22. Juli 2026 · 9:00–15:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

DORA-konformes Schwachstellenmanagement

Anforderungen an Schwachstellenmanagement, Pentests, SIEM & SOC

Banken-Aufsicht-Seminar · 6 CPE-Punkte

- **Konkrete Erwartungen aus MaRisk, DORA und EBA-ICT-Leitlinien**
- **Fragestellungen & häufig identifizierte Schwachstellen in der Praxis**
- **Anforderungen an das (toolunterstützte) Identifizieren und die Behandlung von Schwachstellen**
- **Anforderungen an die Durchführung regelmäßiger PenTests**
- **SIEM-Administration und SIEM-Meldungen innerhalb eines SOC**
- **Anforderungen an das ITSCM/BCM und die Abstimmung mit den IKT-Dienstleistern**

Referenten

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, aktuell SAP Systemservices Architektur, Zentrale IT-Plattform-management Drittprodukte, Bundesbank, Düsseldorf

Jan-Philipp Küsters
Referent Operative Informations-sicherheit im Bereich IT-Governance
Sparkasse Krefeld

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

Programm

Alexander Lohr, Bundesbank · 9:00–12:00 Uhr

Konkrete regulatorische Anforderungen an das Schwachstellenmanagement unter Berücksichtigung der neuen DORA-Anforderungen

- Konkretisierung der Anforderungen der MaRisk und DORA
- Identifikation, Bewertung und Behandlung von Schwachstellen. Anforderungen an die Nutzung eines Schwachstellenscanners (Netzwerkscan/authentifizierter Scan)
- Umgang mit Schwachstellen im Schwachstellenmanagement, Bündelung und Priorisierung, Reporting und Übertragung in das Risikomanagement
- Notwendigkeit regelmäßiger Penetrationstests: Angriffsszenarien, Root-Cause-Analyse, Bewertung der Ergebnisse
- Einsatz eines SIEM-Systems, notwendige Loganbindungen, Anforderungen an die Qualität der Logs und Speicherfristen, Entwicklung von Use Cases
- Security Operations Center (SOC), 24/7 Überwachung, Reporting von SIEM-Alarmen
- Schutz vor Schadsoftware, Datenabfluss, Verschlüsselung, Vorstellung klassischer Datenabflusskanäle
- Management zulässiger Software und IDV, Entwickler-Clients, administrative Benutzer, Skriptausführung und Überwachung
- Einbindung der IKT-Dienstleister in das Schwachstellenmanagement – Prozesstransparenz und Steuerbarkeit
- Identifizierte Schwachstellen in der Praxis

Jan-Philipp Küsters & Marcus Schmidt, Sparkasse Krefeld
13:00–15:00 Uhr

Ganzheitliches Schwachstellenmanagement im IT-Betrieb: Sicherstellung der DORA-Governance und operative Umsetzung in der Infrastrukturpraxis

- Governance: Klare Verantwortlichkeiten zwischen IT-Governance, IT-Betrieb, Informationssicherheitsmanagement (ISM) und Dienstleistern; Definition von Rollen wie Vulnerability Owner und Risk Owner
- Risikoorientierte Priorisierung nach DORA-Vorgaben
- Aufbau und Pflege eines vollständigen IT-Asset- und Servicekatalogs als Fundament für die Priorisierung von Schwachstellen im bankfachlichen Kontext
- End-to-End Vulnerability Management Lifecycle – Integration in bestehende Kontroll- und Meldeprozesse
- CVSS und EPSS als zentrale Bewertungsinstrumente – Nutzung von CVSS und EPSS für einheitliche technische Risikobewertungen (z. B. kritische Geschäftsprozesse, Schutzbedarf, Eintrittswahrscheinlichkeit)
- Tool- und Scanlandschaft in der Praxis – Zusammenspiel aus Netzwerk-, Endpoint-, Cloud- und Applikationsscannern; Umgang mit proprietären Systemen und fehlender Scanbarkeit in spezialisierten Bankumgebungen
- Patch- und Change-Management-Integration – Verzahnung von Schwachstellenbehandlung mit dem Change-Management, Releasezyklen und Freigabeprozessen zur Minimierung von Betriebsrisiken
- Reporting, KPIs und kontinuierliche Verbesserung – Aufbau eines standardisierten Berichtswesens
- Steuerung der Schwachstellenbehandlung im Dienstleister- und Auslagerungsmanagement unter Einhaltung der DORA-Vorgaben für Drittparteien (TPRM)

Seminarziel

Das Schwachstellenmanagement gewinnt zunehmend an Bedeutung in der Finanzwirtschaft. Der Einsatz eines Security Information and Event Management (SIEM)-Systems sowie eines Schwachstellenscanners sind unabdingbar für die Erfüllung eines hohen Schutzbedarfes für sicherheitskritische IT-Systeme. Dementsprechend wachsen auch die regulatorischen Anforderungen an die IT-Systeme der Institute.

Wesentliche Feststellungen zu Sicherheitslücken in dem Bereich der operativen Informationssicherheit zeigen, dass für viele Institute ein Nachholbedarf besteht.

Nicht nur die reine Identifikation möglicher Schwachstellen, sondern auch deren Behebung setzt die Informationssicherheit, nicht zuletzt auch aufgrund der stetig wachsenden IT-Landschaft, vor große Herausforderungen, die mit dem Informationsrisikomanagement in Einklang gebracht werden müssen.

Auch eingebundene Dienstleister müssen die Anforderungen einhalten und von der Informationssicherheit überwacht werden.

* 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, Interne Revision, IT-Revision, IT-Organisation und IT-Notfallbeauftragte
- Informationssicherheit (ISB) und Informationsrisikomanagement
- IT-Sicherheitsmanagement und IT-Architekten
- IT-Compliance und IT-Governance, IT-Grundsatz und Regulatorik

Sowie andere interessierte Fachbereiche bzw. Vorstände/Geschäftsleiter und externe Prüfer*innen sowie Bankdienstleister.

Unsere Referenten

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, aktuell SAP Systemservices Architektur, Zentrale IT-Plattformmanagement Drittprodukte Deutsche Bundesbank*, Düsseldorf

Alexander Lohr ist studierter Wirtschaftsinformatiker und arbeitet seit über 12 Jahren bei der Deutschen Bundesbank. Mehrere Jahre war er als Prüfer im Rahmen von bankgeschäftlichen IT-Prüfungen bei Banken und Sparkassen im Einsatz. Zuvor war er als Programmierer sowie als IT- und Cloud-Architekt für die Bundesbank tätig. Zudem war er projektbezogen für die Europäische Zentralbank (EZB) tätig.

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

Jan-Philipp Küsters ist Referent für Operative Informationssicherheit im Bereich IT-Governance bei der Sparkasse Krefeld. Davor war er als Spezialist IT-Organisator im Bereich IT-Infrastruktur tätig. Als Mitglied im DORA-Projekt 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.

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

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

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

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

Praxis-Umsetzung IT-Sicherheit & Cyber-Sicherheit unter DORA
29. Juni 2026, Online-Veranstaltung

Durchführung DORA-konformer PenTests, TIBER-Tests & TLPTs
9. Juli 2026, Online-Veranstaltung

IKT-Geschäftsfortführungsmanagement im Fokus der Aufsicht
20. Juli 2026, Online-Veranstaltung

DORA-konforme Notfall-Konzepte und BCM-Prozesse unter Einbindung der IKT-DL
16. September 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-konformes
Schwachstellenmanagement

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, 22. Juli 2026
9:00–15:00 Uhr
Online-Zugang ab 8:45 Uhr

Seminar-Nr. 26 07 BA225 W

Teilnahmegebühr

€ 590,– (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.

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 / 26 07 BA225