The Modern Approach to Identity Governance Administration

Whitepaper

ACEN

CRONOS EUROPA

About this publication

This whitepaper is published by Cronos Europa as part of its cybersecurity insight series and features the expertise of ACEN, a sister company within De Cronos Groep specialising in Identity Governance and Administration, Identity and Access Management, Privileged Access Management and cybersecurity.

Introduction

Dear Reader,

Across Europe, digital identity has become more than a cybersecurity topic. It has become a matter of governance, resilience and technological sovereignty.

European institutions and public sector organizations are facing an increasingly complex landscape. New regulations such as NIS2, DORA and the Cyber Resilience Act require stronger controls over identities, access rights and accountability. At the same time, geopolitical tensions and growing concerns about strategic dependencies are forcing organizations to reassess the technologies that underpin their digital operations.

Identity Governance and Administration (IGA) sits at the intersection of these challenges.

An effective IGA strategy enables organizations to understand who has access to which systems, why that access exists, how it is governed and how it evolves over time. It creates visibility, accountability and control across the entire identity lifecycle. These capabilities are essential not only for cybersecurity and compliance, but also for achieving greater digital autonomy and reducing dependency on opaque or closed technology ecosystems.

As Europe places increasing emphasis on technological sovereignty, organizations are being challenged to look beyond traditional security requirements. They must understand where critical dependencies exist, how access to sensitive information is managed, whether they retain sufficient control over their digital assets and how they can maintain operational continuity if technology, suppliers or regulatory environments change.

At Cronos Europa and ACEN, we believe that identity is one of the most strategic building blocks of a secure and sovereign digital environment. Through more than 19 years of experience in Identity and Access Management, Identity Governance, Privileged Access Management and cybersecurity, we have helped organizations across both the public and private sector strengthen their security posture while maintaining control over their digital ecosystem.

This whitepaper outlines our practical approach to Identity Governance and Administration. It explores how organizations can use IGA to support compliance initiatives, strengthen Zero Trust strategies, modernize identity management, improve governance and prepare for a future where cybersecurity, operational resilience and digital sovereignty increasingly converge.

We hope this document provides practical insights and strategic guidance for organizations seeking to build a secure, compliant and future-ready identity foundation.

Kind regards,

Cronos Europa and the ACEN Identity Security Team

Table of contents

Chapter 1

Identity Governance as a Pillar of European Digital Sovereignty

Digital Sovereignty Starts with Control

Across Europe, digital sovereignty has rapidly evolved from a political ambition into a strategic necessity.

The European Union increasingly recognizes that critical digital infrastructure, cloud platforms, software ecosystems and data services are no longer merely technological assets. They have become strategic dependencies that influence economic resilience, public services, national security and organizational continuity.

Through initiatives such as the European Technological Sovereignty Package, the European Commission has made clear that Europe must strengthen its ability to control the digital foundations on which governments, institutions and businesses depend.

This shift is driven by a simple reality.

Many European organizations rely heavily on non-European technology providers for identity management, cloud services, collaboration platforms, infrastructure and software development. While these technologies have enabled innovation and growth, they have also created dependencies that are often poorly understood and rarely assessed from a governance perspective.

As geopolitical tensions increase and regulatory requirements evolve, organizations are increasingly asking new questions:

- Do we know who controls access to our critical systems?
- Can we demonstrate how access decisions are made?
- Do we have sufficient visibility into privileged access?
- Can we migrate to alternative solutions if circumstances require it?
- Do we fully understand our technological dependencies?
- Are we maintaining control over our digital identities?

These questions place identity at the centre of digital sovereignty.

Why Identity Matters

Every digital interaction starts with an identity.

Employees, contractors, citizens, patients, students, partners, applications, service accounts and increasingly AI-driven agents all require access to digital resources.

As organizations modernize their digital environments, the number of identities continues to grow exponentially. At the same time, access rights become more complex due to hybrid infrastructures, cloud adoption, remote work, third-party collaboration and automated processes.

For many organizations, identities have become the new security perimeter.

The challenge is not simply knowing who exists within the organization. The challenge is understanding:

- Who has access to what.
- Why that access exists.
- Whether the access remains appropriate.
- Who approved the access.
- Whether excessive privileges have accumulated over time.
- How access can be reviewed, adjusted or removed.

Without clear governance over identities and access rights, organizations lose visibility and control over one of the most critical elements of their digital environment.

Digital Sovereignty Requires More Than Compliance

Many organizations first encounter Identity Governance and Administration (IGA) through compliance initiatives.

Regulations such as NIS2, DORA, GDPR and national cybersecurity frameworks increasingly require organizations to demonstrate proper governance of identities and access rights.

However, limiting IGA to compliance significantly underestimates its strategic value.

Compliance focuses on proving that controls exist.

Digital sovereignty focuses on ensuring that organizations retain meaningful control over their digital environment.

Identity Governance contributes to this objective by creating transparency, accountability and operational control across the entire identity lifecycle.

Organizations gain the ability to:

- Understand who has access to critical assets.
- Detect inappropriate or excessive permissions.
- Govern third-party access consistently.
- Support segregation of duties requirements.
- Maintain auditability and accountability.
- Reduce operational dependence on manual processes.
- Establish clear ownership over digital identities.

These capabilities are not only important for auditors and regulators. They are essential for organizations seeking greater autonomy and resilience.

The Role of Open Architectures and Open Source

Digital sovereignty does not imply technological isolation.

Organizations will continue to rely on commercial technology providers where they deliver clear business value. The objective is not to eliminate external dependencies entirely, but to manage them consciously and maintain strategic flexibility.

This is where open architectures and open-source technologies increasingly enter the conversation.

Across Europe, organizations are evaluating open-source identity platforms such as MidPoint and Keycloak alongside established commercial solutions.

The motivation is often broader than cost reduction.

Open technologies can provide:

- Greater transparency.

- Improved interoperability.
- Reduced vendor lock-in.
- Enhanced portability.
- Stronger control over configurations and integrations.
- Greater flexibility in deployment models.

However, open source is not automatically more secure, more compliant or easier to manage.

Successful adoption requires professional governance, operational maturity, lifecycle management, monitoring and continuous security oversight.

The real objective is not to replace one dependency with another, but to create an identity ecosystem that provides sufficient control, flexibility and long-term sustainability.

Identity Governance as the Foundation

Identity Governance provides the governance layer that enables organizations to manage identities consistently, regardless of the underlying technologies.

Whether organizations choose commercial platforms, open-source solutions or hybrid environments, they require a governance framework that establishes:

- Identity ownership.
- Role models.
- Access policies.
- Approval workflows.
- Certification processes.
- Audit trails.
- Segregation of duties controls.
- Lifecycle automation.

This governance layer creates consistency across complex environments and enables organizations to maintain control as technology landscapes evolve.

It also provides the foundation for broader initiatives such as Zero Trust, Privileged

Access Management, Identity Threat Detection and Response (ITDR), cloud security and AI governance.

Looking Ahead

Europe's digital future will be shaped by two complementary objectives.

The first is cybersecurity: protecting organizations against increasingly sophisticated threats.

The second is digital sovereignty: ensuring organizations maintain sufficient control over the technologies, identities and infrastructures on which they depend.

Identity Governance and Administration sits at the intersection of both objectives.

It strengthens security, supports compliance, enables operational efficiency and provides the visibility and governance required to reduce strategic dependency.

For European institutions and organizations, identity governance is no longer simply an IAM initiative.

It is a strategic capability that enables resilience, accountability and control in an increasingly interconnected digital world.

The following chapters explore how organizations can translate these principles into practice through a structured Identity Governance and Administration strategy, supported by proven implementation approaches, governance frameworks and real-world use cases.

Chapter 2

Strategic Compliance through NIS2 and Zero Trust with IGA

Overview of NIS2 and Zero Trust

NIS2: The Directive on Security of Network and Information Systems(NIS2) aims to improve the overall level of cybersecurity across the European Union. It establishes comprehensive requirements for risk management, incident response, business continuity, and supply chain security, among other areas. Organizations subject to NIS2 must adhere to these stringent guidelines to enhance their resilience against cyber threats.

Zero Trust: Zero Trust is a cybersecurity framework that mandates strict verification for all users, whether inside or outside the organization's network. The principle of 'never trust, always verify' ensures that access is continuously authenticated and authorized. This approach is critical for meeting the dynamic security requirements outlined in NIS2, as it mitigates risks by assuming that threats could come from anywhere.

Broad Compliance Requirements of NIS2

NIS2 mandates a holistic approach to cybersecurity, including:

- **Risk Analysis and Management**

Conducting regular risk assessments to identify and mitigate potential threats.

- **Incident Response**

Developing and maintaining incident response plans to manage and recover from cybersecurity incidents.

- **Business Continuity Planning**

Ensuring that critical business functions can continue during and after a disruption.

- **Supply Chain Security**

Implementing security measures to protect against risks associated with third-party suppliers and partners.

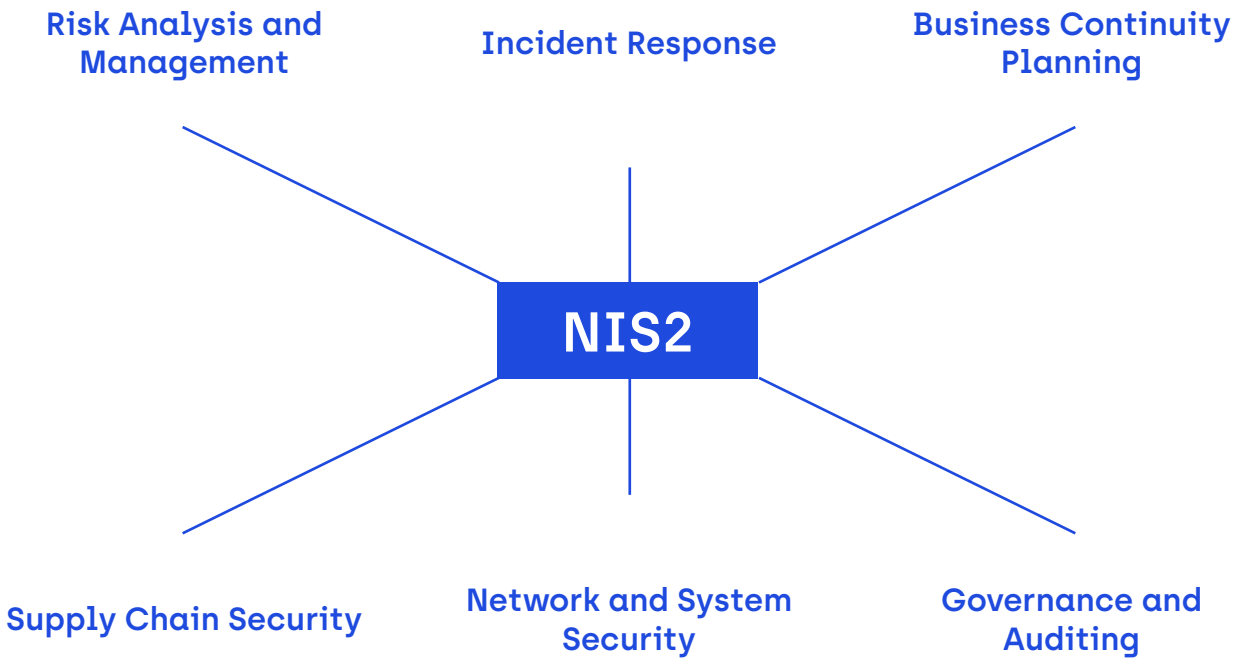
- **Network and System Security**

Protecting IT infrastructure from unauthorized access and ensuring secure system configurations.

- **Governance and Auditing**

Establishing governance frameworks and conducting regular audits to ensure compliance with security policies and regulatory requirements.

IGA plays a crucial role in the broader compliance framework by managing identities and access rights. However, organizations must also implement complementary tools and practices to address all NIS2 requirements comprehensively. This might include endpoint detection and response (EDR), data loss prevention (DLP), and other advanced security measures.



The Role of IGA in Achieving NIS2 Compliance

Identity Governance Administration (IGA) is essential for managing user identities and access rights within an organization. It ensures that access is granted based on the principle of least privilege, meaning users have only the permissions necessary to perform their roles. This aligns with both NIS2 and Zero Trust by providing robust access controls and continuous monitoring of user activities.

To comply with NIS2, organizations must implement a variety of security measures. IGA directly supports several of these requirements:

- **Risk Analysis**

IGA tools help identify and mitigate risks by ensuring that only authorized users have access to critical systems and data.

- **Incident Handling**

Detailed logs and access reports from IGA solutions enable quick identification and response to security incidents.

- **Business Continuity and Crisis Management**

By managing and monitoring access rights, IGA contributes to maintaining operational integrity during disruptions.

- **Supply Chain Security**

IGA controls and monitors third-party access, ensuring that external partners only have access to necessary resources.

- **Network and System Security**

While primarily focused on identities, IGA supports network security by restricting unauthorized access and providing insights into user activities.

- **Auditing and Governance**

IGA provides comprehensive audit trails and reports, which are essential for regulatory compliance and internal governance.

ACEN's Approach to Implementing IGA

Strategy Development: ACEN begins by thoroughly assessing the current cybersecurity measures and compliance status of an organization. This involves understanding existing policies, identifying gaps, and mapping out areas where IGA can provide significant improvements.

Implementation Process: The implementation of IGA by ACEN follows a structured approach:

step one
Initial Assessment

Evaluating the organization's current state and identifying key areas for improvement.

step two
Tailored Strategy Development

Crafting a tailored IGA implementation plan that aligns with the organization's specific needs and compliance requirements.

step three
Tool Deployment

Installing and configuring IGA tools to integrate seamlessly with the existing IT infrastructure.

step four
Policy and Workflow Design

Defining access policies and workflows that adhere to the principle of least privilege and support continuous verification.

step five
Training and Support:

Providing comprehensive training for staff and ongoing support to ensure the effective use of IGA solutions.

step six
Continuous Improvement

Regularly reviewing and updating the IGA implementation to adapt to new threats and evolving compliance requirements.

By leveraging ACEN's expertise and comprehensive IGA solutions, organizations can significantly enhance their compliance posture and overall cybersecurity framework.

Chapter 2
Conclusion

Strategic compliance through the NIS2 Directive and Zero Trust framework requires a comprehensive and integrated approach to cybersecurity. This chapter has detailed the critical elements of NIS2, emphasizing the necessity for risk management, incident response, business continuity, and supply chain security. Zero Trust principles further enhance these requirements by ensuring continuous verification and strict access controls.

Identity Governance Administration (IGA) is pivotal in fulfilling these compliance mandates. By managing identities and access rights, IGA supports risk analysis, incident handling, business continuity, supply chain security, network and system security, and governance and auditing. ACEN's structured approach to implementing IGA, from initial assessment to continuous improvement, equips organizations with the tools and strategies needed to meet NIS2 guidelines effectively. Leveraging ACEN's expertise ensures a robust compliance posture and a fortified cybersecurity framework, positioning organizations to thrive in the face of evolving digital threats.

Chapter 3

Approaches in Identity Governance and Administration (IGA)

This section explores the key methods of IGA, the Lifecycle and Governance approaches, by discussing their functions, advantages, and practical uses with in-depth case studies.

While these approaches are not mutually exclusive and can be combined to achieve optimal results, we typically see a focus on one or the other based on the priorities of the company and who is sponsoring the project. For instance, IT departments tend to favour the Lifecycle Approach, while compliance officers prefer the Governance Approach.

Governance Approach to IGA

The Lifecycle Approach in Identity Governance and Administration (IGA) focuses on the effective management of user permissions through each phase of a person's involvement with an organization. This strategy seeks to automate and simplify access control mechanisms, reducing the workload on IT staff and promoting more efficient oversight by departmental managers.

Organizations that typically implement the Lifecycle Approach are ones with frequently changing personnel structures and high volumes of role modifications. Large organisations, such as educational entities and government bodies, find value in automating user rights assignment and removal, cutting down on manual errors, and ensuring employees have immediate access to the resources they require for their roles.

The Lifecycle Approach is illustrated by the identity lifecycle graphic below, which depicts different phases of an employee's tenure at a company. From the initial employment to the possibility of returning after leaving, each phase demands particular adjustments to access rights. The transitioning nature of user access across these various stages confirms the necessity for an automated process to efficiently manage these changes.

Become a contractor →	Joiner
1st work day →	Provisioning of access
Prolong Contract →	Change End-date
Become Employee →	Identity Conversion & Mover
Name Change →	Master data change
Promotion →	Mover & Manager role
Change department →	Mover
Holiday →	Delegate access
Maternity leave →	Leaver (Temporary)
Return from leave →	Joiner (Return)
Resigns →	Leaver
Rejoins →	Joiner (Rejoin)
Retire →	Leaver

Case Study: VDAB

Context and Challenges: VDAB, a public employment service in Belgium, encountered significant challenges with their manual process of managing access rights. The existing system was not only time-consuming but also prone to errors, with delays often compromising security and productivity.

Tailored IGA Solution: ACEN implemented an automated lifecycle management system tailored to VDAB's specific needs. The solution integrated seamlessly with VDAB's human resources management system, enabling dynamic updates to access rights as employee statuses changed due to promotions, department transfers, or terminations.

Implementation and Results: The automated system significantly reduced the workload on VDAB's IT staff by enabling business users to manage access rights without coding or IT involvement. Automated triggers adjusted access permissions in real-time based on role changes, ensuring employees received appropriate access promptly. This shift not only enhanced operational efficiency but also tightened security measures by eliminating outdated permissions, thereby reducing the attack surface for potential security breaches.

> "Since implementing the IGA solution, our processes for onboarding, offboarding, and managing roles and access rights have become significantly more efficient. Thanks to the HR role catalogue, our business teams can now easily assign the appropriate access rights based on an employee's responsibilities, without requiring additional IT support. This has saved us considerable time and has greatly improved the efficiency of our access management processes. We now have much better visibility and control over who has access to what, allowing us to respond quickly and effectively to personnel changes."

Michaël Devillé

I&T Manager Software Factory

Lifecycle Approach to IGA

Contrasting with the Lifecycle Approach, the Governance Approach prioritizes comprehensive oversight and control over access permissions. This strategy is crucial for organizations that require meticulous records and detailed auditing capabilities to meet strict regulatory compliance standards.

Organizations that typically opt for the Governance Approach are those in heavily regulated industries, such as finance, healthcare, and legal sectors. These organizations need to ensure that every access permission is tracked and auditable, making it easier to comply with stringent regulations and pass audits. The governance approach emphasizes visibility, allowing organizations to monitor access in real-time and respond swiftly to any irregularities.

The Governance Approach focuses on establishing rigorous access controls and maintaining a continuous audit trail of access permissions. This approach is indispensable for maintaining compliance with regulations like GDPR and NIS2, ensuring that organizations can provide detailed reports on who has access to what information and when.

Case Study: Investment Bank

Context and Challenges: An investment bank required a robust mechanism to manage and monitor access rights systematically due to stringent financial regulations and audit requirements. The primary challenge was maintaining a system that was not only compliant with regulations like GDPR but also capable of providing detailed, auditable records on demand.

Tailored IGA Solution: ACEN developed a governance-centred IGA framework for the client that provided granular visibility into access permissions across the organization. This system was engineered to track and log all changes to access rights, providing a comprehensive audit trail that could be accessed and analysed at any moment.

Implementation and Results: The governance approach enabled the bank to proactively manage user access based on real-time data, significantly enhancing their ability to respond to audit inquiries and compliance checks. The system's ability to generate detailed reports on demand reduced the time and resources spent on compliance activities and improved the overall security posture by ensuring only authorized access to sensitive information.

Chapter 3
Conclusion

Both the Lifecycle and Governance approaches to IGA offer distinct advantages that cater to different organizational needs. However, these approaches are not mutually exclusive, and organizations can benefit from adopting elements of both strategies. For instance, investing in automation can make governance easier by reducing human errors, streamlining compliance activities, and providing accurate data for audits. Likewise, investing in governance can make automation easier by establishing clear and consistent role definitions, access policies, and approval workflows. Thus, by balancing automation and governance, organizations can optimize their IGA frameworks and achieve the best outcomes for their security and efficiency goals.

Chapter 4

Transitioning from Legacy IAM to Cutting-edge IGA

This chapter analyses the challenges inherent in legacy Identity and Access Management (IAM) solutions and outlines a strategic approach for transitioning to cloud-based Identity Governance and Administration (IGA) systems. While a complete overhaul can be tempting, a phased approach often proves more manageable and less disruptive.

Challenges of Legacy IAM Systems

Traditional IAM systems, often on-premises and built on rigid architectures, struggle to adapt to the evolving threat landscape and the complexities of modern IT environments. Key challenges include:

Scalability and Performance

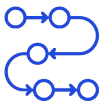
Legacy systems often struggle with the demands of growing user bases and increasing data volumes, impacting performance and user experience.

Limited Visibility and Control

Fragmented systems hinder comprehensive visibility into access rights across the organization, making it difficult to enforce consistent security policies and demonstrate compliance.

Integration Complexities

Integrating legacy systems with cloud applications and emerging technologies often proves costly and time-consuming.



Manual Processes

Reliance on manual provisioning and de-provisioning processes introduces inefficiencies, errors, and security vulnerabilities.

Benefits of Cloud-based IGA

Transitioning to a cloud-based IGA solution offers compelling advantages, including:

Enhanced Security Posture

Centralized access management, automated provisioning and de-provisioning, and robust access control mechanisms strengthen security and reduce the risk of unauthorized access.

Improved Compliance

Streamlined audit trails, automated reporting, and pre-built compliance frameworks simplify regulatory compliance efforts.

Increased Operational Efficiency

Automated workflows for user lifecycle management, access requests, and certification campaigns free up IT resources and reduce operational costs.

Scalability and Flexibility

Cloud-based solutions offer the scalability to accommodate growing user bases and the flexibility to adapt to changing business requirements.

Transitioning to Cloud IGA: A Phased Approach

A "big bang" approach to IGA implementation, while tempting, can be disruptive and risky. A phased approach allows organizations to gradually transition to the new system, minimizing business impact and facilitating a smoother adoption:

Phase 1: Planning and Preparation

1. Define Objectives and Scope:
   Client Responsibility: Clearly articulate your business drivers for change, desired outcomes, and the scope of the IGA implementation.
   ACEN's Role: Assist in refining these objectives to align with best practices and ensure a comprehensive approach.

2. Conduct a Thorough Assessment:
   Client Responsibility: Provide access to current IAM landscapedetails, including systems, processes, users, and applications.
   ACEN's Role: Evaluate the current IAM setup, identify gaps, risks, and opportunities for improvement.

3. Develop a Roadmap:
   Client Responsibility: Collaborate in outlining priorities and critical functionalities.
   ACEN's Role: Create a phased implementation plan, focusing on quick wins and essential features.

4. Establish Communication Channels:
   Client Responsibility: Collaborate in outlining priorities and critical functionalities.
   ACEN's Role: Create a phased implementation plan, focusing on quick wins and essential features.

Phase 2: Parallel Implementation and Evaluation

5. Implement the Cloud IGA Solution:
   Client Responsibility: Provide necessary access and resources for integration.
   ACEN's Role: Configure and integrate the cloud-based IGA system with initial target systems.

6. Run in Read-Only Mode:
   Client Responsibility: Monitor and review access patterns and potential issues.
   ACEN's Role: Deploy the IGA solution in "read-only" mode to observe existing access patterns.

7. Leverage Policy Emulation:
   Client Responsibility: Client Responsibility: Review and provide feedback on access policies.
   ACEN's Role: Utilize the IGA system's policy emulation to validate and refine access policies.

8. Conduct User Acceptance Testing (UAT):
   Client Responsibility: Involve key stakeholders and provide necessary feedback.
   ACEN's Role: ACEN's Role: Facilitate rigorous evaluation to ensure the solution meets business requirements.

Phase 3: Gradual Rollout and Optimization

9. Prioritize Business-Critical Applications:
   Client Responsibility: Identify and prioritize business-critical applications
   ACEN's Role: Integrate these applications with the IGA system, ensuring secure access.

10. Phased User Onboarding:
    Client Responsibility: Provide user lists and support for training.
    ACEN's Role: Gradually onboard users, offering training and support to minimize disruption.

11. Continuous Monitoring and Optimization:
    Client Responsibility: Provide ongoing feedback and report any issues.
    ACEN's Role: Monitor system performance, user feedback, and security events, making necessary optimizations.

Key Considerations for a Successful Transition

- **Business Impact Mitigation**

Anticipate and mitigate potential business disruptions by carefully planning the rollout schedule and providing adequate user support.

- **Image Management**

Proactively manage communication around the IGA implementation to avoid negative perceptions and ensure user buy-in.

- **Collaboration is Key**

IGA implementations are not just technological endeavours. Foster close collaboration between IT, security, and business stakeholders throughout the process.

By adopting a phased approach, organizations can successfully navigate the complexities of transitioning from legacy IAM to cloud-based IGA, reaping the benefits of enhanced security, improved compliance, and increased operational efficiency.

Chapter 4
Conclusion

Transitioning from legacy IAM systems to cloud-based IGA solutions presents notable challenges but also significant benefits. Legacy IAM systems often struggle with scalability, performance, and integration complexities, impeding robust security and compliance. A phased approach to implementation, involving careful planning, assessments, and iterative testing reduces disruptions and ensures a smoother transition by methodically addressing these issues.

The advantages of cloud-based IGA solutions are compelling, including enhanced security, improved compliance, and increased operational efficiency. Automated processes and centralized management streamline user lifecycle management and access controls, making it easier to enforce security policies and meet regulatory requirements. The scalability and flexibility of cloud solutions allow organizations to adapt quickly to changing business needs. By following a structured, phased approach, organizations can effectively leverage cloud IGA to build a more secure and efficient identity management framework.

Chapter 5

The Central Role of Identity in Cybersecurity Strategies with ACEN

Identity management is increasingly recognized as the cornerstone of comprehensive cybersecurity strategies. As digital threats evolve and organizations expand their digital footprints, the role of Identity Governance Administration (IGA) in shaping and securing organizational strategies becomes more critical. ACEN has been at the forefront of integrating robust IGA frameworks that not only protect against immediate threats but also provide a scalable foundation for future security initiatives.

Strategic Importance of Identity Management

The strategic importance of identity management lies in its ability to centralize and streamline access controls, user authentication, and compliance management. This centralization is crucial for organizations to maintain a strong security posture. ACEN assists organizations by implementing IGA solutions that ensure identities are properly managed, thus reducing the risk of data breaches and improving overall security resilience.

Implementing a strong identity management strategy via IGA has proven to make subsequent cybersecurity projects not only faster but also more cost-effective. By having a clear mapping of all identities and their access rights, organizations can quickly adapt to new regulations and security challenges without the need for extensive overhauls or custom solutions.

ACEN's Detailed Approach to IGA Implementation

Initial Assessment and Role Mapping: One of the fundamental steps in ACEN's approach to implementing IGA involves a thorough assessment of the current state of an organization's identity management practices. This assessment is crucial for understanding the existing framework and preparing for a tailored IGA solution. Here's how ACEN conducts this phase:

Discovery of Current Identity Environment

ACEN begins by cataloguing all user identities across the organization's systems and applications. This process includes gathering data on user roles, permissions, and the relationship between different roles across various departments and functions.

Analysis of Role Definitions and Access Rights

The team analyses existing role definitions to identify redundancies, inconsistencies, and gaps in access control. This analysis helps in understanding how roles are structured and how permissions are assigned, which is critical for ensuring that the IGA framework aligns with actual business needs and compliance requirements.

Role Rationalization

Based on the initial findings, ACEN works with stakeholders to rationalize and streamline roles. This involves consolidating similar roles, defining clear access rights for each role, and establishing protocols for role changes. Role rationalization reduces complexity and enhances the manageability of identities and access rights.

Mapping Business Processes to Roles

Important to this phase is mapping business processes to specific roles. ACEN ensures that each role is clearly defined with respect to the business processes it impacts. This alignment is crucial for setting up an IGA framework that supports efficient business operations while maintaining security and compliance.

Strategic Implementation of IGA Solutions: Following the assessment and role mapping, ACEN proceeds with the strategic implementation of the IGA solution tailored to the specific needs of the organization.

Deployment of IGA Tools

ACEN helps organizations select and deploy the IGA solution that best fits their specific requirements. We offer a broad portfolio of leading commercial and open-source platforms, enabling organizations to balance functionality, budget, licensing strategy, and digital sovereignty. By offering multiple vendors, we ensure every customer receives the solution that best aligns with their business, compliance, and security objectives. Once selected, the platform is configured to support refined role definitions, automate identity governance processes, and enforce the access policies established during the role rationalization phase.

Integration with Existing IT Infrastructure

The IGA solution is integrated with the organization's existing IT infrastructure. This integration ensures that all identity and access management functions are seamlessly incorporated into the daily operations of the organization, facilitating smooth transitions and minimizing disruptions.

Continuous Monitoring and Adjustment

Post-implementation, ACEN sets up continuous monitoring mechanisms to track the effectiveness of the IGA framework. This includes regular audits and reviews to adjust roles, permissions, and access controls as necessary to adapt to changes in the organization's structure, compliance requirements, or security landscape.

Training and Support

Comprehensive training sessions are conducted for relevant staff to ensure they are proficient in using the IGA tools and understanding the new role definitions and access protocols. Ongoing support is provided to address any issues and to assist with future adjustments and refinements.

With ACEN's expertise, businesses can reap the following benefits:

- **Efficiency Through Strategic Implementation**

With ACEN's expertise, organizations benefit from strategic implementation that emphasizes efficiency and effectiveness. Our approach ensures that:

- **Identity management aligns with overall business objectives**

Making sure that every identity and access management decision supports broader business goals.

- **Resources are allocated effectively**

Optimizing security investments by prioritizing areas with the highest risk or compliance needs.

The central role of identity in cybersecurity strategies cannot be overstated. As organizations navigate complex digital landscapes, the need for a coherent, identity-centred approach to security becomes essential. ACEN remains dedicated to guiding and supporting our partners through this journey, ensuring that their cybersecurity strategies start on a solid foundation of identity governance and administration.

Chapter 5
Conclusion

Identity management is crucial for effective cybersecurity strategies, providing the foundation for protecting against digital threats and ensuring compliance. ACEN's robust Identity Governance Administration (IGA) framework centralize and streamline access controls, user authentication, and compliance management, enhancing security resilience and operational efficiency.

This ensures that identity management aligns with business objectives and optimizes security investments. By rationalizing roles and integrating IGA tools with existing IT infrastructures, we facilitate smooth transitions and minimize disruptions.

Effective identity management reduces the risk of data breaches, accelerates cybersecurity projects, and allows organizations to quickly adapt to new regulations. ACEN is committed to guiding organizations through these challenges, building a solid foundation for future cybersecurity initiatives.

Chapter 6

Transitioning from Legacy IAM to Cutting-edge IGA

This chapter emphasizes the critical need to continually adapt and modernize Identity Management solutions in the face of an ever-evolving digital landscape. Implementation is not the finish line; the correct tool will evolve alongside your organization's growth and emerging challenges.

The Limitations of Traditional Solutions in a Growing Organization

Traditional Identity management solutions often falter as organizations expand and embrace digital transformation. Consider these common pitfalls:

Scalability Bottlenecks

Legacy systems built for a specific user base and static application landscape struggle to handle significant user surges or rapid application onboarding.

* **Example:** A merger or acquisition bringing hundreds of new employees can overwhelm the capacity of an outdated system, leading to performance degradation and user frustration.

Rigid Architecture Hampering Integration

Point solutions lacking flexibility make integrating new applications, cloud services, or innovative technologies like biometrics cumbersome and costly.

* **Example:** Integrating a new solution with the existing ITSM portal that the organization already uses can be significantly challenging if the new solution only provides its own standalone user interface. This can be particularly difficult when dealing with an inflexible legacy system.

Inability to Leverage Advanced Technologies

Traditional solutions may not support the integration of Artificial Intelligence (AI) and Machine Learning (ML), limiting their capacity for predictive analysis and automated decision-making.

* **Example:** Failing to leverage AI-powered peer analysis and risk scoring can result in reactive, rather than proactive security measures, leaving organizations vulnerable to insider threats and data breaches.

ACEN: Empowering Growth through Modern IGA

ACEN recognizes that a truly future-proof approach to Identity management goes beyond implementation. We partner with organizations to build adaptable and secure IGA solutions that scale seamlessly:

Navigating High-Growth Events

We ensure your Identity management strategy can accommodate rapid organizational changes, be it through mergers and acquisitions, large-scale onboarding, or rapid application adoption.

* **Example:** During an acquisition integrating 500 new employees, our solutions automate user provisioning, role mapping, and access right adjustments across all systems, ensuring a smooth transition with minimal business disruption.

Embracing Technological Advancements

ACEN facilitates the integrat ion of innovative technologies like AI and ML to enhance security posture and streamline Identity management processes.

* **Example:** By implementing AI-driven access request and certification processes, we help organizations move beyond static rule-based approvals to dynamic risk-based assessments, automating routine decisions and freeing up IT personnel for more strategic initiatives.

Proactive Risk Management

We leverage data analytics and predictive modelling to identify and mitigate potential risks before they impact the organization.

* **Example:** Through AI-powered peer group analysis, we detect anomalous access requests that deviate from established user behaviour patterns, potentially uncovering insider threats or unauthorized access attempts.

The Power of Predictive Insights with AI

AI plays an increasingly vital role in modern Identity management. It enables:

- **Automated Access Right Management:**

AI analyses user behaviour patterns, roles, and access requests, providing intelligent recommendations for access provisioning and streamlining the request process.

- **Proactive Threat Detection:**

AI identifies and flags unusual access patterns, such as off-hours login attempts or access to sensitive data outside typical job roles, alerting security teams to potential threats.

- **Improved Decision Making:**

AI analyses vast amounts of data to provide insights and predictive models, supporting informed decisions about access policies, resource allocation, and security investments.

Chapter 6
Conclusion

It is no longer sufficient for organizations to simply manage identities, they need to actively govern and administer access rights intelligently and efficiently.

ACEN empowers organizations to embrace a proactive and future-proof security posture, ensuring secure and seamless IGA even in the face of constant change and accelerating growth. Our solutions and expertise pave the way for a confident and secure digital future.

Chapter 7

Approaches in Identity Governance and Administration (IGA)

The merging of Identity Governance Administration (IGA) with Privileged Access Management (PAM) marks a pivotal integration in the cybersecurity sphere, especially when the management of identities and privileged access grows increasingly intricate. This chapter discusses the strategic benefits and challenges of this integration, based on ACEN's expertise, and outlines a practical approach for merging a new IGA system with an existing PAM solution. A case study illustrates the successful implementation of this integration.

The Current State of IGA and PAM

Market Trends: Recent trends in cybersecurity show a rapid evolution of IGA and PAM, driven by rising regulatory demands and the need to mitigate sophisticated threats. These trends highlight a movement toward integrating IGA and PAM solutions, a strategy that recognizes the limitations of managing identities without overseeing privileged access.

Synergistic Benefits: Integrating IGA and PAM offers numerous advantages, including:

- Strengthened security through joint management of identities and privileged access.
- Enhanced compliance capabilities with detailed auditing of both regular and privileged activities.
- Streamlined operations by unifying identity and access management processes.

At the same time, Integrating IGA and PAM systems also presents distinct challenges:

- The complexity of merging two advanced systems can be substantial.
- Changes in IT management practices and the reallocation of privileged rights might face resistance.
- Aligning policies across both systems to maintain consistency and compliance can be difficult.

ACEN's Approach to Integration

ACEN approaches the integration of IGA and PAM with a focus on strategic alignment and technical precision. For organizations looking to integrate a new IGA system with an existing PAM solution, we advise the following steps:

step one
Define Integration Goals

Determine the desired outcomes of the integration, such as enhanced security or streamlined operations.

step two
Select Compatible Technologies

Ensure that the new IGA system is compatible with the existing PAM solution, or opt for a converged platform that integrates IGA and PAM functionality in a single solution.

step three
Pilot testing

Implement a pilot integration project in a controlled environment to allow for necessary adjustments before full deployment.

step four
Gradual Deployment and Continuous Improvement

Deploy the integrated solution incrementally across the organization, continually monitoring its performance and making adjustments as needed.

Case Study: Financial Institution Implements IGA and PAM Integration

Context

A major financial institution was facing challenges in managing the lifecycle and privileges of high-risk access accounts. The decision to integrate a new IGA system with their existing PAM solution aimed to enhance security and streamline access management.

Solution

- Unified User Profiles: Comprehensive user profiles were created, incorporating regular and privileged access details.
- Automated Workflows: Automated workflows for provisioning and deprovisioning access rights were implemented, integrating IGA lifecycle management with PAM control mechanisms.
- Advanced Monitoring: Enhanced monitoring capabilities for privileged sessions were set up, combined with identity analytics to detect and address anomalous activities.

Outcome

The integration led to a robust framework that significantly minimized the risk of insider threats and improved access management efficiency, bolstering the overall security posture and compliance.

Chapter 7
Conclusion

As digital environments evolve, the integration of IGA and PAM will increasingly become crucial. Anticipated trends include the adoption of artificial intelligence to refine decision-making in access management and the expansion of cloud-based deployments requiring dynamic access controls. Organizations must continue refining their strategies to maximize the benefits of IGA and PAM integration, ensuring robust security and compliance at the highest levels.

Through careful planning, expert execution, and ongoing adaptation, ACEN assists organizations in harnessing the full capabilities of their IGA and PAM systems, securing their critical assets and setting the stage for a secure digital future.

Closing thoughts

Identity Governance and Administration is often introduced as a compliance initiative, an IAM modernization project or a security improvement program.

In reality, it has become much more than that.

As European organizations navigate an increasingly complex digital landscape, identity has emerged as one of the most critical control points within the enterprise. Every cybersecurity strategy, Zero Trust initiative, cloud transformation program and regulatory framework ultimately depends on knowing who has access to what, why that access exists and whether it remains appropriate over time.

At the same time, Europe is entering a new era of technological sovereignty. Organizations are increasingly evaluating not only the security and functionality of their digital platforms, but also the degree of control they retain over data, infrastructure, software and critical operational processes.

Identity governance plays a central role in this evolution. It provides the visibility, accountability and governance required to manage digital ecosystems responsibly, reduce unnecessary dependencies and support informed decisions about technology, suppliers and risk.

The future will not be defined by a choice between cybersecurity and sovereignty. Organizations will need both. Strong cybersecurity protects against attackers. Digital sovereignty protects against excessive dependency. Identity governance provides a foundation for achieving both objectives.

At ACEN, we help organizations build that foundation. Through our expertise in Identity Governance, Identity and Access Management, Privileged Access Management and managed cybersecurity services, we support customers in designing identity strategies that are secure, compliant, resilient and aligned with European values of transparency, control and autonomy.

Whether your organization is starting its identity governance journey, modernizing existing platforms or exploring open and sovereign alternatives, the principles outlined in this whitepaper can serve as a practical roadmap toward a more secure and future-proof digital environment.

The question is no longer whether identity governance is necessary.

The question is whether organizations have sufficient control over the identities that increasingly determine access to everything that matters.

The ACEN Identity Security Team


CRONOS
EUROPA


ACEN