10. Dezember 2024 · 9:30 –17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

IKT Spezial: Identity & Access Management

Vergabeprozesse und Rezertifizierung als häufige Feststellungs-Quelle

Banken-Aufsicht-Seminar · 7,5 CPE-Punkte

Vermeidung von Sicherheitslücken im IAM!

- **Aktuelle regulatorische Vorgaben zur Identitäts-/Rechtevergabe und Rezertifizierung**
- **Häufig identifizierte Schwachstellen in der Praxis**
- **Funktionsbezogene Vergabe von Benutzerberechtigungen nach den Prinzipien der Rechtevergabe (Need-to-know, Least-Privilege, Segretation-of-Duties)**
- **Sichere Vorgehensweise bei der Vergabe, Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten**

20 Jahre AKADEMIE HEIDELBERG

Referierende

Tina Hausknecht
On-Site Inspections IT Security
Deutsche Bundesbank
Mainz

Stephan Wirth
Informationssicherheits- und Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Markus Duda
Geschäftsführer
ReDworks GmbH
Berlin

Programm

Tina Hausknecht, Bundesbank · 9:30 –11:30 Uhr

Aktuelle aufsichtliche Anforderungen zur Steuerung von Benutzerberechtigungen – Prüfungsschwerpunkte und häufig identifizierte Sicherheitslücken

- Anforderungen an das Rollenmodell und die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von nicht mehr benötigten Berechtigungen und Benutzer-Identitäten – Besonderheiten bei Informationsverbünden, Zugangs-/Zutrittsrechten und deren Kontrolle
- Laufende Überwachung des Vergabeprozesses: 4-Augen-Prinzip und weitere Maßnahmen
- Funktionstrennung: Ausführung miteinander unvereinbarer Tätigkeiten durch unterschiedliche Mitarbeiter; Vermeidung von Interessenkonflikten bei Arbeitsplatzwechseln (AT 4.3.1 MaRisk), angemessene technisch-organisatorische Ausstattung (AT 7.2 MaRisk) als Grundvoraussetzungen für ein funktionierendes und aufsichtskonformes IAM
- Überwachung privilegierter Benutzer, insb. Administratoren – Anforderungen an Protokollierung und Überwach.
- 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 Berechtigungsmanagement
- Ausblick: Neuerungen und Änderungen durch DORA

Stephan Wirth, NRW.BANK · 11:45 –14:45 Uhr inkl. Mittagspause

Funktionsbezogene Vergabe von Benutzerberechtigungen und Zugriffsrechten/Zutrittsrechten nach dem Prinzip der minimalen Rechtevergabe (Need-to-know-Prinzip)

- Sicherstellung der Vergabe von Berechtigungen an Benutzer nach dem Prinzip der minimalen Rechtevergabe: Klare Unterscheidung in personalisierte, nicht personalisierte und technische Benutzer und die Funktionstrennung im Rechtekonzept (BAIT Tz. 6.2 und 6.3)
- Praxisanforderungen an den Vergabeprozess und die anlassbezogene Aktualisierung des Berechtigungsmanagementkonzeptes unter Wahrung von 4-Augen-Prinzip und Funktionstrennung
- Prüfung der Notwendigkeit/Zulässigkeit beantragter Rechte
- Zentralisierte Lösungen insbes. für Kernbankensysteme und wesentliche Teile des Informationsverbunds unerlässlich, vor allem bei größeren Instituten
- Genehmigungs- und Kontrollprozesse
- Analyse der Ausgangslage – Vermeidung der Anträge auf »Zuruf« – Schaffung einer einheitlichen Sicht der Funktionen
- Überprüfung eingeräumter Berechtigungen: Vermeidung von Risiken durch regelmäßige Rezertifizierungen
- Datenschutzaspekte bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten
- Identitäts- und Rechtemanagement als Grundlage zur Erfüllung der Anforderungen aus DORA

Markus Duda, ReDworks · 15:00 –17:00 Uhr

Sichere Vorgehensweise bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten – Aktuelle Praxis-Erfahrungen

- Integration mehrerer IT-Systeme in eine zentrale Benutzerverwaltung – Voraussetzungen für eine erfolgreiche Implementierung
- Wichtige Aspekte aus der Umsetzungspraxis – Umgang mit interner Kommunikation, notwendigem Fachwissen und Verfügbarkeit von Ressourcen
- Rezertifizierung unter Beteiligung der Fachbereiche – Wer trägt die Verantwortung für den Prozess?
- Elektronische Benutzerverwaltung und aufsichtsrechtliche Anforderungen: Prüfungssichere Dokumentation von Zugriffsrechten und Rezertifizierungsprozessen
- Rechte privilegierter Nutzer: Vergabe, (Echtzeit-)Überwachung, Protokollierung (Kontrolle) und Auswertung
- Handlungsempfehlungen für die Zusammenarbeit mit externen IT-Dienstleistern (insb. Neuerungen durch DORA)

Seminarziel

Aktuelle Aufsichts-Prüfungen haben zu (teilweise) schwerwiegenden Feststellungen im Bereich des Berechtigungsmanagements (u. a. Rechtevergabe, Rezertifizierung) geführt. Lücken in der Informationssicherheit, die auf ein nicht aufsichtskonformes Berechtigungsmanagement zurückzuführen sind, führen zunehmend häufiger zu Ausfällen kritischer Geschäftsprozesse bei Banken und Dienstleistern. Die Aufsicht hat die zentrale Bedeutung des Rechtemanagements daher noch einmal klar herausgestellt. Die neuen DORA-Vorgaben verschärfen zudem die Anforderungen an die digitale Resilienz.

Der Zugriff auf sensible Bankdaten und -prozesse soll nur durch die Personen erfolgen, die diesen Zugriff auch wirklich benötigen (»Need-to-know«-Prinzip). Aber wie kann der Rechtevergabe-Prozess institutsspezifisch definiert bzw. dokumentiert werden? In der Praxis stimmen eingerichtete Rechte oftmals nicht mit dem Rechtevergabekonzept und der IT-Strategie überein.

Das Institut hat daher nach Maßgabe der Soll-Anforderungen und des Schutzbedarfs entsprechende Prozesse zur Protokollierung und Überwachung einzurichten.
Aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Institut insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten angemessene Prozesse zur Protokollierung und Überwachung einzurichten.

Wissenswertes

Zielgruppe

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

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

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

Unsere Referierenden

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.

Stephan Wirth
Informationssicherheits- und Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Seit über zwanzig 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.

Markus Duda
Geschäftsführer
ReDworks GmbH, Berlin

Markus Duda ist Projektleiter und Spezialist für Identity- and Access-Management mit langjähriger Erfahrung im Banken- und IT-Umfeld. Er begleitet Finanzinstitute ganzheitlich von der Analyse aufsichtsrechtlicher Forderungen sowie der Strukturierung von Prüfungsergebnissen über die Konzeption eines IAM-Zielbildes bis zu deren Umsetzung. Dazu gehören die Entwicklung von übergreifenden Konzepten (z. B. für die Funktionstrennung oder für ein rollenbasiertes IAM), aber auch die Toolauswahl und Einführung eines zentralen IAM-Tools.

Seminar-Vorschläge

Aufbau-Seminar I – Nutzung von KI & ChatGPT
4. November 2024, Online-Veranstaltung

Risikoanalyse von Auslagerungen und IKT-Drittdienstleistern
11. November 2024, Online-Veranstaltung

Abgrenzung Auslagerung/sonst. Fremdbezug/
IKT-Drittdienstleistung nach MaRisk und DORA
12. November 2024, Online-Veranstaltung

IKT Spezial für Compliance & Governance
14. November 2024, Online-Veranstaltung

Fachtag IKT-Aufsicht
18. November 2024, Online-Veranstaltung

IKT-Risikomanagement KOMPAKT
19./20. November 2024, Online-Veranstaltung

Praxis-Umsetzung neuer DORA-Anforderungen
an die IT- & Cyber-Sicherheit
26. November 2024, Online-Veranstaltung

DORA-Umsetzung im Fokus der Aufsicht
2. Dezember 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

IKT Spezial: Identity & Access Management

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, 10. Dezember 2024
9:30 – 17:00 Uhr
Online-Zugang ab 9:15 Uhr

Seminar-Nr. 24 12 BA139 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.

10.24 / 24 12 BA139

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