

DORA Spezial: Informationssicherheit und IKT-Risikomanagement



Banken-Praxis-Seminar · 8 CPE-Punkte

- **Erfahrungsbericht aus einer BaFin-Prüfung mit Fokus auf Informationssicherheit und IKT-Risikomanagement**
- **DORA: von der Informationssicherheit zum IKT-Risikomanagement**
- **Neue Pflichten des ISB, Einführung der IKT-Risikokontrollfunktion**
- **Erweiterte Anforderungen (TPRM) an die Nutzung von IKT-Dienstleistern und Cloud-Services**
- **Anforderungen an die Informationssicherheit und das IKT-Risikomanagement beim Einsatz von Künstlicher Intelligenz (KI)**

Referenten



Mike Bona-Stecki
Leiter Informationssicherheit und Business
Continuity Management, stv. DOR-Beauftragter
DekaBank Deutsche Girozentrale, FFM



Stephan Wirth
Informationssicherheits- und
Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Programm

Stephan Wirth, NRW.BANK · 9:00 – 10:30 Uhr

Verschärfte Anforderungen aus DORA: Informationssicherheit und Informationsrisikomanagement im Spannungsfeld zwischen Regulatorik und Praxis

- Etablierung eines angemessenen IKT-Risikomanagements: IKT-Risiken und Cyber-Risiken stärker im Fokus
- Akzentverschiebung durch DORA: Einführung einer IKT-Risikokontrollfunktion
- Herausforderungen des IKT-Drittparteirisikomanagements
- Operative IKT-Sicherheit: Umsetzungsstand und (weiterhin) bestehende Schwachstellen
- Verschärfte Anforderungen an die Datenqualität
- Konkrete Anforderungen an IKT-Projekte und Anwendungsentwicklung/IDV/IT-Inventare, Berechtigungsmanagement und Schutzbedarf
- Hinweis zur DORA-Umsetzung in der Praxis

Mike Bona-Stecki, DekaBank · 10:45 – 12:15 Uhr

Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog und einem höheren Informationssicherheitsniveau

- Ziel und Nutzen der Strukturanalyse, Schutzbedarfsfeststellung, Sollmaßnahmenkataloge und Risikoanalyse
- Gängige Standards: ISO 27.XXX-Reihe, BSI-Standards
- Erhebung des Informationsverbunds: Identifikation und Gruppierung der IT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- Schutzbedarfsfeststellung auf Informations- und Prozessebene
- Erarbeitung des Sollmaßnahmenkatalogs auf Basis der Schutzbedarfsanalyse, Strukturanalyse und Standards
- Darstellung der Rollen und Zuständigkeiten
- Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog und wie bewerte ich Soll-Ist-Abweichungen?

Stephan Wirth, NRW.BANK · 13:15 – 14:45 Uhr

Neue Pflichten des Informationssicherheitsbeauftragten (ISB) und Einführung der IKT-Risikokontrollfunktion

- Konkretisierung der Verantwortlichkeiten und der Aufgabenbereiche – neue Rechte und Pflichten; inwieweit ist die IKT-Risikokontrollfunktion auslagerbar?
- Wie unterstützen ISB und Risikokontrollfunktion bei der Erstellung von Strategien, Leitlinien und Prozessen zur Erreichung einer angemessenen DORA-Compliance?
- Unterstützung der Fachbereiche bei der DORA-Umsetzung
- Ermittlung von IKT-Risiken und Auswirkungsanalyse
- Best Practices und Standards für ein praxisnahes und effektives IKT-Risikomanagement
- Management von Informationssicherheitsvorfällen: Auswirkungsanalyse und Veranlassung angemessener Nachsorgemaßnahmen; verschärfte DORA-Meldepflichten

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

Erweiterte Anforderungen an IT-Auslagerungen (DORA, BAIT, AI-Act), IKT-Drittdienstleistungen (DORA) und Cyber-Security aus dem Blickwinkel der Informationssicherheit

- Abgrenzung DORA- zu MaRisk-Anforderungen
- Umgang mit Cyberrisiken bei Auslagerungen und deren Verzahnung mit dem Non Financial Risk-Management
- Beurteilung von IT- und Informationssicherheits-Risiken im Rahmen des Auslagerungsprozesses
- Umgang mit besonderen Herausforderungen und Risiken bei dem Bezug und der Nutzung von Cloud-Services
- Anforderungen an die vertraglichen Regelungen zur Informationssicherheit bei Auslagerungen
- Business Continuity Management im Kontext von Auslagerungen und Fremdbezug von IT-Dienstleistungen –
- Aufrechterhaltung der Kontinuität und Qualität der Geschäftstätigkeiten
- Umsetzungshinweise und Praxistipps

Seminarziel

Gestiegene IT-(Dienstleister-)Risiken, Cyber-Angriffe und Lücken in der Informationssicherheit führen zunehmend häufiger zu Ausfällen kritischer Geschäftsprozesse bei Banken und deren Dienstleistern. Insbesondere Angriffe von außen haben sich hierbei zu einer immanenten Bedrohung entwickelt.

Durch die geplante MaRisk-Novelle 2026 und die neuen DORA-Anforderungen kommen weitreichende zusätzliche Regelungen in den Bereichen Informationssicherheit und Informationsrisikomanagement hinzu, um Ausfälle des Geschäftsbetriebs zu vermeiden.

Die Aufsicht erwartet zusätzliche (Sicherheits-)Maßnahmen der Institute. Damit einher gehen somit auch die erweiterten Aufgaben und Verantwortlichkeiten der Informationssicherheitsbeauftragten (ISB).

Auch Cloud-Dienstleistungen sind aus dem Blickwinkel der Informationssicherheit zu beurteilen – doch wie lassen sich damit verbundene Risiken messen, beurteilen und steuern? Ziel muss es in jedem Fall sein, mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zu einem aussagekräftigen Sollmaßnahmenkatalog zu gelangen für ein höheres Informationssicherheitsniveau.

Das Seminar gibt wertvolle Praxistipps zur Herangehensweise und Umsetzung der aktuellen Anforderungen.

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche:

- DORA-Umsetzung, IT und Organisation, Datenschutz und Data Governance
- Informationssicherheit (ISB) und Informationsrisikomanagement (IRM)
- Notfallmanagement und Business Continuity Management (BCM/ITSCM)
- Interne Revision und IT-Revision, IT-Compliance und IT-Governance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung

Sowie andere interessierte Fach- bzw. Grundsatzbereiche, Geschäftsleitung/Vorstandsmitglieder, (IT-)Prüfer*innen und (IKT-)Dienstleister.

Unsere Referenten



Mike Bona-Stecki

Leiter Informationssicherheit und Business Continuity Management stv. DOR-Beauftragter, DekaBank Deutsche Girozentrale*, FFM

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 Business Continuity Management.



Stephan Wirth

Informationssicherheits- und Datenschutzbeauftragter NRW.BANK*, Düsseldorf

Seit über 20 Jahren ist Herr Wirth in den Bereichen Informationssicherheit, Datenschutz und Notfallplanung in verantwortlicher Position tätig. Bei der NRW.BANK hat er seit 2018 die Funktionen des Informationssicherheits- und des Datenschutzbeauftragten inne. Die Etablierung angemessener Prozesse und Verfahren zur nachhaltigen Sicherstellung der Einhaltung der aufsichtsrechtlichen Anforderungen gehört dabei zu seinen Hauptaufgaben.

*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 nehmen auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.

DORA-konformer Umgang mit Eigen-Anwendungen und IDV
2. März 2026, Online-Veranstaltung

TPRM Spezial: Umgang mit SaaS & Cloud-Diensten unter DORA
4. März 2026, Online-Veranstaltung

Zertifikats-Lehrgang Auslagerungsmanagement (MaRisk) & IKT-Dienstleistersteuerung (DORA)
11. bis 13. März 2026, Online-Veranstaltung

Fachtagung DORA & DORA-Umsetzung
16./17. März 2026, Online-Veranstaltung

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA
24. März 2026, Online-Veranstaltung

DORA-konforme Ausgestaltung von DL-Verträgen und SLAs
26. März 2026, Online-Veranstaltung

KI-Governance: Aufsichts-Anforderungen an den Einsatz von Künstlicher Intelligenz
14. April 2026, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen
27. April 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 Spezial: Informationssicherheit und IKT-Risikomanagement

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, 7. Mai 2026
9:00–17:00 Uhr
Online-Zugang ab 8:45 Uhr
Seminar-Nr. 26 05 BA011 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 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