13. März 2025 · 9:00–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

Anforderungen an IT-Infrastruktur & IT-Betrieb unter DORA

Banken-Aufsicht-Seminar · 8 CPE-Punkte

Praxis-Tipps,
Umsetzungs-Hinweise &
Prüfungs-Ansätze!

- **Konkrete Erwartungen der Aufsicht aus MaRisk, DORA und EBA-ICT-Leitlinien**
- **Häufige Fragestellungen und 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**

20 Jahre AKADEMIE HEIDELBERG

Referenten

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

Pasquale Totaro
Leiter Revision IT
DekaBank
Frankfurt/Main

Torsten Zacher
Business Continuity Manager
Certified Lead Auditor ISO 22301
RSM Ebner Stolz, Stuttgart

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA

Programm

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

Konkrete Erwartungen der Aufsicht an ausgewählte Themen der operativen Informationssicherheit aus MaRisk/DORA

- 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 von Software und IDV: Entwickler-Clients, administrative Benutzer, Skriptausführung, Überwachung
- IKT-Dienstleister – Prozesstransparenz und Steuerbarkeit
- Identifizierte Schwachstellen aus aktuellen Prüfungen

Pasquale Totaro, DekaBank · 12:45–14:45 Uhr

IT-Infrastrukturen und operativer IT-Betrieb in Banken: Herausforderungen, Prüfungsansätze und Erfahrungen aus der Praxis der Internen Revision

- Konkretisierung der Aufsichts-Anforderungen an die IT-Infrastruktur und den operativen IT-Betrieb u. a. in MaRisk, DORA und IKT-Leitlinien
- Praxiserfahrungen zu den regulatorischen Anforderungen an den IT-Betrieb und dem Umgang mit Auslagerungen
- Prüfung der IT-Infrastruktur durch die (IT-)Revision:
  - Was gehört zur IT-Infrastruktur einer Bankengruppe?
  - Prüfung der Configuration Management Database
  - Wie können Cloud Anbieter berücksichtigt werden?
- Wie können bei Revisionsprüfungen die 1st/2nd line und die Schnittstellen zu ext. Dienstleistern einbezogen werden?
  - Umgang mit Feststellungen von wesentlichen IKT-Dienstleistern
  - Erkenntnisse aus Prüfungen von Rechenzentren im In- und Ausland
  - Rolle des Auslagerungsmanagements, ISM und IRM
- Prüfung des operativen IT-Betriebs durch die IT-Revision
  - Prüfung des IT-Service Continuity Management (ITSCM)
  - Beurteilung der Datensicherungs- und Auslagerungsverfahren zur Sicherstellung der Daten-Verfügbarkeit
  - Identifikation, Bewertung und Behebung von Schwachstellen
  - Beurteilung des Schwachstellenmanagements
  - Wie erfolgt die Protokollierung und Kontrolle privilegierter Aktivitäten? – Privileged Access Management (PAM)
- Häufige Prüfungsfeststellungen der Internen Revision, Prüfungsansätze, Erkenntnisse und Praxis-Tipps

Torsten Zacher, RMS · 15:00–17:00 Uhr

Erweiterte DORA-Anforderungen an das IKT-Notfallmanagement und das IT-Service-Continuity Management (ITSCM) bei Ausfall der IT-Infrastruktur und Störungen des IT-Betriebs

- DORA-Anforderungen an Notfallprozesse, Verantwortlichkeit und Zuständigkeiten bei IT-Ausfall und IT-Störungen
- Vorgaben zur Gestaltung von Geschäftsfortführungs-, Notbetriebs- und Wiederherstellungsplänen
- Umgang mit BCM-Kennzahlen: RTO, RPO, MTPD für IT-Infrastruktur und IT-Betrieb
- Risikoanalyse: Identifizierung von Risiken, Lücken und Ableitung von Maßnahmen
- Prüfung des Zusammenspiels von Notfallplänen, Notfallprozessen, Wiederanlaufplänen und Notfall-Handbüchern
- Einbindung von Auslagerungsdienstleistern in die risikoorientierte Notfallplanung
- Durchführung und Bewertung von Notfallübungen, inkl. Maßnahmenableitung

Seminarziel

Der Bereich der operativen Informationssicherheit ist facettenreich und entwickelt sich, dem Stand der Technik entsprechend, stetig weiter. So konnte beispielsweise in den letzten Jahren beobachtet werden, dass der Einsatz von Security Information and Event Management (SIEM)-System sowie eines Schwachstellenscanners unabdingbar für die Erfüllung eines hohen Schutzbedarfes für sicherheitskritische IT-Systeme sind. Dementsprechend wachsen auch die aufsichtlichen Anforderungen an die von den Instituten verantworteten IT-Systeme.

Wesentliche Feststellungen in dem Bereich der operativen Informationssicherheit zeigen, dass für viele Institute ein Nachholbedarf bei der Erfüllung der aufsichtlichen Anforderungen haben.

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 (IT-)Revision hat die Einhaltung der in den MaRisk und DORA verankerten Anforderungen entsprechend zu prüfen.

Wissenswertes

Zielgruppe

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

- IT, Interne Revision, IT-Revision, IT-Organisation
- Informationssicherheit (ISB), Informationsrisikomanagement und IT-Notfallbeauftragte
- IT-Sicherheitsmanagement und IT-Architekten
- IT-Compliance und IT-Governance, IT-Grundsatz und Regulatorik
- sowie andere interessierte Fachbereiche bzw. Mitglieder des Vorstands und der Geschäftsleitung, externe Prüfer*innen sowie Bankdienstleister

Unsere Referenten

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, SAP Systemservices Architektur, Zentrale IT-Plattformmanagement Drittprodukte, 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 ist er projektbezogen für die Europäische Zentralbank (EZB) tätig.

Pasquale Totaro
Leiter Revision IT
DekaBank Deutsche Girozentrale, Frankfurt/Main

Pasquale Totaro ist Leiter der IT-Revision der DekaBank und besitzt mehr als 20 Jahre Erfahrung im Bereich der Prüfung von IT, IT-Infrastruktur und des IT-Betriebs. Vor seiner Zeit bei der DekaBank war er für eine große Wirtschaftsprüfungsgesellschaft tätig.

Torsten Zacher
Business Continuity Manager, Certified Lead Auditor ISO 22301
RSM Ebner Stolz, Stuttgart

Torsten Zacher ist seit 20 Jahren im Bankaufsichtsrecht tätig und Experte in den Themenfeldern Business Continuity Management, Krisenmanagement und Outsourcing Management. Seit Mai 2023 bei RSM Ebner Stolz als BCM-Manager tätig. Zuvor arbeitete er als BCM-Beauftragter für die Börse Stuttgart, bei der Mercedes-Benz Bank AG im Bereich Compliance (BCM, zentrales Auslagerungsmanagement, Organisation) und bei LBBW in den Bereichen Compliance und Risikomanagement (BCM, zentrales Auslagerungsmanagement, OpRisk).

DORA Spezial:
Informationssicherheit & IKT-Risikomanagement
23. Januar 2025, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM
29. Januar 2025, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken
17. Februar 2025, Online-Veranstaltung

Mobile-Work-Risiken im Fokus von DORA, IKT-Risikomanagement & IT-Revision
18. Februar 2025, Online-Veranstaltung

Prüfung DORA & DORA-Umsetzung
17./18. März 2025, Online-Veranstaltung

Anforderungen an das Datenqualitätsmanagement (DQM)
26. März 2025, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen
1. April 2025, 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

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA

Name

Vorname

Position

Firma

Straße

PLZ / Ort

Tel./Fax

E-Mail

Name der Assistenz

Datum Unterschrift

Senden Sie Ihre Anmeldung bitte an: **anmeldung@akademie-heidelberg.de**

Termin + Seminarzeiten

Donnerstag, 13. März 2025
9:00–17:00 Uhr
Online-Zugang ab 8:45 Uhr

Seminar-Nr. 25 03 BA145 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, wenn gewünscht, 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 Internet-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.

12.24 / 25 03 BA145

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 28 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de