

the  
**GORILLA**  
**GUIDE**<sup>®</sup> to...



# Modern Identity Governance and Administration

**ED TITTEL**



POWERED BY  **ActualTech**  
MEDIA

the  
**GORILLA**  
**GUIDE**<sup>®</sup> to...



# Modern Identity Governance and Administration

By Ed Tittel

POWERED BY  **ActualTech**  
MEDIA

Copyright © 2024 by Future US LLC  
Full 7th Floor  
130 West 42nd Street  
New York, NY 10036

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

[www.actualtechmedia.com](http://www.actualtechmedia.com)

---

## **PUBLISHER'S ACKNOWLEDGEMENTS**

### **DIRECTOR OF CONTENT DELIVERY**

Wendy Hernandez

### **GRAPHIC DESIGNER**

Sam Richwood

### **HEAD OF SMARTSTUDIO**

Katie Mohr

### **WITH SPECIAL CONTRIBUTIONS FROM IDIRA**

Cassidy Hines

IDENTITY SECURITY CAMPAIGN  
MANAGER

Tricia Peck

SENIOR PRODUCT MARKETING  
MANAGER

# ENTERING THE JUNGLE

- Introduction: Modern Identity Governance and Administration, Express Edition** ..... **7**
  
- Chapter 1: Modern IGA Explored & Explained** ..... **11**
  - Visibility Across Hybrid Environments ..... 11
  - Lifecycle Management and Access Certification Reviews ..... 12
  - Continuous Compliance and Audit Readiness ..... 12
  - Deep Integration with Business Ecosystems ..... 13
  - Centralized Risk and Policy Engine ..... 13
  - Support for Digital Transformation and Zero Trust ..... 14
  - Connecting IGA, AM, and PAM: A Unified Platform ..... 14
  
- Chapter 2: How IGA Supports Security and Compliance** ..... **16**
  - Enabling Continuous Compliance ..... 16
  - Achieving Audit Readiness ..... 17
  - Centralized Risk and Policy Engine ..... 17
  - Reducing Audit Risk and Manual Effort ..... 18
  - Supporting a Culture of Security and Compliance ..... 18
  
- Chapter 3: Integration and Automation** ..... **20**
  - Integrating with Authoritative Identity Sources ..... 20
  - Automation of Identity Events ..... 21
  - Integration with Security Ecosystems ..... 22
  - Reducing Operational Overhead ..... 22
  - Supporting Business Agility and Innovation ..... 24

<b>Chapter 4: A Modern IGA Operating Model</b> .....	<b>26</b>
Ownership in Modern IGA: Roles and Responsibilities .....	27
Automation vs. Exception Governance: What Gets Automated and Why .....	29
How Modern Workflows Replace Legacy Ticket-Based Models .....	30
How Visibility and Accountability Improve Without Adding Friction .....	31
Moving Toward Flexible, Policy-Driven Approaches .....	32
Best Practices Boost Business Outcomes .....	35
<b>Chapter 5: Modern IGA Creates Business and Accelerates Revenue</b> .....	<b>37</b>
Standardizing Identity Governance Across Modern Architectures .....	38
Increased Security Posture, Better Ops Efficiency .....	38
Enabling Zero Trust Security .....	39
Accelerating Innovation Without Compromising Security .....	40
Driving Business Value Through Identity Governance .....	41

# CALLOUTS USED IN THIS BOOK



## SCHOOL HOUSE

In this callout, you'll gain insight into topics that may be outside the main subject but are still important.



## FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.



## BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.



## DEEP DIVE

Takes you into the deep, dark depths of a particular topic.



## EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.



### DEFINITION

Defines a word, phrase, or concept.



### GPS

We'll help you navigate your knowledge to the right place.



### KNOWLEDGE CHECK

Tests your knowledge of what you've read.



### WATCH OUT!

Make sure you read this so you don't make a critical error!



### PAY ATTENTION

We want to make sure you see this!



### TIP

A helpful piece of advice based on what you've read.

## INTRODUCTION

# Modern Identity Governance and Administration, Express Edition

**Welcome to The Gorilla Guide® To... Modern Identity Governance and Administration.** In the chapters ahead, we begin by exploring the critical importance of modern Identity Governance and Administration (IGA), emphasizing its role in unifying, automating, and strengthening your security posture. Indeed, modern IGA operates best as a continuous governance control plane—one that maintains authoritative visibility into identities, entitlements, and access paths across SaaS, cloud, on-premises, and in all privileged environments. Without such a control plane, organizations cannot enforce least privilege, prove audit completeness, nor safely adopt Zero Standing Privilege at scale.

In this Gorilla Guide, Chapter 1 delves into the foundations of modern IGA (access certification and lifecycle management) providing clear explanations of its capabilities and strategic value for overall identity visibility and governance. Subsequent chapters examine the core principles and imperatives for security and compliance, integration, and automation strategies that streamline processes. They also explain and explore how IGA provides core security and IAM functions that serve to unify and secure an organization. Indeed, IGA brings key business functions together—including IAM, compliance,

security, and helpdesk teams that manage access. Because identity is the new security perimeter for organizations, a strong IGA program helps to maintain security and to enforce the principle of least privilege across the entire identity lifecycle.

In today's digital era, where organizations operate across complex, hybrid environments and face relentless cyber threats, the need for robust IGA has never been more paramount. Security and IT executives are tasked with safeguarding sensitive data, ensuring regulatory compliance, and supporting relentless innovation—all while managing a landscape of users, applications, and access rights that is exploding, with huge numbers and types of identities involved. The traditional approaches to identity governance, often fragmented and manual, are simply inadequate to address the velocity and sophistication of modern risks. As digital transformation accelerates, so too does the challenge of governing identities consistently across cloud, SaaS, and on-premises systems.

Modern IGA stands as the strategic control pane organizations require to unify, automate, and elevate an organization's security posture. At its core, IGA is not merely a compliance checkbox or an operational necessity; it is a foundational enabler of business agility, resilience, and trust. By establishing a single authoritative layer to manage identities and access—regardless of where they reside—organizations can enforce consistent policies, apply effective automation, reduce risk exposure, and streamline operations. This unified approach is essential for maintaining visibility and control in an environment where users, devices, and resources are continually proliferating.

The challenges in identity governance are multifaceted and persistent. Organizations grapple with privilege creep as roles change, struggle with onboarding and offboarding inefficiencies, and face mounting pressure to prove compliance with a growing array of regulations. Manual processes and disconnected systems leave gaps that attackers can exploit, resulting in data breaches, audit failures, and

reputational damage. Indeed, when access reviews are manual and lifecycle management likewise, teams get overwhelmed with tickets and backlogs grow large. Furthermore, as organizations embrace cloud migration, SaaS adoption, and remote work, the complexity of managing access across disparate environments intensifies.

Modern IGA addresses these challenges through a comprehensive suite of capabilities designed for today's dynamic enterprise. It unifies governance across all identity sources, automates lifecycle management, and integrates deeply with business-critical systems such as HR, IT Service Management (ITSM), and security platforms. With real-time visibility, automated evidence collection, and adaptive controls, modern IGA delivers continuous monitoring, access controls, and compliance and audit readiness—dramatically reducing manual effort and identity-related risk. It also integrates IGA and Privileged Access Management (PAM), ensuring that both privileged and non-privileged accounts are governed with equal rigor.

The strategic benefits of modern IGA extend beyond security and compliance to operational efficiency, cost savings, and even employee satisfaction. Automation of identity events, such as hires, moves, and terminations, reduces operational overhead and improves the user experience. In fact, using AI to reduce effort allows teams to move faster and focus on more strategic initiatives. This in turn accelerates digital transformation and enables the business to more quickly and securely adopt new technologies/initiatives. Likewise, a centralized risk and policy engine enables organizations to detect toxic combinations, enforce least privilege, and apply adaptive controls based on context, behavior, and regulatory requirements.

As you navigate the evolving landscape of IAM tools, consider the value that a modern IGA platform can provide in enabling a unified, automated and adaptive approach to defining, granting, managing, and certifying access. Modern IGA is not just a technology investment—it's a strategic imperative to protect your organization's most critical assets, and provides a proactive foundation for a resilient

and capable security regime. With these things in mind, let's move onto Chapter 1, in which we'll investigate modern IGA in more detail, and explain what makes it important and different from its legacy predecessors.

## CHAPTER 1

# Modern IGA Explored & Explained

**At the heart of modern Identity Governance and Administration (IGA) lies a commitment to using governance as the backbone of a strong identity security posture with continuous visibility across your entire identity estate.** In turn, this rests on establishing correct policy, automating lifecycle management, and delivering continuous compliance across the enterprise.

These core principles form the foundation upon which organizations can build a resilient and scalable identity framework, capable of adapting to evolving threats and business needs.

## Visibility Across Hybrid Environments

Modern IGA delivers a strategic control pane for security, compliance, and digital transformation by providing end-to-end visibility and identity governance across cloud, SaaS, and on-premises systems. This provides organizations with a single authoritative layer, enabling consistent enforcement of access, security, and compliance policies everywhere. By centralizing and consolidating identity data,

organizations gain comprehensive visibility over who has access to what, reducing the risk of unauthorized access and privilege escalation. This consolidation is especially critical as enterprises adopt multi-cloud strategies and expand their digital footprint.

## **Lifecycle Management and Access Certification Reviews**



Automation is a cornerstone of modern IGA, ensuring that users always have the right access at the right time. Idira IGA automates lifecycle events such as joiner, mover, and leaver changes, using AI-driven access recommendations and streamlined provisioning workflows. Access certification reviews are automated and replace manual spreadsheets with AI-assisted reviews that generate comprehensive, audit-ready evidence packages. Continuous entitlement visibility helps identify and prevent high-risk access, orphan accounts, and segregation of duties violations.

End-to-end lifecycle management accelerates onboarding, reduces friction for users, and eliminates privilege creep—a frequent consequence of manual processes and role changes. Automated provisioning and deprovisioning streamline the management of identities as employees join, move within, or leave the organization. This not only enhances security but also improves operational efficiency, freeing IT teams to focus on higher-value initiatives.

## **Continuous Compliance and Audit Readiness**



Modern IGA is designed to deliver continuous compliance and audit readiness. Real-time monitoring, automated evidence collection, and complete audit trails dramatically reduce manual effort and improve

audit completeness and accuracy. Organizations can demonstrate compliance with internal policies and external regulations, such as NIST, GDPR, HIPAA, NYDFS, and Sarbanes–Oxley (SOX), with confidence and ease. The ability to quickly generate audit reports and respond to regulatory inquiries is vital for maintaining trust and avoiding costly penalties.

## **Deep Integration with Business Ecosystems**

---

A modern IGA solution must integrate deeply with key business systems, including HR, ITSM, and security platforms. To manage identity consistently across all platforms, all applications where users have accounts should also be integrated. Such integrations transform identity events—such as hires, moves, and terminations—into automated, policy-driven actions that strengthen governance and reduce operational overhead. By connecting with authoritative sources of identity and business context, organizations can ensure that access decisions are always aligned with current roles and responsibilities. This is what enables IGA to provide identity management across the entire lifecycle, to properly handle joiners, movers, and leavers within the overall ecosystem.

## **Centralized Risk and Policy Engine**

---

A centralized risk and policy engine enables organizations to detect toxic combinations, enforce least privilege, and apply adaptive controls based on context, behavior, and regulatory requirements. This engine acts as the nerve center of modern IGA, continuously evaluating access requests against defined policies and risk signals.

Adaptive controls allow organizations to dynamically adjust access based on changing risk conditions, supporting both security and business agility.

## **Support for Digital Transformation and Zero Trust**

---

Modern IGA supports digital transformation by standardizing identity governance across contemporary architectures, including SaaS adoption, cloud migration, and Zero Trust initiatives. By providing a consistent governance framework, IGA empowers organizations to innovate rapidly without compromising on security or compliance. The adoption of Zero Trust principles—where trust is never assumed, and access is continuously verified—further underscores the importance of robust identity governance in today’s threat landscape.

## **Connecting IGA, AM, and PAM: A Unified Platform**

---

Finally, modern IGA acts as the connective tissue between the core IAM functions of Identity Governance and Administration, Access Management, and Privileged Access Management. This holistic approach to access governance strengthens the overall security posture and reduces the likelihood of privilege abuse. It also eliminates silos among vendors or tools, and provides a holistic view into and control over the identity landscape. Thus, modern IGA extends well beyond governance of privilege, to include all aspects of identity within an organization.

In summary, the core principles of modern IGA—governance, automation, continuous compliance, deep integration, centralized policy management, and support for digital transformation—provide a comprehensive framework for addressing the challenges of today’s identity landscape. These principles are essential for building a resilient, agile, and compliant organization. In the next chapter we’ll explain how to put these principles into practice to help manage identity including IGA, PAM, and access management under a single consistent, identity security platform.

## CHAPTER 2

# How IGA Supports Security and Compliance

**Security and compliance are the twin pillars upon which successful identity governance programs are built.** As organizations face an ever-expanding regulatory landscape and increasingly sophisticated cyber threats, the ability to maintain continuous compliance and audit readiness is critical. Modern IGA provides the tools and processes required to achieve these objectives, ensuring that organizations can always demonstrate control over access to sensitive data and systems.

## Enabling Continuous Compliance

Continuous compliance is no longer a luxury—it is a necessity for organizations operating in regulated industries or handling sensitive information. Modern IGA delivers continuous compliance through real-time monitoring, automated policy enforcement, and proactive risk management. By continuously evaluating access rights and user activity against defined policies, organizations can identify and remediate policy violations before they escalate into security incidents or audit findings.

Automated evidence collection is another key capability, reducing the manual burden associated with audit preparation and regulatory reporting. IGA solutions can generate comprehensive audit trails, capturing all access decisions, policy changes, and user activity in a centralized repository. This not only streamlines the audit process but also provides a defensible record of compliance for regulators and auditors.

## Achieving Audit Readiness

---

Audit readiness is an ongoing process, not a point-in-time event. Modern IGA equips organizations with the ability to maintain a state of perpetual audit readiness, minimizing the disruption and resource drain typically associated with external audits. Automated controls and reporting capabilities enable organizations to quickly produce evidence of compliance, respond to audit inquiries, and address findings in a timely manner.

The integration of automated controls with business processes ensures that compliance is embedded into day-to-day operations, rather than being an afterthought. This proactive approach reduces the risk of audit failures and the associated financial and reputational consequences.

## Centralized Risk and Policy Engine

---

A centralized risk and policy engine is essential for managing access risk in a dynamic environment. This engine continuously evaluates access requests, user behavior, and environmental context to detect and mitigate risks in real time. By enforcing least privilege and

identifying toxic combinations of access rights, organizations can prevent the accumulation of excessive or conflicting privileges that could be exploited by malicious actors.

Adaptive controls further enhance risk management by allowing organizations to adjust access dynamically based on changing risk signals. For example, access to sensitive data may require additional authentication or approval when risk conditions are elevated. This flexibility supports both robust security and business agility.

## **Reducing Audit Risk and Manual Effort**



One of the most significant benefits of modern IGA is the reduction of audit risk and manual effort. Automated workflows, policy enforcement, and evidence collection minimize the potential for human error and oversight. Organizations can confidently demonstrate compliance with regulatory requirements, internal policies, and industry standards, reducing the likelihood of audit findings and penalties.

In addition, modern IGA provides comprehensive visibility into access rights and user activity, enabling organizations to quickly identify and address anomalies or policy violations. This visibility is critical for maintaining control over access to sensitive systems and data in an increasingly complex threat environment.

## **Supporting a Culture of Security and Compliance**



Finally, modern IGA supports a culture of security and compliance by embedding these principles into the fabric of the organization. Automated controls, continuous monitoring, and real-time reporting

empower security and IT teams to maintain oversight and control without impeding business operations. This balance between security and agility is essential for supporting innovation while managing risk.

In conclusion, modern IGA provides the foundation for achieving continuous compliance, audit readiness, and effective risk management. By automating controls, centralizing policy enforcement, and delivering real-time visibility, IGA enables organizations to navigate the complexities of today's regulatory and threat landscape with confidence and agility. In the next chapter, you'll learn how modern IGA works for key stakeholders to foster business innovation and agility, and how to steer through the processes and cultural changes that adoption and implementation of modern IGA can—and should—bring to your organization.

## CHAPTER 3

# Integration and Automation

**Integration and automation are critical enablers of effective identity governance in today's interconnected enterprise.** Modern IGA solutions are designed to integrate deeply with authoritative sources of identity and business context, such as Human Resources (HR) systems, IT Service Management (ITSM) platforms, and security ecosystems, as well as any other applications that involve using logins and identity. These integrations transform identity events into automated, policy-driven actions that strengthen governance, reduce operational overhead, and support business agility.

## Integrating with Authoritative Identity Sources



A modern IGA platform must connect seamlessly with HR systems, which are typically the authoritative source of employee identity and status. By integrating with HR, IGA solutions can automatically trigger provisioning, deprovisioning, and access changes based on lifecycle events such as hires, transfers, and terminations. This

ensures that users have appropriate access from day one and that access is promptly revoked when no longer needed, reducing the risk of orphaned accounts and privilege creep.

ITSM platforms are another critical integration point, as they manage service requests, incidents, and changes across the organization. By connecting IGA with ITSM, and orchestrating workflows to match, organizations can align identity governance with their overall IT operations. A workflow orientation makes it easy and straightforward to automate access requests, approvals, and fulfillment. Such integration improves efficiency, reduces manual effort, and ensures that access decisions are always aligned with business context and policy.

## Automation of Identity Events



Automation is a defining feature of modern IGA, enabling organizations to manage identities and access at scale. Automated workflows handle the provisioning and deprovisioning of access, enforce policy controls, and monitor user activity in real time. This reduces the administrative burden on IT teams and minimizes the risk of errors or delays that could compromise security or compliance.

Automated lifecycle management ensures that users have the right access at the right time, accelerating onboarding and offboarding processes. By orchestrating and automating workflows that coordinate with ITSM, and reflect prevailing policy on identity, job roles, and associated privileges, IGA ties typical events in the employee lifecycle—such as join, move, or leave—to grants and revocations of access and privilege. This not only enhances the user experience but also supports compliance by ensuring that access is always appropriate and documented. Automation of identity events also supports business agility, enabling organizations to securely manage their

access needs at each step in the employee lifecycle, while providing audit-ready evidence packages on demand or at regular intervals, as needed.

## **Integration with Security Ecosystems**

---

Modern IGA solutions must also integrate with the broader security ecosystem, including Security Information and Event Management (SIEM) platforms, Privileged Access Management (PAM) solutions, and threat intelligence feeds. These integrations enable organizations to correlate identity events with security incidents, detect anomalous behavior, and respond to threats in real time. By connecting identity governance with security operations, organizations can strengthen their overall security posture and reduce the risk of data breaches.

Integration with PAM is particularly important, as privileged accounts represent a significant risk if not properly governed. Modern IGA acts as the connective tissue between IGA and PAM, ensuring that privileged access is subject to the same rigorous controls and oversight as workforce access. This holistic approach closes gaps that attackers frequently exploit and supports compliance with stringent regulatory requirements.

## **Reducing Operational Overhead**

---

Deep integration, AI driven insights and context, plus automation reduce operational overhead by eliminating manual processes and streamlining workflows. This enables IT and security teams to focus on strategic initiatives rather than routine administrative tasks. It also rescues IT workers from all the data-gathering and summary work that AI can handle. Indeed, AI and automation work together

inside modern IGA to eliminate manual role definition work. Within Idira IGA, AI and AI profiles can use pre-approvals to obviate manual redundant efforts, particularly for busy business supervisors or technical management staff.

In addition, integration with business systems provides real-time visibility into access rights and user activity, enabling organizations to monitor and manage access more effectively. This visibility supports both security and compliance objectives, providing a comprehensive view of the identity landscape.

## Measuring IGA Success

Measuring success in an IGA program means proving that [identity governance](#) is not just functioning, but actively reducing risk, strengthening compliance, and accelerating business operations. The most [meaningful metrics](#) fall into a few clear categories.



**Access accuracy:** How often users have the right access at the right time—shows whether governance policies are working; reductions in excessive or orphaned access directly demonstrate lowered attack surface.

**Certification tracking:** Tracks how quickly and accurately managers complete access reviews, review completions and their timing, whether or not reviews produced findings. All these things help to boost audit completeness and accuracy.

**Provisioning and deprovisioning time:** Faster fulfillment of joiner-mover-leaver events proves that IGA is enabling the business rather than slowing it down, while also reducing the window of exposure when access should be removed.

**Policy violation trends (such as SoD conflicts or high-risk entitlements):** Reveal whether governance controls are preventing risky combinations of access before they reach production.

**Application integration:** Checks to make sure that IGA is integrated and in control whenever and wherever identity information is involved (e.g., user logins required).

**Continuous identity connection:** Confirms that IGA is providing constant, accurate data for ongoing, constant visibility, policy, and governance enforcement.

**Automation coverage:** Measures how much of the identity life-cycle is handled without manual intervention; higher automation correlates with fewer errors, lower operational cost, and more consistent enforcement.

Together, these metrics provide a clear, quantifiable view of IGA value: reduced risk, improved compliance posture, and a faster, more secure identity ecosystem that supports the organization's strategic goals.

## Supporting Business Agility and Innovation



Finally, integration and automation support business agility and innovation by enabling organizations to adapt quickly to changing

business requirements. Automated workflows and real-time integrations enable rapid onboarding of new users, applications, and services, supporting digital transformation initiatives without compromising on security or compliance.

In summary, deep integration with directories and applications, including HR, ITSM, and security ecosystems—combined with automation of identity events—empowers organizations to achieve effective, scalable, and resilient identity governance. These capabilities are essential for supporting business growth, managing risk, and maintaining compliance in a dynamic digital environment. In the next chapter, you'll learn what modern IGA can do to boost security and operational efficiency within your organization.

## CHAPTER 4

# A Modern IGA Operating Model

**As infrastructure evolves, identities proliferate, cyber threats increase, and regulatory demands expand, the need for a holistic identity security platform becomes paramount.** Modern IGA solutions, such as those enabled by Idira, are designed to overcome the limitations of legacy systems by automating workflows, improving visibility and operational efficiency, while meeting governance and compliance needs. These advances not only bolster security posture but also streamline compliance and operational efficiency. Security leaders, IT managers, and compliance professionals must understand how these modern practices work in real-world environments to effectively safeguard access and support organizational growth.

**TABLE 1** summarizes the kinds of risks and exposures that a modern IGA solution can provide, based on offsetting capabilities that legacy systems lack. Indeed, manual processes and legacy tools fall under the broad heading of “legacy” approaches on the left-hand side of the table. For more information about the kinds of challenges that legacy tools and manual approaches can pose, and how modern IGA helps to address them, consult the Idira white paper, “[Choosing the Right IGA Solution.](#)”

<b>LEGACY: BUSINESS RISK EXPOSURE</b>	<b>MODERN: RISK AND COST REDUCTION</b>
Manual access management errors	Automated lifecycle management
Privilege creep from role changes	Consistent least privilege enforcement
Disconnected identity systems	Unified governance platform
Slow onboarding/offboarding processes	Streamlined identity events automation
High audit failure risk	Continuous compliance and audit readiness
Limited visibility across environments	Centralized monitoring and controls
Vulnerable to data breaches	Adaptive security controls
Fragmented compliance reporting	Automated evidence collection
Resource-intensive audits	Reduced manual effort

**TABLE 1:** Summary of risks and exposures that modern IGA can provide

## Ownership in Modern IGA: Roles and Responsibilities

Modern IGA benefits from a role-based approach to ownership and collaboration across the business, avoiding painful and centralized bottlenecks that slow down productivity. Indeed, modern IGA helps

manage and coordinate between teams and gives them a central platform from which they can all work and play their individual roles, and carry out their responsibilities for user access reviews and lifecycle management.

- **Application Owners:** Responsible for governing access to their specific applications, reviewing entitlements, and ensuring only authorized users have appropriate permissions.
- **Managers and Business Supervisors:** Oversee direct reports, approve or reject access requests, and participate in periodic certification campaigns.
- **Helpdesk:** Teams that facilitate ticketing for provisioning, problem resolution, change requests, and other employee lifecycle events as they happen, handled within the IGA framework.
- **Identity and Access Management (IAM) Teams:** Architect and maintain the IGA framework, configure automation, and monitor compliance with organizational policies.
- **Governance, Risk, and Compliance (GRC) Professionals:** Define governance policies, ensure regulatory alignment, and audit access controls. Work with business supervisors to ensure that policies also align with business goals and objectives.

By empowering each stakeholder, modern IGA enhances responsiveness and reduces the delays often associated with centralized approval processes.

# Automation vs. Exception Governance: What Gets Automated and Why

---

Automation is at the heart of modern IGA, driving efficiency, consistency, and security. Routine processes such as user provisioning, de-provisioning, and access reviews are automated based on pre-defined policies and triggers (e.g., HR events, role changes). This minimizes manual intervention, reduces errors, and ensures timely updates.

Modern IGA solutions leverage automated processes to enhance efficiency and security across the identity lifecycle. Key activities such as onboarding and offboarding users are automated, ensuring that access is promptly granted or revoked as organizational changes occur. Standard access requests and their approvals are streamlined for common roles, reducing manual intervention and accelerating fulfillment. In addition, periodic access certification campaigns are executed automatically, helping organizations maintain compliance by regularly validating user privileges. Real-time monitoring and alerting for anomalous activities further strengthen security by enabling immediate responses to potential threats. Together, these automated processes reduce errors, minimize delays, and support consistent enforcement of access policies.

Idira IGA uses automation and self-service capabilities to address access requests that may not fall into standard categories or birth-right or suggested access policies. This empowers users to request access for specific business needs, and automates the orchestration of the request workflow for review as needed. In some cases, approval can be automated based on defined policies but in other cases, additional review by establishing clear procedures for these scenarios, organizations can maintain strong governance and security without hindering legitimate business operations.

The beauty of using Modern IGA is that it doesn't matter if access is standard or an outlier. The framework ensures all requests get reviewed and approved (or denied) more quickly—and correctly.

## **How Modern Workflows Replace Legacy Ticket-Based Models**

---

Manual IGA processes often rely on manual, ticket-based workflows for granting or revoking access. These processes are slow, error-prone, and lack transparency, resulting in delayed access, orphaned accounts, and compliance risks. Using a legacy tool doesn't adequately solve the issue, as the difficulties with integrating into modern hybrid infrastructures results in limited or fractured coverage across the IT environment. Modern IGA solutions, such as Idira IGA, replace these outdated workflows with automated, event-driven processes.

In the manual model, access requests were typically submitted via tickets, requiring manual review and approval by IT personnel or managers. This process often led to delayed fulfillment of requests and provided only a limited audit trail, making it difficult to track and ensure compliance. In contrast, a modern IGA workflow streamlines access management by allowing requests to be initiated through a centralized portal, where they will be tracked and logged. Automated routing leverages policies and user roles to direct requests appropriately, while event-driven triggers handle provisioning and de-provisioning tasks. These enhancements enable instant notifications and maintain real-time audit logs, significantly improving both efficiency and transparency in managing access.

### **Example: Event-Driven Access Provisioning in Idira IGA**

When a new employee joins the organization, Idira IGA automatically provisions access to required applications based on their role, department, and location (referred to as “birthright” access). If the employee’s role changes, the system immediately detects this and adjusts their entitlements, removing outdated permissions and granting new ones. All actions are logged for audit purposes, and managers are notified of any exceptions that require review. This eliminates bottlenecks, ensures compliance, and accelerates onboarding.

## **How Visibility and Accountability Improve Without Adding Friction**

Legacy IGA systems often fail to connect or integrate across the entire infrastructure. Thus, the view of access across the organization is incomplete and inconsistent. Although such tools do have dashboards and analytics, they are limited and cover only specific points in time. Modern IGA has comprehensive connectivity which is maintained in real time for continuous visibility. Modern IGA always reflects the current situation and circumstances. That’s how modern IGA can—and does—adapt as the access estate changes.

**ENHANCED VISIBILITY:** Modern IGA platforms deliver significantly improved visibility by providing an integrated view of user entitlements across all applications and systems. With real-time alerts for anomalous access patterns or potential policy violations, organizations can react swiftly to emerging risks. Automated, AI-driven

reporting tools make audits and compliance reviews more efficient, empowering stakeholders to monitor and manage access proactively without added complexity. By contrast, legacy systems are inconsistent, siloed off from one another, and lack a coherent, AI- and policy-driven view into and control over identity information.

### **Example: Automated Access Review Campaigns in Idira IGA**

Idira IGA enables organizations to schedule periodic access review campaigns, automatically notifying managers and app owners of their review responsibilities and providing a user-friendly interface from which to quickly complete their review. The platform provides actionable insights, allowing reviewers to quickly identify excessive or outdated permissions. Automated reminders and escalation workflows ensure timely completion, while comprehensive audit trails support regulatory requirements. This process enhances accountability without burdening stakeholders with manual tasks. In addition, AI-based insights and pre-approval workflows drastically reduce the number of permissions requiring manual approval/review.

## **Moving Toward Flexible, Policy-Driven Approaches**

Historically, infrastructure and IT teams were centralized and legacy IGA systems were built for that outdated centralized model. Such systems don't work well today—they're slow and hard to adapt to changing circumstances. In contrast, modern IGA solutions leverage

dynamic, AI-informed, and policy-driven workflows. These workflows automatically adjust to shifts in organizational structure and can easily handle special requests through self-service portals, ensuring access management remains both efficient and responsive to business needs.

Traditional access management models concentrated control within a central, manual authority, which frequently caused delays. This also increased the likelihood of errors due to the heavy workload placed on a small group of administrators. Modern IGA platforms address this by automating and orchestrating the approval workflow, and applying pre-approvals in an intelligent manner with the help of AI. Centralized policies remain in place to ensure consistency and compliance across the organization, enabling faster decision-making without sacrificing security or oversight.

These contrasts highlight the transformative potential of modern IGA, making organizations more agile and secure.

## **ACCESS CERTIFICATION AUTOMATION WITH IDIRA**

**SCENARIO:** Quarterly access certifications are a regulatory requirement in many organizations. Traditionally, these reviews involved manual spreadsheets and emails, often resulting in late findings and incomplete records.

**IDIRA IGA SOLUTION:** Idira IGA automates the entire certification process. Access data is compiled and presented to managers and app owners through an intuitive dashboard, highlighting high-risk entitlements and overdue reviews. Automated notifications and escalation workflows ensure that certifications get completed on time. The Idira IGA system maintains a detailed audit trail, simplifying compliance audits and reducing administrative burden.

**BUSINESS OUTCOME:** Faster, more accurate certifications; reduced risk of unauthorized access; improved regulatory compliance.

## PRIVILEGED ACCESS MANAGEMENT INTEGRATION

**SCENARIO:** Privileged accounts represent a significant risk if not properly managed. Legacy systems often offered limited and incomplete integration between IGA and PAM, leading to visibility gaps. Indeed, such systems were hard to configure, expensive, and lacked the detail needed to provide proper oversight for privileged accounts.

**IDIRA IGA SOLUTION:** Idira IGA seamlessly integrates with Idira's PAM platform, ensuring that privileged access is visible in one tool and is governed by robust policies and workflows.

**BUSINESS OUTCOME:** Enhanced control over privileged access; minimized insider risk; streamlined compliance with security policies and regulations.

## PRE-APPROVED ACCESS GETS AUTOMATED FOR LIFECYCLE EVENTS

**SCENARIO:** As employees experience lifecycle events—typically identified as joiners, movers, or leavers—they require grants or revocations of access to reflect their current situations. Joiners need access to applications and services based on their new job roles, while movers need revocations of no-longer-necessary apps and services and access to new ones. Leavers must have all access revoked to leave no openings for unwanted intrusions.

**IDIRA IGA SOLUTION:** Idira IGA offers automated AI-based profiles that include pre-approved access for users based on current job title, department, or location. Most subsequent access reviews show that this covers over 80% of access grants, and enables automation to carry the bulk of the load quickly and accurately

**BUSINESS OUTCOME:** Automated approval and provisioning for virtually all routine access grants expedites employee productivity, and frees managers and supervisors to focus attention where it's most needed.

## SELF-SERVICE REQUEST HANDLED QUICKLY, ACCURATELY AND WITHIN POLICY GUIDELINES

**SCENARIO:** Employees routinely need access to new applications, data sets, and services, but traditional ticket-based processes slow them down. Requests often get routed to the wrong team, managers approve without context, and IT spends too much time manually fulfilling routine access instead of focusing on higher-value work.

**IDIRA IGA SOLUTION:** Idira IGA provides a unified, self-service access catalog that integrates with all enterprise systems—cloud, on-premises, and legacy. Users request access through a guided interface, and Idira IGA automatically delegates approvals to the correct owners or groups based on policy, role, and risk. Continuous monitoring ensures every request is evaluated against current identity data, SoD rules, and policy changes, not just point-in-time snapshots.

**BUSINESS OUTCOME:** Employees get the access they need quickly and confidently, managers approve with full context, and IT sees a major reduction in manual workload. The organization gains faster fulfillment, stronger governance, and a continuously validated record of who requested what—and why.

## Best Practices Boost Business Outcomes

Modern IGA, as exemplified by Idira, delivers significant advantages over legacy approaches. By automating routine processes, distributing ownership, and enhancing visibility, organizations can reduce risk, accelerate audits, and improve productivity. Best practices include:

- Clearly defining ownership roles and responsibilities
- Leveraging automation and AI to perform routine tasks more efficiently
- Replacing manual, ticket-based workflows with event-driven automation
- Utilizing dashboards and automated reporting to improve visibility and accountability
- Integrating IGA with PAM to secure privileged access

For security leaders, IT managers, compliance professionals, and anyone concerned with identity and access management, embracing these practices is essential to building a resilient and responsive identity governance program to support business objectives and regulatory requirements. In the next and final chapter, you'll learn how modern IGA maps into and enhances broader transformation initiatives and brings measurable business improvements to those who adopt and use its capabilities well.

## CHAPTER 5

# Modern IGA Creates Business and Accelerates Revenue

**AI, identity management, and infrastructure evolution are reshaping the way organizations operate, innovate, and compete.** The whole process is often loosely defined as “digital transformation.” Indeed, as enterprises migrate to the cloud, adopt SaaS solutions, and embrace remote work, the challenges of managing identities and access have grown exponentially. In fact, security experts now consider identity management essential to establishing a security perimeter, because identity based breaches are increasingly prevalent and dangerous.

Today, modern IGA is a critical enabler for digital transformation. It uses AI-driven insights, automation, and current, continuous intelligence to establish, protect, and manage identities (both human and otherwise). That’s how modern IGA provides the robust and resilient framework needed to secure, manage, and protect today’s complex hybrid and multi-cloud environments.

# Standardizing Identity Governance Across Modern Architectures

---

One of the primary challenges in digital transformation is the proliferation of identities, applications, and data across diverse environments. Modern IGA addresses this challenge as it works across all platforms—cloud, SaaS, and on-premises. Most importantly, IGA defines a centralized control plane for visibility, as it ensures that access policies are consistently enforced, as organizations carry out compliance and lifecycle management activities.

By centralizing identity governance, organizations gain a holistic view of their identity landscape, enabling more effective risk management and compliance. Modern IGA also simplifies adding new applications, services, directories, and more, through its simple, visually oriented central control plane.

## Increased Security Posture, Better Ops Efficiency

---

Cloud migration and SaaS adoption are central to many organizations' digital transformation strategies. However, these initiatives introduce new complexities in managing identities and access. Modern IGA provides the tools and integrations needed to govern access across multiple cloud providers and SaaS platforms, ensuring that security and compliance are not compromised in the pursuit of agility and scalability. Modern IGA helps to securely manage identity across the entire lifecycle, and throughout the entire digital estate.

# Enabling Zero Trust Security

Zero Trust is a security paradigm that assumes no user or device should be trusted by default, regardless of location. Access is continuously verified based on identity, context, and behavior. Modern IGA helps to enable and support Zero Trust, by providing the identity-centric controls needed to enforce least privilege, monitor access, and respond to risk signals dynamically.

By integrating IGA with Zero Trust architectures, organizations can ensure that access is always appropriate, justified, and aligned with business policy. Adaptive controls and continuous monitoring enable organizations to detect and mitigate threats before they can be exploited, supporting both security and business objectives.

## Now Hear This: Actionable Guidance for Executives

Modernizing IGA is not a one-size-fits-all journey, but there are clear steps executives can take to drive success:

- 1. Assess Current State:** Map out existing processes for user access reviews, lifecycle management, plus related technologies, and pain points. Roll out best IGA options where needed, and identify where legacy limitations are impeding outcomes.
- 2. Define Success Metrics:** Establish clear, measurable goals—such as reduced access risk, faster onboarding, or improved audit performance.



**3. Engage Stakeholders:** Bring together business, IT, and security leaders to align on priorities and secure buy-in for transformation.

**4. Adopt Continuous Governance:** Prioritize solutions that automate access management, provide real-time visibility, and support dynamic policy enforcement.

**5. Leverage Idira Expertise:** Partner with Idira to design and implement a modern IGA strategy tailored to your organization's needs.

**6. Foster a Culture of Security:** Embed identity security into business processes and decision making, ensuring that it becomes a driver of value rather than a blocker.

By following these steps, executives can ensure that their IGA modernization efforts deliver the outcomes that matter—reduced risk, enhanced compliance, operational efficiency, and business enablement.

## Accelerating Innovation Without Compromising Security

Digital transformation is driven by the need to innovate rapidly and respond to changing market conditions. Modern IGA empowers organizations to accelerate innovation by automating manual processes or labor intensive and point in time processes, making them more continuous. This reduces team efforts so they can focus on accelerating innovation in other areas. Standardized processes and automated workflows enable rapid onboarding of new users, applications, and services, supporting business growth and agility.

At the same time, modern IGA ensures that security and compliance are never sacrificed in the pursuit of innovation. By providing a consistent governance framework, organizations can maintain control over access to sensitive data and systems, even as the technology landscape evolves.

## Driving Business Value Through Identity Governance



Ultimately, modern IGA is not just a security or compliance tool—it is a driver of business value. By enabling secure digital transformation, supporting innovation, and reducing operational costs, IGA provides a compelling return on investment for organizations of all sizes and industries.

A strategic approach to identity governance ensures that organizations can adapt to changing business requirements, regulatory demands, and threat landscapes with confidence and agility. By investing in modern IGA, security and IT executives can position their organizations for success in the digital age.

### LEARN MORE

Idira stands ready to help your organization make the most of Identity Governance and Administration in your world, on your terms. Please visit [Choosing the Right IGA Solution](#) to learn more about Idira's offerings.

# ABOUT IDIRA



Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at [paloaltonetworks.com](https://paloaltonetworks.com).

# ABOUT ACTUALTECH MEDIA



ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit [actualtechmedia.com](https://actualtechmedia.com).