

IKT Spezial: Identity & Access Management (IAM)

Berechtigungsvergabe und Rezertifizierung als häufige Fehler-Quelle



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

- 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, Segregation-of-Duties) – NEU nach DORA: »Need-to-use« Prinzip
- Sichere Vorgehensweise bei der Vergabe, Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten

Referierende



Tina Hausknecht
On-Site Inspections IT Security
Deutsche Bundesbank
Mainz



Stephan Wirth
Informationssicherheits- und
Datenschutzbeauftragter
NRW.BANK, Düsseldorf



Markus Duda
Geschäftsführer
IAM-Experte
ReDworks, Berlin

Programm

Tina Hausknecht, Bundesbank · 9:00 –11:00 Uhr

Aktuelle Anforderungen an die Steuerung von Benutzerberechtigungen – Schwerpunkte und häufig identifizierte Sicherheitslücken in der Praxis

- Anforderungen an Identitätsmanagement und Zugangskontrolle nach DORA und den ergänzenden RTS RMF
- Rollenmodelle, Berechtigungsvergabe und -entzug sowie Least-Privilege-, Need-to-know- und Need-to-Use-Prinzip
- Funktionstrennung und Vermeidung von Interessenkonflikten
- Regelmäßige Überprüfung und Rezertifizierung von Berechtigungen sowie Verantwortlichkeiten der Fachbereiche
- Umgang mit privilegierten Berechtigungen und Administrator-Accounts einschließlich Protokollierung und Überwachung
- Technische und organisatorische Maßnahmen (ToMs) zur Vermeidung unberechtigter Zugriffe und zur Umgehung des Berechtigungsmanagements
- Besonderheiten bei physischen und logischen Zugangsrechten sowie bei kritischen ICT-Systemen

Stephan Wirth, NRW.BANK · 11:15 –14:15 Uhr · inkl. Mittagspause

Funktionsbezogene Vergabe von Benutzerberechtigungen und Zugriffsrechten/Zutrittsrechten nach den Prinzipien einer sinnvollen und aufsichtskonformen Rechtevergabe

- Identitäts- und Rechtemanagement als Grundlage zur Erfüllung der Anforderungen aus MaRisk und DORA
- Analyse der Ausgangslage – Vermeidung der Anträge auf »Zuruf« – einheitlicher Sicht und Rolle der Funktionen
- Sicherstellung der Vergabe von Berechtigungen an Benutzer nach dem Prinzip der minimalen Rechtevergabe
- Klare Unterscheidung in personalisierte, nichtpersonalisierte und technische Benutzer und die Funktionstrennung im Rechtekonzept
- Praxisanforderungen an den Vergabeprozess

- Anlassbezogene Aktualisierung des Berechtigungskonzeptes unter Wahrung der Funktionstrennung
- Genehmigungs- und Kontrollprozesse im Rahmen des Identity Lifecycle Management
- Häufige Schwachstelle: Ungenügende Kontrolle der Umsetzung in den IT-Systemen und fehlende Einbindung der fachlich verantwortlichen Unternehmensbereiche
- Überprüfung eingeräumter Berechtigungen: Vermeidung von Risiken durch regelmäßige Rezertifizierungen
- Zentralisierte Lösungen insbesondere für Kernbankensysteme und wesentliche Teile des Informationsverbunds unerlässlich, vor allem bei größeren Instituten
- Datenschutzaspekte bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten
- Herausforderungen in Cloud- und KI-Umgebungen

Markus Duda, ReDworks · 14:30 –16:30 Uhr

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

- 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 (Process-Owner)?
- 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 IKT-Dienstleistern (insbesondere hinsichtlich der Neuerungen durch DORA)

Seminarziel

Überprüfungen des IAM führen nicht selten zu (teilweise) schwerwiegenden Feststellungen im Bereich des Berechtigungsmanagements (u. a. Rechtevergabe, Rezertifizierung). IKT-Risiken, Cyber-Angriffe und Lücken in der Informationssicherheit, die auf ein nicht konformes Berechtigungsmanagement zurückzuführen sind, führen immer häufiger zu Ausfällen kritischer Geschäftsprozesse bei Banken und Unternehmen.

Die neuen DORA-Vorgaben verschärfen zudem die Anforderungen an die digitale Resilienz (z. B. beim Identity Lifecycle Management).

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. Die Aufsicht fordert daher explizit eine risikoorientierte regelmäßige Überprüfung kritischer IT-Berechtigungen.

Aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Institut insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten (Admin, Super-User) angemessene Prozesse zur Protokollierung und Überwachung einzurichten.

Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche:

- IT, Organisation und Projektmanagement, IT-Compliance und IT-Governance
- IKT-Risikokontrollfunktion und IKT-Risikomanagement
- Notfallmanagement BCM/ITSCM und IKT-Geschäftsfortführungsmanagement
- IT-Revision, Datenschutz und Data Governance
- Auslagerungsmanagement, Dienstleistersteuerung und IKT-Drittparteienrisikomanagement

Sowie andere interessierte Fach- bzw. Grundsatzbereiche, Geschäftsleitung/ IT-Vorstandsmitglieder und externe (IT-)Prüferinnen und Prüfer sowie (IT-)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

Informationssicherh.- u. 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, IAM-Experte, ReDworks GmbH*, Berlin

Markus Duda ist Projektleiter und Spezialist für Identity- und 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.

* Die Referierenden geben ausschließlich ihre persönliche Auffassung und nicht die eines bestimmten Instituts, der Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wieder. Die Referierenden nehmen auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.

DORA-konformer Umgang mit Eigen-Anwendungen & IDV
8. Oktober 2026, Online-Veranstaltung

IKT und DORA im Fokus: Informationssicherheit &
IKT-Risikomanagement
13. Oktober 2026, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement
14./15. Oktober 2026, Online-Veranstaltung

Steuerung & Begleitung von IT-Projekten
15. Oktober 2026, Online-Veranstaltung

Fachtagung DORA & DORA-Umsetzung
3./4. November 2026, Online-Veranstaltung

Berechtigungsmanagement im Fokus der Aufsicht
10. November 2026, Online-Veranstaltung

Zertifizierter KI-Governance-Officer (CAIGO)
7. bis 9. Dezember 2026, 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 (IAM)

Name
Vorname
Position
Firma
Straße /Nr.
PLZ / Ort
Telefon
E-Mail
Name der Assistenz
Datum/Unterschrift

Senden Sie Ihre Anmeldung bitte an: anmeldung@akademie-heidelberg.de

Termin und Seminarzeiten

Dienstag, 15. Dezember 2026
9:00–16:30 Uhr
Online-Zugang ab 8:45 Uhr
Seminar-Nr. 26 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
auf Wunsch 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 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 für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de