KPMG
cutting through complexity

Regulatorische Herausforderungen in der Identity- und Access-Governance

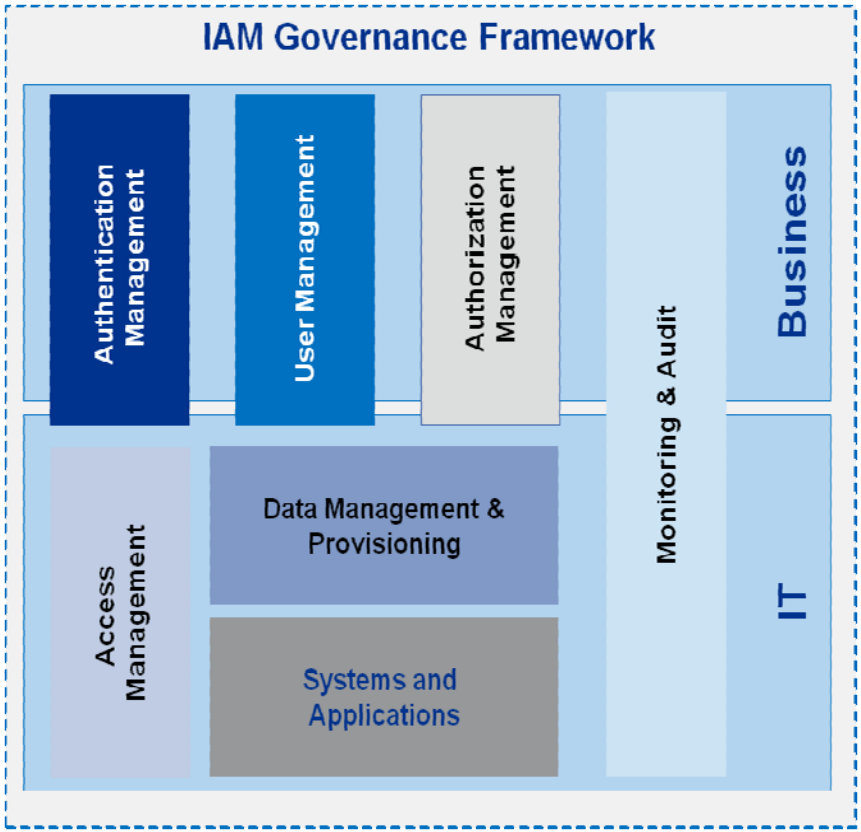
Seminar “Auditsicher mit Identity & Access Intelligence” – 07.11.2014

Identity and Access Management – Eine kurze Sicht auf den Inhalt

The policies, processes and systems for efficiently and effectively governing and managing who has access to which resources within an organisation.

Identity & Access Management (IAM) is the process of creating value and addressing IT governance and compliance through effectively and efficiently:

- managing users,
- authenticating the identity of users,
- managing users' access to IT resources,
- monitoring what users are doing with that access.



* Definition basierend auf der globalen KPMG IAM methodology

Wesentlicher Fokus ist derzeit die aufsichtsrechtliche Sicht auf die Herausforderungen im Berechtigungsmanagement

Instituts-interne Sicht

- Regelmäßige/Häufige Feststellungen bei Prozess-/Systemprüfungen der internen Revision / Abschlussprüfer (auch mit Klassifizierung „high risk“)
- In Teilen Sonderprüfungen mit alleinigem Fokus auf das systematische Berechtigungsmanagement des Instituts

Aufsichtsrechtliche Sicht*

- Regelmäßige/Häufige Feststellungen bei §44-Prüfungen der Aufsicht (BaFin/Bundesbank) (auch mit Feststellung des Schweregrads F4)
- Mit der Entwicklung der BAIT ist eine weitere Detaillierung der MaRisk-Anforderungen zu erwarten

Risiko-Sicht

- Erhöhung der Sicherheit von Informationen bzw. Reduzierung des Risikos für finanzielle oder Reputationsschäden aufgrund bekannter Schadensfälle in der Branche, wie z. B.:
  - Interne Diebstähle von Kundendaten (z.B. Steuer-CDs)
  - Finanzielle Verluste durch unautorisierte Geschäfte

* nur nationale Betrachtung. Für internationale Institute ergibt sich im Regelfall ein ähnliches Bild auch für Nicht-deutsche Aufsichtsbehörden.

Die Aufsicht führt verstärkt Prüfungen im Bereich der IT-Organisation von Banken durch

- Die Prüfung der „Ordnungsmäßigkeit der Geschäftsorganisation hinsichtlich des Einsatzes der elektronischen Datenverarbeitung“ nach § 44 KWG durch die Aufsicht hat zu einer **wesentlichen Anzahl, in Teilen schwerwiegenden Feststellungen geführt**
- Dies betraf und betrifft im **Wesentlichen die Vorgaben, Prozesse und Kontrollen im Bereich des Berechtigungsmanagements**
- In den Banken werden derzeit **zahlreiche Projekte zur Abarbeitung vorhandener Feststellungen** in der IT durchgeführt
- Die aktuellen Vorgaben aus MaRisk und KWG bieten insbesondere zu IT-Fragestellungen **hohe Auslegungs- und Interpretationsmöglichkeiten**
- Die Aufsicht erwartet in Teilen eine regelmäßige **Statusberichterstattung zum Fortschritt von Berechtigungsmanagement-Projekten** bei vorhandenen Defiziten

* nur nationale Betrachtung. Für internationale Institute ergibt sich im Regelfall ein ähnliches Bild auch für Nicht-deutsche Aufsichtsbehörden.

Die Anforderungen an ein ordnungsgemäßes Identity and Access Management sind in verschiedenen Regularien enthalten

- Die **wichtigsten regulatorischen Anforderungen** an ein ordnungsgemäßes Identity and Access Management sind in den folgenden Regularien enthalten:
  - **MaRisk**
    Mindestanforderungen an das Risikomanagement
  - **GoBS**
    Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
  - **BDSG**
    Bundesdatenschutzgesetz
  - **IDW RS FAIT I**
    IDW Stellungnahme zur Rechungslegung: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie

Mindestanforderungen an das Risikomanagement (4. Novelle der MaRisk, 2012)

Die MaRisk geben Instituts-weit umzusetzende Anforderungen an die Ausgestaltung von Prozessen und Kontrollen in einem ordnungsmäßigen Berechtigungsmanagement vor:

- **AT 4.3.1 Aufbau- und Ablauforganisation:** Dies beinhaltet auch die regelmäßige und **anlassbezogene** Überprüfung von IT-Berechtigungen, Zeichnungsberechtigungen und sonstigen eingeräumten Kompetenzen. Das gilt auch bezüglich der **Schnittstellen zu wesentlichen Auslagerungen.**
- *Konkretisierung: Überprüfung von Berechtigungen und Kompetenzen*
  Zumindest bei IT-Berechtigungen …**mindestens jährliche**, bei kritischen IT-Berechtigungen eine mindestens **halbjährliche** Überprüfung erwartet.
- **AT 7.2 Technisch-organisatorische Ausstattung:**…insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass **jeder Mitarbeiter** nur über die Rechte verfügt, die er für seine Tätigkeit benötigt; die **Zusammenfassung von Berechtigungen in einem Rollenmodell** ist möglich.
- *Konkretisierung: Zugriffsrechte*
  Die eingerichteten Berechtigungen dürfen nicht im **Widerspruch zur organisatorischen Zuordnung von Mitarbeitern** stehen. Insbesondere bei Berechtigungsvergaben im Rahmen von Rollenmodellen ist darauf zu achten, dass Funktionstrennungen beibehalten beziehungsweise **Interessenkonflikte** vermieden werden.

Konkretisierungen der Vorgaben an Instituts-spezifische Bereiche finden sich im besonderen Teil der MaRisk (Modul BT)

- **BTO 2.2.1 Tz. 6 Handel:** Ein Händler darf nur **unter seiner eigenen Händleridentifikation** Handelsgeschäfte eingeben können, Erfassungstag und -uhrzeit sowie fortlaufende Geschäftsnummern müssen automatisch vorgegeben werden und dürfen vom Händler nicht veränderbar sein.
- **BTO 2.2.1 Tz. 9 Handel:** Organisatorisch dem Handelsbereich zugeordnete Mitarbeiter dürfen nur gemeinsam mit Mitarbeitern eines handelsunabhängigen Bereichs über Zeichnungsberechtigungen für Zahlungsverkehrskonten verfügen.
- **BTO 2.2.1 Tz. 10 Handel:** Das Institut hat durch geeignete Maßnahmen sicherzustellen, dass die Positionsverantwortung von Händlern jährlich für einen ununterbrochenen Zeitraum von mindestens 10 Handelstagen an einen anderen Mitarbeiter übertragen wird. In diesem Zeitraum hat das Institut dafür Sorge zu tragen, dass **kein Zugriff eines abwesenden Händlers** auf die von ihm verantworteten Positionen erfolgt.

Weitere Konkretisierungen zu IAM sind aus regulatorischer Sicht zu erwarten

- Die **wichtigsten Anforderungen dieser Regularien** können wie folgt zusammengefasst werden:
  - Es sind angemessene Prozesse für die IT-Berechtigungsvergabe sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege einzurichten, welche
  - eine Berechtigungsvergabe nach dem Minimalprinzip (Beschränkung auf Berechtigungen, die zur Ausführung der Tätigkeit notwendig sind),
  - eine restriktive Vergabe von kritischen Berechtigungen sowie
  - eine ordnungsgemäße Funktionstrennung (keine Vergabe sich gegenseitig ausschließender Rechte) gewährleisten
- **Konkretisierungen** durch die Aufsicht sind im Rahmen der Entwicklung des BAIT (Bankenaufsichtliche Anforderungen an die IT) zu erwarten.
- Weitere Vertiefungen sind über den neuen **Baustein Identitäts- und Berechtigungsmanagement** vom BSI zu erwarten
- Mögliche Erweiterungen sind aus Regularien im Zahlungsverkehr PSD II, SecuRePay zu erwarten

Die Erwartungshaltung der Aufsicht sowie externer und interner Prüfung kollidieren in der Praxis mit der Auslegung der regulatorischen Anforderungen durch die Institute

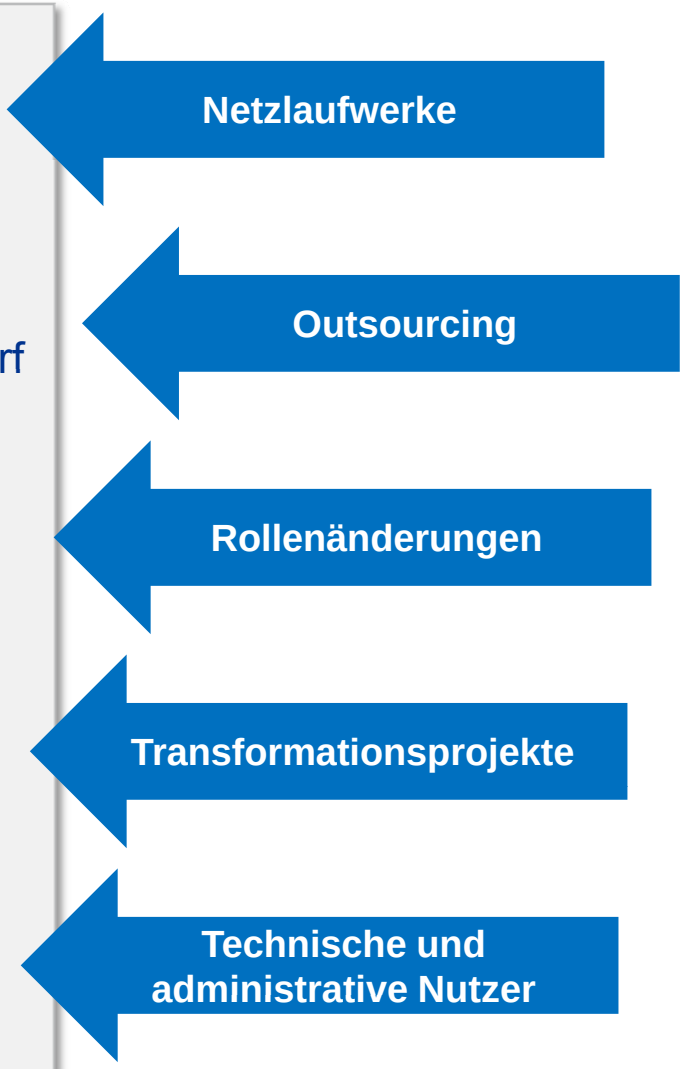
Die Realität zeigt Lücken auch in Form aufsichtsrechtlicher Prüfungsfeststellungen

- Unklare Richtlinien / Vorgaben sowie fehlende / unzureichende Prozess- und Berechtigungsdokumentation
- Uneinheitliche und unabgestimmte Vorgehensweisen bei der Benutzerverwaltung sowie unklare (de-)zentrale Verantwortlichkeiten
- Fehlende/unzureichende Kontrollprozesse zur Überwachung der Funktionsfähigkeit des Berechtigungsmanagements
- Unzureichender Berechtigungsvergabe-Prozess und fehlende Übersicht über Soll-Berechtigungen
- Verstöße gegen Need-to-Know-Prinzip und Funktionstrennung bei Systemprüfungen
- Kein/unzureichender Entzug von Berechtigungen bei Wechsel/Austritt (auch Externe)
- Kein umfassender Überblick über vergebene Zugriffsrechte und unzureichende Überprüfung von Berechtigungen (Rezertifizierung / Soll-Ist-Abgleich)
- Unzureichende Verfahren für privilegierte Benutzer (u.a. unpersonifizierte Benutzerkonten, keine differenzierten Zugriffsrechte für Administratoren (z.B. vollständige Leserechte auf Daten), keine Protokollierung und Kontrolle administrativer Aktivitäten)
- Unzureichendes Berechtigungsmanagement bei unstrukturierten Daten (z.B. Windows Verzeichnisse, Sharepoint)

Aktuelle Themen im Berechtigungsmanagement aus regulatorischem Fokus

Die Umsetzung eines ordnungsmäßigen Berechtigungsmanagements ist durch viele Instituts-spezifische Faktoren beeinflusst.

- **Netzlaufwerke:** Der Zugriff auf Netzlaufwerke erfordert ebenso Richtlinien, Prozesse und Kontrollen wie der für Anwendungen
- **Outsourcing:** Ein ausgelagertes Berechtigungsmanagement bedarf weitergehender Kontrollen im Rahmen der Auslagerungssteuerung
- **Rollenänderungen:** Die Änderungen an bestehenden Rollen sind mit Auswirkungen auf bestehende Berechtigungen zu betrachten
- **Transformationsprojekte:** Änderungen der Organisationsstruktur oder der Anwendungslandschaft bergen das Risiko nicht mehr benötigte Berechtigungen nicht wirksam zu erkennen und zu entziehen.
- **Technische und administrative Nutzer:** Häufig unterliegen technische und administrative Nutzer eigenen Prozessen. Besondere Anforderungen (z. B. Nicht personalisiert) sind zu berücksichtigen



Im wesentlichen ergeben sich zwei typische Vorgehensweisen, die von der Gesamtzahl und Schwere der Feststellungen und der Reife der Organisation abhängen – „isoliert/reaktiv“ oder „nachhaltig/proaktiv“

1 „Isoliert / Reaktiv“

- Einzelne Maßnahmen werden aufgrund der einzelnen Feststellungen aufgesetzt.
- Feststellungen werden isoliert und individuell behandelt.
- Berechtigungsmanagement wird im wesentlichen als IT-Aufgabe verstanden.

2 „Nachhaltig / proaktiv“

- Ein fehlendes / unzureichendes übergreifendes Management wird als Ursache für eine Vielzahl an Feststellungen erkannt.
- Ein nachhaltiger Ansatz soll jetzige Missstände beheben und Zukünftige verhindern.
- Eindeutige Verantwortlichkeiten (nicht nur in der IT) und eine übergreifende Koordination sind

Vor- / Nachteile

+ Klarer Scope

+ Schnelle Ergebnisse

- Ähnliche Feststellungen in der Zukunft nicht unwahrscheinlich

- Wenige Synergien, ggf. sogar redundante Lösungen

+ Nachhaltige Lösung mit langfristigen Vorteilen

+ Optimalere Ressourcennutzung bzw. Nutzung von Synergien

- Komplexere Projekte

- Längere Zeit bis Ergebnisse sichtbar werden

Die Umsetzung verteilt sich auf Governance-bezogene Aktivitäten einerseits und konkrete Umsetzungen auf Basis des Governance-Modells andererseits.

1 Governance-Aktivitäten*

- Erstellung der BM-Richtlinie(n) inkl. Abgleich mit relevanten Standards und weiteren internen/externen Vorgaben
- Entwicklung der BM-Strategie (abgeleitet aus Business-/ IT-/ Security-Strategie)
- Entwicklung der konzernweit gültigen Standards (Prozessmodell, Kontroll-Framework, BM-Konzept, Templates, etc.)
- Definition der Rollen und Verantwortlichkeiten (strategische / taktische / operative Ebene)
- Entwicklung eines Monitoring-Konzepts zur Überwachung und Bewertung der Wirksamkeit des Berechtigungsmanagements
- Entwicklung der konzernweit gültigen Referenzarchitektur
- Definition der Konzern-Shared Service-Dienste und -BM-Systeme

* Standard-Projekt und –Projektmanagement-Aktivitäten wie IST-Aufnahme, Gap-Analyse. Maßnahmenplan, Meilenstein- und Umsetzungsplanung, etc. werden hier nicht explizit aufgeführt.

Zur Umsetzung sind sowohl fachliche als auch IT-seitige Aktivitäten notwendig

2 Fachliche Aktivitäten*

- Rollout der fachlichen Verantwortlichkeiten
- Umsetzung der BM-Standards (u.a. Berechtigungsdokumentation, Prozesse, SOD-Regeln) und Überprüfung und Bereinigung der Fachanwendungen
- Etablierung BM-Monitoring und Reporting
- Entwicklung von Business-Rollen
- Integration der HR-Daten und –Prozesse
- Effizienzsteigerung und Automatisierung

3 IT-Aktivitäten*

- Aufbau und Bereitstellung der definierten BM Shared Services und -Systeme
- Umsetzung der BM-Standards und Überprüfung & Bereinigung der IT-Infrastruktur
- Etablierung BM-Monitoring und Reporting
- Einschränkung / Überwachung privilegierter Benutzer
- Effizienzsteigerung und Automatisierung

Die Umsetzung beginnt im Regelfall mit einer Pilotphase, um die Governance-Vorgaben zu validieren und Akzeptanz zu gewinnen. Anschließend erfolgt die Umsetzung risiko-orientiert in mehreren Phasen

* Standard-Projekt und –Projektmanagement-Aktivitäten wie IST-Aufnahme, Gap-Analyse. Maßnahmenplan, Meilenstein- und Umsetzungsplanung, etc. werden hier nicht explizit aufgeführt.

KPMG

cutting through complexity

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

KPMG

Martin Wick
Director
Consulting Financial Services
Tel. +49 69 9282-4776
mwick@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft,
a subsidiary of KPMG Europe LLP