

Management des IKT-Drittparteienrisikos

Von der Dienstleister-Auswahl zur DORA-konformen TPRM-Resilienz



DORA-Praxis-Seminar · (2,5 CPE-Punkte)

- Risikoorientierte Vorabprüfung vor Vertragsabschluss
- Typische Prüfungsschwerpunkte, Prüfungslogik und Erkenntnisse aus dem ersten Jahr
- Vorfalls- und Ausstiegssfähigkeit sicherstellen
- Abhängigkeiten und Konzentrationsrisiken beherrschbar machen
- Informationsregister als Steuerungsinstrument nutzen
- Laufende Überwachung wirksam organisieren

Referent



Florian Kertscher
CIA, CISA
Senior Expert IT-Compliance
FinPlanet GmbH

Programm

Florian Kertscher, FinPlanet · 9:00–11:00

Management des IKT-Drittparteienrisikos: Von der Auswahl zur Resilienz (DORA-konform)

- Ein Jahr DORA – was 2026 wirklich zählt: Aufsichtsfokus auf Wirksamkeit, typische Schwachstellen, Prüferwartungen und Erkenntnisse aus dem ersten DORA-Jahr
- Abhängigkeiten und Konzentrationsrisiken beherrschbar machen: Konzentrationen, »Single Points of Failure« und Dienstleistungsketten systematisch erkennen, bewerten und begrenzen
- Vorfallsteuerung durchgängig gestalten: Dienstleister verbindlich in Melde- und Krisenprozesse einbinden, Zeitkritik, Eskalationswege und Nachweisanforderungen sicherstellen
- Exit-Strategien und Ersetzbarkeit praxisnah umsetzen: Realistische und testbare Exit-Strategien, Auslöser, Migrations- und Betriebsrisiken sowie Mindestanforderungen an Übergangsleistungen
- DORA als Zielbild für das IKT-Drittparteienrisiko: Rollen und Verantwortlichkeiten, Drei-Linien-Modell sowie Schnittstellen zwischen Drittparteienmanagement, Informationssicherheitsmanagementsystem und Notfallmanagement
- Kritikalität und Geltungsbereich festlegen: »Kritische oder wichtige Funktionen«, Abhängigkeitsbild, Zuordnung von Leistungen und IT-Komponenten sowie Risikoklassen
- Informationsregister in der Praxis nutzen: Datenquellen, Datenqualität, Lieferketten-Transparenz und Ableitung konkreter Steuerungsimpulse
- Vorabprüfung vor Vertragsabschluss risikoorientiert ausrichten: Prüfbausteine, Mindestnachweise, angemessene Prüftiefe und pragmatische Ansätze bei Standardverträgen
- DORA-konformes Vertrags-Set praxistauglich gestalten: Mindestinhalte, Prüf- und Zugriffsrechte, Regelungen zu Unterbeauftragungen sowie Kündigungs- und Beendigungsrechte einschließlich Exit-Regelungen
- Laufende Überwachung wirksam organisieren: Kennzahlen und Risikoindikatoren, Kontrollprüfungen, Nachweise sowie Prüfberichte und Bescheinigungen richtig einordnen – jederzeit auskunfts- und nachweisfähig
- Unterbeauftragungen und Lieferkette steuern: Mindeststeuerbarkeit entlang der Kette, Informationsrechte, Durchgriff und pragmatische Kontrollmodelle
- EU-Aufsicht und Einordnung kritischer IKT-Drittanbieter (CTPP): Bedeutung der CTPP-Liste und Aufsichtserkenntnisse sowie institutsseitig erforderliche Steuerungsmaßnahmen
- Erfahrungsberichte, Praxis-Hinweise und Umsetzungs-Tipps

Seminarziel

Ziel des Seminars ist es, den Teilnehmenden ein klares, praxistaugliches Vorgehensmodell für das Management des IKT-Drittparteienrisikos unter DORA zu vermitteln. 2026 steht dabei weniger die Dokumentation im Vordergrund als die nachweisbare Wirksamkeit – gerade mit Blick auf Vorfälle, Abhängigkeiten und aufsichtliche Prüfungen.

Im Mittelpunkt steht die Frage, wie Dienstleisterbeziehungen über den gesamten Lebenszyklus wirksam gesteuert werden: Von der risiko-orientierten Kritikalitätsbewertung und der Vorabprüfung vor Vertragsabschluss über ein umsetzbares Mindestanforderungs-Set in Verträgen bis hin zur laufenden Überwachung, der Einbindung in das Vorfallsmanagement und testbaren Ausstiegsstrategien.

Typische Zielkonflikte (z. B. Standardisierung vs. Diversifikation, begrenzte Verhandlungsspielräume bei marktmächtigen Dienstleistern) sowie die für 2026 erwarteten Prüferwartungen werden aufgegriffen und in konkrete Handlungsbausteine übersetzt. Die Teilnehmenden nehmen eine sofort anwendbare Struktur einschließlich praxisbewährter Prüflisten-Logik mit, um Steuerungsfähigkeit, Belegbarkeit und Resilienz nachhaltig zu erhöhen.

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche:

- IKT-Risikomanagement und IKT-Risikokontrollfunktion
- (Zentrales) Auslagerungsmanagement und IKT-Dienstleistersteuerung
- IT und Organisation, Regulatorik und Grundsatz
- Interne Revision und IT-Revision
- IKT-Strategie und Gesamtbanksteuerung
- Corporate Governance, Outsourcing-Governance und DOR-Beauftragte

sowie andere interessierte Fachbereiche, Mitglieder des Vorstands/der Geschäftsleitung, Führungskräfte, externe Prüfer*innen und Bankdienstleister.

Unsere Referent



Florian Kertscher, CIA, CISA

Senior Expert IT-Compliance
FinPlanet GmbH*

Florian Kertscher ist Experte für IT-Compliance und Informationssicherheit mit über zehn Jahren Berufserfahrung in der Finanz- und Versicherungsbranche. Er ist Certified Internal Auditor (CIA) und Certified Information Systems Auditor (CISA) und verfügt über fundierte Praxis in der Umsetzung regulatorischer Anforderungen und gängiger Standards (u. a. DORA, BAIT/VAIT, ISO-2700x, COBIT).

Seit 2025 ist er als Senior Expert IT-Compliance tätig und unterstützt Organisationen bei der wirksamen Ausgestaltung von Governance-, Kontroll- und Nachweisstrukturen in komplexen IT-Umgebungen. Zuvor verantwortete er als IT Audit Manager Prüfungen mit fachlicher Leitung von Prüfteams und stimmte Ergebnisse regelmäßig bis auf C-Level ab.

Als Informationssicherheitsbeauftragter einer großen Sparkasse steuerte er den Informationssicherheitsprozess, führte Audits durch, untersuchte Sicherheitsvorfälle und berichtete quartalsweise an den Gesamtvorstand; zudem verantwortete er die Steuerung externer Dienstleister.

Weitere Stationen in der Internen Revision sowie in der Beratung (u. a. IT-Prüfungen im Bankenumfeld und Datenintegritätsprüfungen im Rahmen von EZB-Prüfungen) runden sein Profil ab. Seine Stärke liegt in der Verbindung von regulatorischer Sicherheit, prüfungsfester Dokumentation und praxistauglicher Umsetzung.

** Der Referent gibt ausschließlich seine persönliche Auffassung und nicht notwendigerweise die eines bestimmten Instituts, der Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wieder. Der Referent nimmt auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.*

DORA-konforme Auslagerungsverträge/SLAs

26. März 2026, Online-Veranstaltung

Neue DORA- & Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM

20. April 2026, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen

27. April 2026, Online-Veranstaltung

Abgrenzung und parallele Steuerung von Auslagerungen (MaRisk) & IKT-Dienstl. (DORA)

28. April 2026, Online-Veranstaltung

Auslagerungen und IKT-Dienstleistungen im Fokus von Aufsicht, neuen MaRisk & DORA

29. April 2026, Online-Veranstaltung

Risikoanalyse von Auslagerungen (MaRisk) & IKT-DL (DORA)

5. Mai 2026, Online-Veranstaltung

DORA Spezial:

Informationssicherheit und IKT-Risikomanagement

7. Mai 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

Management des IKT-Drittparteienrisikos

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, 6. Mai 2026
9:00–11:00 Uhr
Online-Zugang ab 8:45 Uhr
Seminar-Nr. 26 05 BA216 W

Teilnahmegebühr

€ 220,— (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