4. Juni 2024 · 9:30–16:30 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

BAIT Spezial: Informationssicherheit & Informationsrisikomanagement

Banken-Praxis-Seminar · 7 CPE-Punkte

TOP-Aktuelle Praxis-Hinweise und Umsetzungs-Tipps!

- **Erfahrungsbericht aus einer aktuellen BaFin-Prüfung mit Fokus Informationssicherheits- und Informationsrisikomanagement**
- **Umsetzungs-Schwachstellen aus MaRisk- und BAIT-Vorgaben und Auswirkungen der EBA-Vorgaben zu ICT-Risiken auf LSI-Banken**
- **Neue Pflichten und erweiterte Aufgaben des ISB durch DORA**
- **Erweiterte Anforderungen an die Nutzung von Cloud-Dienstleistern**
- **Oft vernachlässigte Schadenspotenziale aus Cyber-Risiken**
- **Anforderungen an die Informationssicherheit beim Einsatz von Künstlicher Intelligenz (KI)**

Referenten

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

Stephan Wirth
Informationssicherheits- und Datenschutzbeauftragter
NRW.BANK, Düsseldorf

BAIT Spezial: Informationssicherheit & Informationsrisikomanagement

Programm

Stephan Wirth, NRW.BANK · 9:30–10:45 Uhr

Verschärfte BAIT-Umsetzungs-Anforderungen: Informationssicherheit und Informationsrisikomanagement im Spannungsfeld zwischen Regulatorik und Praxis

- Erweiterte MaRisk-/BAIT-Anforderungen an Informationssicherheit und IT-Governance: IT-Risiken und Cyber-Risiken stärker im Fokus
- Wie ist der Digital Operational Resilience Act (DORA) einzuordnen?
- Akzentverschiebung durch DORA: Einführung einer IKT-Risikokontrollfunktion
- Operative IT-Sicherheit: Umsetzungsstand und (weiterhin) bestehende Schwachstellen
- Verschärfte Anforderungen an die Datenqualität im Informations-Risiko-Management für alle Institute (LSI+SI)
- Konkrete Anforderungen an IT-Projekte und Anwendungsentwicklung/IDV/IT-Inventare, Berechtigungsmanagement und Schutzbedarf

Mike Bona-Stecki, DekaBank · 11:00–12:30 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
- Neuerungen durch »DORA« im Rahmen der »Digital Finance Strategie« der EU – Hinweis zur Umsetzung in der Praxis
- Erhebung des Informationsverbunds
- Identifikation und Gruppierung der IT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- Schutzbedarfsfeststellung und Vererbung auf Informations- und Prozessebene
- Erarbeitung des Sollmaßnahmenkatalogs auf Basis der Schutzbedarfsanalyse, Strukturanalyse und gängiger Standards
- Welche Herausforderungen entstehen in der Praxis und wie kann man sie meistern?
- Darstellung der Rollen und Zuständigkeiten
- Wie gelangt man mithilfe der Strukturanalyse und Schutzbedarfsfeststellung zum Sollmaßnahmenkatalog und wie bewertet man Soll-Ist-Abweichungen?

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

Neue Aufgaben und Pflichten des Informations-Sicherheits-Beauftragten (ISB) und Zusammenspiel mit dem Informationsrisikomanagement

- Konkretisierung der Verantwortlichkeiten und des Aufgabenbereichs des ISB – neue Rechte und Pflichten – inwieweit sind Informationssicherheitsbeauftragte (noch) auslagerbar?
- Wie unterstützt der ISB den Vorstand und die Geschäftsleitung bei der Erstellung von Leitlinien und Konzepten für die Informationssicherheit? Überprüfung und Quantifizierung der Geschäfts- und IT-Strategieziele (strategische Informationssicherheit)
- Unterstützung der Fachbereiche bei der Umsetzung (operative Informationssicherheit) der regulatorischen Anforderungen
- Vorgehensweise des IBS bei der Ermittlung von Informationssicherheitsrisiken – Häufige Probleme hinsichtlich der Auswirkungsanalyse von IT-Projekten – Umgang mit identifizierten Risiken – Rückführung in das Informationsrisikomanagement – Regelmäßige Dokumentation
- Best Practices und Standards für ein praxisnahes und effektives Informationsrisikomanagement
- Management von Informationssicherheitsvorfällen (SIEM): Zeitnahe Analyse der Auswirkungen und Veranlassung angemessener Nachsorgemaßnahmen; verschärfte Meldepflichten aus DORA

Mike Bona-Stecki, DekaBank · 15:00–16:30 Uhr

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

- Aktuelle regulatorische und gesetzliche Vorgaben zum Outsourcing
- Cyber-Governance entlang der Wertschöpfungskette – Umgang mit Cyberrisken bei Auslagerungen und deren Verzahnung im Rahmen des Non Financial Risk-Managements
- Beurteilung von IT- und Informationssicherheits-Risiken im Rahmen des Auslagerungsprozesses
- Umgang mit besonderen Herausforderungen und Risiken bei dem Bezug und der Nutzung von Cloud-Dienstleistungen
- 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.

Die MaRisk und BAIT haben daher die Anforderungen an die Informationssicherheit und das Informationsrisikomanagement schon deutlich erhöht und übernehmen auch die Anforderungen der EBA-Leitlinien zum IKT-/ICT-Risiko in die nationale Aufsichtspraxis.

Zudem kommen mit den neuen DORA-Anforderungen weitreichende zusätzliche Regelungen und Pflichten hinzu.

Die Aufsicht erwartet aufgrund der aktuellen geopolitischen Lage und stark erhöhter Cyber-Risiken zusätzliche (Sicherheits-)Maßnahmen der Institute. Damit einher gehen somit auch die erweiterten Aufgaben und Verantwortlichkeiten des Informationssicherheitsbeauftragten (ISB) und des Informationsrisikomanagements, um Ausfälle des Geschäftsbetriebs zu vermeiden.

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

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

Wissenswertes

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

- IT und Organisation
- Informationssicherheit (ISB) und Informationsrisikomanagement (IRM)
- Notfallmanagement und Business Continuity Management (BCM/ITSCM)
- Interne Revision und IT-Revision
- Datenschutz (DSB) und Data Governance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- IT-Compliance und IT-Governance
- sowie andere interessierte Fach- bzw. Grundsatzbereiche, Geschäftsleiter*innen/ IT-Vorstandsmitglieder, externe Prüferinnen und Prüfer sowie Dienstleister

Unsere Referenten

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

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. Mike Bona-Stecki ist seit über 20 Jahren im Bereich der Informationssicherheit im Bereich des Bundes und im Finanzsektor u. a. als Informationssicherheitsbeauftragter tätig sowie Lehrbeauftragter für den Bereich IT-Sicherheit an der Berufsakademie Rhein-Main. Mike Bona-Stecki veröffentlicht als freier Autor regelmäßig praxisorientierte Beiträge und Fachbücher zu den Themen Informationssicherheit, Business Continuity Management und Outsourcing und ist zudem gefragter Referent in diesen Themengebieten.

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.

IT-Schutzbedarf & Soll-Konzepte aufsichtskonform umsetzen
9. April 2024, Online-Veranstaltung

OpRisk: IT-Risiken im Fokus der Aufsicht
15. April 2024, Online-Veranstaltung

Aufbau eines aufsichtskonformen & revisionssicheren Internen Kontrollsystems (IKS)
18./19. April 2024, Online-Veranstaltung

Berechtigungsmanagement im Fokus der Aufsicht
22. April 2024, Online-Veranstaltung

DORA-Umsetzung im Fokus der Aufsicht
23. April 2024, Online-Veranstaltung

IT-Risiken im Fokus der Aufsicht
29. April 2024, Online-Veranstaltung

IT-Auslagerungen & IT-Notfallmanagement im Fokus der Aufsicht
15./16. Mai 2024, Online-Veranstaltung

Fachtagung IT-Aufsicht
17./18. Juni 2024, Online-Veranstaltung

BAIT Spezial für Compliance & Governance
26. Juni 2024, 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

BAIT Spezial: Informationssicherheit & Informationsrisikomanagement

Name

Vorname

Position

Firma

Straße

PLZ / Ort

Tel./Fax

E-Mail

Name der Assistenz

Datum Unterschrift

An **anmeldung@akademie-heidelberg.de** oder per Fax an: **06221/65033-29**

Termin + Seminarzeiten

Dienstag, 4. Juni 2024
9:30 – 16:30 Uhr
Online-Zugang ab 9:15 Uhr

Seminar-Nr. 24 06 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, 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.

03.24/2406BA011

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 28 · 69123 Heidelberg
Telefon 06221/65033-0 · Fax 06221/65033-69
info@akademie-heidelberg.de
www.akademie-heidelberg.de