PATECCO
dynamic identity systems.

Seit 2009. Hohe Expertise in Identity and Access Management Kompetenz

Dezember 2021

# Wie können Management/Fachabteilung, Audit und IT mithilfe einer gemeinsamen Daten-Basis den Identity Governance-Prozess vereinfachen

## WHITEPAPER

- Ziele eines IGA Projektes
- Herausforderung
- Lösungsvorschlag
- Risikoanalyse mit SVG Access Risk Control

# Table of Contents


1. **Ziele eines IGA Projektes** ..... 3
2. **Herausforderung** ..... 3
3. **Menschen – Prozesse – Technologie** ..... 4
4. **Reduzierung von Sicherheitsrisiken** ..... 5
5. **Lösungsvorschlag** ..... 6
6. **Compliance mit Rezertifizierungskampagnen** ..... 7
7. **Lifecycle von Rollen mit SVG Workflows** ..... 8
8. **Analytics – Risikoanalyse mit SVG Access Risk Control** ..... 8
9. **Fazit** ..... 9

# Wie können Management/Fachabteilung, Audit und IT mithilfe einer gemeinsamen Daten-Basis den Identity Governance-Prozess vereinfachen

Der Bedarf an Governance-Produkten ist zur Normalität großer Organisationen geworden, um Manipulationen von Identitäten und deren Zugriff zu vermeiden.

Unternehmen setzen vermehrt Risikokontrollen ein, z. B. Role Mining, Zertifizierungskampagnen, Berichterstattung, um sowohl interne als auch externe Bedrohungen zu kontrollieren.

Identity and Access Management (IAM) ist ein sehr großer Bereich, der People-Processes und Technologie in Einklang bringen muss. In der Regel erfordert es eine Gruppe von IAM Lösungen, die diese Aufgabe ganzheitlich bewältigen kann. Ein erfolgreiches IAM Projekt erfordert eine sehr enge Zusammenarbeit von der IT-Abteilung und den Fachbereichen, so dass die Identity Governance and Administration (IGA) Anforderungen entsprechend der operationalen Funktionstrennung in den IT-Systemen widergespiegelt werden.

## O Ziele eines IGA Projektes

- Reduzierung der Administration in der IT (Einsparung von Arbeit für Administratoren und Helpdesk)
- Automation der IGA-Prozesse (schnellere Lifecycle-Prozesse, Reconciliation, Verringerung der menschlichen Fehler)
- Reduzierung der Risiken in der IT-Sicherheit (Least Privileged, SoD/SA, eingeschränkter Zugriffskatalog, Passwortrichtlinien)
- Unterstützung der Einhaltung von Gesetzen und Vorschriften (einfache und schnelle Rezertifizierung, Berichte)
- Senkung der Betriebskosten (Auditkosten, Anwendungslizenzen, Zeitersparnis)

## O Herausforderung

Um die Herausforderung besser zu verstehen, sollten wir wissen was Identity Governance and Administration (IGA) bedeutet.

IGA ist eine Reihe von Prozessen und damit verbundenen Rollen und Kontrollen, die von den Prozessverantwortlichen in ihrem jeweiligen Verantwortungsbereich umgesetzt werden müssen.

IGA deckt alles ab, was die geschäftlichen, technischen, rechtlichen und regulatorischen Belange einer Organisation betrifft.

Das bedeutet, die Fachabteilung neben den Anforderungen des Daily-Business auch für die Einhaltung von Gesetzen, Regularien und Compliance wie ISO 27001 sorgen muss.

Ziel ist es, die folgenden Fragen zu beantworten:

- Wissen wer die Person hinter dem Konto1 ist?
- Wissen, warum die Person den Zugriff haben soll?

In diesen Szenarien sollte ein Fachabteilungsleiter/in in die Lage versetzt werden, die IT-Anforderungen zu verstehen.

Auf der anderen Seite muss der IT-Leiter die Geschäftsanforderungen verstehen und die IT für den Endbenutzer einfach gestalten, um sichere und produktive Betriebsabläufe zu gewährleisten.

Die einzige Möglichkeit für Business und IT, dieses gemeinsame Ziel zu erreichen, besteht in der Zusammenarbeit. Der erste Schritt in diesem Fall besteht darin, sich auf ein gemeinsames „Wording" zu einigen, eine Liste von Akronymen und Definitionen, die jeder versteht. 1 Zum Beispiel muss man verstehen, dass es einen enormen Unterschied zwischen einem „Benutzer" und einem „Konto" gibt, oder dass die IT-Rolle „ENPS_GESTSTATI_RILTEC", die für die IT-Abteilung (vielleicht) offensichtlich selbsterklärend ist, für einen CxO, Linienmanager oder Benutzer bedeutungslos ist.

## O **Menschen – Prozesse – Technologie**

Eine IGA-Strategie ist nicht nur eine technische Aufgabe, sondern ein komplexer Entwurf, der sich auch auf die Organisationsstruktur auswirken kann und die Übernahme von Verantwortung durch Menschen erfordert. Um eine sachgerechte Funktionstrennung umzusetzen, benötigt die Organisation mindestens einen Benutzer-, Abteilungs-, Risiko- und Anwendungsmanager mit unterschiedlichen Zuständigkeiten und Aufgabenbereichen, um zu vermeiden, dass eine einzige Person mehrere Rollen und Zuständigkeiten hat, die einfach in SoD-Verletzung laufen können.

Der zweite Schritt besteht darin, dass die Geschäftsprozesse in der IT wieder gespiegelt werden.

Nach 20 Jahren IAM/IGA wurde eine Reihe leistungsfähiger Prozesse definiert, die fast alle IGA-Anwendungsfälle abdecken können und als Standard gelten, wie z. B. Joiner, Mover, Leaver, Rollenerstellung, Rollenänderung, Zugriff Rezertifizierung.

Bei der Definition eines Prozesses ist es wichtig, den Anwendungsbereich von IAM/IGA zu verstehen. Zum Beispiel ist die „Bestellung eines neuen Computers für einen Mitarbeiter/in" ein HR-Prozess, und kein IAM-Prozess. Die gute Nachricht ist, dass IAM ihn auslösen kann. Das heißt, wenn ein Computer vom Lieferanten nicht geliefert wird, könnte der HR-Prozess für den Joiner noch offen sein, aber aus Sicht von IAM ist er bereits abgeschlossen!

Bei der Tool Auswahl ist es wichtig, dass eine möglichst praxisnahe Spiegelung der Prozesslandschaft in der IT umsetzbar ist.

### O **Reduzierung von Sicherheitsrisiken**

- Löschen verwaister Konten
    - Das Konto "könnte" immer noch Zugang zu exponierten Ressourcen haben wie: E-Mail, Webanwendung, Geschäftsräume.
    - Bösartige externe Benutzer können diesen Zugang als Zugang zur Organisation nutzen.
    - Bösartige interne Benutzer können diesen Zugang nutzen, um die persönliche Sicherheitskontrollen und „Verantwortlichkeit" zu umgehen.
    - Standard-Sicherheitsrichtlinien werden einen „korrekt" angelegten Benutzer wahrscheinlich nicht erkennen.

- Durchsetzung zentraler Zugriffsregeln
    - Zugriffskontrollrichtlinien vermeiden eine Korrelation der Bedrohung (Sensitive Access (SA))
    - Vermeidung von Segregation of Duties-Risiken (SoD) durch Zuweisung mehrerer widersprüchlicher Rollen an eine einzige Person.
    - Implementierung von Beantragungsprozessen für Zugriffsberechtigungen.
    - Implementierung von Prozessen zur „Regelmäßigen Rezertifizierung von Zugriffsberechtigungen".

- Einheitliche Zugriffsregeln über Systemgrenzen hinweg
    - Verwaltung von Passwortrichtlinien auf allen Zielsystemen

- Regelmäßige Überprüfung der Regeln, Rezertifizierung
    - Regelmäßige Erstellung von IGA-Berichten.
    - Erweiterte Überwachung durch die Integration mit einem SIEM-System (z.B. QRadar).

## O **Lösungsvorschlag**

Module zur Abdeckung der Use Cases mit der IBM Security Verify Governance (SVG)

*Lifecycle*

- User Management (create, modify, activate)
- Account Management (Accounts and Entitlements Management)
- Provisioning & Reconciliation
- Access Request Workflow & Password Management (User Portal)
- Reporting

*Compliance*

- Access Certification
- Risk Management - SoD, SA

*Analytics*

- Role Mining and Modelling
- Risk Scoring
- Role Lifecycle

## O Compliance mit Rezertifizierungskampagnen

Für Movers werden einige Rollen übertragen und einige werden als Standardrechte hinterlegt. Diese übertragenen Rollen müssen geprüft werden, ob sie in Verbindung mit einer „Visability Violation" Warnung stehen oder für die neue Organisationseinheit eine SA- oder SoD-Risiko erzeugen. Diese Kampagnen können durch ein oder mehr Ebene rezertifiziert werden.

Zertifizierungskampagnen in SVG sind dazu da, Risiken bei Entitäten (Benutzer- oder OU-Zuweisung, Konto, Berechtigungen oder Risiken) zu erkennen und zu reduzieren. Zertifizierungskampagnen können individuell auf den erforderlichen Bedarf angepasst und erweitert werden, z.B. Custom-Rules (Regeln) zur Erkennung von definierten Attributen.

Wenn wir nur die Rezertifizierung des Benutzerzugriffs in den Fokus nehmen, gibt es oft Anforderungen für eine mehrstufige Rezertifizierung. Dies kann mit zwei parallelen Kampagnen und mit definierten Regeln im Datensatz der Zertifizierungskampagne durchgeführt werden.

Eine der neuen Funktionalitäten ist, dass die Komplexität von Zertifizierungskampagnen stark reduziert wird.

Die Lösung liefert standardmäßig Benutzerzuweisungskampagnen. Es wird unterschieden zwischen definierten Hierarchien, Anwendungen oder Berechtigungen wer rezertifizieren soll. Neu ist, dass alle diese Elemente in der Konfiguration der Kampagne sinnvoll kombiniert werden.

Mit einer Option zur Freigabe durch einen Benutzer kann einem Administrator die Möglichkeit gegeben werden, die Überprüfung als Massenoperation zu beenden.

Es gibt noch ein paar weitere Verbesserungen, wie z.B. einen Fortschrittsbalken, der sowohl dem Reviewer als auch dem Supervisor den Fortschritt seiner Kampagnen anzeigt.

Besonders interessant ist neben der mehrstufigen Kampagne die Option, eine Lookup Tabelle mit vordefinierten Optionen für Widerrufe zu erstellen, was wiederum wertvolle Zeit für die Überprüfung der Kampagne spart.

## O Lifecycle von Rollen mit SVG Workflows

Das Modul „Process Designer" administriert alle Prozessschritte, Workflows, Eskalations- und Direktprozesse.

Der Prozess Designer deckt einzelne Prozesse ab, wie z.B. die passive Übersicht über alle Anträge durch Antragsberichte oder die aktive Übersicht über die tägliche Arbeit für eine bestimmte Administratorrolle.

Aktiv und passiv bedeutet in diesem Teil, dass ein Benutzer mit ausstehenden Anträgen interagieren kann, sie genehmigen oder ablehnen kann, während passiv nur einen Überblick über die Antragsdetails bietet. Eine Verbesserung in diesem

Bereich ist die Sortierung von Aufgaben, die einem Administrator hilft, seine Aufgaben mit immer stärkerer Filterung zu finden und zu priorisieren.

Eine weitere Erweiterung ist die Option, ein Antrag aus der passiven Übersicht der Anträge zu stornieren.

Die zweite Art von einstufigen Prozessen sind Eskalationen. Sie decken die Eskalation von nicht rechtzeitig bearbeiteten Anträgen oder von Anträgen mit erkannten Konflikten (SoD/SA) ab, die im Modul „Access Risk Control" (ARC) vordefiniert sind.

**Berechtigungsvergabe für einen User ist ein Prozess, der immer gefragt wird. Komplexe Workflows mit mehrstufigen Genehmigungsprozessen werden in der Lösung entwickelt. Diese müssen auch mögliche risikokritische Punkte erkennen und mindern (SoD/SA).**

Die Workflows hingegen haben wichtige Verbesserungen erhalten, insbesondere bei der Risikokontrolle. Jetzt kann ein Administrator ein Risiko direkt mindern, nachdem SVG es erkannt und gekennzeichnet hat. Dies wird zwar immer noch zur Überprüfung durch das Risiko-Team eskaliert, kann aber eine immer benötigte Zeit reduzieren.

Die häufigste Workflow-Anforderung ist das Hinzufügen oder Entziehen von Benutzerzugriff. Dies ist OOTB aus einem Workflow, der jedoch je nach Anforderung in zwei separate Workflows aufgeteilt werden kann. Die Anforderungen können in Bezug auf die Anzahl der Genehmigungsschritte oder auf die Überwachung dieser Schritte erforderlichen Administratorrollen variieren. So kann beispielweise ein Workflow nur für die Zuweisung von Benutzerzugriff vorgesehen werden, der in der Regel wesentlich komplexer ist als der für den Entzug.

In diesem Prozess ist oft ein Konflikt-Eskalationsschritt erforderlich, der Prozesse in SVG vom aktiven Workflow zum Eskalationsprozess und zurückschaltet, wenn diese Eskalation genehmigt und gemildert wird. Je nach Rollenkonfiguration können zusätzliche Genehmigungsschritte für Benutzermanager, Anwendungs- oder Berechtigungseigner erforderlich sein.

All dies wird standardmäßig zur Verfügung gestellt und erfordert keine Anpassungen, was natürlich über die Prozessdesigner Rule Engine möglich ist.

### O Analytics – Risikoanalyse mit SVG Access Risk Control

Informationen, die aus verschiedenen Quellen kommen, bergen verschiedene Risiken, die bearbeitet und unter Kontrolle gebracht werden müssen.

Die Analyse von zwei Arten von Risiken (SoD und SA) ist ein starkes Tool von SVG. Das Risiko-Management-Team, kann seine vorbereiteten Risiko-Daten, z.B. Risiko-Tabellen importieren, die das Modul „Access Risk Control" (ARC) zur Analyse der Berechtigungen verwendet.

Die Übersetzten Daten sind für die Fachbereichsleiter in einem verständlichen Format, was ein wesentlicher Vorteil von SVG ist.

Die importierten Prozessschritte (Business Activities (BA)) werden in einer Risikomatrix in der Lösung abgebildet. Sie entsprechen genau der Risikomatrix des Risikomanagements. Die Prozessschritte werden den konkreten Systemberechtigungen auf unterster Ebene zugeordnet und in der Kombination auf Risiken analysiert.

Damit muss das System Informationen zur Risikominderung für bestimmte Gruppierungen von Geschäftsaktivitäten vorhalten, um eine automatische Risikoerkennung anzuzeigen.

Nach der Synchronisierung all dieser Informationen für den aktiven Konfigurationssatz beginnt SVG mit der Analyse der definierten Risiken und zeigt Flaggen für alle Benutzer oder Rollen an, die widersprüchliche Berechtigungen enthalten.

Diese Analysen laufen immer im Hintergrund und zeigen die aktuelle Situation bei jeder generierten Anfrage oder erstellten Rolle. Auf diese Weise wird für jede Anfrage/Rolle eine vordefinierte Flagge angezeigt, die vom Schweregrad des Risikos abhängt, das gemindert werden muss.

## O **Fazit**

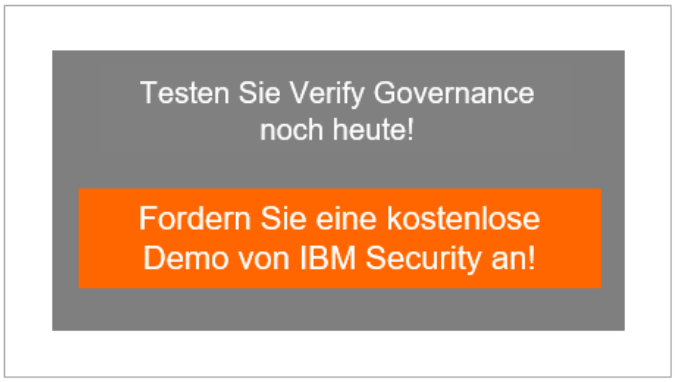
Compliance- und Corporate-Governance sind nach wie vor die Haupttreiber für IGA- und IAM-Projekte. Die Nachverfolgung des Benutzerzugriffs, der Genehmigungen durch das Management, der Risiken und der Dokumentation, wer wann auf welche Daten zugegriffen hat, ist ein wichtiger Bestandteil der Einhaltung gesetzlicher Vorschriften und kann einen reibungsloseren Audit-Prozess gewährleisten.

IBM Security Verify Governance (SVG) ist eine leistungsstarke IGA-Lösung, die die Einhaltung gesetzlicher Vorschriften unterstützt. SVG automatisiert die Audit-Berichterstattung und vereinfacht die Prozesse zur Einhaltung von Vorschriften.

Effizienz, Sicherheit und Compliance sind wichtige Schlüssel für das Identitäts- und Zugriffsmanagement. Die Vorteile einer starken IGA-Lösung liegen auf der Hand. Die Komplexität von IGA-Projekten und die Kosten der Implementierung können leicht unterschätzt werden und die Organisation aus dem Konzept bringen. Eine robuste IGA-Lösung schafft Effizienz in den Abläufen der Organisation in Form von automatisierte Provisionierung und De-Provisionierung.

Die Benutzerproduktivität wird stark verbessert, während gleichzeitige Kosten gesenkt werden. Die Belastung für die IT wird verringert und das Unternehmen wird mit umfassenden Daten versorgt, die bei der Einhaltung gesetzlicher Vorschriften helfen.

Wenn Sie mehr darüber erfahren möchten, wie Ihr Unternehmen mit IBM Security Verify Governance von Lifecycle Management, Compliance und Analytics profitiert, lesen Sie den folgenden Bericht und fordern Sie jetzt die IBM Security Verify Governance DEMO an über den https://www.ibm.com/de-de/products/verify-governance Link oder klicken Sie auf das Bild unten.




Unsere IAM Experten Beraten Sie gern in einem ersten Gespräch, welche Faktoren zu berücksichtigen sind, damit ihr IAM Projekt erfolgreich umgesetzt werden kann.

Rufen Sie noch heute an und vereinbaren Ihren ersten Beratungstermin gratis mit uns!

Melden Sie sich bitte bei uns:

72 Ringstrasse; 44627 Herne, Germany,

+49 (0) 23 23 987 97 96; info@patecco.com www.patecco.com