

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



Banken-Praxis-Seminar · 4,5 CPE-Punkte

Mobiles Arbeiten:
- Aufsichtskonform
- Datenschutzkonform
- Revisionsicher

- Mobiles Arbeiten im Spannungsfeld zwischen Regulatorik & Praxis
- Aktuelle Anforderungen an das mobile Arbeiten und Einbezug von «Mobile-Work-Risiken» in das (IKT-)Risikomanagement
- Datenschutz und die IT-Sicherheit bei mobilem Arbeiten und Home-Office – insb. bei Nutzung von Clouds und »Familien-Netzwerken«
- Mitarbeiter-Awareness für Ransomware und Cyber-Attacks
- Prüfung & Beurteilung der Risiken aus dem mobilen Arbeiten und Revisions-Prüfungen «aus dem Home-Office» (Remote-Prüfungen)

20 Jahre
AKADEMIE
HEIDELBERG.

Referenten

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

Jürgen Krug
IT-Revisor und
stv. Leiter Zentralrevision
Frankfurter Sparkasse

Programm

Mike Bona-Stecki, DekaBank · 12:30–14:30 Uhr

Aktuelle DORA-Anforderungen an das mobile Arbeiten und Einbezug von »Mobile-Work-Risiken« in das IKT-Risikomanagement

- IKT-Governance, Informationssicherheit und Informationsrisikomanagement im Spannungsfeld zwischen Regulatorik (u. a. DORA) und Praxis
- IKT-, Digitalisierungs- und Cyber-Risiken als expliziter Aufsichts-Schwerpunkt
- Begriffsdefinition und Abgrenzung: Mobiles Arbeiten vs. Home Office – Abgrenzung gesetzlicher und aufsichtlicher Anforderungen und unterschiedlicher Teil-Risiken
- Sicheres mobiles Arbeiten in der Praxis – (IKT-)Risiken und (IKT-)Schwachstellen
- Fallstricke bei Cloud-Anwendungen im Zusammenhang mit mobilem Arbeiten, Maßnahmen zum sicheren Einsatz von Kollaborationsplattformen
- Risiken beim Einsatz privater Devices, aktuelle Entwicklung im Bereich der Aufsichtsbehörden
- Identifikation und Bewertung von »Mobile Work-Risiken« im Rahmen des Informationsrisikomanagements – inwieweit sind die (dezentralen) Risiken des mobilen Arbeitens (zentral) steuerbar?
- Auswirkungen von »Mobile-Work« auf die Kontinuitätsanforderungen von Geschäftsprozessen – Sicherstellung eines angemessenen Umgangs mit Kontinuitätsrisiken!
- Risiken von Cyberangriffen in der Home-Office-Umgebung und Sicherstellung der Mitarbeiter-Awareness für IT-Sicherheitsvorfälle, SIEM, SOC und Cyber-Risiken
- Was tun bei einem Incident im Home-Office?
- Cyber-Resilienz – Maßnahmen zur Erkennung und Steuerung von Cyber-Angriffen im Rahmen von New Work und Home Office!

Jürgen Krug, Frankfurter Sparkasse · 14:45–16:30 Uhr

Aktuelle MaRisk-/DORA-Anforderungen an den Datenschutz und die IT-Sicherheit bei mobilem Arbeiten und Home-Office bzw. Remote-Prüfungen – insb. bei Cloud-Nutzung

- Erweiterte DORA-Anforderungen an mobiles Arbeiten und Datenschutz im Home Office und bei Remote-Prüfungen
- Revisions-sichere Überwachungs- und Schutzmaßnahmen – insb. bei Cloud-Nutzung
- Erweiterter Aufgabenbereich des Datenschutzbeauftragten (DSB)/IT-Sicherheitsbeauftragten (ISB) im Rahmen der Schutzbedarfsanalysen (SBA)
- Identifikation und Analyse von Risiken bei Fernzugriffen, Cloud- und Portalanwendungen (u. a. BYOD) – Besondere Anforderungen an die technisch-organisatorische Ausstattung (AT 4.3.1)
- Sicheres mobiles Arbeiten in der Praxis – Anwendung von Standards (BSI-Anforderungskatalog Cloud Computing, ISO/IEC 27017)
- Besondere Kontroll- und Prüfungsschwerpunkte für IT-Organisation und IT-Revision
- Umgang mit unterschätzten Gefahren (z. B. »Familienzugriff«, Benutzerberechtigung, Passwortvergabe, Social Engineering, Social-Media-Zugriffe) und Umgang mit neue IT-Risiken – Handlungsempfehlungen

Prüfung und Beurteilung der Mobile-Work-Risiken und Revisions-(Remote-)Prüfungen »aus dem Home-Office«

- Prüffelder der Revision i.Z.m. mobilem Arbeiten – wo liegen die Risiken und Prüfungsschwerpunkte?
- Anhand welcher Daten kann die Revision die Risiken einschätzen und prüfen?
- Überprüfung der notwendigen (laufenden) Prozess-Kontrollen der IT-Organisation und des ISB
- Durchführung risikogerechter und prüfungssicherer Remote-Prüfungen durch die Interne Revision
- Prüfung und Beurteilung von Cyber-Risiken

Seminarziel

Mobiles Arbeiten hat sich in den Arbeitsmodellen etabliert. Doch mittlerweile sind zunehmende Bedrohungen durch IKT-Risiken, Cyber-Angriffen und Lücken in der Informationssicherheit durch das mobile Arbeiten erkennbar.

Die neuen DORA-Vorgaben stellen daher weitreichende Anforderungen an die Resilienz von Mobile-Work-Konzepten. Die (Über-)Prüfbarkeit der Tätigkeiten im Home-Office und aus dem Home-Office stellt aber insbesondere die Bereiche Revision, IT/Orga und IKT-Risikomanagement vor neue und schwer steuerbare Herausforderungen.

Die Nutzung offener Familiennetzwerke oder das Versenden vertraulicher Informationen über unverschlüsselte Leitungen ist nicht nur datenschutzrechtlich ein Problem. Durch Cyber-Angriffe und Maleware kann der mobile Arbeitsplatz schnell zu einer Sicherheitslücke und Einfallstor werden und dadurch zum Risiko für das gesamte Haus werden. Ausfälle kritischer Geschäftsprozesse bei Banken, Versicherungen und Unternehmen sind dann die Folge. Die Bedrohung durch die aktuelle geopolitische Lage könnte diese Risiken noch deutlich verschärfen.

Hier gelten besondere Anforderungen an die technisch-organisatorische Ausstattung (AT 4.3.1 MaRisk). Dies gilt auch für Remote-Prüfungen der Internen Revision und den Zugriff auf (vertrauliche) Unternehmensdaten.

Wissenswertes

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der folgenden Bereiche:

- IT und Organisation, Informationssicherheit (ISB) und Informationsrisikomanagement
- Notfallmanagement und Business Continuity Management (BCM)
- Interne Revision und IT-Revision
- Compliance, Datenschutz und Data Governance
- sowie andere interessierte Fach- bzw. Grundsatzbereiche, Mitglieder des Vorstands und der Geschäftsleitung, externe Prüfer*innen sowie Bankdienstleister

Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu spezifischen Aufsichtsanforderungen an das mobile Arbeiten und die Durchführung von Remote-Prüfungen
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut
- Sie erhalten wertvolle Praxistipps im Erfahrungsaustausch mit den Referenten
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit anderen Praktiker*innen

Unsere Referenten

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 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.

Jürgen Krug

IT-Revisor und stv. Leiter Zentralrevision
Frankfurter Sparkasse

Jürgen Krug ist studierter Informatiker und besitzt über 20 Jahre Erfahrung als IT-Revisor in der Zentralrevision der Frankfurter Sparkasse. Zu seinen Schwerpunkten gehören u. a. die Prüfung von Schnittstellen zum IT-Bereich und den IT-Dienstleistern sowie die Prüfung von Software unter Wesentlichkeitsgesichtspunkten und die Prüfung von Weiterverlagerungen im Bereich der IT-Dienstleistungen und Cloud-Service-Provider.

Seminar-Vorschläge

Nutzung von KI & ChatGPT (Modulreihe)
Ab 22. 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

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

Cloud-Nutzung:
Aufsichts-Anforderungen & Praxis-Umsetzung
24. Februar 2025, Online-Veranstaltung

DORA Spezial für Versicherungen
26. Februar 2025, Online-Veranstaltung

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

IKT-Infrastruktur & IT-Betrieb im Fokus der Aufsicht
13. 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

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

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, 18. Februar 2025
12:30 – 16:30 Uhr
Online-Zugang ab 12:15 Uhr
Seminar-Nr. 25 02 BA046 W

Teilnahmegebühr

€ 390,- (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 · Fax 06221/65033-69
info@akademie-heidelberg.de
www.akademie-heidelberg.de