

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen



Banken-Aufsicht-Seminar · 7 CPE-Punkte

Konkrete Bank-Praxis-
Berichte mit Handlungs-
empfehlungen und
Umsetzungshinweisen!

- **Erweiterte Aufsichtserwartungen zur Bestimmung der IT-Schutzobjekte**
- **Die neue IKT-Kontrollfunktion als Nachfolger des ISB**
- **Praxis-Anforderungen an Schutzbedarfs- & Risikoanalysen unter Einbezug von IDV und externen Dienstleistern (DORA!)**
- **Praxis-Bericht: Schutzbedarfsanalyse entlang eines Prozesses (Owner-Prinzip!) – Bedeutung der Data-Governance**
- **Häufige Schwachstellen und identifizierte Mängel**

20 Jahre
**AKADEMIE
HEIDELBERG**

Referenten

Alexander Rothländer
Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank
Frankfurt/Main

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

Lars Ehrenfeld
Abteilungsleiter Prozessmanagement
und IT-Governance
Kreissparkasse Heilbronn

Programm

Alexander Rothländer, Bundesbank · 10:00–12:00 Uhr

Informationsrisikomanagement und Schutzbedarfsanalyse nach DORA – Neue Anforderungen der Aufsicht

- Wegfall der BAIT: Erweiterte Anforderungen aus DORA, MaRisk und EBA-ICT-Leitlinien an die Schutzbedarfsanalyse (SBA) bzw. Kritikalitätseinstufung
- Die IKT-Kontrollfunktion als Nachfolger des Informationssicherheitsbeauftragten (ISB)
- Erläuterung des Begriffs »kritische oder wichtige Funktion« nach DORA, aufsichtliche Erwartungen zur Auslegung und Diskussion von Lösungsansätzen
- Auswirkungen von DORA auf den Sollmaßnahmenkatalog
- Die Schutzbedarfsanalyse bzw. Kritikalitätseinstufung als Schnittstelle zwischen den Fachbereichen und der IT – konkrete Anforderungen an die einzurichtenden Rollen, die Durchführung und die Kontrollprozesse
- Bestimmung und Management von IT-(Rest)Risiken
- Diskussion alternativer Lösungsansätze für das Informationsrisikomanagement nach DORA
- Prüfungshandlungen im Zusammenhang mit der Schutzbedarfsanalyse bzw. Kritikalitätseinstufung und anderen Teilen des Informationsrisikomanagements
- Häufige Schwachstellen und identifizierte Mängel aus bankgeschäftlichen Prüfungen

Lars Ehrenfeld, Kreissparkasse Heilbronn · 12:45–14:45 Uhr

Praxis-Anforderungen an Schutzbedarfs- & Risikoanalysen unter Einbezug von IDV und externen IKT-Dienstleistern

- Neue DORA-Anforderungen bei IT-Dienstleistungen i.Z.m. IT-Schutzobjekten
- Strukturanalyse der IT-Architektur: Identifikation und Gruppierung der IT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- Zuordnung geplanter bzw. nachträglich identifizierter IDV-Anwendungen zu einer Schutzbedarfsklasse
- Schutzbedarfsklassifizierung der Dienstleister – Entstehende Risiken und notwendige Sollmaßnahmen

- Praxisempfehlungen für die Durchführung und Auswertung von Risiko- und Restrisikoanalysen
- OpRisk-Reporting – Berichte über IKT-Risiken unter Einbezug externer Dienstleister

Mike Bona-Stecki, DekaBank · 15:00–17:00 Uhr

Praxis-Bericht: Schutzbedarfsanalyse entlang eines Prozesses: GAP-Analyse zum IT-Schutzbedarf – Besonderheiten im Informationsverbund – Ableitung von Schutzmaßnahmen

- Auswirkungen von DORA auf die Schutzbedarfsanalyse
- Aufbau- und ablauforganisatorische Regelungen zur Schutzbedarfsanalyse
- Bewertung und Kontrolle des Schutzbedarf – SOLL versus IST, ermitteln von GAPs
- Schnittstellen und Unterschiede zwischen fachlicher und technischer Schutzbedarfsanalyse – vom Geschäftsprozess zur Assetbewertung
- Berücksichtigung von Unternehmenswerten bei der Ermittlung der Kritikalität von Prozesse und Assets
- Die Schutzbedarfsanalyse als Basis für die Ermittlung der kritischen und wichtigen Funktionen nach DORA
- Schnittstellen und übergreifende Aspekte zu anderen 2nd-line-Funktionen
- Anwendung des Maximal-, Kumulations- und Verteilungsprinzips – Umgang mit Konzentrationsrisiken
- Schnittstellen zwischen der Schutzbedarfsanalyse, dem Sollmaßnahmenkatalog und dem Business Continuity Management (Was passt mit den Anforderungen aus der Schutzbedarfsanalyse im Notfall?)
- Die (neue) Rolle des ISB bei der Schutzbedarfsanalyse – sinnvolle Kontroll- und Überwachungshandlungen
- Erhöhte Anforderungen an die Schutzbedarfs-Dokumentation
- Soll-Maßnahmen als Basis einer angemessenen Risikobewertung,
- Verfahren zur Ermittlung, Bewertung und transparenten Ausweisung von IKT- und Sicherheitsrisiken

Seminarziel

Durch DORA, 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 Bundesbank und der (IT-)Revision und erhöhen die Anforderungen an die Fachbereiche.

Die Schutzbedarfsanalyse ist ein Teil des IT-Sicherheitskonzepts nach dem IT-Grundschutz. 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), Informationsrisikomanagement, Datenschutz (DSB), Data Governance und neue IKT-Konrollfunktion
- 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



Alexander Rothländer

Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank, Frankfurt/Main

Alexander Rothländer arbeitet als Bankgeschäftlicher Prüfer und Prüfungsleiter für die Deutsche Bundesbank. In dieser Funktion prüft er die Risikomanagementprozesse von Banken »vor Ort«. Die Prüfungen erstrecken sich auf bedeutende und weniger bedeutende Kreditinstitute im nationalen und internationalen Umfeld. Vor seiner Tätigkeit als Prüfer hat er als Entwickler und IT-Projektleiter Erfahrungen in den Bereichen Entwicklung, Betrieb und Ablösung von IDV-Anwendungen gesammelt



Mike Bona-Stecki

Leiter Informationssicherheit und Business Continuity Management
DekaBank Deutsche Girozentrale, Frankfurt am 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 schwerpunktmäßig mit der Umsetzung der aufsichtsrechtlichen Anforderungen an das IT/Informationssicherheits- und das BCM.



Lars Ehrenfeld

Abteilungsleiter Prozessmanagement und IT-Governance
Kreissparkasse Heilbronn, Heilbronn

Lars Ehrenfeld ist bei der Kreissparkasse Heilbronn für die Abteilung Prozessmanagement & IT-Governance verantwortlich. Zu seinen Schwerpunkten gehört u. a. das IT-Aufsichtsrecht. Als Referent aus der Praxis verfügt er über ein breites Wissen und gibt dieses als Dozent an verschiedenen Bildungseinrichtungen weiter.

Seminar-Vorschläge

Nutzung von Robotic (RPA) und Echtzeitreporting zur Prozessoptimierung in Banken
13. Februar 2025, Online-Veranstaltung

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

IKT-Governance im Fokus der Aufsicht
18. Februar 2025, Online-Veranstaltung

Aufbau-Seminar I – Nutzung von KI & ChatGPT
20. Februar 2025, Online-Veranstaltung

Eigen-Anwendungen und IDV im Fokus der Aufsicht
10. März 2025, Online-Veranstaltung

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA
13. März 2025, Online-Veranstaltung

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

KI-Governance: Einsatz Künstlicher Intelligenz (KI) & Anforderungen des AI Act
25. März 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

Dienstag, 1. April 2025
10:00–17:00 Uhr
Online-Zugang ab 9:45 Uhr
Seminar-Nr. 25 04 BA152 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 Homepage 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.



AH **AKADEMIE**
HEIDELBERG

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