In einer zunehmend digitalen Welt ist es für Unternehmen entscheidend, zu kontrollieren, **wer Zugriff auf welche Systeme und Daten** hat. Zwei zentrale Konzepte in diesem Kontext sind **Identity Governance (IG)** und **Access Governance (AG)**. Dieser Artikel erklärt beide Begriffe, zeigt Unterschiede und Gemeinsamkeiten auf und beleuchtet, warum sie unverzichtbar sind.

Was ist Identity Governance?

Identity Governance ist ein Teilbereich des **Identity Access and Governance Management (IAGM auch bekannt als IAM / IGA)**. Sie beschäftigt sich mit der **Verwaltung und Kontrolle digitaler Identitäten** sowie deren Rollen im Unternehmen.

Wichtige Funktionen:

- **Lebenszyklus-Management** Verwaltung von Identitäten über den gesamten Mitarbeiterzyklus (Einstellung, Wechsel, Austritt – JML).
- **Rollenbasierte Zugriffskontrolle (RBAC)** Standardisierte Rollen definieren, welche Funktionen und Zuständigkeiten eine Person im Unternehmen hat und in welcher Abteilung sie arbeitet.**Prozesse für die Beantragung von individuellen Rollenmitgliedschaften** Steuerung und Genehmigung von Rollenmitgliedschaften durch definierte Workflows.
- **Provisionierung & Deprovisionierung** Daraus folgt im IAM die automatische Erstellung und Löschung von Konten sowie Anpassung von Rechten.
- **Zertifizierung & Rezertifizierung** Regelmäßige Überprüfung, ob Identitäten und Rollen noch korrekt und notwendig sind.
- **Segregation of Duties (SoD)** Trennung kritischer Aufgaben und Funktionen, um Machtkonzentrationen und Risiken wie Betrug zu verhindern.
- **Audit & Compliance-Fähigkeit** Dokumentation aller Prozesse zur Einhaltung gesetzlicher Anforderungen wie DSGVO, SOX oder ISO 27001.

Ziel:

„Verwalte Identitäten zentral, nachvollziehbar und regelkonform – mit klaren Rollen, Zertifizierungen und SoD-Prüfungen.“

Was ist Access Governance?

Access Governance konzentriert sich auf das **Management und die Kontrolle von konkreten Zugriffsrechten**. Es geht darum sicherzustellen, dass **nur autorisierte Personen** Zugriff auf bestimmte Systeme und Daten erhalten – und das **nur solange wie nötig**.

Zentrale Aufgaben:

- **Rezertifizierung von Zugriffsrechten** Regelmäßige Überprüfung, ob Berechtigungen noch gerechtfertigt sind.
- **Access-Request-Prozesse** Steuerung und Genehmigung von Rechteanforderungen durch definierte Workflows.
- **Analyse von Zugriffsmustern** Überwachung auffälliger Aktivitäten (z. B. untypische Zugriffe, geographisch ungewöhnliche Anmeldungen).

Ziel:

„Schaffe Transparenz und Kontrolle über bestehende Zugriffe und sorge dafür, dass sie mit Sicherheitsrichtlinien im Einklang stehen.“

Unterschiede & Gemeinsamkeiten

Aspekt	Identity Governance	Access Governance
Fokus	Verwaltung digitaler Identitäten	Kontrolle der Zugriffsrechte
Zentrale Frage	Wer ist die Person im System?	Was darf die Person im System tun?
Beispiele	Rollenvergabe, SoD, Lebenszyklus	Zugriff auf Datei X, System Y prüfen
Verantwortliche	HR, IT, Compliance, Management	IT-Security, Fachbereiche

Beide sind Teil von IAGM und ergänzen sich gegenseitig.

Typische Anwendungsfälle

- **Onboarding**: Neue Mitarbeitende erhalten automatisch passende Rollen und darüber die für ihre Rollen benötigten Berechtigungen.
- **Abteilungswechsel**: Alte Rollen entfallen, neue Rollen werden automatisch zugewiesen.
- **Rechte-Review**: Führungskräfte bestätigen oder entziehen Zugriffe in regelmäßigen Abständen.
- **Individuelle Rollenmitgliedschaften**: Bestellung von individuellen Rollen für

besondere Aufgaben und Zuständigkeiten – diese werden geprüft und dokumentiert.
- **Zugriffsanfrage**: Mitarbeitende beantragen Zugriff – dieser wird geprüft und dokumentiert.

Herausforderungen bei der Einführung

- Qualität der Stammdaten
- Komplexität der IT-Systemlandschaft
- Definition eines sinnvollen Rollenmodells
- Einbindung aller relevanten Abteilungen

Erfolgreiche Projekte benötigen **gute Planung**, **klare Verantwortlichkeiten** und **transparente Prozesse**.

Fazit

Identity Governance und Access Governance sind zwei Seiten derselben Medaille. Sie helfen Unternehmen:

- Identitäten korrekt zu verwalten
- Aufgaben und Zuständigkeiten der Mitarbeitenden und die dafür benötigten Zugriffe transparent und sicher zu steuern
- Compliance-Anforderungen effizient zu erfüllen

In Zeiten von Cloud, Remote Work und Cyberangriffen sind sie kein „Nice-to-have“, sondern ein geschäftskritischer Bestandteil moderner IT-Sicherheit.