# INTELLIGENTE ACCESS GOVERNANCE & BENUTZERVERWALTUNG

## DEN RICHTIGEN WERKZEUGKASTEN FINDEN

Die erste Einführung eines Identity and Access Management Systems (IAM) ist für die meisten Unternehmen ein von technischen Ansätzen und Lösungen geprägtes Unterfangen: IT-Prozesse werden angepasst, Anwendungssysteme an eine zentrale Datendrehscheibe angebunden, Schnittstellen erstellt und das neue IAM-System durch weniger große oder umfassendere Anpassungsarbeiten auf die Bedürfnisse des Kunden zugeschnitten. Erst eine solche technisch funktionsfähige IAM-Lösung stellt die Voraussetzung dar, sich den bestehenden erweiterten fachlichen Anforderungen an das IAM zu widmen. Identity and Access Governance (IAG) beschäftigt sich als Teilgebiet des IAMs mit der fortlaufenden Prüfung, Optimierung, Bereinigung und Kontrolle von Anwendungsberechtigungen und Unternehmensrollen über die Mitarbeiter, Kunden oder Lieferanten Zugriff auf interne oder cloudbasierte Anwendungssysteme erhalten. Es stellt durch geeignete Maßnahmen die Einhaltung von globalen oder unternehmensspezifischen Richtlinien mit Hilfe von beispielsweise regelmäßigen Berechtigungsprüfungen (Rezertifizierungen/Attestierungen), Segregation of Duty (SoD) Regeln oder Qualitätsstandards für Stammdaten von Mitarbeitern, Berechtigungen und Geschäftsrollen sicher.

IN DER PRAXIS ZEIGT SICH IMMER MEHR, WIE WICHTIG EINE GUT FUNKTIONIERENDE KOMBINATION AUS ANALYSEVERFAHREN UND VERSTÄNDLICHER ERGEBNISAUFBEREITUNG FÜR FACHBEREICHE IN UNTERNEHMEN IST.

Dr. Ludwig Fuchs, Geschäftsführer, Nexis GmbH, www.nexis-secure.com

Während IAG meist wenig Beachtung beim initialen Aufbau von IAM-Systemen erfährt, erlangt es später im Betrieb hohe Relevanz bei der Erfüllung verschiedenener externer Anforderungen (SOX, Basel III, ISO 27001) oder auch industriespezifischer sowie interner Qualitätsstandards. Ohne eine transparente, verständlich bedienbare, audit-sichere und regulierende Steuerzentrale, ist es für Unternehmen schwer, Sicherheitsrisiken im IAM unter Kontrolle zu halten und gleichzeitig die Qualität im Berechtigungsmanagement fortlaufend zu erhöhen. Ohne die klare Definition und der technischen Durchsetzung eines Regelwerks für die Vergabe, den Entzug und die Kombinatorik von Zugriffsrechten, werden Fehlern und Sicherheitslücken unnötige Spielräume gewährt.

### Die Probleme in der Praxis

Viele Unternehmen klagen über eine hohe Komplexität und Intransparenz ihrer Berechtigungsstrukturen. Trotz des Einsatzes von zentralen IAM-Tools erkennen Firmen immer mehr, dass IAG nicht mit einem ausschließlich technischen Ansatz gelöst

werden kann. Einerseits ist es aufgrund des stetigen Wandels von fachlichen Prozessen und Organisationsstrukturen händisch unmöglich, Berechtigungsstrukturen bestehend aus vielen tausenden von Berechtigungsobjekten, fortlaufend zu kontrollieren und deren korrekten Zustand aufrecht zu erhalten. Gleichzeitig sind die IT-Abteilungen auf den Input von Fachabteilungen ohne technischen Hintergrund angewiesen. Komplexe Benutzerschnittstellen und unverständliche Informationen behindern die Kommunikation zwischen den verschiedenen Beteiligten – und lassen IAM und IAG zu einer ungeliebten Aufgabe werden.

Ohne Tool-Support müssten die richtigen Daten und Informationen aus den verschiedenen Daten-Silos manuell aufbereitet, überarbeitet und dann in den Fachbereichen präsentiert und diskutiert werden. Daneben entstehen permanent neue Herausforderungen durch den technologischen Fortschritt. Beispiele hierfür sind die strukturierte Erhebung und Pflege der Verantwortlichkeiten für Berechtigungen und Geschäftsrollen (On-premises und in Cloud-Applikationen), die anwendungsübergreifende Prüfung von Richtlinienverletzungen oder die fachlich verständliche Bereinigung oder Rezertifizierung von IAM-Daten in einer immer stärker von der fortschreitenden Adaption cloudbasierter Services geprägten Systemlandschaft.

## Theorie & Praxis

Die notwendige Datengrundlage für erfolgreiches IAG haben die meisten Unternehmen mit der technischen Einführung eines IAM-Systems bereits geschaffen. In der Praxis setzt sich jedoch immer mehr das Verständnis durch, dass eine erfolgreiche fachliche Umsetzung von IAG nur durch intelligente und dezentral einsetzbare Werkzeuge mit starkem Fokus auf die User Experience zum Einbeziehen der Fachabteilungen sichergestellt werden kann. Im Idealfall sorgt dies gleichzeitig auch für eine hohe Transparenz beziehungsweise durchgängige Nachvollziehbarkeit und erlaubt die Delegation von IAG-Tätigkeiten (etwa der Kontrolle von Prüfergebnissen, die Modellierung von neuen Berechtigungen oder das Nacharbeiten von bestehenden Geschäftsrollen) in Richtung der Fachbereiche.

## Der Werkzeugkasten: Das brauchen Unternehmen wirklich!

### a) Das Regelwerk

Der erste Schritt vor einer fortlaufenden Kontrolle und korrekten Abbildung von Berechtigungen ist die Erhebung, Modellierung und Freigabe eines gültigen Satzes von IAG-Regeln. Das kann von der einfachen Abbildung einer SoD-Matrix über die Hinterlegung von Mindestqualitätskriterien für Personalstammdaten oder Berechtigungen bis hin zu Modellrestriktionen (zum Beispiel: Einschränkungen zu erlaubten Verknüpfungen von Berechtigungen und Geschäftsrollen) oder Kritikalitätsrichtlinien (zum Beispiel: Keine Geschäftsrolle darf eine geringere Kritikalität aufweisen, als die in ihr enthaltenen Berechtigungen) reichen. Eine passende Lösung muss es ermöglichen, alle relevanten Regeln ohne Anpassungen nativ umsetzen, kontrollieren und berichten zu können. Außerdem muss sie mit kollaborativen Funktionen den Aufbau und das Lifecycle-Management der Regelwerke selbst abbilden – von der Modellierung, Freigabe und Produktivsetzung einer Regel bis hin zu deren audit-gesicherten und nachvoll-


**Bild 1:** Der IAG-Werkzeugkasten von NEXIS Controle.

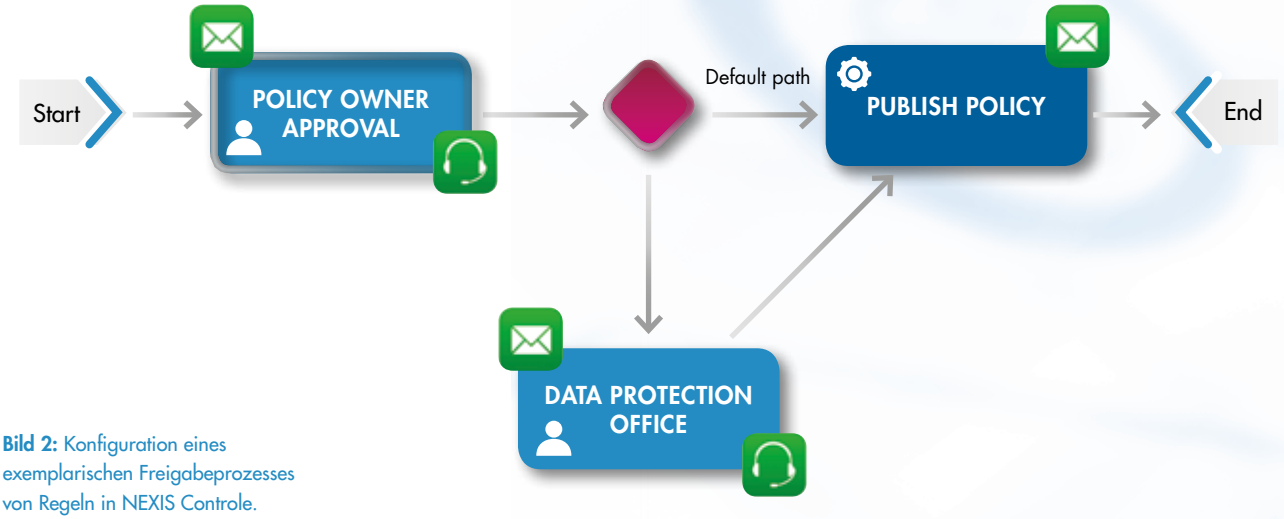


**Bild 2:** Konfiguration eines exemplarischen Freigabeprozesses von Regeln in NEXIS Controle.

ziehbaren Änderung oder sogar Löschung bei Wegfall der Bedingung.

### b) Standard-Workflows

Nach der Erkennung von Regelverletzungen oder fehlerhaft modellierten Berechtigungen benötigen Unternehmen eingebettete Standard-Mechanismen zur weiteren Behandlung der Ergebnisse. Insbesondere im Falle eines Regelverstoßes ist nicht alleine die Identifikation eines Verstoßes wichtig, sondern dessen Behandlung durch Korrektur oder Mitigation. Moderne Tools wie die Software NEXIS Controle unterstützen hier mit Workflow-Systemen, die nicht nur Konflikte automatisiert oder bedarfsbezogen erkennen, sondern auch die jeweiligen Verletzungen an die richtige Stelle dirigieren. Solche auf Kundenbedürfnisse zugeschnittene, erprobte und fertig verfügbare Best Practice Workflows bieten meist eine wesentlich einfachere und schnellere Konfiguration als generische und oftmals mit Programmieraufwand verbundene Workflow-Systeme.

### c) Schnelle Konfigurierbarkeit

In der Praxis sehen Unternehmen immer mehr Schwierigkeiten bei einem zu hohen Grad an Customizing der eingesetzten technischen IAG-Lösung. Eine zentrale Anforderung ist die Konfigurierbarkeit von Workflows, Regeln und analytischen Funktionen ohne Anpassungen auf Code-Ebene. Vor allem im Rahmen der Kommunikation mit Fachbereichen muss für jede Stakeholder-Gruppe (Regelverantwortlicher, Abteilungsleiter, Rollenverantwortlicher, Governance-Team, …) eine möglichst passende, eigene Darstellung von Ergebnissen erfolgen: Während Abteilungsleiter mit kompakten Informationen schnell eine Entscheidung treffen können müssen, wollen Mitglieder einer Compliance Task-Force oder der internen Revision umfassende Auswertungsfunktionen im Rahmen des gleichen Workflows. Mit wenigen Klicks müssen Ansichten und Voreinstellungen für die jeweiligen Empfänger vorbereitet werden, so dass Anwendbarkeit und Akzeptanz gesichert sind. Diese Akzeptanz ist für die Beteiligung und Lösung von Regelkonflikten, aber auch für alle weiteren IAM-Aktivitäten wie Rezertifizierungen, Rollenmodellierung, Bereinigungsaktionen oder Freigaben von essenzieller Bedeutung. Unternehmen berichten hier häufig von Hürden durch technisch vorgegebene und starre Einstellungen, die für Verwirrung oder Unverständnis bei den jeweiligen involvierten Fachbereichen sorgen. Die Wahl eines flexiblen, einfach anzupassenden, aber trotzdem leistungsstarken IAG-Systems schafft hier Abhilfe.

DIE WAHL DER RICHTIGEN IAG-WERKZEUGE UND DEREN KONSEQUENTER EINSATZ STELLEN NEBEN DER ORGANISATORISCHEN VERANKERUNG DEN WICHTIGSTEN ERFOLGSFAKTOR FÜR IAG DAR.

Dr. Michael Kunz, Head of Professional Services, Nexis GmbH, www.nexis-secure.com

### d) Einfachheit für Fachbereiche

Besonders IT-fremde Fachbereiche und Stakeholder empfinden IAG oft als lästige Herausforderung. Halbjährliche Reviews von hunderten von Berechtigungen, die Modellierung von Rollen oder die Korrektur von Regelverletzungen kann meist nur mit Unterstützung der IT-Abteilung erfolgen. Moderne IAG-Lö-

sungen müssen sich an aktuellen Standards für die Usability von Software orientieren und das gesamte Spektrum von umfassenden Analyseoptionen und Modellierungsfunktionalitäten für die IT-Experten bis hin zu einer einfachen Darstellung technischer Sachverhalte für nicht-IT Personal abdecken. Hierfür spielt vor allem die Nutzung geeigneter Visualisierungstechniken eine entscheidende Rolle. NEXIS Controle bietet beispielsweise mehr als 25 verschiedene matrix- und tabellenbasierte Visualisierungen an, die sowohl in der IT-Abteilung Transparenz über alle Daten und deren Strukturen schaffen als auch im Fachbereich schnelle Entscheidungs- und Vergleichsmöglichkeiten erlauben. Einerseits erhöht sich dadurch die Bereitschaft zur Mitarbeit, andererseits kann das IAM-Team den Geschäftsverantwortlichen so eine Plattform bieten, in der sich Wissensträger jederzeit über die aktuelle Situation in Ihrem Bereich informieren und auf mögliche Missstände hingewiesen werden können. Moderne IAG-Lösungen wie die Software NEXIS Controle bieten die freie Konfigurierbarkeit und Bereitstellung der notwendigen Ansichten im Tool für die jeweiligen Stakeholder, die schnelle Einschränkbarkeit der nutzbaren Funktionen und ein integriertes Hilfesystem für Fachbereiche pro Aufgabenschritt. Davon profitieren in der Praxis auch die IT-Abteilungen in einem großen Maße, da die Anzahl von Hilfeanfragen aus den Fachbereichen (etwa während unternehmensweiten Rezertifizierungen) deutlich sinkt.

## Resümee

Generell zeigt sich, dass moderne Software-Lösungen Identity and Access Governance intelligenter und damit schneller und umfassender einsetzbar machen. An dieser Stelle sei darauf hingewiesen, dass technische Lösungen jedoch immer auf die Erhebung oder das Vorliegen von eindeutigen organisatorischen Regelwerken und Zielen angewiesen sind. Sie stellen den Werkzeugkasten für die Automatisierung und die optimale Einbindung von Fachbereichen bereit und beschleunigen damit die Bewältigung der immer größer werdenden Herausforderungen im IAG-Bereich. Klare Projektstrukturen, konkrete Anforderungserhebungen und eine realistische Zeitplanung sind jedoch die unerlässliche Basis, um vom Softwareangebot profitieren zu können. NEXIS Controle als Lösung unterstützt neben der technischen Umsetzung von IAG-Funktionalitäten aus diesem Grund auch bewusst die organisatorische Komponente mit verlässlichen Analysen und datenbezogenen Aussagen, so dass schon vor dem technischen Einsatz im operativen Betrieb die Rahmenbedingungen schnell und zielgerichtet geklärt werden können. IAG entwickelt sich aktuell zu einem der wichtigsten Themen im globalen IAM-Markt, weshalb der Zeitpunkt gerade günstig ist, sich schon jetzt für die zukünftigen Herausforderungen zu wappnen.

***Dr. Ludwig Fuchs, Dr. Michael Kunz***

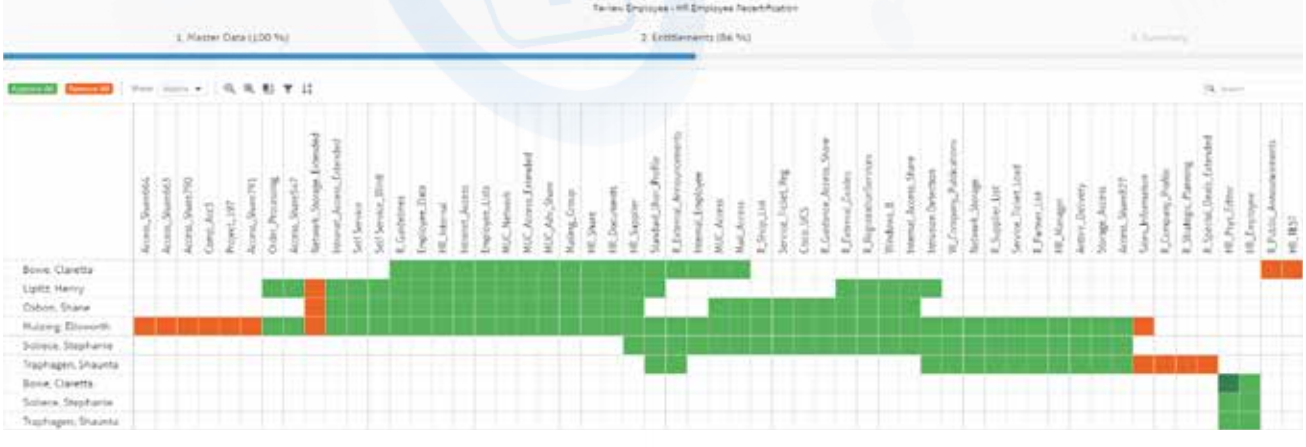

**Bild 3:** Matrix-basiertes Access Review durch den Fachbereich.