29. Juni 2026 · 10:00–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

DORA-Anforderungen an IT- & Cyber-Sicherheit

Informationssicherheit im Spannungsfeld zw. Regulatorik und Praxis

Banken-Praxis-Seminar · 8 CPE-Punkte

- Aktuelle Bedrohungslage in der deutschen Finanzindustrie
- Informationssicherheit im Spannungsfeld zw. Regulatorik & Praxis
- Von Informationssicherheit zum IKT-Risikomanagement
- IKT-Risiken und Cyber-Risiken stärker im Fokus der Aufsicht
- Cyber-Attacke: Prävention, (frühzeitige) Entdeckung & Maßnahmen
- Besondere Anforderungen bei IT-/Cloud-Auslagerungen
- Praxisfall Ransomware & Sicherstellung der Mitarbeiter-Awareness

Referenten

Dr. Markus Held
Referatsleiter Sicherheit in der IT-Konsolidierung
BSI, Bonn

Florian Emmerich
Senior Associate, Spezialist für Data Privacy und Cybersecurity
Clyde & Co Europe LLP, Düsseldorf

Jan-Philipp Küsters
Referent Cybersicherheit und Operative Informationssicherheit
Sparkasse Krefeld

Marcus Schmidt, MBA, CISA, CISM, CGEIT
Leiter IT-Governance
Sparkasse Krefeld

DORA-Anforderungen an IT- und Cyber-Sicherheit

Programm

Dr. Markus Held, BSI · 10:00–12:00 Uhr

Aktuelle DORA-Anforderungen an die IT- & Cyber-Sicherheit – Chancen und Herausforderungen

- IT-Governance: Strategische und regulatorische Anforderungen an die Identifizierung, Bewertung und Überwachung von Cyber-Risiken sowie die Entwicklung von DOR-Strategien zur IKT-Risikominderung
- Erhöhte Transparenzanforderungen bzgl. IKT-Risiken
- Meldung schwerwiegender IKT- und Cyber-Vorfälle
- Standardisierung und Optimierung der Prozesse und der IKT zur Förderung einer effizienten IT-Governance
- Stärkung der IKT-Resilienz zur Verbesserung der institutsweiten Informationssicherheit
- Zunehmende Schwierigkeiten durch steigende Komplexität in der IT-Landschaft und IT-Infrastruktur
- Testen der digitalen operationalen Resilienz (z. B. TLPT)
- Die Bedeutung der IT-Governance für die Anpassung an rasche technologische Veränderungen und zunehmende Bedrohungen durch hybride und Cyber-Angriffe
- Besondere Anforderungen an die Informationssicherheit und die IT-Governance bei Nutzung von Cloud-Anwendungen und IT-Service-Providern

Florian Emmerich, Clyde & Co · 13:00–14:30 Uhr

Aktuelle Bedrohungslage durch Cyberangriffe & Ransomware: konkrete Fallbeispiele für Cyber- & IKT-Vorfälle aus der Praxis

- Aktuelle Lage der IT-Sicherheit und Cyber-Sicherheit in Deutschland sowie im deutschen Finanzwesen
- Identifikation kritischer Geschäftsprozesse sowie kritischer und wichtiger Funktionen (kowFs)
- Typischer Ablauf eines Cyber-Incidents anhand konkreter Fallbeispiele aus der Praxis
- Vorgehen bei der Einleitung von (Gegen-)Maßnahmen
- Haftung für (datenschutzrelevante) Cyber-Schäden

Jan-Philipp Küsters, Marcus Schmidt, Sparkasse Krefeld
14:45–17:00 Uhr

Schwachstellenmanagement wirksam gestalten

- Typische Herausforderungen in der praktischen Umsetzung
- Einbindung in das IKT-Risikomanagement gem. DORA

SIEM-Protokollierung als Grundlage wirksamer Detektion

- Relevante Logquellen und SIEM Detection Rules
- Anforderungen an eine angemessene Protokollierung
- Grenzen und Herausforderungen beim Einsatz eines SIEM
- Protokollierung zur Früherkennung von Cyberangriffen

IKT-Vorfallsmanagement in der Praxis

- Rollen/Verantwortlichkeiten im Incident-Response-Lifecycle
- Strukturierte Bearbeitung von Security Incidents
- Kommunikationsmanagement im Vorfalls-Fall
- Meldung und Behandlung von IKT-Vorfällen gemäß DORA

Governance, Management-View und IKT-Risikomanagement

- Einbettung von Cyber-Security in das Risikomanagement
- Entscheidungsrelevante Kennzahlen (KPIs/KRIs)
- Steuerung, Überwachung und Reporting von IKT-Risiken
- Anforderungen aus DORA an Governance-Strukturen und Kontrollmechanismen

Schutzbedarfs- & Risikoanalysen: Grundlage d. Cyber-Resilienz

- Zielsetzung und Methodik von Schutzbedarfsanalysen
- Durchführung von Risikoanalysen im IKT-Kontext
- Ableitung angemessener Sicherheitsmaßnahmen
- Priorisierung von Risiken und Maßnahmen

Schulung und Sensibilisierung von Mitarbeitenden und Leitungsorganen

- Bedeutung des Faktors Mensch in der Cyber-Security

Seminarziel

IT-Risiken, Cyber-Angriffe und Lücken in der Informationssicherheit führen zunehmend häufiger zu Ausfällen kritischer Geschäftsprozesse bei Banken und Unternehmen. Insbesondere Angriffe von außen (z. B. Cyber-Attacken, Ransomware) haben sich hierbei zu einer immanenten Bedrohung entwickelt, die durch die aktuelle geopolitische Lage noch verschärft werden.

Die DORA-Vorgaben erhöhen daher deutlich die Anforderungen an die IT-Sicherheit und Cyber-Sicherheit. Damit einhergehen somit auch die erweiterten Aufgaben und Verantwortlichkeiten der Informationssicherheitsbeauftragten (ISB/CISO), um Ausfälle des Geschäftsbetriebs zu vermeiden und das Institut vor Schaden zu schützen.

Auch Cyber-Risiken (u. a. aus Cloud-Dienstleistungen) sind aus dem Blickwinkel der Informationssicherheit zu beurteilen – doch wie lassen sich die mit dieser Auslagerung verbundenen Risiken messen, beurteilen und steuern? Das Seminar gibt wertvolle Praxistipps zur Herangehensweise und Umsetzung der neuen DORA-Anforderungen in diesem Bereich.

---

* 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.

Zielgruppe

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- IT & Organisation, Informationssicherheit (ISB) & Informationsrisikomanagement
- IT-Revision, Notfallmanagement und Business Continuity Management (BCM)
- IT-Compliance, Datenschutz, Data Governance und Cyber-Sicherheit

Unsere Referenten

Dr. Markus Held
Referatsleiter Sicherheit in der IT-Konsolidierung des Bundes
Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Bonn

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 BSI. 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.

Florian Emmerich
Senior Associate, Spezialist für Data Privacy und Cybersecurity
Clyde & Co Europe LLP*, Düsseldorf

Florian Emmerich ist Senior Associate im Team Datenschutz und Privatsphäre bei Clyde & Co in Düsseldorf. Er ist spezialisiert auf Datenschutz und Cybersicherheit, insbesondere kundenorientierte Technologien, Betroffenenansprüche und Datenschutzverletzungen.

Jan-Philipp Küsters
Referent Cybersicherheit und Operative Informationssicherheit im Bereich IT-Governance, Sparkasse Krefeld*

Jan-Philipp Küsters ist seit 2024 Referent für Operative Informationssicherheit im Bereich IT-Governance bei der Sparkasse Krefeld. Als Mitglied im DORA-Projekt der Sparkasse Krefeld hat er die Umsetzung der Themen IKT-Vorfallsmanagement, Protokollierung, Schwachstellenmanagement, Cyberbedrohungen und Testmanagement verantwortet und ist auch weiterhin für diese Themen verantwortlich.

Marcus Schmidt, MBA, CISA, CISM, CGEIT
Leiter IT-Governance, Sparkasse Krefeld*

Marcus Schmidt ist Leiter IT-Governance bei der Sparkasse Krefeld. Davor war er in den Bereichen Steuerung, Strategie, Informationssicherheit und Notfallmanagement tätig. Er ist verantwortlich für die Erstellung der IT-Strategie sowie die Überwachung der Einhaltung von KPI und KRI. Als Projektleiter leitete er das Projekt DORA in der Sparkasse Krefeld.

Herausforderungen im Umgang mit KI-Dienstleistern
10. Juni 2026, Online-Veranstaltung

Fachtagung IKT-Aufsicht
15./16. Juni 2026, Online-Veranstaltung

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

Basis-Seminar Business Continuity Management (BCM)
22. Juni 2026, Online-Veranstaltung

IKT Spezial für Compliance & Governance
23. Juni 2026, Online-Veranstaltung

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA
23. Juni 2026, Online-Veranstaltung

Risikosteuerung und Audits von KI-Dienstleistern
2. Juli 2026, Online-Veranstaltung

TPRM Spezial: Anforderungen an SaaS- & Cloud-Dienste
8. 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

DORA-Anforderungen an IT- und Cyber-Sicherheit

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, 29. Juni 2026
10:00–17:00 Uhr
Online-Zugang ab 9:45 Uhr

Seminar-Nr. 26 06 BA181 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

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

04.26 / 2606BA181