

# DORA Spezial: Umgang mit Software-/ IKT-Service-Providern & Cloud-Dienstleistern



## Banken-Praxis-Seminar · 8 CPE-Punkte

- Neue Aufsichts- und DORA-Anforderungen an die Nutzung von SaaS, Cloud-Anwendungen und IKT-Service-Providern
- Third Party Risk Management bei SaaS und Cloud-Dienstleistungen
- Aufsichtsrechtliche und zivilrechtliche Anforderungen an die Ausgestaltung von Dienstleistungsverträgen und Cloud-SLAs
- Mindestinhalt, Dienstleistungsgüte und Leistungsbeschreibung
- Festlegung angemessener Informations- und Prüfungsrechte
- Software-Einführungen und Release-Wechseln bei Fremdsoftware

### Referenten



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



Dr. Christoph Krück  
Rechtsanwalt  
SKW Schwarz  
Rechtsanwälte, München



Jochen Wurster  
Lead Business Development  
Chapter IT-Management, PSD Bank  
RheinNeckarSaar eG, Stuttgart

## Programm

**Dr. Markus Held, BSI** · 9:00–11:00 Uhr

**Besondere Aufsichts- und DORA-Anforderungen an die Informationssicherheit und die IKT-Governance bei Nutzung von Cloud-Anwendungen und IKT-Service-Providern**

- Grundsätze und Prinzipien von Third Party Risks und Drittpartei-Risikomanagement
- Neue DORA-Vorgaben: Neue regulatorische Anforderungen im Kontext der Nutzung von Cloud-Diensten und IKT-Service-Providern
- Anforderungen an die Identifikation, Klassifikation und Berichterstattung von IKT-, Cloud- und SaaS-Risiken im Rahmen von OpRisk-Reporting und IKT-Risk-Assessments
- Anforderungen an Prüfungsrechte und Vorgehensweisen, um regulatorische und aufsichtskonforme Prüfungen von Cloud-Anbietern und IKT-Service-Providern sicherzustellen
- Methoden zur Schutzbedarfsfeststellung und Risikoanalyse für Cloud-Anwendungen und deren Bedeutung für die IT-Governance und Compliance-Anforderungen
- Notfallmanagement und Third Party Risk: Anforderungen an Business Continuity Management (BCM) und IT Service Continuity Management (ITSCM), einschließlich Notfalltests und Integration von Dienstleistern in Notfallpläne
- Erwartungen der Aufsicht an die Implementierung von TOMs durch Cloud-Dienstleister, um einschlägige Sicherheitsstandards einzuhalten
- Governance-Strukturen und Kooperation: Zusammenarbeit zwischen IT, Risikomanagement, Fachbereichen und Leitungsebene bei der Einhaltung von IT-Governance-Vorgaben
- Überblick über DORA-Anforderungen an verpflichtende Penetrationstests (TLPT), ihre Durchführung und die daraus resultierenden Chancen und Herausforderungen

**Dr. Christoph Krück, SKW Schwarz** · 11:15–15:00 Uhr

inkl. ca. 45 Min. Mittagspause

**Aufsichtsrechtliche und zivilrechtliche Anforderungen an die Gestaltung von Auslagerungsverträgen und SLAs insbesondere bei Software as a Service und Cloud-Diensten**

- Grundsätzliche zivilrechtliche Aspekte bei Cloud und SaaS-Verträgen im Auslagerungsbereich beziehungsweise bei Outsourcing, insbesondere
  - Bedeutung der Leistungsbeschreibung
  - Haftungs- und Kündigungsregelungen
- Aufsichtsrechtliche Anforderungen an die Ausgestaltung von Cloud und SaaS-Verträgen bei Auslagerungsverträgen und SLAs, insbesondere konkretisierte Mindestinhalte (MaRisk AT9, BaFin-Hinweise, DORA), wie insbesondere
  - Spezifizierung der zu erbringenden Leistung
  - Vereinbarte Dienstleistungsgüte
  - Informations- und Prüfungsrechte
  - Regelungen zum Exit-Management
  - Regelungen bzgl. Weiterverlagerungen, Unteraufträge

**Jochen Wurster, PSD-Bank RheinNeckarSaar** · 15:15–17:00

- Umsetzung in der Praxis: Die Wahl des richtigen Software-Dienstleisters – Wann ist es sinnvoll, Software extern zu beziehen oder Anwendungen in die Cloud auszulagern?
- Welche Einsatzmöglichkeiten für externe Software, Lizenzen und Cloud-Technologien bieten sich in Banken an? Was spricht dafür? Wieviel Spielraum lässt DORA zu?
- Begleitung von Software-Einführungen und Release-Wechseln bei Fremdsoftware durch die IT
- Entwicklung von Life-Cycle-Prozessen für die Nutzung von SaaS-Lösungen (inkl. dokumentierter Exit-Strategien)
- Beispiele zu Kriterien einer Risikobeurteilung – ab wann sollte von IT-Auslagerungen (AT 9) bzw. IKT-Drittdienstleistung (DORA) gesprochen werden? Abgrenzung zum Software-Fremdbezug – Empfehlungen aus der Praxis
- Identifikation kritischer oder wichtiger Funktionen und Umgang mit kritischen IKT-Dienstleistern?

## Seminarziel

DORA sowie die von der BaFin geforderten umfassenden Mindestinhalte bei Auslagerungs- und Dienstleistungsverträgen sowie SLAs stellen die Institute, insbesondere im Zusammenhang mit SaaS und Cloud-Diensten, vor große Herausforderungen.

Das Seminar zielt darauf ab, die Teilnehmenden umfassend über die aufsichtsrechtlichen und zivilrechtlichen Anforderungen an Auslagerungsverträge und SLAs, insbesondere bei Software as a Service und Cloud-Diensten, zu informieren. Dabei werden grundsätzliche zivilrechtliche Aspekte behandelt, wie Vertragstypologie, AGB-rechtliche Vorgaben, Leistungsbeschreibungen, Haftungs- und Kündigungsregelungen sowie der Umgang mit Schutzrechten und Lizenzen. Ein besonderer Fokus liegt auf den aufsichtsrechtlichen Anforderungen, wie MaRisk AT9 und DORA, und deren Umsetzung in der Praxis.

Die erfahrenen Referenten geben praxisnahe Einblicke in die Wahl des richtigen Software-DL, die Integration von Fremdsoftware, die Entwicklung von Life-Cycle-Prozessen für SaaS-Lösungen und die Sensibilisierung der Mitarbeitenden für Risiken.

Die Teilnehmenden erhalten konkrete Beispiele und Empfehlungen zur Risikobeurteilung und umfassende Praxisberichte zu den besonderen Anforderungen an die Ausgestaltung von Auslagerungsverträgen und SLAs bei der Nutzung von Software-, Cloud- und Lizenz-Lösungen.

## Zielgruppe

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- Auslagerungsmanagement, Dienstleistersteuerung und Providermanagement
- IT, Organisation, Risikomanagement und Gesamtbanksteuerung
- Bankrecht und Vertragsrecht, Interne Revision und IT-Revision
- Regulatorik, Grundsatz und Corporate Governance
- Sowie andere interessierte Fachbereiche, Vorstandsmitglieder/Geschäftsleitung, Führungskräfte, externe Prüferinnen und Prüfer sowie Bankdienstleister

## Unsere Referenten

---



### Dr. Markus Held

Referatsleiter, Bundesamt für Sicherheit in der Informationstechnik (BSI\*)

*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 Bundesamt für Sicherheit in der Informationstechnik. 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.*



### Dr. Christoph Krück

Rechtsanwalt, SKW Schwarz Rechtsanwälte\*, München

*Dr. Christoph Krück hat seinen Tätigkeitsschwerpunkt im IT-Recht und Digital Business. Sein Fokus liegt auf der Gestaltung und Verhandlung von AGB, Lizenz-, Cloud-, SaaS- und sonstigen IT-Verträgen. Er begleitet zudem die Entwicklungen rund um die Regulierung von neuen Technologien wie künstlicher Intelligenz, Algorithmen oder Blockchain. Er ist Autor verschiedener Vertrags-Musterformularen (u. a. zu SaaS, Housing) und Mitglied im Blockchain Bundesverband und der ITechLaw – International Technology Law Association.*



### Jochen Wurster

Lead Business Development, Chapter IT-Management  
PSD Bank RheinNeckarSaar eG\*, Stuttgart

*Jochen Wurster verantwortet als Lead Business Development in der PSD Bank RheinNeckarSaar die konzeptionelle und techn. Weiterentwicklung der IT mit Schwerpunkt auf Digitalisierung und Automatisierung. Davor war er jahrelang Leiter einer klassischen Orga-Abteilung der Bank. Als diplomierter Bankbetriebswirt VR ist er seit vielen Jahren im genossenschaftlichen FinanzVerbund tätig und hatte seinen Tätigkeitsschwerpunkt immer im Bereich IT- und Prozessmanagement.*

\*Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht notwendigerweise die eines bestimmten Instituts, einer bestimmten Kanzlei, der Deutschen Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wider. Die Referenten geben auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte wider.

**IKT Spezial – Identity- & Access-Management (IAM)**  
22. Juli 2026, Online-Veranstaltung

**Neuer IKT-Risikomanagement-Rahmen nach DORA**  
11. September 2026, Online-Veranstaltung

**DORA-konforme Auslagerungsverträge/SLAs**  
16. September 2026, Online-Veranstaltung

**Praxis-Umsetzung aktueller DORA- und Aufsichts-  
Anforderungen in der DL-Steuerung**  
22. September 2026, Online-Veranstaltung

**Abgrenzung und parallele Steuerung von  
Auslagerungen (MaRisk) & IKT-Dienstl. (DORA)**  
24. September 2026, Online-Veranstaltung

**DORA-konformer Umgang mit Eigenanwendungen und IDV**  
8. Oktober 2026, Online-Veranstaltung

**DORA-konformes IKT-Risikomanagement**  
14./15. Oktober 2026, 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](mailto:b.wehling@akademie-heidelberg.de)

## Anmeldeformular

**DORA Spezial: Umgang mit Software-/  
IKT-Service-Providern & Cloud-Diensten**

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

### Termin und Seminarzeiten

Montag, 21. September 2026  
9:00–17:00 Uhr  
Online-Zugang ab 8:45 Uhr  
Seminar-Nr. 26 09 BA106 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 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 für Fortbildung Heidelberg GmbH**  
Maaßstraße 32/1 · 69123 Heidelberg  
Telefon 06221/65033-0  
[info@akademie-heidelberg.de](mailto:info@akademie-heidelberg.de)  
[www.akademie-heidelberg.de](http://www.akademie-heidelberg.de)