4. Mai 2026 · 9:00–16:45 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

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**
- **Häufige Schwachstellen im IKT-Risikomanagement**
- **Funktionsbezogene und kompetenzgerechte Berechtigungsvergabe – Besonderheiten bei privilegierten Nutzern**
- **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, CISSP, CISA, CRISC, CGEIT, Informationssicherheitsbeauftragter, Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Roland Hein
Inhaber, Geschäftsführer
bit Informatik GmbH
Trier

Berechtigungsmanagement im Fokus der Aufsicht

Programm

Dr. Thomas Klühspies, Bundesbank · 9:00–11:00 Uhr

Aktuelle Anforderungen an die Steuerung von Benutzerberechtigungen – Sicherheitslücken als hohes Risiko

- 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
- Beurteilung 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. Mittagpause

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

- IAM als Grundlage zur Erfüllung der DORA-Anforderungen
- Sicherstellung des Prinzips der minimalen Rechtevergabe
- 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

Roland Hein, bit Informatik · 15:15–16:45 Uhr

Berücksichtigung von ESG-Risiken in Risikomanagement- und Governance-Prozessen sowie bei Ratings und Scorings in der Bank-Praxis

- IT-unterstütztes Berechtigungsmanagement
- Integration der IT-Systeme in zentrale Benutzerverwaltung
- Wichtige Aspekte aus der Umsetzungspraxis
- Elektronische Benutzerverwaltung und aufsichtsrechtliche Anforderungen: Prüfungssichere Dokumentation
- Rechte privilegierter Nutzer: Vergabe, (Echtzeit-) Überwachung, Protokollierung (Kontrolle) und Auswertung
- Zusammenarbeit mit externen IT-Dienstleistern
- Rezertifizierung unter Beteiligung der Fachbereiche
- SoD Matrix – Besondere Anforderungen
- Vorbereitungs-Maßnahmen vor Prüfungen durch die Aufsicht, Wirtschaftsprüfer oder Verbandsprüfer
- Aktive Begleitung einer Prüfung durch einen externen Spezialisten

Seminarziel

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 Rechtevergabekonzept 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 überprüfbar machen, 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, IT-Compliance, Datenschutz (DSB) und Data Governance
- Informationssicherheit (ISB) und Informationsrisikomanagement
- Notfallmanagement (BCM), Interne Revision, IT-Revision und Regulatorik
- (Zentrales) Auslagerungsmanagement und Dienstleistersteuerung
- sowie andere interessierte Fach- bzw. Grundsatzbereiche, Mitglieder der Geschäftsleitung/des IT-Vorstands, externe Prüfer*innen und Bankdienstleister

Unsere Referenten

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

Dr. Thomas Klühspies ist seit 13 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, CISSP, CISA, CRISC, CGEIT
Informationssicherheitsbeauftragter, 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.

Roland Hein
Inhaber, Geschäftsführer, bit Informatik GmbH*, Trier

Roland Hein stellt Instituten der deutschen Kreditwirtschaft seit fast 30 Jahren workflow-basierte Anwendungen zur ganzheitlichen und aufsichtskonformen Umsetzung der MaRisk- und BAIT-Anforderungen zur Verfügung. Seine Schwerpunkte liegen hierbei u. a. in der systemgestützten Abbildung, Vergabe und Überwachung von (IT-)Berechtigungen (MaRisk AT 4.3), der Dienstleistersteuerung sowie der Steuerung des Informationsverbunds.

**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 Referierenden nehmen auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.

Fachtagung DORA & DORA-Umsetzung
16./17. März 2026, Online-Veranstaltung

KI-gestützte Prozessautomatisierungen
23. März 2026, Online-Veranstaltung

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA
24. März 2026, Online-Veranstaltung

KI-Governance: Aufsichts-Anforderungen an den Einsatz von Künstlicher Intelligenz
14. April 2026, Online-Veranstaltung

Aufsichts-Anforderungen an DQM & Data-Governance
15. April 2026, Online-Veranstaltung

IT-Schutzbedarf & Soll-Konzepte DORA-konform umsetzen
27. April 2026, Online-Veranstaltung

Abgrenzung und parallele Steuerung von Auslagerungen (MaRisk) & IKT-Dienstleistungen (DORA)
28. April 2026, Online-Veranstaltung

DORA Spezial: Informationssicherheit & IKT-Risikomanagement
7. Mai 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

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**

Termin und Seminarzeiten

Montag, 4. Mai 2026
9:00–16:45 Uhr
Online-Zugang ab 8:45 Uhr

Seminar-Nr. 26 05 BA053 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.

02.26 / 2605 BA053

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de