

Navigating the Evolving Compliance Landscape:

The Role of Identity Governance in Meeting Regulatory and Security Challenges



Table of Contents

Executive Summary	1
Rise of Regulatory Oversight.....	2
From Scandal to Safeguards	2
The Evolution of Compliance	3
The GDPR Era: A Paradigm Shift in Privacy Compliance	3
A New Focus on Cybersecurity in the EU: NIS2 and DORA	4
The United Kingdom’s Approach to Compliance Post-Brexit	5
The Modern Compliance Challenge.....	6
Why IGA is Essential to Overcoming These Challenges	6
The Growing Challenge of Global Regulatory Compliance	7
Embracing Security Frameworks	8
NIST Cybersecurity Framework (CSF).....	8
ISO/IEC 27000 Series	9
CIS Critical Security Controls	9
How Identity Governance and Administration can help.....	10
Identity Lifecycle Management.....	10
Entitlement Governance & Risk Management	10
Business Workflows & Process Automation	11
Audit & Compliance Tracking.....	11
The Role of Generative AI in IGA.....	12
IGA as a Strategic Asset for Compliance & Beyond	12
Omada Identity Cloud.....	13
Glossary.....	14

Executive Summary

The complexity of global regulations like GDPR, SOX, NIS2, and DORA is reshaping how organizations approach compliance. Identity Governance and Administration (IGA) has emerged as a strategic enabler for organizations to streamline compliance processes, reduce risk, and support business agility. IGA strengthens access controls, automates user lifecycle management, and simplifies audit preparations.

Maintaining compliance is not without its challenges. Organizations face an ever-evolving landscape of regulatory demands, which often differ across jurisdictions. The need for comprehensive access control in hybrid and remote work environments has introduced new complexities, as organizations must manage user access across multiple cloud platforms and devices. This increase in access points heightens the risk of unauthorized access and data breaches. Further complicating compliance efforts are resource constraints, as IT and security teams are required to manage growing regulatory obligations with limited personnel and budgets.

This whitepaper provides an overview of the compliance landscape and a perspective on how organizations can address regulatory challenges and transform compliance from a costly burden into a strategic advantage. Key principles like Role-Based Access Control (RBAC), Least Privilege, and Zero Trust are essential to meet the ever-expanding list of regulatory requirements. We will examine how modern Identity Governance and Administration solutions can provide a valuable enabler in adherence to these key principles.



Identity Governance and Administration (IGA) refers to the systems and processes that control user access, manage roles, and ensure compliance with security and regulatory requirements.

Rise of Regulatory Oversight

Corporate scandals in the early 2000s involving Enron and WorldCom exposed serious deficiencies in financial oversight and access control. Executives and employees were able to manipulate financial data, fabricate profits, and concealed liabilities due to a lack of accountability and the absence of **Segregation of Duties (SoD)**—a fundamental control principle ensuring no single person has complete authority over key processes. Without SoD, employees could authorize, process, and conceal fraudulent transactions, leaving auditors and stakeholders blind to the fraud.

The fallout from these scandals led to global regulatory reforms, most notably the **Sarbanes-Oxley Act (SOX) of 2002** in the U.S. This legislation mandated stricter internal controls, demanding executives certify the accuracy of financial reports (Section 302) and requiring organizations to verify the effectiveness of their internal controls (Section 404) with oversight from external auditors. SOX redefined corporate governance and compelled organizations to adopt systems that enforce role-based access, automate user certifications, and maintain clear audit trails.

From Scandal to Safeguards

The Enron and WorldCom scandals underscored the risks of inadequate access controls:



Unrestricted Access: Employees accessed and altered financial data without oversight.



Conflicts of Interest: A lack of segregation of duties allowed individuals to manipulate transactions without checks or balances.



Absence of Audit Trails: Critical actions, such as unauthorized changes to financial records, approval of unverified transactions, or modifications to user access rights, went undocumented. Without a clear audit trail, these actions left no evidence for auditors to identify discrepancies, trace suspicious activity, or uncover fraudulent behavior.

The lessons from these scandals revealed that unrestricted access and weak access controls can expose businesses to catastrophic risks. In response, Identity Governance and Administration (IGA) emerged to enforce stricter role-based access controls and segregation of duties, ensuring no single individual can bypass essential safeguards. This approach is grounded in the principle of least privilege—granting users only the minimal access necessary for their roles—within a **Zero Trust Architecture (ZTA)**, which assumes no user or device should be trusted by default, even within the network. Additionally, **Role-Based Access Control (RBAC)** has become foundational, assigning access permissions based on a user's job role to enforce structured and consistent access management. Together, these practices reduce opportunities for fraud, enhance accountability, and form the cornerstone of modern compliance and security risk programs.

The Evolution of Compliance

The evolution of compliance reflects a shift from reactive responses to proactive governance, driven by the need for stricter oversight, enhanced accountability, and operational resilience. While SOX addressed financial oversight, subsequent regulations extended its principles to other domains. Regulations and industry standards like **GDPR**, **HIPAA** and **PCI DSS** expanded access control requirements to safeguard personal data, healthcare information, and payment systems. These regulations highlighted the growing role of identity governance and access control as foundational pillars of security and trust in a rapidly digitizing world.

The GDPR Era: A Paradigm Shift in Privacy Compliance

In 2018, the regulatory landscape experienced a seismic shift with the introduction of the **General Data Protection Regulation (GDPR)**. As one of the most comprehensive privacy regulations in the world, the European Union (EU) set a new standard for the handling of personal data, with broad applicability to any organization processing data of EU residents. Unlike earlier regulations, GDPR introduced a **privacy-by-design** approach, requiring companies to embed data protection principles into every facet of their operations.

The operational impact of GDPR was profound. Companies were required to implement stricter access controls, obtain explicit user consent for data collection, and maintain comprehensive records of data processing activities. Non-compliance came with heavy penalties—up to **4% of global annual revenue or €20 million**, whichever was higher. This led to several high-profile enforcement actions. Some recent cases from 2024 include:

Uber

In August 2024, the Dutch Data Protection Authority fined Uber €290 million (\$324 million) for transferring European drivers' personal data to the U.S. without adequate safeguards. The data included sensitive information such as account details, taxi licenses, location data, photos, payment details, identity documents, and, in some cases, criminal and medical records. Uber plans to appeal the decision, asserting compliance during a period of regulatory uncertainty between the EU and the U.S. ([The Verge](#))

LinkedIn

In October 2024, Ireland's Data Protection Commission fined LinkedIn €310 million (\$335 million) for processing personal data for advertising purposes without a lawful basis, violating the principles of lawfulness, fairness, and transparency under the GDPR. LinkedIn stated that it believes it has complied with the rules but is taking steps to ensure its advertising practices meet regulatory requirements. ([AP News](#))

Meta

In September 2024, the European Union's privacy regulator fined Meta €91 million (\$101.5 million) for storing user passwords without encryption. The issue was discovered five years ago when Meta informed Ireland's Data Protection Commission of storing some passwords in 'plaintext,' which were not accessed by external parties. Meta addressed the problem immediately upon discovering it during a 2019 security review, ensuring the passwords were not abused or improperly accessed. ([Reuters](#))

Beyond the financial cost, these fines highlighted the operational strain of GDPR compliance. Companies faced challenges in managing consent, handling access requests, and ensuring timely breach notifications. Given GDPR's emphasis on data access, privacy-by-design, and user rights, IGA plays a vital role in ensuring companies can control user permissions, track user access, and maintain audit-ready records for compliance inquiries.

A New Focus on Cybersecurity in the EU: NIS2 and DORA

The scope of regulatory compliance widened with the introduction of two landmark regulations in the European Union—**NIS2 (Network and Information Security Directive 2)** and **DORA (Digital Operational Resilience Act)**. These frameworks signaled a shift from simple compliance exercises to **operational resilience** and **cybersecurity readiness**.



NIS2 applies to essential and important sectors like healthcare, energy, transportation, and digital infrastructure. Unlike its predecessor, NIS2 mandates that organizations adopt robust security measures, such as **Role-Based Access Control (RBAC)** and **Multi-Factor Authentication (MFA)**, to safeguard critical systems. Incident reporting is now more stringent, requiring organizations to notify authorities of significant cybersecurity incidents within **24 hours**, followed by a full incident report within **72 hours**. This shift emphasizes the importance of speed, transparency, and accountability in responding to cyber threats.

DORA targets financial services, including banks, insurers, and fintech companies. The regulation ensures that financial institutions can withstand operational disruptions caused by cyber threats. DORA requires firms to strengthen third-party risk management, conduct **penetration testing**, and ensure that **ICT service providers** adhere to strict security protocols. As with NIS2, incident reporting is a key requirement, with financial institutions obligated to notify regulators of major Information- and Communication Technology (ICT) incidents in a timely manner.

These regulatory frameworks not only heighten accountability but also standardize reporting requirements, making it easier for organizations to manage multiple obligations simultaneously. Both **NIS2 and DORA** align in their emphasis on incident notification within 24 hours and comprehensive follow-up reports within 72 hours. IGA solutions provide organizations with the ability to monitor and manage role-based access in real-time, ensuring that only authorized users have access to critical infrastructure at any given moment. This approach simplifies cross-sector compliance, ensuring consistency in how incidents are tracked, reported, and resolved.

The United Kingdom's Approach to Compliance Post-Brexit





Following Brexit, the United Kingdom redefined its compliance strategy. While it retained elements of EU regulations, it also established new frameworks that prioritized national cybersecurity. Key developments included the **Telecommunications (Security) Act 2021 (TSA)**, which imposed new security obligations on public telecommunications providers. Companies are now required to strengthen supplier risk management, protect critical networks from unauthorized access, and manage security risks across their supply chains.

Another key initiative was the introduction of **Cyber Essentials**, a government-backed certification program designed to improve baseline cybersecurity standards. It promotes the use of secure configurations, access control, malware protection, and timely patch management. Certification demonstrates an organization's commitment to best practices, making it an essential requirement for UK businesses bidding for government contracts.

The UK also retained a version of **GDPR**, known as **UK GDPR**, which mirrors the EU's GDPR while accommodating the specific regulatory needs of the UK. Other frameworks, such as the **Network and Information Systems Regulations 2018 (NIS Regulations)**, continue to regulate critical services and digital service providers, although with a more limited scope than the EU's NIS2.

The Modern Compliance Challenge

As organizations navigate this web of regulations, they face an ever-growing list of operational and technological challenges. Four primary trends illustrate the evolving compliance landscape:

 Cloud Migration	As organizations transition to cloud-based systems, maintaining visibility and control over data becomes increasingly complex.
 Hybrid and Remote Workforces	The shift to remote work introduces new risks, as employees access sensitive data from various locations and devices.
 Expanding Regulations	GDPR has inspired similar legislation worldwide, increasing the regulatory burden on global businesses.
 Resource Constraints	IT departments are being asked to “do more with less,” juggling security, compliance, and operational efficiency with limited resources.

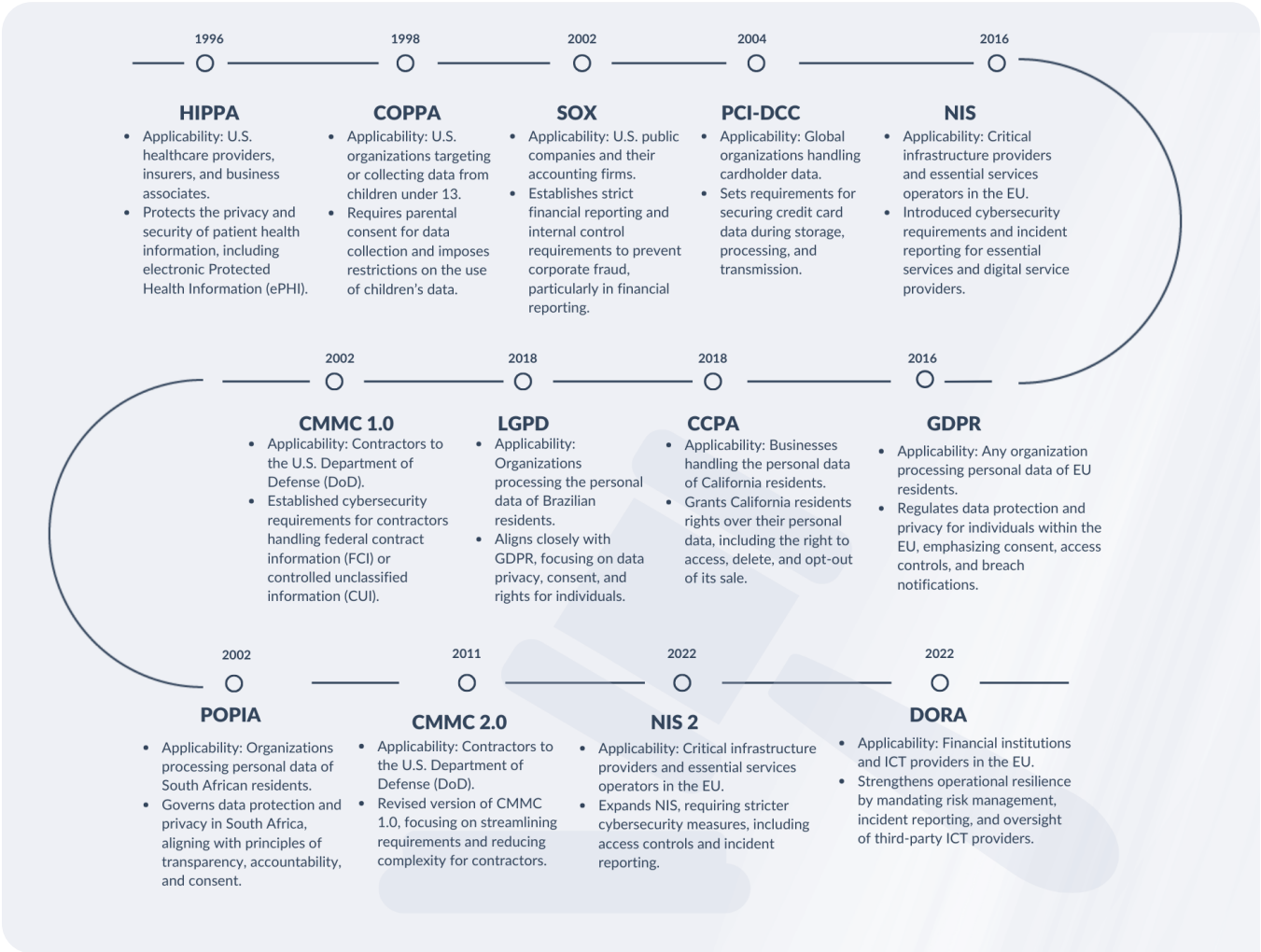
Why IGA is Essential to Overcoming These Challenges

The growing complexity of compliance demands an approach that centralizes access controls, tracks user activity, and enables automation. IGA addresses each of these needs, providing organizations with the tools to manage compliance at scale. By adopting modern IGA platforms, organizations can achieve:

- ✓ **Stronger Access Control:** Enforcing role-based access control (RBAC) ensures that users only access what they need.
- ✓ **Conflicts of Interest:** Audit-Ready Records: Comprehensive audit trails ensure that all access decisions are fully documented, simplifying compliance with GDPR, NIS2, and DORA.
- ✓ **Automation at Scale:** Self-service workflows, automated certifications, and AI-assisted access approvals reduce administrative burden and improve compliance efficiency.

With these capabilities, IGA provides a **unified approach to access governance, compliance, and risk mitigation**, allowing organizations to stay ahead of regulatory change and reduce operational complexity.

Compliance Timeline



The Growing Challenge of Global Regulatory Compliance

Operating across multiple jurisdictions requires organizations to confront an intricate web of ever-evolving regulatory requirements. Each region imposes distinct rules for how data must be accessed, stored, and managed. Europe's GDPR enforces stringent privacy mandates. Globally we find similar initiatives such as China's PIPL, that emphasizes data localization, and California's CCPA, that prioritizes consumer rights. Together, these and other acronyms of regulations form a "patchwork" that demands precise navigation and strategic alignment.

Industry-specific regulations add another layer of complexity. Financial institutions must balance the operational demands of the EU's DORA with the internal control requirements of the U.S. SOX Act. Healthcare providers in the U.S. must adhere to HIPAA's data privacy rules, while other regions enforce similar healthcare data protection standards. Critical infrastructure operators are subject to NIS2's heightened cybersecurity obligations, and U.S. Department of Defense (DoD) contractors face the

stringent requirements of CMMC 2.0. These overlapping mandates create a regulatory “storm” that demands careful orchestration to avoid penalties and disruptions.

The pace of regulatory change shows no signs of slowing. Emerging regulations like India’s DPDP and the UAE’s PDPL signal a growing emphasis on privacy and data protection across previously unregulated markets. To remain compliant, organizations must go beyond legal interpretation. They need a proactive strategy that aligns operations, policies, and technology with a shifting regulatory landscape. This requires agility, foresight, and the right tools to adapt to a “moving finish line” of regulatory requirements. Without clear processes and effective governance structures, the risk of falling behind increases—potentially exposing the organization to financial penalties, reputational damage, and operational inefficiencies.

Embracing Security Frameworks

To navigate regulatory challenges, organizations are turning to established cybersecurity frameworks. These frameworks provide clear, structured guidelines for **managing access, identities, and security controls, enabling companies** to strengthen their compliance posture. Three of the most influential frameworks are:

1. NIST Cybersecurity Framework (CSF)
2. ISO/IEC 27000 Series
3. CIS Critical Security Controls



NIST Cybersecurity Framework (CSF)

The **NIST CSF** is a globally adopted standard that guides organizations in managing cybersecurity risks. Built on five core functions — **Identify, Protect, Detect, Respond, and Recover** — it provides a flexible model for improving security posture.

Relevant to **IGA** the **Identify** function emphasizes the need to inventory users, roles, and access privileges. The Protect function requires the enforcement of access control principles like Least Privilege and Role-Based Access Control (RBAC). The Detect function supports anomaly detection, where deviations from expected user behavior are flagged for review.

By adopting NIST CSF, organizations can strengthen identity lifecycle management, streamline access reviews, and improve their overall compliance with regulatory requirements like NIS2 and GDPR.



ISO/IEC 27000 Series

The **ISO/IEC 27000 series** defines global standards for information security management. **ISO 27001** is widely recognized for its focus on the creation, implementation, and maintenance of **Information Security Management Systems (ISMS)**. It provides clear guidelines for access control, identity management, and auditability — key components of modern **IGA**.

Key areas for IGA compliance under **ISO 27001** include:

- **Access Control (Annex A.9)**, which mandates formal processes for assigning, revoking, and reviewing user access.
- **User Access Reviews (A.9.2.5)**, which require periodic review of access rights to ensure alignment with job roles.
- **Logging and Monitoring (A.12.4)**, which ensures that user actions are logged and that any unauthorized access attempts are flagged for investigation.

Adhering to **ISO 27001** enables companies to formalize their identity governance processes, enforce segregation of duties, and maintain audit trails, which are all critical to **SOX, GDPR, NIS2, and HIPAA** compliance.



CIS Critical Security Controls

The **CIS Critical Security Controls** offer a practical, cost-effective approach to security by focusing on essential controls. Unlike ISO's more exhaustive approach, CIS focuses on implementing a prioritized set of "must-have" controls.

Key IGA-relevant CIS controls include:

- **Account Management (Control 5)**: Ensures proper onboarding, offboarding, and role changes for all system accounts.
- **Access Control Management (Control 6)**: Mandates **Least Privilege** and **Multi-Factor Authentication (MFA)** for sensitive systems.
- **Application Security (Control 16)**: Enforces proper access controls within applications, ensuring that only authorized users can access sensitive data.

These controls align directly with IGA, helping organizations **automate identity lifecycle management** and enforce access rules that reduce risks and simplify audit preparation.

How Identity Governance and Administration can help



Identity Lifecycle Management

Ensuring that users have the right access to the right resources at the right time is one of the most persistent challenges in regulatory compliance. As employees are hired, promoted, or leave, their access needs shift. Managing these transitions efficiently while maintaining security and compliance requires a robust Identity Governance and Administration (IGA) solution.

IGA enables organizations to grant, adjust, and revoke access based on user roles and responsibilities, ensuring that only necessary permissions are assigned. This Role-Based Access Control (RBAC) approach aligns access rights with job roles, supporting compliance with regulations like GDPR, which mandates adherence to the principles of Least Privilege and Need-to-Know Access.

Modern IGA solutions automate key aspects of the identity lifecycle, such as onboarding, offboarding, and role changes. For example, when a new employee is hired, an IGA system creates a user profile in the central HR system and assigns predefined access rights for systems like Active Directory, email, and shared drives. As employees change roles, access is automatically updated to reflect their new responsibilities, ensuring unnecessary permissions are removed to prevent “entitlement creep” — a major compliance risk.



Entitlement Governance & Risk Management

Once access is granted, maintaining control is critical to avoid excessive permissions that can lead to security breaches or compliance failures. Over time, users often accumulate access rights they no longer need — a phenomenon known as entitlement creep. This issue is especially prevalent in large organizations where employees, contractors, and auditors frequently change roles or take on temporary assignments.

Without a proper system to track access, managers may grant permissions quickly to avoid delays in operations, resulting in over-privileged users. This creates compliance risks, as auditors may discover employees with access beyond what is required for their role. Modern IGA solutions reduce this risk by enforcing least privilege access, supporting role-based access reviews, and automatically revoking outdated permissions.

For example, if an IT contractor’s role changes, an IGA system can automatically remove access to old systems and assign access to new ones according to their updated responsibilities. This process is often driven by automated workflows that prompt managers to review and approve access changes, ensuring accountability and auditability.

IGA systems also introduce classification tags (e.g., “GDPR personal data” or “high-risk data”) to categorize resources, ensuring that specific access rights are aligned with compliance requirements. By continuously verifying user access and periodically prompting system owners to review entitlements, IGA solutions reduce compliance risk and ensure system integrity.

How Identity Governance and Administration can help



Business Workflows & Process Automation

Effective IGA is not just about managing identities — it's about managing the business workflows that grant, review, and revoke access. When workflows are manual, inconsistencies and delays are inevitable. IT teams often use spreadsheets to track access changes, a practice that is error-prone and non-compliant with applicable regulations.

Automating workflows ensure that access requests, approvals, and removals follow a consistent, auditable process. Users submit access requests via a centralized portal, which triggers approval workflows for managers and system owners. This automation eliminates the delays and human error that occur with manual processes.

Automated workflows also enable certification campaigns, where system owners review and verify access rights on a periodic basis. Instead of relying on manual spot-checks, IGA systems automatically generate review reports for compliance audits, providing clear evidence of who had access, when, and why. Audit trails are maintained, capturing every access decision for future reference.



Audit & Compliance Tracking

Auditability is a key compliance requirement under regulations like GDPR, NIS2, and DORA, which mandate the tracking of user access activities. IGA solutions provide a centralized audit trail that captures all actions related to identity and access — from initial requests and approvals to access changes and revocations. This data is stored in a secure, tamper-proof log, offering organizations end-to-end visibility into who accessed what, when, and for what reason.

Relying on spreadsheets to track access requests can result in fragmented records that fail to meet compliance requirements. IGA systems solve this problem by automatically recording all access decisions, along with the justification for those decisions. This approach improves audit readiness and allows companies to quickly respond to regulatory inquiries.

Advanced IGA solutions also offer interactive dashboards, such as an Audit Trail Dashboard or an Identity History Dashboard, which allow administrators to drill down into specific user activity and view permission changes, access requests, and certification reviews. This level of transparency significantly reduces the workload of IT and compliance teams, who would otherwise spend hours preparing audit evidence.

The Role of Generative AI in IGA

Emerging technologies like **Generative AI (GenAI)** and **Machine Learning (ML)** are transforming IGA by introducing smarter, more efficient access request and approval processes. With AI-powered systems, users can request access via conversational interfaces like **Microsoft Teams**, where natural language processing (NLP) allows users to type simple requests like, "Grant access to the HR system." The IGA platform interprets this request and initiates an approval workflow, recommending role-appropriate access while flagging any potential risks.

AI also supports **context-aware approvals**, where business approvers receive recommendations for access decisions based on **peer-group analysis**. For example, if five employees in the same role have access to a particular system, the IGA system may flag this as "standard access" and recommend automatic approval. If the request is unusual or could create a **Segregation of Duties (SoD) conflict**, the system may recommend further review.

According to **Gartner**¹, by 2027, **20% of business processes** will be autonomously managed by AI-driven analytics. The adoption of **AI-assisted access approvals** allows businesses to reduce human error, enhance security, and increase compliance. Additionally, AI-powered automation allows **low-risk access requests** to be auto-approved without human intervention, reducing decision fatigue for managers.

IGA as a Strategic Asset for Compliance & Beyond

Modern **IGA solutions** have evolved from simple access management tools to essential components of operational resilience and compliance. By automating the full **identity lifecycle**, organizations can reduce manual intervention, improve accuracy, and enhance security. **Access reviews and audit trails** ensure compliance with regulatory standards like **GDPR, NIS2, and DORA**, while **AI-driven automation** reduces decision fatigue for business managers.

By embedding IGA into daily business operations, organizations achieve:

- ✓ **Faster onboarding** for employees, contractors, and third parties.
- ✓ **Automatic removal of outdated access rights** to prevent entitlement creep.
- ✓ **Comprehensive auditability** with dashboards for audit readiness.
- ✓ **Automated certification campaigns** that ensure ongoing compliance.

With IGA, businesses can shift from reactive compliance to proactive security, treating identity governance as a **strategic asset**. Rather than focusing on access control alone, modern IGA systems enable organizations to manage **operational efficiency, regulatory compliance, and risk mitigation** in one unified platform. By doing so, companies position themselves for growth, resilience, and regulatory alignment in an ever-evolving compliance landscape.

Omada Identity Cloud

Omada's modern, cloud-native approach to IGA transcends traditional compliance measures by embedding identity governance into the core of business operations. By using AI, automation, real-time visibility, and scalable workflows, Omada empowers organizations to not only meet regulatory obligations but also enhance their security posture and operational efficiency. In an increasingly dynamic and high-stakes regulatory environment, Omada's solutions provide the tools and methodologies required to navigate complexity with confidence and precision.

Omada is a global market leader in Identity Governance and Administration (IGA) that offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach. Omada has operations in North America and Europe, delivering solutions directly and via a network of skilled partners and system integrators.

Glossary

AI - Artificial Intelligence

Simulation of human intelligence processes by machines, enabling tasks like learning and problem-solving.

CIS - Center for Internet Security

A nonprofit organization that develops globally recognized best practices for securing IT systems and data.

CMMC - Cybersecurity Maturity Model Certification

A framework developed by the U.S. Department of Defense to assess and enhance the cybersecurity posture of defense contractors.

DORA - Digital Operational Resilience Act

An EU regulation aimed at strengthening the resilience of financial institutions against cyber threats and operational disruptions.

DPDP - Digital Personal Data Protection Act

India's data protection law establishing principles for data processing, consent, and penalties, similar to GDPR.

FCI - Federal Contract Information

Information provided by or generated for the U.S. government under contract, not intended for public release.

GDPR - General Data Protection Regulation

An EU regulation governing data protection and privacy for individuals within the European Union and the European Economic Area.

HIPAA - Health Insurance Portability and Accountability Act

A U.S. federal law establishing national standards to protect sensitive patient health information.

IGA - Identity Governance and Administration

Processes and technologies for managing and controlling access to enterprise resources, ensuring appropriate access rights.

ISO/IEC - International Organization for Standardization / International Electrotechnical Commission

Organizations that develop and publish international standards, including the ISO/IEC 27000 series for information security.

MFA - Multi-Factor Authentication

An authentication method requiring two or more verification factors to gain access to a resource, enhancing security.

NIS2 - Network and Information Security Directive 2

An updated EU directive expanding the scope of cybersecurity requirements for essential and important services.

NIST - National Institute of Standards and Technology

A U.S. federal agency that develops technology, metrics, and standards, including the NIST Cybersecurity Framework.

PCI DSS - Payment Card Industry Data Security Standard

A set of security standards designed to ensure that all companies processing credit card information maintain a secure environment.

PDPL - Personal Data Protection Law

Data protection laws, such as the UAE's PDPL, focusing on consent, data processing, and transfers, aligning with GDPR principles.

PIPL - Personal Information Protection Law

China's data protection law governing the handling of personal information, emphasizing data localization and stricter transfer controls.

RBAC - Role-Based Access Control

An approach to restricting system access to authorized users based on their role within an organization.

SOX - Sarbanes-Oxley Act

A U.S. federal law enacted in 2002 to protect investors from fraudulent financial reporting by corporations.

TSA - Telecommunications (Security) Act

A UK act imposing new security obligations on public telecommunications providers to enhance infrastructure security.

UK GDPR - United Kingdom General Data Protection Regulation

The UK's data protection regulation mirroring the EU's GDPR following Brexit.



About Omada

Omada Identity simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

www.omadaidentity.com