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

AKADEMIE HEIDELBERG

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen

Banken-Aufsicht-Seminar · 7 CPE-Punkte

- **IT-Schutzobjekte richtig bestimmen – erweiterte Anforderungen im Überblick**
- **Die neue IKT-Kontrollfunktion im Zusammenspiel mit dem ISB/CISO**
- **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**

Referenten

Dirk Mühlhausen
Prüfer der Finanzaufsicht
Deutsche Bundesbank
Mainz

Mike Bona-Stecki
Leiter Informationssicherheit und
BCM, stellv. DOR-Beauftragter
DekaBank, Frankfurt/Main

Roland Hein
Inhaber, Geschäftsführer
bit Informatik GmbH
Trier

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen

Programm

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

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

- Kritische oder wichtige Funktionen – 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
- IKT-Assests: Identifikation, Klassifizierung, Inventarisierung
- Bedrohungsanalyse
- Katalog der IKT-Sicherheitsmaßnahmen & Überprüfung der Umsetzung (inkl. Vereinbarungen mit den Dienstleistern)
- Identifikation, Bewertung und Behandlung von IKT-Risiken
- Verfahren und Methodik einer Risikoüberwachung
- Sonderfall: Risiken von IKT-Altsystemen
- Anforderungen an die Berichterstattung von IKT-Risiken

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

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

- Aktuelle Regelungen zur Schutzbedarfsanalyse
- Schnittstellen und Unterschiede zwischen fachlicher und technischer Schutzbedarfsanalyse – vom Geschäftsprozess zur IKT-Assetbewertung
- Die Schutzbedarfsanalyse als Basis für die Ermittlung der kritischen und wichtigen Funktionen nach DORA
- Schnittstellen und übergreifende Aspekte zu anderen 2nd-line-Funktionen (u. a. Dokumentationsanforderungen)
- Anforderungen an die Schutzbedarfs-Dokumentation
- DORA-Auswirkungen auf die Schutzbedarfsanalyse
- Anwendung des Maximal-, Kumulations- und Verteilungsprinzips – Umgang mit Konzentrationsrisiken
- Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog
- Schnittstellen zwischen der Schutzbedarfsanalyse, dem Sollmaßnahmenkatalog und dem BCM
- Die neue Rolle der IKT-Risikokontrollfunktion als 2nd-line im Rahmen der Schutzbedarfsanalyse – sinnvolle Kontroll- und Überwachungshandlungen

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

Praxis-Bericht: GAP-Analyse zum IT-Schutzbedarf – Besonderheiten im Informationsverbund – Erkennung von Lücken bei Kritikalitätsanalysen und IKT-Sicherheitsmaßnahmen

- IT-Schutzbedarf nach DORA, welche Ausprägungen werden benötigt
- Bewertung des Schutzbedarfs – SOLL versus IST, ermitteln von GAPs
- Ablauf einer Risikobetrachtung
- Fachliche Objekte (Datenklassen, Geschäftsprozesse, Verträge, Anwendungen)
- Technische Objekte (DV-Systeme, Verbindungen, Räume, Sonstige Objekte)
- Verbindung der Objekte des Informationsverbundes mit weiteren Objekten
- Organisationshandbuch (OHB)
- Hardware-Verwaltung/CMDB und Berechtigungskonzept
- Fachliche Vorgehensweise beim Aufbau/Umsetzung eines Informationsverbundes
- Erstellen von Protokollierungskonzepten und Protokollauswertungskonzepten
- Durchführung von Business Impact Analysen
- Notwendige Funktionen wie Workflows, regelmäßige Überprüfung und Auswertungen
- Häufig identifizierte Schwachstellen in der Praxis

Seminarziel

Durch DORA, den Wegfall der BAIT, die zunehmende Komplexität der IT-Landschaft und die sich daraus ergebenden erweiterten Prozesspflichten rücken die Themen Schutzbedarf und Risikoanalyse stärker in den Fokus von Prüfungen der (IT-)Revision sowie externer Prüfer*innen 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-Risikokontrollfunktion in Verbindung mit der (IT-)Revision in der Prüfungspflicht.

Das Seminar beantwortet aktuelle Praxisfragen und gibt wertvolle Handlungsempfehlungen und Anwendungstipps.

Zielgruppe

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

- Informationssicherheit (ISB/IKT-Kontrollfunktion), Informationsrisikomanagement
- IT, IT-Organisation, Notfallmanagement und BCM/ITSCM
- Interne Revision, IT-Revision und IT-Compliance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung

Sowie andere interessierte Fach- bzw. Grundsatzbereiche, IT-Vorstandsmitglieder, externe Prüfer*innen und Bankdienstleister.

Unsere Referenten

Dirk Mühlhausen
Prüfer der Finanzaufsicht, Deutsche Bundesbank, Mainz

Als Prüfungsleiter und Leiter von Prüfungsteams der Finanzaufsicht verfügt Dirk Mühlhausen über langjährige Erfahrung in der Prüfung von Finanzinstituten – insbesondere in den Bereichen ICT-Risikomanagement und ICT-Continuity-Management. Darüber hinaus ist er projektbezogen auch im internationalen Kontext tätig. Der Referent vertritt seine persönliche Auffassung und nicht diejenige der Deutschen Bundesbank bzw. der Finanzaufsicht und gibt keine offiziellen Auslegungen zu regulatorischen Vorgaben ab.

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

Mike Bona-Stecki ist seit 2018 als Leiter Informationssicherheit und Business Continuity Management bei der DekaBank Deutsche Girozentrale für das Informationssicherheits-, IT-Risiko- und Business Continuity Management verantwortlich. Er leitet ein Team von Sicherheitsexperten und beschäftigt sich mit der Umsetzung der aufsichtsrechtlichen Anforderungen an das IT-/Informationssicherheits- und Business Continuity Management.

Roland Hein
Inhaber, Geschäftsführer, bit Informatik GmbH, Trier

Herr Hein stellt Instituten Anwendungen zur ganzheitlichen und aufsichtskonformen Umsetzung der Regulatorik 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) sowie des Informationsverbunds.

**Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht notwendigerweise die eines bestimmten Instituts, der Deutschen Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wieder. Die Referenten geben auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte wieder.*

DORA- und Praxis-Anforderungen an das Berechtigungsmanagement und die SOD-Matrix
13. Juli 2026, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken
21. Juli 2026, Online-Veranstaltung

DORA KOMPAKT!
10. September 2026, Online-Veranstaltung

Neuer IKT-Risikomanagement-Rahmen nach DORA
11. September 2026, Online-Veranstaltung

DORA-konforme Auslagerungsverträge/SLAs
16. September 2026, Online-Veranstaltung

DORA-konforme Notfall-Konzepte und BCM-Prozesse unter Einbindung der IKT-Drittdienstleister
16. September 2026, Online-Veranstaltung

DORA-konformer Umgang mit Software- und Cloud-Diensten
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

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen

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

Donnerstag, 17. September 2026
10:00–17:00 Uhr
Online-Zugang ab 9:45 Uhr

Seminar-Nr. 26 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 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

09_26 / 2609BA152