

IKT-Governance im Fokus der Aufsicht

DORA-Umsetzung – IKT-Drittdienstleistungen – Schutzbedarf – IAM



Banken-Aufsicht-Seminar · 7 CPE-Punkte

Konkrete Praxis-
Hinweise zur
Stärkung der
IT-Governance!

- Chancen und Herausforderungen für die IT-Governance durch DORA
- Besondere Anforderungen an die IT-Governance bei der Nutzung von Cloud-Anwendungen und IKT-Drittdienstleistern
- Aktuelle IT-Governance-Anforderungen der Aufsicht im Bereich Benutzerberechtigungen (IAM) – Prüfungsschwerpunkte und häufig identifizierte Sicherheitslücken
- IT-Governance-Anforderungen an Schutzbedarfs- und Risiko-Klassifizierungen unter Einbezug von IDV, BCM/ITSCM und externen IKT-Drittdienstleister

20 Jahre
AKADEMIE
HEIDELBERG

Referierende



Dr. Markus Held
Referatsleiter
Bundesamt für Sicherheit in der
Informationstechnik (BSI), Bonn



Tina Hausknecht
On-Site Inspections IT Security
Deutsche Bundesbank
Mainz



Lars Ehrenfeld
Abteilungsleiter Prozess-
management und IT-Governance
Kreissparkasse Heilbronn, Heilbronn

Programm

Dr. Markus Held, BSI · 10:00–12:00 Uhr

Chancen und Herausforderungen für die IT-Governance durch DORA

- IT-Governance: strategische und regulatorische Anforderungen
- Chancen und Herausforderungen für die IT-Governance durch DORA
- Erhöhte Transparenzanforderungen bzgl. IKT-Risiken
- Standardisierung der Prozesse und der IKT zur Förderung einer effizienten IT-Governance
- Stärkung der IKT-Resilienz zur Verbesserung der institutsweiten Informationssicherheit
- Herausforderungen und Chancen durch den »Stand der Technik« als Ziel einer regelungskonformen DORA-Umsetzung (Kosten-/Projektrisiken und Innovationschancen)
- Zunehmende Schwierigkeiten in der IT-Compliance durch wachsende Komplexität in der IT-Landschaft und IT-Infrastruktur
- Die Bedeutung der IT-Governance für die Anpassung an rasche technologische Veränderungen (u.a. KI) und zunehmenden Cyber-Bedrohungen
- Besondere Anforderungen an die Informationssicherheit und die IT-Governance bei Nutzung von Cloud-Anwendungen und IT-Service-Providern

Tina Hausknecht, Bundesbank · 12:45–14:45 Uhr

Aktuelle IT-Governance-Anforderungen der Aufsicht im Bereich Benutzerberechtigungen (IAM) – Prüfungsschwerpunkte und häufig identifizierte Sicherheitslücken

- IT-Governance-Anforderungen an das Rechtemanagement und die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von nicht mehr benötigten Berechtigungen und Benutzer-Identitäten – Besonderheiten bei Zugangs-/Zutrittsrechten und deren Kontrolle

- Laufende Überwachung des Vergabeprozesses – 4-Augen-Prinzip und andere Maßnahmen
- Funktionstrennung: Sicherstellung, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt und auch bei Arbeitsplatzwechseln Interessenkonflikte vermieden werden (AT 4.3.1 MaRisk) sowie angemessene technisch-organisatorische Ausstattung (AT 7.2 MaRisk) als Grundvoraussetzungen für ein funktionierendes und aufsichtskonformes Identitäts- und Rechtemanagement
- Prüfung der Notwendigkeit und Zulässigkeit beantragter Rechte: Organisatorische und technische Sicherstellung der minimalen Rechtevergabe
- Rezertifizierung unter Beteiligung der Fachbereiche – Wer trägt die Verantwortung für den Prozess? Angemessene Turnusse für die Überprüfung von Berechtigungen
- Technisch-organisatorische Maßnahmen zur Vermeidung der Umgehung des Berechtigungsmanagements
- Neuerungen und Änderungen durch DORA im Bereich IAM

Lars Ehrenfeld, KSK Heilbronn · 15:00–17:00 Uhr

IT-Governance-Anforderungen an Schutzbedarfs- und Risiko-Klassifizierungen unter Einbezug von IDV, BCM/ITSCM und externen IKT-Drittdienstleister

- IKT-Assetmanagement: Identifikation und Gruppierung der IKT-Schutzobjekte (Anwendungen, Systeme, Infrastruktur)
- Zuordnung geplanter bzw. nachträglich identifizierter IDV-Anwendungen zu einer Schutzbedarfsklasse
- Schutzbedarfsklassifizierung der Dienstleister – Welche Risiken entstehen dabei und welche Sollmaßnahmen sind einzuleiten?
- Durchführung von Risiko- und Restrisikoanalysen – Welche Konsequenzen sind nach der Ermittlung zu ziehen? – Praxisempfehlungen
- OpRisk-Reporting – Berichte über IT-Risiken unter Einbezug externer IKT-Drittdienstleister

Seminarziel

Die IT-Governance steht vor weitreichenden Herausforderungen, insbesondere durch DORA und die zunehmende IT-Komplexität. Hier sind weitreichende Anpassungen notwendig, um die digitale Resilienz und IT-Compliance sicherzustellen.

Insgesamt ist eine ganzheitliche Betrachtung der IT-Governance unerlässlich. Institute müssen aber nicht nur auf die spezifischen Anforderungen von DORA reagieren, sondern auch ihre gesamte IT-Governance-Strategie auf die aufsichtlichen Anforderungen ausrichten. Hierfür ist ein institutsweit einheitliches Vorgehen u. a. bei der Schutzbedarfs- und Risiko-Klassifizierung unter Berücksichtigung von IDV, BCM/ITSCM und externen IKT-Drittdienstleistern sowie bei der Ausgestaltung des Identitäts- und Rechtemanagements notwendig.

Um erfolgreich auf diese Herausforderungen zu reagieren, ist eine kontinuierliche Überwachung der regulatorischen Entwicklungen, eine flexible Anpassung der IT-Governance-Strategien inkl. der DOR-Strategie und eine enge Zusammenarbeit zwischen der IT und den anderen Fachbereichen unter Einbeziehung des Managements erforderlich.

Nur so kann eine IT-Governance erreicht werden, die nicht nur den regulatorischen Anforderungen entspricht, sondern auch die langfristige Sicherheit und Effizienz der IT-Landschaft gewährleistet.

Wissenswertes

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- IT, IT-Governance, IT-Compliance und IT-Organisation
- Informationssicherheit (ISB) und Informationsrisikomanagement (IRM)
- IT-Notfallmanagement und Business Continuity Management (BCM/ITSCM)
- Interne Revision und IT-Revision, Datenschutz und Data Governance
- (Zentrales) Auslagerungsmanagement und IT-Dienstleistersteuerung
- sowie andere interessierte Fach- und Grundsatzbereiche, Mitglieder der Geschäftsleitung und des (IT-)Vorstands, externe (IT-)Prüfer*innen sowie (IKT-)Dienstleister

Unsere Referierenden



Dr. Markus Held

Referatsleiter

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Dr. Markus Held war 2010 bis 2015 bei der BaFin in der Aufsicht über die IT bei Banken tätig und wechselte anschließend als Referatsleiter zum Bundesamt für Sicherheit in der Informationstechnik. Er befasst sich seit Beginn seines Berufslebens aus verschiedenen Perspektiven mit IT-Regulierung, Informationssicherheit, IT-Infrastrukturen, Cloud Computing und IT-Governance, insbesondere in der Finanzindustrie und in der Bundesverwaltung. Er erwarb 2006 sein Diplom in Informatik an der Eberhard Karls Universität in Tübingen, wo er dann 2010 zum Dr. rer. nat. promoviert wurde.



Tina Hausknecht

On-Site Inspections IT Security

Deutsche Bundesbank, Mainz

Tina Hausknecht ist seit 2002 bei der Bundesbank tätig. Sie war mehrere Jahre im IT-Projektmanagement im Bereich bankenaufsichtliches Meldewesen tätig, bevor sie in den Bereich bankgeschäftliche Prüfungen wechselte. Als Prüfungsleiterin und Teamleiterin ist sie spezialisiert auf die Themengebiete Informationsrisiko- und Informationssicherheitsmanagement, Identitäts- und Rechtemanagement sowie Interne (IT-)Revision.



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

Überprüfung der DORA-Konformität von (IKT-)Dienstleistern & Cloud Service Providern
21. Januar 2025, Online-Veranstaltung

Cyber-Risiken – aktuelle Sicherheitslücken und direkt wirksame (Gegen-)Maßnahmen
22. Januar 2025, Online-Veranstaltung

DORA Spezial:
Informationssicherheit & IKT-Risikomanagement
23. Januar 2025, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM
29. Januar 2025, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement
5./6. Februar 2025, Online-Veranstaltung

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

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

IKT-Governance im Fokus der Aufsicht

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, 18. Februar 2025
10:00 – 17:00 Uhr
Online-Zugang ab 9:45 Uhr
Seminar-Nr. 25 02 BA148 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 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 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