umsetzung**
- **Von der prinzipienbasierten (MaRisk) zur regelungsorientierten Regulierung nach DORA (insb. RTS/ITS)**
- **Identifizierte Fallstricke und bestehende blinde Flecken bei der bisherigen DORA-Umsetzung**
- **Weitere notwendige Anpassungen im IKT-Risikomanagement**
- **DORA in der Praxis: Überprüfung der DORA-Konformität von (IKT-)Dienstleistern und Cloud Service Providern**

Umstellung der Dienstleister- & Dienstleistungs-Prozesse!

20 Jahre AKADEMIE HEIDELBERG

Referenten

Dr. Jens Gampe
Ehem. BaFin-Referent
im Bereich Überwachung, IT-MMDL, Krisenprävention und Incident-Reporting

Dr. Markus Held
Referatsleiter Sicherheit in der IT-Konsolidierung des Bundes
BSI, Bonn

Prof. Dr. Ralf Kühn, CIA, CISA
Wirtschaftsprüfer, CPA, Steuerberater
Finance Audit GmbH, Wirtschaftsprüfungs-gesellschaft, Steuerberatungsgesellschaft

DORA-UpDate! – Aktueller Stand!

Programm

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

DORA – aktueller Stand der Umsetzung: IKT-Risiken als wesentliche Herausforderung für die operative Resilienz, Leistungsfähigkeit und Stabilität der Banken und Sparkassen

- Aktuelle Lage der Digitalen Operationalen Resilienz im Finanzsektor – aktuelle Cyber-Bedrohungslage und operative Auswirkungen für Finanzinstitute
- 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
- IKT-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 und Abgrenzung der DORA-Anforderungen zu bestehenden nationalen Anforderungen; Status quo

Dr. Markus Held, BSI · 12:45–14:45 Uhr

Weitere proportionale DORA-Umsetzung: Vorgehensweisen und weitere notwendige Anpassungen im IKT-Risikomanagement

- Von der Prinzipien- zur Regelungsorientierung: DORA als Zäsur in der IT-Regulierung – wie sich die Qualität der Anforderungen von MaRisk/BAIT zu DORA verändert hat
- DORA-Governance: Verantwortung des Leitungsorgans
- Weitere notwendige Harmonisierungen der Tools und Prozesse durch das IKT-Risikomanagementrahmenwerk – Aufbau und Steuerung eines effektiven IKT-RMS
- Neue Anforderungen an die IKT-Entwicklung, Überwachung (SIEM/SOC), Notfallübungen und Systemhärtung aus Sicht von DORA
- IKT-Drittparteienmanagement: Abschied von der Unterscheidung »Auslagerung vs. Fremdbezug«
- Cloud, KI & kritische Abhängigkeiten: Umgang mit asymmetrischen Informationslagen, geopolitischem Risiko und dem Trend zur Konzentration bei Big-TECs
- Gap-Analyse und Maßnahmenmanagement: SMART-Ziele, Dokumentationspflichten und DORA-Projektsteuerung
- Fallstricke und blinde Flecken: Typische IT-Management-Fehler der DORA-Umsetzung und deren Vermeidung
- DORA als Chance zur Effizienzsteigerung

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

DORA in der Praxis: Überprüfung der DORA-Konformität von (IT-)Dienstleistern und Cloud Service Providern

- Gap-Analyse bei (IKT-)Dienstleistern zur Identifizierung von (Sicherheits-)Lücken: Welche Prüfungen sind (vor Ort)
- Einzelprüfung oder Sammelprüfung – Kontrollmöglichkeiten der Institute bei Dienstleistern und Cloud-Anbietern
- Überprüfung der von Dienstleistern betriebenen/gewarteten IKT-Systeme auf DORA-Konformität
- Beurteilung der Frühwarnsysteme für IKT-Vorfälle und des Reifegrads der angeschlossenen Meldeprozesse
- Bewertung von Konzentrationsrisiken (insb. bei Weiterverlagerungen und Sub-Dienstleistungen)
- Schwachstellenscans und Penetrationstests mit konkreter Ausrichtung auf neue DORA-Vorgaben (TPRM)
- Handlungsbedarf: Behebung aktueller »BAIT«-Probleme
- Anforderungen an die Dienstleister bzgl. der Unterstützung »ihrer Kunden«-Institute (u. a. beim Thema Cyber-Risikomanagement)

Seminarziel

Die Umsetzung der DORA-Verordnung stellt Banken und Sparkassen vor erhebliche praktische und strategische Herausforderungen: Viele Institute kämpfen mit der Komplexität der neuen Anforderungen, unklaren Abgrenzungen zu bestehenden Regelwerken wie MaRisk und den außer Kraft gesetzten BAIT sowie mit der strukturellen und operativen Integration zahlreicher RTS und ITS. Besonders das IKT-Risikomanagement, Meldepflichten bei Cybervorfällen und die Kontrolle ausgelagerter IKT-Dienstleistungen verursachen großen Umsetzungsaufwand.

Gleichzeitig wächst die Bedrohungslage durch Cyberangriffe und geopolitische Instabilitäten – digitale Resilienz wird zur Überlebensfrage im Finanzsektor.

Im Seminar »DORA-UpDate!« erhalten Teilnehmende einen kompakten, praxisnahen Überblick über die DORA-Vorgaben und den Umsetzungsstand bei Aufsicht und Instituten. Im Fokus stehen dabei das Leitungsorgan, Anforderungen an das IKT-Risiko-management, Meldepflichten, Resilienztests, Registerpflichten sowie der Umgang mit IKT-Drittdienstleistern und kritischen Cloud-Anbietern. Zudem werden zentrale Konfliktlinien zur nationalen Regulierung behandelt. Die Teilnehmenden lernen, wie sie DORA-konforme Gap-Analysen, Prüfungen und Maßnahmenprogramme effizient gestalten – inklusive Good Practices für IT-Governance, Reifegradmodelle und DORA-Strategie.

Zielgruppe

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- Interne Revision und IT-Revision
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- (IT-)Risikomanagement und IKT-Kontrollfunktion
- Informationssicherheit (ISB) und Informationsrisikomanagement
- Datenschutz und Data Governance sowie Organisation
- Compliance und Regulatorik
- sowie andere interessierte Fach- bzw. Grundsatzbereiche, externe Prüfer*innen, Dienstleister und Mehrmandantendienstleister

Unsere Referenten

Dr. Jens Gampe
Ehem. BaFin-Referent im Bereich Überwachung, IT-MMDL
Krisenprävention und Incident-Reporting

Dr. Jens Gampe ist seit dem 1. August 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. Nach Veröffentlichung der BAIT-Novelle war er u. a. für die operative IT-Mehrmandanten-dienstleister-Überwachung und die Krisenprävention im Finanzsektor zuständig.

Dr. Markus Held
Referatsleiter Sicherheit in der IT-Konsolidierung des Bundes
Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Dr. Markus Held war 2010 bis 2015 bei der BaFin in der Aufsicht über die IT bei Banken tätig und wechselte anschließend als Referatsleiter zum BSI. Er befasst sich seit Beginn seines Berufslebens aus verschiedenen Perspektiven mit IT-Regulierung, Informationssicherheit, IT-Infrastrukturen, Cloud Computing und IT-Governance, insbesondere in der Finanzindustrie und in der Bundesverwaltung.

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

Prof. Dr. Ralf Kühn ist Geschäftsführender Gesellschafter einer mittelständischen Wirtschafts-prüfungs- 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. Als Referent aus der Praxis für die Praxis greift er auf einen umfassenden Erfahrungsschatz zurück.

Prüfung (IT-)Auslagerungen (MaRisk) & (IKT-)Drittdienstleistungen (DORA)
9. Juli 2025, Online-Veranstaltung

Zertifikats-Lehrgang Auslagerungsmanagement (MaRisk) & IKT-Dienstleistersteuerung (DORA)
16. bis 18. Juli 2025, Online-Veranstaltung

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

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

DORA-konformes IKT-Risikomanagement
23./24. September 2025, Online-Veranstaltung

DORA-konforme Auslagerungsverträge & SLAs
30. September 2025, Online-Veranstaltung

DORA-konformer Umgang mit Eigenanwendungen und IDV
7. Oktober 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

DORA-UpDate! – Aktueller Stand!

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

Mittwoch, 17. September 2025
9:30–17:00 Uhr
Online-Zugang ab 9:15 Uhr

Seminar-Nr. 25 09 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, 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.

06.25 / 25 09 BA099

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