

# Berechtigungsmanagement im Fokus der Aufsicht



## Banken-Aufsicht-Seminar · 6 CPE-Punkte

- 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/Super-Usern
- Sichere Vorgehensweise bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten

### 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 Anforderungen an die Steuerung von Benutzerberechtigungen – 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
- 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 IAM
- 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
- 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
- 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 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 unsauberes 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 Rechtevergabekonzept und der IT-Strategie überein. Eine risikoorientierte Überprüfung der IT-Berechtigungen ist daher notwendig.

Das Institut hat zudem 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.

## Zielgruppe

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der 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.

## 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

*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.*

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

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen  
19. September 2026, Online-Veranstaltung

DORA Spezial: Umgang mit Software-/IKT-Service-Providern & Cloud-Dienstleistern  
21. September 2026, Online-Veranstaltung

Basis-Seminar Business Continuity Management (BCM)  
22. September 2026, Online-Veranstaltung

Anforderungen an das Datenqualitätsmanagement (DQM) & Beurteilung der Data-Governance  
5. 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

Neue DORA- & Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM  
21. Oktober 2026, Online-Veranstaltung

► Diese und weitere Seminar-Angebote finden Sie bei uns online unter [www.akademie-heidelberg.de/online-seminare](http://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](mailto:b.wehling@akademie-heidelberg.de)

Anmeldeformular

Berechtigungsmanagement  
im Fokus der Aufsicht

|                    |
|--------------------|
| 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](mailto:anmeldung@akademie-heidelberg.de)

Termin und Seminarzeiten

Dienstag, 10. November 2026  
9:00–15:00 Uhr  
Online-Zugang ab 8:45 Uhr  
Seminar-Nr. 26 11 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 auf Wunsch gerne zusenden.  
Diese können Sie jederzeit auch auf unserer Website einsehen: [www.akademie-heidelberg.de/agb](http://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](mailto:info@akademie-heidelberg.de)  
[www.akademie-heidelberg.de](http://www.akademie-heidelberg.de)