15. Juni 2026 · 10:00–17:00 Uhr
16. Juni 2026 · 9:00–17:00 Uhr

AKADEMIE HEIDELBERG

Fachtagung IKT-Aufsicht

Praxis- & Prüfungs-Berichte zu aktuellen Themen der IKT-Regulatorik

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

- **Weitere DORA-Umsetzung – Notwendige Anpassungen in den Instituten**
- **Erstes Anwendungsjahr von DORA in der Praxis**
- **Erfahrungen aus einer EZB-Prüfung durch die IKT-Aufsicht**
- **Clusterings zur Bewertung von IKT-Dienstleistungen**
- **DORA-konformes Schwachstellenmanagement**
- **Identifikation und Abgrenzung von kritischen oder wichtigen Funktionen (kowFs) und Steuerung im TPRM**
- **DORA-Prüfungserfahrungen aus aktuellen Jahresabschlussprüfungen einer Wirtschaftsprüfungsgesellschaft**

Referenten

Daniel Schmidt
Prüfungsleiter Bankgeschäftliche Prüfungen
Deutsche Bundesbank
Hannover

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

Jens-Philip Merkle
Abteilungsdirektor Zentrales Auslagerungsmanagement
DZ BANK AG, Frankfurt/M.

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, aktuell SAP Systemservices Architektur, Zentrale IT-Plattform-management, Deutsche Bundesbank, Düsseldorf

Christian Wettlaufer
Auslagerungsbeauftragter Deka-Gruppe (stellv.), Zentrales Auslagerungsmanagement
DekaBank Deutsche Girozentrale, Frankfurt/M.

Ralph Hüsemann
Partner, Wirtschaftsprüfer, Vorsitzender des IDW-Arbeitskreises »Prüfung DORA«, Baker Tilly Wirtschaftsprüfungsgesellschaft, Frankfurt/M.

Omid Shams
Senior Manager, CISA
Baker Tilly Wirtschaftsprüfungsgesellschaft, Frankfurt/M.

Fachtagung IKT-Aufsicht

Programm 1. Tag · **Montag, 15. Juni 2026**

Daniel Schmidt, Bundesbank* · 10:00–12:00 Uhr

DORA: IKT-Risikomanagement als solide Basis für die Schaffung operationeller Resilienz – Vorgehen hinsichtlich der weiteren DORA-Umsetzung – Notwendige 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) IKT-Drittdienstleister
- Stolpersteine und häufige Missverständnisse bei der Umsetzung der Anforderungen
- Was ändert sich durch die MaRisk-Novelle bzgl. der Abgrenzung des Auslagerungsmanagements gegenüber der IKT-Dienstleistersteuerung nach DORA?
- Häufige Probleme im IKT-Risikomanagement

Dirk Mühlhausen, Bundesbank* · 13:00–15:00 Uhr

DORA-Umsetzungsstand: Erfahrungen aus dem ersten Anwendungsjahr von DORA in der Praxis

- Umsetzungsstand nach mehr als einem Jahr DORA
- Auswirkungen von DORA für LSI und »kleine« Institute: Inwieweit kann die Proportionalität durch verhältnismäßige Regulierung und Überwachung gewährleistet werden?
- Stolpersteine bei der Festlegung von Methoden zur Identifikation und Bewertung von kritischen oder wichtigen Funktionen
- Übergreifende Anforderungen, Mindestumfang und Überprüfung des IKT-Risikomanagementrahmens
- Mögliche Schwachstellen bei der Festlegung einer Risikotoleranzschwelle
- Bekannte Schwächen bei der Identifikation, Bewertung und Behandlung von IKT-Assets
- Defizite bei der Definition von IKT-Sicherheitsmaßnahmen und deren Umsetzungs-Überprüfung (inkl. Dienstleister)
- Schwachstellen in den Verfahren und Methoden zur Identifikation, Bewertung, Behandlung und Überwachung von IKT-Risiken
- Sonderfall: Risiken von IKT-Altsystemen
- Mögliche Schwierigkeiten bei der Implementierung eines IKT-Geschäftsfortführungsmanagements
- Anforderungen an die Berichterstattung von IKT-Risiken

Jens Merkle, DZ Bank* · 15:15–17:00 Uhr

Erfahrungen aus einer EZB-Prüfung durch die IKT-Aufsicht – Praxis-Möglichkeiten des Clusterings zur Bewertung von IKT-Dienstleistungen

- Praxis-Erfahrungen aus EZB-Prüfungen durch die Aufsicht
- Clustering als Analysewerkzeug: Gruppierung von IKT-Dienstleistungen nach Risikoprofil, Komplexität und Abhängigkeiten zur strukturierten Relevanz-Bewertung
- Einsatz von Clustering zur Trennung von »kritischen oder wichtigen Funktionen« sowie »nicht-kritischen« Services im Sinne der DORA-Anforderungen
- Praxis-Anwendung des Clusterings: Gruppierung einer Großzahl von IKT-Dienstleistungen nach den Prinzipien der Risikoorientierung und Proportionalität zur Schaffung beherrschbarer Analyse-Einheiten
- Einsatz von Entscheidungsbäumen: Gewährleistung eines systematischen und homogenen Bewertungsprozesses von IKT-Dienstleistungen anhand regulatorischer Merkmale zur nachhaltigen Verankerung in Fachbereichen und der Retained Organisation
- Nutzung des Verhältnismäßigkeitsprinzips: Systematische Einstufung der Relevanz von IKT-Dienstleistungen zur passgenauen, nachvollziehbaren und prüfungssicheren Steuerung des Analyseaufwands
- Cluster-basierte Ressourcen-Allokation: Gezielte Steuerung von Expertenressourcen auf Basis der Risikobewertung zur Effektivitätssteigerung im Auslagerungsmanagement
- Erleichtertes und übersichtlicheres Monitoring und Reporting durch clusterbasierte Dashboards für effizientes Reporting gegenüber Aufsicht und Management
- Skalierbarkeit des Bewertungsrahmens: Gestaltung eines zukunftssicheren Prozesses zur effizienten Handhabung einer wachsenden Anzahl und Komplexität von IKT-Dienstleistungen
- Praxis-Tipps für den Einsatz proportionaler Dienstleistungs-Cluster

Programm 2. Tag · **Dienstag, 16. Juni 2026**

Alexander Lohr, Bundesbank* · 9:00–12:00 Uhr

Ansätze für ein DORA-konformes Schwachstellenmanagement – Konkrete Erwartungen an ausgewählte Themen der operativen Informationssicherheit aus MaRisk und DORA

- Konkretisierung der Anforderungen der DORA an das Schwachstellenmanagement und die operative Informationssicherheit
- Identifikation, Bewertung und Behandlung von Schwachstellen – Anforderungen an die Nutzung eines Schwachstellenscanners (Netzwerkscan/authentifizierter Scan)
- Umgang mit Schwachstellen im Schwachstellenmanagement, Bündelung und Priorisierung, Reporting und Übertragung in das Risikomanagement
- Notwendigkeit regelmäßiger Penetrationstests: Angriffsszenarien, Root-Cause-Analyse, Bewertung der Ergebnisse
- Einsatz eines SIEM-Systems, notwendige Loganbindungen, Anforderungen an die Qualität der Logs und Speicherfristen, Entwicklung von Use Cases
- Security Operations Center (SOC), 24/7 Überwachung, Reporting von SIEM-Alarmen
- Schutz vor Schadsoftware, Datenabfluss, Verschlüsselung, Vorstellung klassischer Datenabflusskanäle
- Management zulässiger Software und IDV, Entwickler-Clients, administrative Benutzer, Skriptausführung und Überwachung
- IKT-Dienstleister – Prozesstransparenz und Steuerbarkeit
- Identifizierte Schwachstellen in der Praxis

Christian Wettlaufer, DekaBank* · 13:00–15:00 Uhr

Identifikation und Abgrenzung von IKT-Dienstleistungen zur Unterstützung von kritischen oder wichtigen Funktionen (kowFs) und Steuerung im TPRM – Erfahrungen aus ersten DORA-Prüfungen

- Identifikation von IKT-Dienstleistungen und kritischen oder wichtigen Funktionen gemäß DORA
- Organisatorische Rahmenbedingungen im TPRM für eine sinnvolle und risikoorientierte Steuerung der Auslagerungen, Fremdbezüge und IKT-Drittdienstleistungen
- Wesentlichkeit gemäß MaRisk vs. kritisch oder wichtige Funktionen gemäß DORA
- Abbildung des gesamten Zyklus einer Auslagerung bzw. eines Fremdbezuges in der TPRM-Prozesslandkarte – Auswirkungen der Abgrenzungsentscheidung auf die Bank- und Steuerungsprozesse
- Ausgestaltung einer Drittpartei-Risikobewertung nach DORA: Plausible und nachvollziehbare Einschätzung von IKT-Risiken (Risikobewertung = Risikoanalyse?)
- Praxisbeispiele für relevante kowF-Unterstützungsleistungen – Problemfeld »fehlende Auslagerungs-Governance«
- Gestaltung von Exit-Strategien für kowF-Dienstleistungen – Migration auf einen anderen Dienstleister, Auslagerungsbeendigung und Rückverlagerung
- Ausgestaltung von Service-Level Agreements und Durchführung von Kontrollhandlungen bei kowF-Dienstleistungen
- Best Practices und Handlungsempfehlungen für die parallele Steuerung von Auslagerungen, sonstigen Fremdbezügen und IKT-Dienstleistungen, die kowFs unterstützen

Ralph Hüsemann/Omid Shams, Baker Tilly*

15:15–17:00 Uhr

Prüfungserfahrungen aus DORA-Umsetzungsprüfungen und Erkenntnisse aus aktuellen Jahresabschlussprüfungen – Prüfungsansätze aus dem IDW EPS 528 (Prüfung aufsichtlicher DORA-Anforderungen) für die Interne Revision

- Erste DORA-Umsetzungsprüfungen: Prüfungserfahrungen und aktueller Stand in den Instituten
- Erkenntnisse aus aktuellen Jahresabschlussprüfungen
- Erweiterte und neue Prüfungsanforderungen, Prüfungsansätze und Prüffelder durch DORA:
  - Prüfung der DORA-Angemessenheit von Bankorganisation und Bankstruktur
  - Prüfung des IKT-Risikomanagementrahmens einschließlich Rollen und Verantwortlichkeiten
  - Prüfung des IKT-Informationsregisters auf Vollständigkeit und Aktualität aller IKT-Assets
  - Neues Prüfungsfeld: Identifikation und Klassifizierung »kritischer oder wichtiger Funktionen«
  - Prüfung des IKT-Vorfallsmeldewesens nach EU-weit einheitlichen Kriterien
  - Prüfung regelmäßiger Resilienztests jenseits klassischer Notfalltests zur Bestimmung der Widerstandsfähigkeit der IKT-Landschaft
  - Prüfung des IKT-Drittparteienrisikomanagements inkl. Ausstiegsstrategien
  - Einbezug externer IKT-Dienstleister in die Prüfungsreichweite
  - Neues Prüffeld: Informationsaustausch zu Cyberbedrohungen
- Möglichkeit der Nutzung proportionaler Prüfungsansätze durch die Interne Revision
- Praxis- und Prüfungs-Tipps für Fachbereiche, Interne Revision, externe Prüfer*innen und Geschäftsleitung

* 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.

Unser Referenten-Team

Daniel Schmidt
Prüfer Bankgeschäftliche Prüfungen
Deutsche Bundesbank*
Hannover

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

Jens-Philip Merkle
Abteilungsdirektor Zentrales
Auslagerungsmanagement
DZ BANK AG*, Frankfurt/M.

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, SAP Systemservices
Architektur, Zentrale IT-Plattformmanagement Drittprodukte
Deutsche Bundesbank*, Düsseldorf

Christian Wettlaufer
Auslagerungsbeauftragter Deka-Gruppe (stellv.)
Zentrales Auslagerungsmanagement
DekaBank Deutsche Girozentrale*, Frankfurt/M.

Ralph Hüsemann
Partner, Wirtschaftsprüfer, Vorsitzender des Arbeitskreises
»Prüfung DORA« beim IDW Baker Tilly GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft*, Frankfurt/M.

Omid Shams
Senior Manager, CISA
Baker Tilly GmbH & Co. KG Wirtschaftsprüfungsgesellschaft*
Frankfurt/M.

* 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.

Seminar- und Zertifikats-Vorschläge

DORA Spezial:
Informationssicherheit & IKT-Risikomanagement
7. Mai 2026, Online-Veranstaltung

IKT-Drittpartei-Risiken & Third Party Risk Management (TPRM) im Fokus von Aufsicht und DORA
18. Mai 2026, Online-Veranstaltung

Zertifizierter KI-Governance-Officer
17. bis 19. Juni 2026, Online-Veranstaltung

Zertifikats-Lehrgang Auslagerungsmanagement (MaRisk) & 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

Fachtagung IKT-Aufsicht

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

Montag, 15. Juni 2026
10:00–17:00 Uhr
Dienstag, 16. Juni 2026
9:00–17:00 Uhr

Seminar-Nr. 26 06 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 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de

03.26 / 26 06 BA068