18. September 2025 · 10:00–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen

Banken-Aufsicht-Seminar · 7 CPE-Punkte

Konkrete Bank-Praxis-Berichte mit Handlungsempfehlungen und Umsetzungshinweisen!

- **Erweiterte Aufsichtsanforderungen zur Bestimmung der IT-Schutzobjekte – u. a. vor dem Hintergrund neuer DORA-Vorgaben**
- **Die neue IKT-Kontrollfunktion im Zusammenspiel mit dem ISB**
- **Praxis-Anforderungen an Schutzbedarfs- und Risikoanalysen unter Einbezug von IDV und externen IKT-Dienstleistern (DORA!)**
- **Praxis-Bericht: Schutzbedarfsanalyse entlang eines Prozesses (Owner-Prinzip!) – Bedeutung der Data-Governance**
- **Häufige Schwachstellen und identifizierte Mängel in der Praxis**

20 Jahre AKADEMIE HEIDELBERG

Referenten

Dirk Mühlhausen
IT-Prüfer und Prüfungsleiter
Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Mainz

Mike Bona-Stecki
Leiter Informationssicherheit und
Business Continuity Management
DekaBank, Frankfurt/Main

Roland Hein
Inhaber, Geschäftsführer
bit Informatik GmbH
Trier

Mit freundlicher Unterstützung von:

bit INFORMATIK

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen

Programm

Dirk Mühlhausen, Bundesbank · 10:00–12:15 Uhr

DORA-Vorgaben zur Identifikation, Bewertung und Behandlung von IKT-Assets

- Kritische oder wichtige Funktionen (kowF) – Methoden der Identifikation und Bewertung
- IKT-Risikomanagementrahmen – Übergreifende Anforderungen und Mindestumfang
- IKT-Sicherheitsleit- und -richtlinien – Was ist zu beachten?
- Neue Anforderungen und Aufgaben der Kontrollfunktion des IKT-Risikomanagements (IKT-Risikokontrollfunktion)
- Festlegung einer Risikotoleranzschwelle
- Identifikation, Klassifizierung und Inventarisierung von IKT-Assests
- Bedrohungsanalyse
- Katalog der IKT-Sicherheitsmaßnahmen (inkl. Vereinbarungen mit den Dienstleistern)
- Überprüfung der Umsetzung der IKT-Sicherheitsmaßnahmen (inkl. Dienstleister)
- Identifikation, Bewertung und Behandlung von IKT-Risiken
- Verfahren und Methodik einer Risikoüberwachung
- Sonderfall: Risiken aus IKT-Altsystemen
- Anforderungen an die Berichterstattung von IKT-Risiken

Mike Bona-Stecki, DekaBank · 13:00–15:15 Uhr

Praxis-Bericht: Ermittlung der Kritikalität (Schutzbedarfsanalyse) entlang eines Prozesses und Ableitung angemessener SOLL-Anforderungen unter Berücksichtigung von DORA

- Aufbau- und ablauforganisatorische Regelungen zur Schutzbedarfsanalyse
- Schnittstellen und Unterschiede zwischen fachlicher und technischer Schutzbedarfsanalyse – vom Geschäftsprozess zur IKT-Assetbewertung
- Informationen als Basis für die Bewertung von Prozessen
- Die Schutzbedarfsanalyse als Basis für die Ermittlung der kritischen und wichtigen Funktionen nach DORA
- Schnittstellen zu anderen 2nd-line-Funktionen
- Anwendung des Maximal-, Kumulations- und Verteilungsprinzips – Umgang mit Konzentrationsrisiken
- Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog; Ableitung von Schutzmaßnahmen zur Stärkung der digitalen operationalen Resilienz
- Schnittstellen zwischen der Schutzbedarfsanalyse, dem Sollmaßnahmenkatalog und dem Business Continuity Management (Anforderungen an das Notfallmangement)
- Die neue Rolle der IKT-Kontrollfunktion als 2nd-line im Rahmen der SBA – sinnvolle Kontrollhandlungen

Roland Hein, bit Informatik · 15:30–17:00 Uhr

Praxis-Bericht: GAP-Analyse zum IT-Schutzbedarf – Besonderheiten im Informationsverbund

- IT-Schutzbedarf, welche Ausprägungen werden benötigt
- Schutzbedarf-Bewertung – SOLL versus IST, GAP-Analysen
- Ablauf einer Risikobetrachtung
  - Bewertung von möglichen Risiken (BSI)
  - Anwendung von Maßnahmen (BSI)
  - Erneute Bewertung der Risiken (BSI)
  - Ggf. Anwendung von zusätzlichen Maßnahmen
- Objekte eines Informationsverbundes und deren Beziehungen zueinander
  - Fachliche Objekte, u. a. Datenklassen, Geschäftsprozesse
  - Technische Objekte, u. a. DV-Systeme, Verbindungen
- Verbindung der Objekte des Informationsverbundes mit weiteren Objekten
  - Organisationshandbuch (OHB)
  - Hardware-Verwaltung/CMDB
  - Berechtigungskonzepten
- Fachliche Vorgehensweise beim Aufbau/Umsetzung eines Informationsverbundes
- Erstellen von Protokollierungs- und Auswertungskonzepten
- Durchführung von Business Impact Analysen (BIAs)
- Regelmäßige Überprüfung und notwendige Workflows

Seminarziel

Durch DORA, den Wegfall der BAIT, die zunehmende Komplexität der IT-Landschaft und die sich daraus ergebenden erweiterten Prozesspflichten zur institutsindividuellen Festlegung des Schutzbedarfs, rücken die Themen Schutzbedarf und Risikoanalyse stärker in den Fokus von Prüfungen der (IT-) Revision sowie der Bundesbank und erhöhen die Anforderungen an Fachbereiche und IKT-Kontrollfunktion.

Die Schutzbedarfsanalyse bildet mit der Bewertung des Schadenspotentials auf Ebene der Geschäftsprozesse die Basis für eine sachgerechte Risikoermittlung und Bewertung. Anhand der drei Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit müssen alle Daten analysiert und deren Schutzbedarf prüfungssicher dokumentiert werden.

Wichtig ist dabei auch eine realistische Einschätzung der möglichen Folgeschäden im Rahmen der Risikoanalyse und die Ableitung angemessener (Schutz-)Maßnahmen. Nur so kann das Risiko von Datenverlust, Diebstahl oder sogar kriminellen Handlungen minimiert werden. Hier sind insbesondere die Informationssicherheits-Beauftragten (ISB) bzw. die neue IKT-Kontrollfunktion in Verbindung mit der (IT-)Revision in der Prüfungspflicht

Das Seminar beantwortet aktuelle Prüfungs- und Praxisfragen und gibt wertvolle Handlungsempfehlungen und Anwendungstipps für die Institutspraxis.

Wissenswertes

Zielgruppe

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

- Informationssicherheit (ISB/IKT-Kontrollfunktion), Informationsrisikomanagement, Datenschutz (DSB) und Data Governance
- IT, IT-Organisation und IT Service Continuity Management (ITSCM)
- Notfallmanagement und Business Continuity Management (BCM)
- Interne Revision, IT-Revision und IT-Compliance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung

sowie andere interessierte Fach- bzw. Grundsatzbereiche, IT-Vorstandsmitglieder, externe Prüferinnen und Prüfer sowie Bankdienstleister

Unsere Referenten

Dirk Mühlhausen
IT-Prüfer und Prüfungsleiter Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Mainz

Dirk Mühlhausen besitzt langjährige Erfahrungen als Prüfer und Teamleiter in der Banken- und Finanzaufsicht der Deutschen Bundesbank im Bereich der MaRisk-Prüfungen für Finanzinstitute unterschiedlicher Art und Größe, sowohl national als auch international. Seine Schwerpunkte liegen insbesondere auf Prüfungen des IT-Risikomanagements für bedeutende und weniger bedeutende Institute sowie bei verschiedenen IKT-Dienstleistern.

Mike Bona-Stecki
Leiter Informationssicherheit und Business Continuity Management
DekaBank Deutsche Girozentrale, Frankfurt am Main

Mike Bona-Stecki ist als Leiter Informationssicherheit und BCM bei der DekaBank für das Informationssicherheits-, IT-Risiko- und Business Continuity Management verantwortlich. Er leitet ein Team von Sicherheitsexperten und beschäftigt sich schwerpunktmäßig mit der Umsetzung der aufsichtsrechtlichen Anforderungen zu diesen Themen.

Roland Hein
Inhaber, Geschäftsführer
bit Informatik GmbH, Trier

Roland Hein stellt Instituten aus dem gesamten Drei-Säulen-Modell der deutschen Kreditwirtschaft seit fast 30 Jahren workflowbasierte Anwendungen zur ganzheitlichen und aufsichtskonformen Umsetzung der MaRisk- und BAIT-Anforderungen zur Verfügung. Seine Schwerpunkte liegen hierbei u. a. in der systemgestützten Abbildung, Vergabe und Überwachung von (IT-)Berechtigungen (MaRisk AT 4.3), der Dienstleistersteuerung (MaRisk AT 9, DORA) sowie der Abbildung und Steuerung des Informationsverbunds.

IKT Spezial für Compliance & Governance
25. Juni 2025, Online-Veranstaltung

Prüfung (IT-)Auslagerungen (MaRisk) &
(IKT-)Drittdienstleistungen (DORA)
9. Juli 2025, Online-Veranstaltung

Anforderungen an IT-Infrastruktur &
IT-Betrieb unter DORA
10. Juli 2025, Online-Veranstaltung

Praxis-Umsetzung der IT-Sicherheit &
Cyber-Sicherheit unter DORA
21. Juli 2025, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)
24. Juli 2025, Online-Veranstaltung

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

DORA-konformes IKT-Risikomanagement
23./24. September 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

IT-Schutzbedarf & Soll-Konzepte
DORA-konform umsetzen

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, 18. September 2025
10:00–17:00 Uhr
Online-Zugang ab 9:45 Uhr

Seminar-Nr. 25 09 BA152 W

Teilnahmegebühr

€ 690,– (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 Hompage 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.

05.25 / 25 09 BA152

AKADEMIE HEIDELBERG

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