17. Februar 2025 · 13:00–16:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

IKT Spezial – Identity- & Access-Management (IAM)

Vergabeprozess und Rezertifizierung als häufige Schwachstelle

Banken-Praxis-Seminar · 4,5 CPE-Punkte

Konkretisierte DORA-Anforderungen an das Identitäts- und Rechtemanagement!

- **Aktuelle Aufsichts-Vorgaben zum Identitäts-/Rechtemanagement**
- **Häufig identifizierte Schwachstellen in der Vergabe-Praxis**
- **Funktionsbezogene Vergabe nach den IAM-Prinzipien Need-to-know, Need-to-have, Need-to-use (DORA) & Segretation-of-Duties**
- **Sichere Vorgehensweise bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten**
- **IT-unterstützte Vergabe, Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Benutzerrechten**

20 Jahre AKADEMIE HEIDELBERG

Referent

Markus Duda
Geschäftsführer
ReDworks GmbH
Berlin

Programm

Markus Duda, Redworks · 13:00–16:00 Uhr

Neue DORA-Anforderungen und aktuelle aufsichtliche Anforderungen zur Steuerung von Benutzerberechtigungen – Häufig identifizierte Sicherheitslücken in der Praxis

- Ablösung der BAIT-Vorgaben durch DORA: Erweiterte Anforderungen an das Rollenmodell und die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von nicht mehr benötigten Berechtigungen und Benutzer-Identitäten – Neues Need-to-use-Prinzip nach DORA
- Prüfung der Notwendigkeit und Zulässigkeit beantragter Rechte (Zugriffssteuerung) – Organisatorische und technische Sicherstellung der minimalen Rechtevergabe
- 4-Augen-Prinzip und Funktionstrennung – Laufende Überwachung im Vergabeprozess (z. B. Alarmmeldungen) und anlassbezogene Aktualisierung der Berechtigungskonzepte – auch unter dem Gesichtspunkt der Effizienz! Erweiterte Protokollierungsanforderungen durch DORA
- Funktionstrennung – Sicherstellung, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeitende durchgeführt und auch bei Arbeitsplatzwechseln Interessenkonflikte vermieden werden (AT 4.3.1 MaRisk)
- Überwachung privilegierter Benutzer (Super-User, Notfall-User), insb. Systemadministratoren – Anforderungen an Logging, Protokollierung und Protokollauswertung
- 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 – Vermeidung der Umgehung der IAM-Governance

Funktionsbezogene Vergabe von Benutzerberechtigungen nach den IAM-Prinzipien (Need-to-know, Need-to-have, Need-to-use und Segretation-of-Duties)

- 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 (BAIT Tz. 6.2, 6.3)
- 4-Augen-Prinzip und Funktionstrennung
- Prüfung der Notwendigkeit und Zulässigkeit beantragter Rechte
- Zentralisierte Lösungen insbes. für Kernbankensysteme und wesentliche Teile des Informationsverbunds unerlässlich, vor allem bei größeren Instituten
- IAM-Governance: Genehmigungs- und Kontrollprozesse – Sicherstellung, dass die fachlichen Vorgaben eingehalten werden – Häufige Schwachstelle: Ungenügende Kontrolle der Umsetzung in den IT-Systemen und fehlende Einbindung des fachlich verantwortlichen Unternehmensbereichs (BAIT Tz. 6.4)
- Analyse der Ausgangslage – Vermeidung der Anträge auf »Zuruf« – Schaffung einer unternehmensweiten Sicht der Funktionen
- Überprüfung eingeräumter Berechtigungen: Vermeidung von Risiken durch regelmäßige Rezertifizierungen

DORA-konforme und sichere Vorgehensweise bei der Überprüfung, Rezertifizierung und Dokumentation von Identitäten und Rechten

- Integration der IT-Systeme in eine zentrale Benutzerverwaltung – Voraussetzungen für die Implementierung
- Wichtige Aspekte aus der Implementierungspraxis – Umgang mit interner Kommunikation, notwendigem Fachwissen und Verfügbarkeit von Ressourcen
- 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
- Rezertifizierung unter Beteiligung der Fachbereiche – Wer trägt die Verantwortung für den IAM-Prozess?

Seminarziel

Das Seminar vermittelt fundierte Kenntnisse zu den aktuellen und neuen Anforderungen (DORA) für die sichere und effiziente Steuerung von Benutzerberechtigungen und Zugangsrechten. Ziel ist es, den Teilnehmenden ein umfassendes Verständnis für die Implementierung eines robusten IAM zu vermitteln, das regulatorischen Standards entspricht und Sicherheitslücken minimiert.

Zentrale Themen sind die abgelösten BAIT-Vorgaben durch DORA, erweiterte Anforderungen an Rollenmodelle und verwaltungstechnische Prozesse zur Anlage, Änderung und Löschung von Berechtigungen.

Weitere Inhalte behandeln die Rezertifizierung von Benutzerrechten unter Einbezug der Fachbereiche, um die Aktualisierung und Einhaltung der IAM-Governance sicherzustellen. Die Teilnehmenden lernen, wie privilegierte Nutzer wie Systemadministratoren und Super-User durch Logging und Protokollauswertung überwacht werden können.

Das Seminar bietet praxisnahe Einblicke in IAM-Governance-Modelle und Governance-Prozesse, darunter die zentrale Benutzerverwaltung und elektronische Dokumentation von Zugriffsrechten. Es werden Richtlinien für die Zusammenarbeit mit externen IKT-Dienstleistern besprochen sowie Empfehlungen für eine effiziente, auditkonforme IAM-Struktur gegeben.

Wissenswertes

Zielgruppe

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

- IT, Organisation und Berechtigungsmanagement (IAM)
- Informationssicherheit (ISB) und Informationsrisikomanagement
- Notfallmanagement und Business Continuity Management (BCM)
- Interne Revision und IT-Revision
- Datenschutz (DSB) und Data Governance
- (Zentrales) Auslagerungsmanagement und (IKT-)Dienstleistersteuerung
- IT-Compliance und IT-Regulatorik
- sowie andere interessierte Fach- bzw. Grundsatzbereiche, Mitglieder von Geschäftsleitung und Vorstand, externe Prüfer*innen sowie Bankienstleister

Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu spezifischen Aufsichtsanforderungen zum Thema Rechtevergabe, Rezertifizierung und Access-Management
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut
- Sie erhalten wertvolle Praxistipps im Erfahrungsaustausch mit dem Referenten
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit anderen Praktiker*innen

Unser Referent

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 das rollenbasierte Berechtigungsmanagement, aber auch die Toolauswahl und Einführung eines zentralen IAM-Tools.

Überprüfung der DORA-Konformität von (IKT-)Dienstleistern & Cloud Service Providern
21. Januar 2025, Online-Veranstaltung

DORA Spezial: Informationssicherheit & IKT-Risikomanagement
23. Januar 2025, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM
29. Januar 2025, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement KOMPAKT
5./6. Februar 2025, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken
17. Februar 2025, Online-Veranstaltung
(**KOMBITERMIN** am Vormittag)

Mobile-Work-Risiken im Fokus von DORA, IKT-Risikomanagement & IT-Revision
18. Februar 2025, Online-Veranstaltung

IKT-Governance im Fokus der Aufsicht
18. Februar 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

IKT Spezial – Identity- & Access-Management (IAM)

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

Montag, 17. Februar 2025
13:00 – 16:00 Uhr
Online-Zugang ab 12:45 Uhr

Seminar-Nr. 25 02 BA098 W

Teilnahmegebühr

€ 290,– (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.

11.24 / 25 02 BA098

AKADEMIE HEIDELBERG

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