FORUM

Glossar Berechtigungsmanagement kompakt

Von A - Z

Ihr schneller Einstieg für Fach- und Führungskräfte

Sehr geehrte Leser*innen,

Berechtigungsmanagement ist für Banken und Versicherungen ein wesentlicher Baustein der IT-Sicherheit und Compliance. Dabei spielen Fachbegriffe und Abkürzungen eine zentrale Rolle.

Dieses Glossar bietet Ihnen einen kompakten Überblick über die wichtigsten Begriffe – von technischen Konzepten bis zu regulatorischen Vorgaben wie BAIT und DORA. Es unterstützt IT, Compliance und Fachbereiche beim besseren Verständnis und in der täglichen Zusammenarbeit.

Wir wünschen Ihnen eine gewinnbringende Lektüre und viel Erfolg bei der praktischen Umsetzung.

Über den Autor

Dr. Martin Diez
Specialist Identity & Access Management,
KfW Bankengruppe,
Frankfurt am Main

Dr. Martin Diez ist bei der KfW Bankengruppe in Berlin tätig und beschäftigt sich dort hauptsächlich mit Vorgaben und Prozessen im Identity & Access Management (IAM) sowie der Begleitung von internen und externen Prüfungen (Revision, Wirtschaftsprüfer, BaFin). Zuvor war Dr. Diez lange als Berater tätig und hat das Thema IAM in unterschiedlichen Unternehmenskonstellationen kennengelernt. Seine inhaltlichen Schwerpunkte sind u.a. die Formulierung einer prüfungsfesten SfO (schriftlich fixierten Ordnung), die Erstellung von Vorgaben für praktikable und prüfungssichere Berechtigungskonzepte sowie die Etablierung und Weiterentwicklung von SoD (Segregation of Duties - Funktionstrennung).

A

2FA — Zwei-Faktor-Authentifizierung

Eine eingeschränkte Form der Mehr/Multi-Faktor-Authentifizierung (siehe MFA), in der der Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (bspw. Passwort + Token) sichergestellt wird.

aBK — Applikationsspezifisches Berechtigungskonzept

Auch: "Berechtigungskonzept", "anwendungsspezifisches Berechtigungskonzept" oder "Applikations- Berechtigungskonzept". Enthält Informationen zu den fachlichen und technischen Tätigkeiten einer Applikation und Details zu den dafür erforderlichen Applikations- (IT-) Rollen, Berechtigungen (Entitlements) und nicht-personalisierten Konten.

AD — Active Directory

Verzeichnisdienst von Microsoft Windows Server. Active Directory ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern. Dazu verwaltet es verschiedene Objekte in einem Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Den Benutzern des Netzwerkes können Zugriffsbeschränkungen erteilt werden. So darf zum Beispiel nicht jeder Benutzer jede Datei ansehen oder jeden Drucker verwenden.

AR — Applikationsrolle

Mittlere Ebene der Berechtigungsstruktur im IAM-System (fachlich/technisch). Applikationsrollen werden als erste technische Ebene den Fach-/Business-Rollen zugewiesen (Beziehung 1:n, bei Bedarf 1:1). Beinhaltet im Regelfall Berechtigung aus mehreren Zielsystemen, um eine Aufgabe in einer Applikation mit einer Bestellung freizuschalten. Sind je nach Bedarf Berechtigungsstruktur bestellbar oder nicht bestellbar. Fachlich und anwendungs- bzw. systemspezifisch mit Kritikalitäts- u. SoD-Kennzeichen.

B

BaFin — Bundesanstalt für Finanzdienstleistungsaufsicht

Aufsichtsorgan in Deutschland. Prüft i. d. R. auch das Thema IAM in Banken und Versicherungen

BAIT — Bankaufsichtliche Anforderungen an die IT

Die Bankaufsichtlichen Anforderungen an die IT, abgekürzt BAIT, sind Verwaltungsanweisungen, die mit einem Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für die sichere Ausgestaltung der IT-Systeme sowie der zugehörigen Prozesse und diesbezüglicher Anforderungen an die IT-Governance in deutschen Kreditinstituten veröffentlicht wurden. Im Januar 2025 wurden die aufsichtlichen Anforderungen an die IT durch die BaFin größtenteils

zugunsten von Verordnung (EU) 2022/2554, besser bekannt als DORA, aufgehoben. Die BAIT bleiben nur noch für die Institute anwendbar, die durch das am 27. Dezember 2024 beschlossene Finanzmarktdigitalisierungsgesetz (FinmadiG) neu unter DORA reguliert werden. § 65a Abs. 3 KWG sieht dafür eine Übergangsfrist bis zum 1. Januar 2027 vor.

BerKon — Berechtigungskonzept

Dokumentation der Regeln, Rollen und Prozesse zur Vergabe und Kontrolle von Zugriffsrechten auf IT-Systeme

BK — Berechtigungskonzept

Siehe BerKon

BM/BRM — Berechtigungsmanagement

Das Berechtigungsmanagement ist Teil des Identity & Access Managements. U.A. werden unter diesem Begriff die Gesamtheit der benötigten Werkzeuge, Prozesse, Verantwortlichkeiten und Vorgaben gefasst, welche den Mitarbeitern die benötigten Zugriffe auf Systeme, Applikationen etc. zur vollständigen Arbeitsfähigkeit gewährleisten.

BR — Business-Role, deutsch Fachrolle

Siehe FR

BSI — Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine deutsche Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat mit Sitz in Bonn, die für Fragen der IT-Sicherheit zuständig ist.

C

C-IAM — Consumer/Customer Identity & Access Management

Das C-IAM ist ein unternehmensweiter IT-Unterstützungsprozess. Es stellt sicher, dass jede/r Kunde/Kundin bzw. Interessent identifiziert wird und ihre/seine Zugriffsmöglichkeit auf den eigenen Daten- und Vertragsbestand beschränkt sind.

D

DORA — Digital Operational Resilience Act

Mit der Verordnung (EU) 2022/2554 verpflichtet die Europäische Union Finanzunternehmen zur Stärkung ihrer digitalen operationalen Resilienz. Auch im deutschsprachigen Raum haben sich die englische Bezeichnung „Digital Operational Resilience Act“ und deren Abkürzung DORA etabliert. DORA enthält Vorgaben für die Resilienz von IKT-Systemen für verschiedene Arten von Finanzunternehmen, wie beispielsweise für Kreditinstitute (Banken) und Versicherungsunternehmen sowie für deren IKT-Dienstleister. Die Verordnung betrifft in der Europäischen Union schätzungsweise 22.000 Finanzunternehmen, davon 3.600 in Deutschland.

F

FR — Fachrolle

Oberste Ebene der Berechtigungsstruktur im IAM-System (fachlich): Fachrolle (Business Rolle). Fachrollen umfassen ein Leistungsspektrum / Aufgabenfeld / Unternehmensfunktion von diversen Applikationsrollen u. gehören zur Organisation, einem Bereich, einer OE oder einer Funktion. Beschreibung fachlicher Attribute der jeweiligen Rolle. Organisatorisch und anwendungsübergreifend.

H

HA — High-Availability, deutsch: Hochverfügbarkeit

Bezeichnet die Fähigkeit eines Systems, trotz Ausfalls einer seiner Komponenten den Betrieb zu gewährleisten. Hierfür werden redundante Systeme mit gespiegelten Daten an verschiedenen Standorten benötigt. Je nach Branche gibt es Vorgaben für die Distanz zwischen den Standorten.

HPA — High Privileged Accounts - Hochprivilegierte Konten

Gemeint sind i. d. R. nicht personalisierten Konten mit risikobehafteten Rechten, also administrative oder Rechte. Die Berücksichtigung von fachlich kritischem Kontent unter dieser Vokabel wird nicht empfohlen.

HPR — High Privileged Rights - Hochprivilegierte Rechte

Gemeint sind i. d. R. risikobehaftete Rechte, also administrative Rechte. Die Berücksichtigung von fachlich kritischen Rechten unter dieser Vokabel wird nicht empfohlen.

HPU — High Privileged User - Hochprivilegierte Benutzer

Wird häufig synonym zu HPA verwendet. Der Begriff "User" ist im Kontext zu betrachten. Teilweise sind Identitäten/Personen, teilweise aber auch Konten gemeint.

I

IAG — Identity & Access Governance

Die Einhaltung von Vorgaben im Kontext des Identity & Access Managements

IAM — Identity & Access Management

Das IAM (Identity & Access Management) ist ein unternehmensweiter IT-Unterstützungsprozess. Das IAM stellt sicher, dass jede/r Mitarbeiter/in ihre/seine spezifische Aufgabe über passgenaue IT-Zugriffe wahrnehmen kann. Gleichzeitig werden durch Einschränkungen von Zugriffen regulatorische und interne Vorgaben, wie z. B. das Sparsamkeitsprinzip (auch: Need-to-know-Prinzip) oder die Funktionstrennung, (siehe SOD) eingehalten.

IDM	Identity Management bzw. Identity Manager

Gemeint ist i. d. R. das System, mit dem das IAM technisch umgesetzt wird. Also die konkrete Software, die die Daten zu Identitäten über Rollen in Richtung der Berechtigungen und notwendigen Konten zusammenführt und synchronisiert.

IKS	Internes Kontrollsystem

Das interne Kontrollsystem besteht aus systematisch gestalteten technischen und organisatorischen Regeln zur Einhaltung von internen Vorgaben sowie zur Minimierung von Risiken.

IR	Interne Revision

Prüft als 3rd Line of Defense im unternehmensinternen Kontrollsystem (IKS) die anweisungskonforme Arbeit der 1st Line (i. d. R. IT-Betrieb) und der 2nd Line (i.d.R. CISO/ISO) of Defense.

ITR	IT-Rolle

Identisch zu AR (siehe dort, Nutzung von Applikationsrolle wird empfohlen)

J

JAP	Jahresabschlussprüfer/Wirtschaftsprüfer

Externe Prüfer im Auftrag des eigenen Unternehmens. Erfüllen Prüfauftrag gemäß Prüfordnung und erfüllen damit auch einen aufsichtsrechtlich relevanten Prüfauftrag der BaFin.

L

LDAP	Lightweight Directory Access Protocol

LDAP ist ein Netzwerkprotokoll zur Abfrage und Änderung von Informationen verteilter Verzeichnisdienste. LDAP ist der De-facto-Industriestandard für Authentifizierung, Autorisierung sowie Adress- und Benutzerverzeichnisse. Die meisten Softwareprodukte, die mit Benutzerdaten umgehen müssen und am Markt relevant sind, unterstützen LDAP.

M

MaRisk	Mindestanforderungen an das Risikomanagement

Von der BaFin veröffentlicht als Rundschreiben zur Ausgestaltung des Risikomanagements bei deutschen Finanzinstituten und Versicherungen.

MFA	Mehr/Multi-Faktor-Authentifizierung

Identitätsnachweis (Authentifizierungsprozess) eines Nutzers mittels einer Kombination mehrerer unterschiedlicher und insbesondere unabhängiger Komponenten (bspw. Passwort + Token). Die Kombination nutzt die Bereiche Wissen (z. B. Passwörter, PINs, besondere Daten oder Antworten auf besondere Fragen), Besitz (z. B. Token-Generator, Ausweiskarte mit RFID, elektronsicher Personalausweis, Smartphone), Biometrie (z.B.

Fingerabdruck, Gesichtserkennung, Iris-Scan). Die MFA sollte in Abhängigkeit der Kritikalität (z. B. Vertraulichkeit der Daten, Zugriffszeit, Zugriffsweg) genutzt werden, um unkritische Zugriffe nicht unnötig aufwändig zu gestalten.

N

NPU — Nicht-personalisierter User

Ein nicht-personalisierter Benutzer (User) ist meist ein technischer Benutzer welcher Dienste betreibt, Daten abholt und liefert, Schnittstellen bedient, Services startet oder betreibt. Diese nicht- personalisierten Benutzer haben meist aufgrund ihrer Funktion ein nicht trennbares Set an Lese-, Veränderungs- und Löschungsberechtigungen.

O

oBK — Organisationsspezifisches Berechtigungskonzept

Organisationsspezifisches Berechtigungskonzept je Fachbereich, IT-Abteilung oder Großprojekt. Dokumentation der zulässigen Rechtestrukturen in einem Fachbereich bzw. einer IT-Abteilung. Ist entbehrlich, sofern ein adäquates Business Rollen-Modell existiert. Hier werden teilweise auch die Begriffe "Rollenkonzept" oder "bankweites Berechtigungskonzept" verwendet.

OE — Organisationseinheit

Abstrakte Bezeichnung für eine aufbauorganisatorische Instanz (z. B. ein Team, eine Gruppe, eine Abteilung, ein Bereich, ein Dezernat)

O2A/OTA — Order-to-Admin

Order-to-Admin ist eine im Identity & Access Management Kontext verbreitete Methode, bei der nicht abbildbare automatisierte Prozesse durch eine manuelle Administration gelöst werden. Auf Zielsystemebene ist hier im Kontext des Berechtigungsmanagements die typische asynchrone Berechtigungssteuerung durch einen Administrator über manuelle Berechtigungszuweisungen gemeint.

P

PAM — Privileged Access Management

Privileged Access Management. PAM dient der Kontrolle, Überwachung, Sicherung und Prüfung aller menschlichen und nicht menschlichen privilegierten Identitäten und Aktivitäten in einer geschäftlichen IT-Umgebung (i. d. R. durch den Einsatz spezieller Software, die auch forensische Analysen ermöglicht und Security-Alerts an ein SIEM meldet).

R

RACF — Ressource Access Control Facility

Resource Access Control Facility (RACF) ist IBMs Implementierung der Sicherheitsschnittstelle SAF (System Authorization Facility) der Großrechnerbetriebssysteme MVS (Kern des z/OS) und – in einer älteren Version – z/VM. Der heutige Name lautet SecureWay Security Server – RACF. Der RACF- Administrator pflegt mittels RACF-Kommandos die RACF-Datenbank. Diese enthält in sogenannten Profilen die Benutzerschlüssel (AccountIDs, UserIDs), die zu schützenden Ressourcen (Resources) und Gruppen (Groups).

RBAC — Role Based Access Control, deutsch: Rollenbasierte Zugriffskontrolle

Mittels Role Based Access Control wird der Zugriff auf IT-Systeme über die Definition und Verwendung von Business-Rolle, IT-Rollen und Berechtigungen gesteuert. RBAC ist ein Standard der NIST seit 1992, seit 2004 als ANSI-Norm 359-2004.

RDS — Remote Desktops Services

Früher auch „Terminal Services“ genannt sind eine Komponente von Microsoft Servern zum Aufbau interaktiver Sessions und Applikationen. Diese werden i.d.R. auch im Umfeld PAM benötigt.

ReCon — Reconciliation

Abgleich zwischen IAM-System und Zielsystem über die Benutzerkonten, Berechtigungen und deren Zuweisungen. Der Soll-Zustand des IAM-Systems wird mit dem Ist-Zustand des Zielsystems verglichen und bei Abweichungen ggfs. korrigiert.

RolV — Rollenverantwortliche/r

Rollenverantwortliche konzipieren und pflegen ihre Rollen im Kontext des Berechtigungsmanagements.

S

SFO — Schriftlich fixierte Ordnung

Schriftlich fixierte Ordnung. Umfasst alle verbindlichen Arbeitsanweisungen und Prozesse einer Organisation.

SIEM — Security Information & Event Management

Im Security Information and Event Management (SIEM) erfolgt die Echtzeitanalyse von Sicherheitsalarmen aus Anwendungen und Netzwerkkomponenten. SIEM dient damit der IT-Sicherheit einer Organisation.

SOC — Security Operation Center

Einheit im Unternehmen die in der Regel an 7 Tagen mit 24 Stunden besetzt ist, um Sicherheitsalarme unverzüglich beurteilen zu können.

SOD

Segregation of Duties

Trennung nicht vereinbarer Funktionen, um Missbrauch vorzubeugen. Ein Beispiel ist die Trennung von Markt und Marktfolge, etwa beim ersten und zweiten Votum für eine Kreditentscheidung. Je nach Branche gibt es verschiedene, abweichende Vorgaben und Detaillierungen zur Funktionstrennung. Auch ergänzende interne Vorgaben sind üblich.

SSO

Single-Sign-On

Zusammenfassung mehrerer IT-System oder IT-Applikationszugänge zu einem Login-Vorgang. Häufig wird hier eine zentrale Identität als Autorisierung herangezogen (etwa die O365 Identität oder Windows-AD Identität) um weitere Login-Vorgänge dahinterliegend zu vereinfachen.

SU

Super User

Personalisiertes oder nicht personalisiertes administratives Benutzerkonto, dem administrative Berechtigungen zugewiesen sind. Super User werden von Netzwerk-, System- und Datenbank-Administratoren verwendet.

U

UID

Unique Identifier

Eindeutiger Bezeichner, bestehend aus Codes in Form von Zeichenketten aus Zahlen und Buchstaben. Sie machen ein Objekt eindeutig identifizierbar. UIDs kann es für unterschiedliche Arten von Objekten geben (z. B. für Benutzerkonten, Bestellungen oder IT-Rollen).

V

VIV

Vertraulichkeit - Integrität – Verfügbarkeit

Klassische Schutzziele der Informationssicherheit. Typischerweise werden Applikationen den VIV-Stufen 1 bis 4 zugeordnet.

Z

ZSA

Zielsystemabgleich, engl.: Reconciliation

Regelmäßige Prüfung der Übereinstimmung der Verknüpfungen zwischen Konto und Berechtigungsobjekten im zentralen IAM-System auf der einen Seite sowie zwischen Kennung und Zugriffsobjekten im Zielsystem auf der anderen Seite. (siehe auch ReCon)

Praxiswissen für Ihren Erfolg im Job

Unsere Seminare und Weiterbildungen liefern aktuelles und praktisches Know-how zu unterschiedlichen Themen aus den Bereichen Insolvenz, Sanierung, Abwicklung und Restrukturierung.
Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Telefon: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.de