

# Prüfung DORA & DORA-Umsetzung

Erste DORA-Prüfungserfahrungen – Prüfungsschwerpunkte & neue Prüffelder



## Banken-Aufsicht-Seminar · 14 CPE-Punkte

- Erste Prüfungserfahrungen aus DORA-Umsetzungsprüfungen
- Erwartungen der Aufsicht hinsichtlich der weiteren Umsetzung und Anpassungen in den Instituten
- Umgang mit Drittpartei-Risiken und ICT-Risiken bei IKT-Dienstleistungen
- Idealtypischer Auslagerungsprozess gem. DORA
- Prüfung AT 9 MaRisk in der Aufsichtspraxis vor dem Hintergrund der neuen DORA-Anforderungen und dem Wegfall der BAIT
- DORA in der Prüfungspraxis: Erweiterte Prüfungshandlungen und neue Prüffelder für Revision und externe Prüfer

Direkt anwendbare  
Praxishinweise und  
Umsetzungstipps!

**20** Jahre  
**AKADEMIE  
HEIDELBERG**

### Referenten



Axel Leckner (angefragt)  
Prüfungsleiter IT-Prüfungen im Rahmen  
der Bankgeschäftlichen Prüfung  
Deutsche Bundesbank, Hannover



Dr. Christopher Stolz  
Prüfungsleiter IT-Prüfungen  
Bankgeschäftliche Prüfungen  
Deutsche Bundesbank, Frankfurt/Main



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



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



Hinnerk Heise  
Geschäftsführer  
one.point.five TPRM Consulting &  
Services GmbH, Hannover

## Programm Tag 1 · 17. März 2025 · 10:00–16:45 Uhr

**Axel Leckner, Bundesbank (angefragt)** · 10:00–12:00 Uhr

Erste Prüfungserfahrungen aus DORA-Umsetzungsprüfungen – Erwartungen der Aufsicht hinsichtlich der weiteren Umsetzung und Anpassungen in den Instituten

- Erste DORA-Umsetzungsprüfungen: Prüfungserfahrungen und aktueller Stand in den Instituten
- Weiterer Umsetzungs- und Anpassungsbedarf
- Was ändert sich durch den Wegfall der BAIT?
- Inwieweit bleiben die BAIT-Anforderungen in der aufsichtlichen Prüfungspraxis erhalten

**Dr. Thomas Klühspies, Bundesbank** · 13:00–15:00 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 Unterauftragsvergaben und 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

**Hinnerk Heise, TPRM Consulting** · 15:15–16:45 Uhr

Idealtypischer Auslagerungsprozess gem. DORA sowie Umsetzungsmöglichkeiten zur zügigen Erreichung einer DORA-Grund-Compliance – Praxis- und Umsetzungs-Berichte

- Darstellung eines idealtypischen Auslagerungsprozesses unter Berücksichtigung der DORA-Anforderungen
- Umsetzungsmöglichkeiten der Klassifizierungsmethodik um IKT-Dienstleistungen gemäß DORA
- Umsetzungsmöglichkeiten der Risikobewertung gemäß DORA (u. a. im Zusammenspiel mit bestehenden Risikoanalysen und Risikobewertungen)
- Nützliche Praxis-Tipps für die operative Umsetzung des Auslagerungsmanagements

## Programm Tag 2 · 18. März 2025 · 10:00–16:30 Uhr

**Dr. Christopher Stolz, Bundesbank** · 10:00–12:30 Uhr

Aktuelle Praxis-Erfahrungen zu IKT-Governance und IKT-Organisation nach DORA – Auslagerungen vs. IKT-Drittleistungen in der Aufsichts-Praxis

- Governance und IKT-Organisation (DORA)
- Digital Operational Resilience Strategie (DOR-Strategie)
- Auslagerungsmanagement (MaRisk) und IKT-Drittparteienrisikomanagement (DORA)
- Anforderungen an das neue Informationsregister (DORA) und Abgrenzung zum Auslagerungsregister (MaRisk)

**Prof. Dr. Ralf Kühn, Finance Audit** · 13:30–16:30 Uhr

DORA in der Prüfungspraxis: Erweiterte Prüfungshandlungen und neue Prüffelder – Häufige Mängel und vermeidbare Feststellungen

- Anforderungen an die neue DOR-Strategie und Einbindung in die IKT-Governance der Institute: IKT-Risiken & Cyber-Risiken stärker im Fokus der Aufsicht
- IKT-Dienstleistungen im Fokus: Prüfung von Unterauftragsvergabe bis zum letzten Sub-Dienstleistungs-Level (!?) – Anforderungen an vertragliche Gestaltung – Spezialfall Cloud-Auslagerungen
- Erwartungen an den IT-Betrieb und das IT-Sicherheitsmanagement/IT-Notfallmanagement (BCM; SIEM) gemäß DORA
- Prüfung konkreter Anforderungen an IT-Projekte und Anwendungsentwicklung/IDV/IT-Inventare
- Prüfung des Berechtigungsmanagements (IAM): Rezertifizierung im Aufsichts-Fokus – Einstufung und Protokollierung kritischer Zugriffsrechte zur Sicherstellung der digitalen operationalen Resilienz
- Anforderungen an die Datenqualität im IKT-Risikomanagement – verschärfte Anforderungen an alle Institute (LSI+SI)
- Neue Anforderungen im BCM/IT-SCM – Praxisorientierte Notfallübungen als Schwerpunkt
- Prüfungserfahrungen und Praxishinweise

## Seminarziel

Die ersten DORA-Umsetzungsprüfungen starten direkt nach Inkrafttreten der DORA und dem Wegfall der BAIT Mitte Januar 2025. Eine Übergangsfrist für kleinere Institute und LSI-Institute besteht nicht.

Das Seminar »Prüfung DORA & DORA-Umsetzung« vermittelt praxisorientiertes Wissen zu den aktuellen DORA-Anforderungen und deren Prüfung durch die Aufsicht.

Teilnehmende erhalten Einblicke in erste Prüfungserfahrungen, Erwartungen der Aufsicht sowie den aktuellen Stand der Umsetzung in den Instituten.

Im Fokus stehen der Umgang mit Drittpartei- und ICT-Risiken, von der Risikobewertung über vertragliche Vereinbarungen bis zur Dienstleisterüberwachung.

Weitere Schwerpunkte bilden der idealtypische Auslagerungsprozess gemäß DORA, die Integration der neuen Anforderungen in bestehende MaRisk-Strukturen sowie häufige Mängel und Handlungsempfehlungen.

Anhand praxisnaher Berichte und Umsetzungstipps werden erweiterte Prüfungshandlungen, Anforderungen an IT-Governance, Sicherheitsmanagement und das neue Informationsregister vermittelt.

Ziel ist es, den Teilnehmenden konkrete Handlungshilfen zur Erreichung der DORA-Compliance und zur Vorbereitung auf Prüfungen zu bieten.

## Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- DORA-Umsetzungsverantwortliche und DORA-Projektmitglieder
- Interne Revision und IT-Revision
- IT und IT-Organisation
- Informationssicherheit und IKT-Risikomanagement
- Notfallmanagement, BCM und ITSCM
- IT-Regulatorik, IT-Compliance, Grundsatz und Governance
- Vorstandsstab

sowie andere interessierte Fach- und Grundsatzbereiche, Mitglieder des Vorstands und der Geschäftsleitung sowie externe Prüfer\*innen und Dienstleister.

## Unsere Referenten



### Axel Leckner (angefragt)

Prüfungsleiter IT-Prüfungen im Rahmen der Bankgeschäftlichen Prüfung Deutsche Bundesbank, Hannover

*Axel Leckner ist seit Ende 2005 bei der Deutschen Bundesbank, Hauptverwaltung Hannover, im Referat Bankgeschäftliche Prüfungen beschäftigt. Seine Tätigkeitsschwerpunkte liegen in den Bereichen IT-Prüfungen, Outsourcing, Business Continuity Management, Risikoklassifizierung sowie OpRisk.*



### Dr. Thomas Klühspies

Prüfungsleiter Bankgeschäftliche IT-Prüfungen Deutsche Bundesbank, München

*Herr Dr. Klühspies ist seit 12 Jahren im Bereich der Bankgeschäftlichen IT-Prüfungen der Bankenaufsicht tätig, davon zwei Jahre als Data Analysis Officer bei der Europäischen Bankenaufsicht (EBA). Bei der Bundesbank führt er als Prüfungsleiter IT-Prüfungen bei Banken und Finanzdienstleistern unterschiedlicher Größe durch.*



### Hinnerk Heise

Geschäftsführer one.point.five TPRM Consulting & Services GmbH, Hannover

*Hinnerk Heise besitzt weitreichende Praxiserfahrungen im Auslagerungsmanagement. Er berät und unterstützt nationale und internationale Banken, Finanzdienstleister und Versicherungen in der Umsetzung regulatorischer Vorgaben gem. KWVG, VAG, EBA-Leitlinien als auch der DORA-Verordnung. Im Rahmen der Behebung von Feststellungen aus §44er-Sonderprüfungen agiert er als Projektleiter oder Subject Matter Expert.*



### Dr. Christopher Stolz

Prüfungsleiter IT-Prüfungen, Bankgeschäftliche Prüfungen Deutsche Bundesbank, Frankfurt/Main

*Dr. Christopher Stolz ist seit 2015 Bankgeschäftlicher Prüfer in der Hauptverwaltung der Deutschen Bundesbank in Frankfurt am Main tätig. Er wird dabei sowohl als IT-Prüfer als auch als Prüfungsleiter bei nationalen und internationalen IT-Prüfungen eingesetzt.*



### Prof. Dr. Ralf Kühn, CIA, CISA

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

*Prof. Dr. Ralf Kühn besitzt langjährige Erfahrung in der Betreuung von nationalen und internationalen 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, den er als Dozent an verschiedenen Hochschulen und Bildungseinrichtungen weitergibt.*

# Seminar-Vorschläge

Cyber-Risiken – aktuelle Sicherheitslücken und direkt wirksame (Gegen-)Maßnahmen (**KOSTENFREI**)  
22. Januar 2025, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM  
29. Januar 2025, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement  
5./6. Februar 2025, Online-Veranstaltung

Geschäftsmodell-Analyse (BMA) & Aufbau tragfähiger, resilienter Geschäftsmodelle  
13. Februar 2025, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken  
17. Februar 2025, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)  
17. Februar 2025, Online-Veranstaltung

IKT-Governance im Fokus der Aufsicht  
18. Februar 2025, Online-Veranstaltung

Mobile-Work-Risiken im Fokus von DORA, IKT-Risikomanagement & IT-Revision  
18. Februar 2025, Online-Veranstaltung

DORA-konforme Dienstleistersteuerung bei Unterauftragsvergabe & Dienstleister-Konzentrationen  
19. Februar 2025, Online-Veranstaltung

Aufbau-Seminar I – Nutzung KI & ChatGPT  
20. Februar 2025, Online-Veranstaltung

DORA Spezial für Versicherungen  
26. Februar 2025, Online-Veranstaltung

Abstimmung der Notfall-Konzepte und BCM-Prozesse mit dem IKT-Drittdienstleister nach DORA  
27. Februar 2025, Online-Veranstaltung

Eigen-Anwendungen und IDV im Fokus der Aufsicht  
10. März 2025, Online-Veranstaltung

Auslagerungsmanagement Spezial: Umgang mit Software as a Service (SaaS) & Cloud-Diensten  
11. März 2025, Online-Veranstaltung

DORA-Anforderungen an IKT-Infrastruktur & IT-Betrieb  
13. März 2025, Online-Veranstaltung

► Diese und weitere Seminar-Angebote finden Sie bei uns online unter [www.akademie-heidelberg.de/online-seminare](http://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

Prüfung DORA & DORA-Umsetzung

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](mailto:anmeldung@akademie-heidelberg.de)

### Termine + Seminarzeiten

Montag, 17. März 2025  
10:00–16:45 Uhr  
Dienstag, 18. März 2025  
10:00–16:30 Uhr  
Online-Zugang jeweils ab 9:45 Uhr

Seminar-Nr. 25 03 BA186 W

### Teilnahmegebühr

€ 980,- (zzgl. gesetzl. USt)  
Die Gebühr beinhaltet die Teilnahme am Online-Seminar sowie die Präsentation als PDF-Datei. Sie erhalten außerdem ein Zertifikat, das Ihnen die Teilnahme an der Fortbildung bestätigt.

### Allgemeine Geschäftsbedingungen

Es gelten unsere AGB vom 01.01.2010, die wir Ihnen auf Wunsch gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: [www.akademie-heidelberg.de/agb](http://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 28 · 69123 Heidelberg  
Telefon 06221/65033-0  
info@akademie-heidelberg.de  
[www.akademie-heidelberg.de](http://www.akademie-heidelberg.de)