27. Mai 2025 · 10:00–17:00 Uhr
28. Mai 2025 · 9:00–16:00 Uhr

AKADEMIE HEIDELBERG

Fachtagung IKT-Aufsicht

Aktuelle Aufsichts-Anforderungen – Erste DORA-Prüfungserfahrungen

Banken-Aufsicht-Tagung · 16,5 CPE-Punkte

- **DORA: Aktueller Stand und erste Prüfungserfahrungen**
- **Aufsichtliche Anforderungen an die KI-Nutzung und das Risikomanagement bei KI-Einsatz**
- **Microsoft-Praxisbericht: DORA aus Sicht eines Cloud-Dienstleisters – Zentrale Aspekte der IKT-Compliance bei der Nutzung von Hyperscalern**
- **DORA-Anforderungen zum IKT-Geschäftsfortführungsmanagement**
- **Umgang mit Drittpartei-Risiken und ICT-Risiken**
- **Erste Melde-Erfahrungen zum DORA-Informationsregister – Anpassungsbedarf in der Praxis und künftige Abgrenzung zum Auslagerungsregister und Auslagerungsmeldungen gemäß MaRisk**

Konkrete und direkt wirksame Verbesserungen Ihrer IKT-Governance!

20 Jahre AKADEMIE HEIDELBERG

Referenten

David Rother
Prüfungsleiter & Teamleiter
Bankgeschäftliche IT-Prüfungen,
Deutsche Bundesbank, München

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

Dr. Markus Held
Referatsleiter Informationssicherheit
Bundesamt für Sicherheit in der
Informationstechnik (BSI), Bonn

Dr. Thomas Klühspies
Prüfungsleiter Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank
München

Bastian Bahnemann
FSI Compliance & Business Development Lead
Microsoft
Hannover

Carsten Hoeschel
Experte Outsourcing Governance
Deutsche Börse AG
Eschborn

Fachtagung IKT-Aufsicht

Programm Tag 1 · 27. Mai 2025

David Rother, Bundesbank · 10:00–12:00 Uhr

DORA: IKT-Risikomanagement als solide Basis für die Schaffung operationeller Resilienz – Erwartungen hinsichtlich der weiteren Umsetzung und Anpassungen in den Instituten

- DORA-Umsetzung: Eine Standortbestimmung
- IKT-Risikomanagement als solide Basis für die Schaffung operationeller Resilienz
- Festlegung Schutzbedarf vs. Identifikation kritischer/wichtiger Funktionen
- Einbindung (kritischer) Drittdienstleister
- Stolpersteine und häufige Missverständnisse bei der Umsetzung der Anforderungen
- Was ändert sich durch den Wegfall der BAIT? – Inwieweit bleiben die BAIT-Anforderungen in der aufsichtlichen Prüfungspraxis erhalten
- Häufige Schwachstellen im IKT-Risikomanagement

Dr. Markus Held, BSI · 13:00–15:00 Uhr

Aufsichtliche Anforderungen an die KI-Nutzung und das Risikomanagement bei KI-Einsatz

- Überblick über relevante Regulatorische Rahmenbedingungen (u. a. DORA, AI Act) für den Einsatz von KI-Modellen und deren Auswirkungen auf den Finanzsektor
- Risiken und Risikoklassifizierung von KI-Systemen und Einbindung von KI-Systemen in das Risikomanagementsystem
- IT-Sicherheitsanforderungen zum Schutz vor Manipulationen, Datenlecks und anderen Cyber-Bedrohungen bei KI-Einsatz
- Wege zur Behandlung KI-spezifischer Risiken
- Anforderungen an Datenmanagement und Datenqualität für den Einsatz von KI-Modellen – neue betriebliche IT-Risiken (z. B. »Halluzinationen« der KI)
- Verantwortlichkeiten für die Entwicklung, Nutzung und Überwachung von KI-Systemen innerhalb der Organisation
- Möglichkeiten des Monitorings und der laufenden Überwachung von KI-Anwendungen
- Notfall- und Eskalationsmanagement für eine schnelle und effektive Fehlerbehebung
- Entwicklung von KI-Stresstests zur Prüfung der Robustheit von KI-Systemen

Bastian Bahnemann, Microsoft · 15:15–17:00 Uhr

Microsoft-Praxisbericht: DORA aus Sicht eines Cloud-Dienstleisters – Zentrale Aspekte der IKT-Compliance bei Nutzung von Hyperscalern

- Auswirkung der DORA-Anforderungen und DORA-Umsetzung auf die Dienstleistungsbeziehungen zwischen Microsoft und seinen Kunden aus dem Banken- und Finanzdienstleistungssektor
- Einordnung von Microsoft im Rahmen der neu geplanten (direkten) Beaufsichtigung kritischer Infrastrukturen
- Umgang mit Auslagerungssachverhalten bei Hyperscalern – Anforderungen an die Wahrnehmung von Prüfrechten und Durchgriffsrechten der Aufsicht sowie der auslagernden Institute
- DORA: Förderung transformativer Cloud-Technologie-Initiativen oder Überregulierung des europäischen Finanzplatzes – Deutsche Banken und Versicherungen im Vergleich zu Internationalen Microsoft-Kunden
- Unterstützungsleistungen von Microsoft zur Ermöglichung einer sicheren und resilienten Nutzung der IKT-Dienstleistungen im Rahmen finanzregulatorischer Erwartungen

Programm Tag 2 · 28. Mai 2025

Alexander Rothländer, Bundesbank · 9:00–11:00 Uhr

DORA-Anforderungen an das IKT-Geschäftsfortführungsmanagement

- Überblick über die rechtlichen Rahmenbedingungen im Geschäftsfortführungsmanagement und Berücksichtigung des Business Continuity Managements nach DORA
- Von der Übersicht über die Funktionen bis zur Auswertung von Testergebnissen: Aufsichtliche Erwartungen an die Prozesse im IKT-Geschäftsfortführungsmanagement
- Notwendigkeit aussagekräftiger und wirksamer Konzepte für das Geschäftsfortführungsmanagement: IKT-Geschäftsfortführungspläne und IKT-Reaktions- und Wiederherstellungspläne
- Anforderungen an einzurichtenden Kontrollen und Umgang mit Geschäftsfortführung bei IKT-Drittbezügen, auch von Cloudanbietern
- Prüfungshandlungen und häufige Feststellungen im IKT-Geschäftsfortführungsmanagement
- Praxishinweise und Tipps zur Umsetzung

Programm Tag 2 · 28. Mai 2025

Dr. Thomas Klühspies, Bundesbank · 11:15–13:00 Uhr
Umgang mit Drittpartei-Risiken und ICT-Risiken bei IKT-Dienstleistungen

- Aufsichtliche Anforderungen an den Umgang mit Drittpartei-Risiken und ICT-Risiken bei IKT-Dienstleistungen und Cloud-Services
- Anforderungen an die Risikobewertung und Due-Diligence-Verfahren vor der Auslagerung von IKT-Dienstleistungen zur Identifizierung potenzieller Risiken und Schwachstellen
- Erwartungen an die klaren vertraglichen Vereinbarungen und SLAs bezüglich der Definition und Abgrenzung der zu erbringenden Leistungen
- Abhängigkeiten von (Sub-)Dienstleistern – Umgang mit Dienstleisterkonzentrationen
- Regelmäßige Sicherheitsüberprüfungen des Dienstleisters
- Anforderungen an die regelmäßige Überwachung und unabhängige Prüfung der Drittparteien – Notwendigkeit von Vor-Ort-Prüfungen!?
- Exit-Strategie: Aufstellung realistischer Szenarien für einen reibungslosen Dienstleisterwechsel bei (kurzfristiger) Auslagerungsbeendigung

Carsten Hoeschel, Deutsche Börse · 13:45–16:00 Uhr
Erste Melde-Erfahrungen zum DORA-Informationsregister – Anpassungsbedarf in der Praxis und künftige Abgrenzung zum Auslagerungsregister gemäß MaRisk

- Erfahrungen aus der erstmaligen Meldung des DORA-Informationsregisters
- Anpassungsbedarf bzgl. Aufbau und Pflege eines vollständigen, aktuellen und übersichtlichen Informationsregisters (DORA) parallel zum zentralen Auslagerungsregister (MaRisk)
- Verantwortlichkeiten für die Erstellung, Befüllung und Aktualisierung des neuen Informationsregisters sowie die parallele Weiterführung des Auslagerungsregisters in der 2nd Line (Zugriffsberechtigungen!)
- Abgrenzung zwischen (wesentlichen) Auslagerungen und (sonstigen) Fremdbezügen sowie (kritischen/wichtigen) Drittdienstleistungen im Auslagerungsregister und Informationsregister
- Besondere Bedeutung der Erfassung von Sub-Dienstleister-Informationen und Dienstleister-Konzentrationen – auch im Informationsverbund!
- Praxisprobleme bei der Erfassung von neuen/geänderten Auslagerungsverträgen/SLAs

Tagungsziel

Die IKT-Risiken der Banken und Sparkassen haben deutlich zugenommen. Als Reaktion darauf hat die Bankenaufsicht ihre IT-Prüfungen spürbar intensiviert und ausgeweitet. Dabei sind teilweise schwerwiegende Mängel und Sicherheitslücken identifiziert worden. Die Aufsicht begegnet den zunehmenden Risiken im Bereich »IKT« daher mit weitreichenden neuen Anforderungen (u .a. DORA!).

Die Fachtagung IKT-Aufsicht beschäftigt sich mit den schlagenden Themen und aktuellen aufsichtlichen Anforderungen an die IKT und das Informationsrisikomanagement. Vertreter der Aufsicht und Experten aus der Praxis berichten über Ihre Erfahrungen und geben wertvolle Hinweise zum Umgang mit den aktuellen Problemstellungen.

Zielgruppe

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeiter*innen der Bereiche

- IT und Organisation
- Interne Revision und IT-Revision
- Informationssicherheit (ISB), Cyber-Sicherheit und Informationsrisikomanagement
- Notfallmanagement und Business Continuity Management (BCM)
- Datenschutz Data Governance
- (Zentrales) IT-Auslagerungsmanagement und IKT-Dienstleistersteuerung
- IT-Compliance und IKT-Governance
- Regulatorik und Grundsatz,

sowie andere interessierte Fachbereiche bzw. Grundsatzbereiche, Vorstände bzw. Geschäftsleitung und externe Prüfer*innen sowie Bankdienstleister

Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how für eine effiziente und dennoch institutsindividuelle Umsetzung der aktuellen aufsichtlichen Anforderungen in den Bereichen IKT und Informationsrisikomanagement
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut und Ihren Bereich
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit den erfahrenen Praxis-Referenten
- Sie erhalten wertvolle Praxis- und Prüfungstipps im Erfahrungsaustausch mit anderen Praktikern*innen

Referenten


David Rother
Prüfungsleiter & Teamleiter
Bankgeschäftliche Prüfungen,
Deutsche Bundesbank, München


Dr. Markus Held
Referatsleiter Informationssicherheit
Bundesamt für Sicherheit in der
Informationstechnik (BSI), Bonn


Bastian Bahnemann
FSI Compliance & Business Development Lead
Microsoft
Hannover


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


Dr. Thomas Klühspies
Prüfungsleiter Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank
München


Carsten Hoeschel
Experte Outsourcing Governance
Deutsche Börse AG
Eschborn

Seminar-Vorschläge

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

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

Auslagerungen & IKT-Dienstleistungen im Fokus von Aufsicht, MaRisk & DORA
2. April 2025, Online-Veranstaltung

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

Fachtagung IKT-Aufsicht

Name

Vorname

Position

Firma

Straße

PLZ / Ort

Telefon/Fax

E-Mail

Name der Assistenz

Datum Unterschrift

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

Termin und Seminarzeiten

Dienstag, 27. Mai 2025
10:00–17:00 Uhr
Mittwoch, 28. Mai 2025
9:00–16:00 Uhr
Seminar-Nr. 25 05 BA068 W

Teilnahmegebühr

€ 1.190,– (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 28 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de

03.25 / 25 05 BA068