10. März 2025 · 10:00–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

Eigen-Anwendungen & IDV im Fokus der Aufsicht

Erweiterte Anforderungen aus aktuellen IT-Prüfungen – Testpflicht!

Banken-Aufsicht-Seminar · 7 CPE-Punkte

Ansätze zur Verankerung einer IDV-Richtlinie in den Arbeits-anweisungen!

20 Jahre AKADEMIE HEIDELBERG

- **Konkrete Erwartungen der Aufsicht an die Nutzung von Eigen-Anwendungen und IDV-Anwendungen – Neuerungen durch DORA**
- **Anforderungen an das IDV-Register und Umsetzung von IDV-Richtlinien in Arbeitsanweisungen, Risikoanalysen und Schutzbedarfseinstufungen**
- **3-Lines Modell im Kontext von IDV und Rolle des ISB**
- **Entwicklung, Testen und Produktivnahme für neue/veränderte IDV**
- **Prüfung von IDV-Anwendungen – Besonderheiten bei KI-Anwendungen (z. B. ChatGPT)**
- **Häufige Feststellungen und identifizierte Schwachstellen in der Praxis**

Referierende

Alexander Rothländer
Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank
Frankfurt/Main

Stephan Wirth
Informationssicherheits- und
Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Natalie Rosenbach
Abteilungsleiterin/Direktorin
Interne IT-Revision
KfW, Frankfurt

Eigen-Anwendungen & IDV im Fokus der Aufsicht

Programm

Alexander Rothländer, Bundesbank · 10:00–12:15 Uhr

Konkrete Erwartungen der Aufsicht an die Nutzung von Excel-Anwendungen und IDV – DORA-Anforderungen an das Software-Register und Umsetzung von IDV-Richtlinien – Ausgestaltung der Entwicklungsprozesse

- Anforderungen aus DORA an die Nutzung von IDV
- Konkretisierung der Anforderungen für Anwendungsentwicklung und Freigabeverfahren
- Zur Geschäftsstrategie konsistente IT-Strategie: Management der im IT-Betrieb und Fachbereich selbst betriebenen/entwickelten Hardware- und Software
- Anforderungen an die Schutzbedarfsfeststellung und ggf. Restrisiko-Analysen von (fremden) IDV-Anwendungen
- IDV im Kontext der Nutzung von KI-Systemen – Hinweise zur Anwendung und Klassifizierung
- Notwendigkeit eines zentralen IDV-Registers, sowie technisch-organisatorische Ansätze zur Bestandserhebung
- Anwendung des IDV-Registers als Steuerungsinstrument im IT-Betrieb und im Falle von BMAs im Fachbereich
- Etablierung eines regulatorisch angemessenen Entwicklungsprozesses für IDV (Fachliche Anforderungen, Entwicklung, Testmanagement, IT-Betrieb und Wartung, Dokumentation, IDV-Richtlinien, DevOps Ansatz)
- Praxisbericht: Identifizierte Schwachstellen und häufige Feststellungen aus aktuellen Prüfungen

Stephan Wirth, NRW.BANK · 13:00–15:00 Uhr

Rolle des Informationssicherheitsbeauftragten (ISB) und des Datenschutzbeauftragten (DSB) im Umgang mit Excel und IDV – Häufige Feststellungen und identifizierte Schwachstellen in der Praxis

- Vorgehensweise bei der Entwicklung von datenschutzkonformen und prüfungssicheren Konzepten für die Nutzung von Excel-Anwendungen und IDV
- Individuelle Datenverarbeitung (IDV) mit angemessenen Prozessen unter Berücksichtigung der Schutzbedarfsfeststellung und der Risikobewertung
- Dokumentation von IDV-Anwendungen in Zusammenarbeit mit den Fachabteilungen und mit Bezug zum Verzeichnis der Verarbeitungstätigkeiten – Identifizierung von nicht autorisierten »Schatten-Anwendungen«
- Anforderungen an die Datenerfassung im Software-Register (Name und Zweck der Anwendung, Versionierung, Fremd- oder Eigenentwicklung, Fachverantwortung und technische Verantwortlichkeiten, Risikoklassifizierung und Schutzbedarfseinstufung)
- Praxisbericht: Änderungen für den DSB aus neuen DORA-Vorgaben mit Bezug Excel-Anwendungen und IDV
- ChatGPT als neue Herausforderung

Natalie Rosenbach, KfW · 15:15–17:00 Uhr

Prüfung von IT-Applikationen, IDV-Eigenanwendungen und Software-Auslagerungen

- Prüfung IT-Governance und der IT-Prozesse/-Applikationen – Inwieweit existiert angemessene Personalausstattung/Fachkenntnis für das Management von Informationsrisiken/-sicherheit, IT-Betrieb und Anwendungsentwicklung?
- Beurteilung des Risikomanagements für IDV-Anwendungen und Schutzbedarfsklassifizierung – häufige Schwachstellen und Mängel bei der Risikoanalyse
- Überprüfung der Versionierung der Programmdateien
- Prüfung durchgeführter Qualitätssicherungsmaßnahmen
- Bedeutung und Funktion der Kommunikation zwischen den Fachbereichen und der IT
- Excel- und IDV-Prüfung durch die (IT-)Revision: häufige Feststellungen – Vorgehensweise – Praxistipps
- Prüfung der angemessenen Überführung der Restrisiken in den OpRisk-Management-Prozess – Revisionsberichterstattung über (veränderte) IT-Risikolage
- Besondere Anforderungen an die Nutzung von Excel-Anwendungen und IDV durch die Interne Revision selbst
- Auslagerung und Fremdbezüge von Software(-Dienstleistungen) – Erweiterte Pflichten und Prüfungserfordernisse – Prüfpflichten des IT-Dienstleisters

Seminarziel

Zunehmend wesentliche Feststellungen bei Aufsichts-Prüfungen haben dazu geführt, dass verschärfte Anforderungen an Excel-Anwendungen und IDV in die Aufsicht über Institute, Versicherungen, Kryptoverwahrer und Rechenzentren Einzug erhalten haben. Hinzu kommen weitere Anforderungen durch DORA.

Excel, IDV und »Schatten-IT« sind aber ein fester Bestandteil in nahezu allen Prozessen geworden. Ob selbst programmiert oder extern eingekauft, zunehmend werden IDV-Anwendungen in den Fachabteilungen implementiert und teilweise selbst administriert, deren Nutzung im Laufe der Zeit selbstverständlich und komplexer wird. Dies führt oft zu (operationellen) Risiken, die aber mangels Erfassung nicht im Risikomanagement abgebildet und gesteuert werden können!
KI-Anwendungen (z. B. ChatGPT) sind vor dem Hintergrund von IT-Auslagerungen ebenfalls zu beurteilen!

Hier gilt es, aufsichtskonforme IDV-Richtlinien zu erstellen und prüfungssicher in den Arbeitsanweisungen zu implementieren. Alle bestehenden und genutzten IDV- und Excel-Anwendungen im Institut müssen identifiziert, getestet und genehmigt werden vor der weiteren Verwendung. Risikoanalyse und Schutzbedarfsklassifizierung sind sauber aufzusetzen und zu dokumentieren.

Wissenswertes

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

- Interne Revision und IT-Revision
- Risikomanagement und IT-Risikomanagement, Risikocontrolling und OpRisk-Management
- IT-Organisation, Informationssicherheit (ISB) und Informationsrisikomanagement
- Datenschutz (DSB) und Data Governance
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- IT-Compliance und IT-Governance, IT-Grundsatz und Regulatorik
- sowie andere interessierte Fachbereiche bzw. Vorstandsmitglieder/ Geschäftsleitung, externe Prüferinnen und Prüfer sowie Bankdienstleister

Unsere Referierenden

Alexander Rothländer
Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank, Frankfurt/Main

Alexander Rothländer arbeitet als Bankgeschäftlicher Prüfer 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-Anwend. gesammelt.

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.

Natalie Rosenbach
Abteilungsleiterin/Direktorin Interne IT-Revision
KfW, Frankfurt

Natalie Rosenbach ist Abteilungsleiterin der Internen Revision bei der KfW in Frankfurt. In dieser Position ist sie für die Revisionsprüfungen der IT-Prozesse, IT-Applikationslandschaft, IT-Betrieb und IT-Infrastruktur sowie der IT/IS-Sicherheitsvorgaben zuständig. Vor ihrer Tätigkeit bei der KfW sammelte sie fundierte Erfahrungen in verschiedenen Revisions-Bereichen und in der Informationssicherheit als 2LoD einer Großbank sowie als Software-Entwicklerin (1LoD) in einer Versicherungsgruppe.

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

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken
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

Eigen-Anwendungen & IDV 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

Montag, 10. März 2025
10:00 – 17:00 Uhr
Online-Zugang ab 9:45 Uhr

Seminar-Nr. 25 03 BA055 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.

12.24 / 25 03 BA055

AKADEMIE HEIDELBERG

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