

Berechtigungsmanagement im Fokus der Aufsicht



Banken-Aufsicht-Seminar · 6 CPE-Punkte

Vergabeprozess und
Rezertifizierung als
häufige Quelle von
Prüfungs-Feststellungen

- Aktuelle regulatorische Vorgaben (u. a. DORA!) zur Identitäts-/ Rechtevergabe (IAM/SOD) und Rezertifizierung
- Verantwortung im Spannungsfeld zw. IT- und Fachbereichen
- Prüfungsschwerpunkte und häufig identifizierte Schwachstellen
- Funktionsbezogene und kompetenzgerechte Berechtigungsvergabe – Besonderheiten bei privilegierten Nutzern
- Sichere Vorgehensweise bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten

20 Jahre
AKADEMIE
HEIDELBERG.

Referenten



Dr. Thomas Klühspies
Prüfungsleiter
Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank, München



Stephan Wirth
Informationssicherheits- und
Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Programm

Dr. Thomas Klühspies, Bundesbank · 9:00–11:00 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 Informationsverbänden, Zugangs-/Zutrittsrechten und deren Kontrolle
- 4-Augen-Prinzip und Funktionstrennung – Laufende Überwachung des Vergabeprozesses (z. B. Alarmmeldungen) und anlassbezogene Aktualisierung des Berechtigungsmanagementkonzeptes
- 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
- Überwachung privilegierter Benutzer (User), insb. Systemadministratoren – Anforderungen an Logging, Protokollierung und Protokollauswertung
- 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
- Soll/Soll und Soll/Ist-Abgleiche – Häufige Schwachstellen aufgrund mangelnder Schutzbedarfsanalyse
- Technisch-organisatorische Maßnahmen zur Vermeidung der Umgehung von Berechtigungskonzepten
- Auswirkungen von DORA auf das Identitäts- und Rechtemanagement – auch für externe IT-Dienstleister – insb. neue Rezertifizierung von Firewall-Regeln
- Aufsichtliche Abgrenzung der Prinzipien »Need-to-know«, »Need-to-have« und »Need-to-use« (neu gem. DORA!)

Stephan Wirth, NRW.BANK · 11:15–15:00 Uhr inkl. Mittagspause

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

- Identitäts- und Rechtemanagement als Grundlage zur Erfüllung der Anforderungen aus DORA
- Sicherstellung der Vergabe von Berechtigungen an Benutzer nach dem Prinzip der minimalen Rechtevergabe
- Integration mehrerer IT-Systeme – Voraussetzungen für die Implementierung einer zentralen Benutzerverwaltung
- Praxisanforderungen an den Vergabeprozess und die anlassbezogene Aktualisierung der Berechtigungskonzepte
- Notwendigkeits-/Zulässigkeits-Prüfung beantragter Rechte
- Zentralisierte Lösungen insbes. für Kernbankensysteme und wesentliche Teile des Informationsverbunds
- Sicherstellung der Genehmigungs- und Kontrollprozesse
- Vermeidung der Anträge auf »Zuruf« – Schaffung einer unternehmensweiten Sicht der Funktionen
- Herausforderungen in Cloud- und KI-Umgebungen

Sichere Vorgehensweise bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten

- Notwendigkeit der regelmäßigen Rezertifizierung in IAM
- Integration mehrerer IT-Systeme – Voraussetzungen für die Implementierung einer zentralen Benutzerverwaltung
- 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
- Beachtung von Datenschutzaspekten bei der Überprüfung, Rezertifizierung und Dokumentation von Berechtigungen
- Handlungsempfehlungen für die Zusammenarbeit mit externen IT-Dienstleistern (insb. Neuerungen durch DORA)

Seminarziel

DORA stellt hohe Anforderungen an digitale Sicherheitsaspekte in Banken. Aktuelle Prüfungen der Aufsicht haben zu (teilweise) schwerwiegenden Feststellungen im Bereich des Berechtigungsmanagements/IAM (u. a. Rechtevergabe, Rezertifizierung) geführt. IT-Risiken, Cyber-Angriffe und Lücken in der Informationssicherheit, die auf ein nicht aufsichtskonformes Berechtigungsmanagement zurückzuführen sind, führen zunehmend häufiger zu Ausfällen kritischer Geschäftsprozesse bei Banken und Unternehmen. Die neuen DORA-Vorgaben verschärfen die IAM-Anforderungen zur Sicherstellung der digitalen Resilienz noch.

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 Rechtevergabe-konzept und der IT-Strategie überein. Die Aufsicht fordert daher explizit eine risikoorientierte regelmäßige Überprüfung kritischer IT-Berechtigungen.

Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung und Überwachung einzurichten, die sicherstellen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden, insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten.

Wissenswertes

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- IT und Organisation sowie Interne Revision und IT-Revision
- Informationssicherheit (ISB), Informationsrisikomanagement, Datenschutz (DSB) und IKT-Kontrollfunktion gem. DORA
- Notfallmanagement und Business Continuity Management (BCM)
- (Zentrales) Auslagerungsmanagement und IKT-Dienstleistersteuerung
- Compliance und Regulatorik

sowie andere interessierte Fach- bzw. Grundsatzbereiche, IT-Vorstandsmitglieder, Geschäftsleitung, externe Prüferinnen und Prüfer sowie Bankdienstleister.

Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu spezifischen Aufsichtsanforderungen an das IAM zu den Themen Rechtevergabe, Identitäten und Rezertifizierung
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut
- Sie klären offene Fragen für Ihren Bereich mit den erfahrenen Referenten
- Sie erhalten wertvolle Praxistipps im Erfahrungsaustausch mit anderen Praktiker*innen

Unsere Referenten



Dr. Thomas Klühspies

Prüfungsleiter Bankgeschäftliche IT-Prüfungen
Deutsche Bundesbank, München

Herr Dr. Klühspies ist seit 12 Jahren im Bereich der Bankgeschäftlichen IT-Prüfungen der Bankenaufsicht tätig, davon zwei Jahre als Data Analysis Officer bei der Europäischen Bankenaufsicht (EBA). Bei der Bundesbank führt er als Prüfungsleiter IT-Prüfungen bei Banken und Finanzdienstleistern unterschiedlicher Größe durch.



Stephan Wirth

Informationssicherheits- und Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Stephan Wirth ist seit über zwanzig Jahren 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.

Seminar-Vorschläge

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA
13. März 2025, Online-Veranstaltung

Prüfung DORA & DORA-Umsetzung
17./18. März 2025, Online-Veranstaltung

KI-Governance: Einsatz Künstlicher Intelligenz (KI) &
Anforderungen des AI Act
25. März 2025, Online-Veranstaltung

Aufbau eines aufsichtskonformen und reversionssicheren IKS
27./28. März 2025, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-Konform umsetzen
1. April 2025, Online-Veranstaltung

Auslagerungen & IKT-Dienstleistungen im Fokus
von Aufsicht, MaRisk & DORA
2. April 2025, Online-Veranstaltung

Fachtagung IKT-Aufsicht
27./28. Mai 2025, Online-Veranstaltung

DORA Spezial:
Informationssicherheit und IKT-Risikomanagement
3. Juni 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

Berechtigungsmanagement 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, 5. Mai 2025
9:00–15:00 Uhr
Online-Zugang ab 8:45 Uhr
Seminar-Nr. 25 05 BA053 W

Teilnahmegebühr

€ 690,- (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.



02.25 / 25 05 BA053

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