

Herausforderungen im Umgang mit KI-Dienstleistern durch DORA/MaRisk/KI-VO



Banken-Praxis-Seminar · (7 CPE-Punkte)

- Weitreichender Anpassungsbedarf in der Dienstleistersteuerung durch DORA-, neue MaRisk- und die KI-Verordnung
- Erläuterung der laufenden/initialen Risikoanalyse und Überwachung von KI-Dienstleistern
- Risikoorientierte Einbindung von KI-Dienstleistern in das (IT-)Notfallmanagement/BCM/ITSCM im Rahmen von DORA
- Aufsichtskonforme Verwaltung und Steuerung von Auslagerungsverträgen, DL-Verträgen und Service Level Agreements (SLAs)

Referenten

Dr. Sebastian Brauer, CISA
Partner, Wirtschaftsprüfer, Lead Auditor
PECB Certified ISO/IEC 27001
SIGNOS Wirtschaftsprüfung, Hamburg

Roland Hein
Inhaber, Geschäftsführer
bit Informatik GmbH
Trier

Bastian Bahnemann
FSI Compliance &
Business Development Lead
Microsoft, Hannover

Programm

Dr. Sebastian Brauer, SIGNOS · 10:00–12:45 Uhr – inkl. 15 Min. Pause

Weitreichender Anpassungsbedarf in der Dienstleistersteuerung durch DORA, neue MaRisk und KI-Verordnung

- Schnittmengen der Anwendungsbereiche von DORA, neue MaRisk und KI-VO auf Institute und deren KI-Dienstleister
- Besonderheiten der Regulierung von KI-Dienstleistern und deren Behandlung im Risikomanagement von Instituten
- Erläuterung der laufenden/initialen Risikoanalyse und Überwachung wesentlicher/kritischer KI-Auslagerungen
- Risikoorientierte Einbindung von KI-Dienstleistern in das (IT-)Notfallmanagement/BCM/ITSCM
- Besonderheiten bei Exit-Strategien, Konzentrationsrisiken und Weiterverlagerungen mit KI-Bezug
- Anforderungen an die Zertifizierung von Dienstleistern nach aktuellen Standards (ISO/IDW/ISAE)
- PRAXISBERICHT: Erfahrungen aus Audits bei Dienstleistern von Banken zum Auslagerungsmanagement

Roland Hein, bit Informatik · 13:30–15:00 Uhr

Was müssen (kritische) IKT-Drittdienstleister ab sofort bei Auslagerungssachverhalten beachten unter DORA?

- Information an die Mitarbeitenden des Hauses – Schulung zum Thema DORA, MaRisk, EU AI Act, NIS-2, KI-VO, BSI, etc., Konsequenzen bei Nichteinhaltung
- IST Analyse und Herausarbeitung von GAPs
- Internes Projekt aufsetzen und umsetzen, Meilensteine festlegen und den Kunden erläutern
- Gespräch mit Kunden und Wirtschaftsprüfern: Welche Dokumente und Inhalte werden gefordert?
- Definition interner/externer Compliance Verantwortung
- Überprüfung und gegebenenfalls Anpassung der Rahmenverträge/Unterverträge/Leistungsscheine
- Notwendige Begleitdokumente wie Auftragsdatenverarbeitung, Fernwartungsvertrag, Data Protection by Design, Escrow, etc.

- Umsetzung von KI-Anforderungen
- Bereitstellung von SBOM-Daten im CycloneDX-Format
- Notwendige Zertifizierungen und Aktualität sicherstellen
- Installieren von jährlich durchzuführenden Prozessen
- Bereitstellung von Dienstleister-Berichten
- Die Geschäftsführung/der Vorstand eines IKT-Dienstleisters muss für seine Mitarbeitenden als Vorbild fungieren

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

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

- Aktuelle technische und regulatorische Entwicklungen in der Finanzindustrie mit Fokus auf Cloud-Nutzung und (agentischer) KI
- Auswirkung der DORA-Anforderungen und DORA-Umsetzung auf die Dienstleistungsbeziehungen zwischen Microsoft und seinen Kunden aus dem Banken- und Finanzdienstleistungssektor
- Nutzung von KI im Einklang mit DORA und dem EU AI Act
- Was bedeutet die Einstufung als »kritischer IKT-Dienstleister«? – Einordnung von Microsoft im Rahmen der neuen (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- & KI-Technologie-Initiativen oder Überregulierung des europäischen Finanzplatzes – Deutsche Banken und Versicherungen im Vergleich zu Internationalen Microsoft-Kunden
- Unterstützungsleistungen von Microsoft zur Ermöglichung einer sicheren, resilienten und »complianten« Nutzung der IKT-, Cloud- und KI-Dienstleistungen im Rahmen finanzregulatorischer Erwartungen

Seminarziel

Mit DORA hat die Bankenaufsicht ein europaweit einheitliches Aufsichts-Rahmenwerk für digitale Risiken der Informations- und Kommunikationstechnologien (IKT) von Banken, Versicherungen und für (kritische) IKT-Dienstleister geschaffen. Hiermit gehen ebenfalls weitreichende Veränderungen in den Prozessen der Dienstleistersteuerung und des Informationsrisikomanagements einher.

Durch die MaRisk-Novellierung sollen 2026 Klarheit bei der Abgrenzung von DORA und den MaRisk geschaffen, IKT-Risiken in die Risikoinventur aufgenommen und die Aufgabenverteilung in der Dienstleistersteuerung neu organisiert werden.

Mit der KI-Verordnung ergeben sich für Institute zusätzliche regulatorische Anforderungen sowohl in der eigenen Nutzung von KI als auch in der Überwachung der KI-Nutzung bei den beauftragten Dienstleistern.

Die Wechselwirkungen zwischen den Rahmenwerken von DORA, den neuen MaRisk und der KI-Verordnung werden im Seminar ausführlich erläutert sowie mit praxisnahen Berichten zum derzeitigen Umsetzungsstand verdeutlicht.

Hinzu kommt ein Praxisbericht von Microsoft zum Umgang mit kritischen IKT-Dienstleistern, Hyperscalern und Cloud-Service-Providern.

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an Entscheidungsträger und Mitarbeitende der folgenden Bereiche:

- Interne Revision & IT-Revision, Account Management (IT-)Risikomanagement
- Organisation, Einkauf, Informationssicherheit, Informationsrisikomanagement
- Datenschutz & Data Governance, Compliance & Regulatorik
- sowie andere interessierte Fach- bzw. Grundsatzbereiche von Dienstleistern

Unsere Referenten



Dr. Sebastian Brauer, CISA

Partner, Wirtschaftsprüfer, Steuerberater, PECB Certified ISO/IEC 27001, Lead Auditor, SIGNOS GmbH WPG*, Hamburg

Dr. Sebastian Brauer unterstützt Kreditinstitute und deren Dienstleister bei den regulatorischen Herausforderungen der Informationssicherheit, insbesondere unter Einbindung der Anforderungen zur Dienstleistersteuerung. Ebenso auditiert Herr Dr. Brauer Software- und Serviceanbieter für Institute nach den anerkannten Standards.



Roland Hein

Inhaber, Geschäftsführer
bit Informatik GmbH*, Trier

Herr Hein stellt Unternehmen aus dem Drei-Säulen-Modell der deutschen Kreditwirtschaft sowie KRITS Unternehmen seit mehr 30 Jahren mit der Standardsoftware bit-Compliance eine Anwendung zur Verfügung, um ganzheitlich die regulatorischen Anforderungen aus MaRisk-, DORA, EBA Guidelines, NIS-2 etc. umzusetzen.



Bastian Bahnemann

FSI Compliance & Business Development Lead
Microsoft*, Hannover

Herr Bahnemann besitzt mehr als 15 Jahre Erfahrung in führenden Positionen bei internationalen Technologie- und Finanzunternehmen. Seit Dezember 2024 leitet er bei Microsoft die Zusammenarbeit mit regulierten Finanzinstituten und deren Aufsichtsbehörden in Deutschland. Zuvor war er bei Amazon Web Services tätig.

* Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht notwendigerweise 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

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

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

Dienstleister-Steuerung & Dienstleister-Berichte
in der Auslagerungs- & DORA-Praxis
11. Mai 2026, Online-Veranstaltung

DORA im Fokus von Aufsicht & Prüfern
12. Mai 2026, Online-Veranstaltung

IKT-Geschäftsfortführungsmanagement und
IT-Notfallmanagement im Fokus
9. Juni 2026, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)
22. 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

Herausforderungen im Umgang mit
KI-Dienstleistern durch DORA/MaRisk/KI-VO

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

Mittwoch, 10. Juni 2026
10:00–17:00 Uhr
Online-Zugang ab 9:45 Uhr
Seminar-Nr. 26 06 BA112 W

Teilnahmegebühr

€ 290,- (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.



**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