ORACLE

Transitioning from Oracle Identity Governance to Oracle Access Governance

July 2025, Version 1.0

Public

ORACLE

Purpose Statement

This document serves as a comprehensive guide for organizations that are currently using Oracle Identity Governance and are considering a transition to Oracle Access Governance.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Table of Contents

Executive Summary **4**

Introduction **4**

Why Transition from Identity Governance to Access Governance? **5**

Cost Savings 5

Improved Efficiency and Productivity 5

Enhanced Security and Compliance 5

Enhanced Visibility and Insights 6

Comprehensive Governance for Hybrid Environments 6

Transition Options **6**

Option 1: Move “All at Once” to Access Governance as the Primary IGA System 6

Option 2: Gradual Migration from Identity Governance to Access Governance 8

Best Practices for Transitioning to Access Governance **11**

Plan and Assess 11

Integrate Systems 12

Test and Validate 12

Unlearn and Relearn 12

Clean Up Data 13

Train Users and Manage Change 13

Provide Post-Migration Monitoring and Support 13

High-Level Project Plan **13**

Phase 1: Initiate and Plan 14

Phase 2: Analyze and Design 14

Phase 3: Configure and Implement 15

Phase 4: Test and Validate 15

Phase 5: Deploy 15

Phase 6: Monitor and Optimize 16

Project Schedule Guidance **16**

Conclusion **17**

Appendix A: Identity Governance and Access Governance Feature Comparison **18**

Appendix B: Oracle@Oracle Case Study: Oracle's Journey to Modernize IGA **19**

Key Objectives Driving the Transition 19

A Phased Strategy for a Seamless Transition 19

Ensuring Success Through Enablement and Support 20

The Future: Intelligent, Always-on Governance 20

Executive Summary

Oracle's Identity and Access Management (IAM) software portfolio includes Oracle Identity Governance, an Identity Governance and Administration (IGA) solution that has been deployed at many customer sites. Oracle Access Governance is a modern, cloud native offering that provides IGA capabilities. Although both platforms manage access rights and identities across diverse systems, they differ significantly in their architecture and deployment models. Identity Governance is a more traditional solution, often deployed on premises or in containerized environments, and offering extensive customization capabilities. In contrast, Access Governance represents Oracle's strategic direction for modern IGA, providing a next generation, cloud native software-as-a-service (SaaS) solution built on Oracle Cloud Infrastructure (OCI). This architectural shift brings numerous advantages, positioning Access Governance as the logical evolution for organizations seeking to modernize their identity governance framework.

This document serves as a comprehensive guide for organizations that are currently using Identity Governance and are considering a transition to Access Governance. In addition to providing best-in-class functionality, the move to Access Governance offers the benefits of cloud native architecture, including scalability, high availability, and automated updates. Access Governance also uses artificial intelligence (AI) and machine learning (ML) to provide intelligent insights into identity access, automate access controls, streamline access reviews, and enable periodic and micro certifications. These capabilities enhance security and compliance with reduced manual intervention. The platform also boasts a simplified implementation process and an intuitive user experience, which empowers business users to participate more effectively in governance processes.

This document examines the specific reasons why an organization should consider this transition, outlines best practices for a smooth migration, presents a sample project plan that encompasses typical phases and activities, and provides sample estimated durations for such projects based on the complexity of the existing Identity Governance environment.

Introduction

Oracle Identity Governance has long been recognized as a comprehensive solution for managing user identities, provisioning access, and ensuring compliance across a wide range of enterprise systems. Its strength lies in its robust configuration and customization options, making it suitable for complex Identity and Access Management (IAM) environments. Typically deployed on premises or as containerized virtual machine images, Identity Governance has served as a cornerstone of the identity management strategy for many organizations.

Oracle Access Governance represents the next generation of Oracle's IGA offerings. As a cloud native SaaS solution built on Oracle Cloud Infrastructure (OCI) and Oracle Autonomous Database, Access Governance emphasizes ease of use, rapid deployment, and the integration of advanced technologies such as AI and ML. This modern approach allows organizations to seamlessly extend their IAM strategies to multicloud, hybrid, and on-premises environments. The shift to cloud adoption is a significant trend across the IT landscape, driven by the need for increased agility and scalability, and reduced operational complexity. In this evolving landscape, identity governance plays a crucial role in ensuring secure and compliant access to resources, which makes the transition to cloud native solutions like Access Governance a strategic imperative for many organizations.

This document aims to provide a detailed roadmap for organizations planning to undertake this transition, covering the key considerations and steps involved in migrating from Oracle Identity Governance to Oracle Access Governance.

ORACLE

Why Transition from Identity Governance to Access Governance?

Several key advantages of Oracle Access Governance make the transition from Oracle Identity Governance a compelling proposition.

Cost Savings

The shift to a cloud native architecture with Access Governance offers many operational benefits. As a SaaS solution, Access Governance provides inherent scalability—automatically adjusting resources to meet demand—and high availability as part of its cloud service offering. Organizations can also benefit from automated updates and patches managed by Oracle, which significantly reduces the burden of system maintenance and upgrades that are typically customer-driven and require regular attention with on-premises products. Additionally, overall DevOps cost is near zero because Access Governance is managed by Oracle, and support cost is included in the subscription fees. This reduced operational overhead allows IT teams to focus on strategic initiatives rather than routine maintenance tasks.

Improved Efficiency and Productivity

Access Governance's integration of AI and ML technologies provides a more intelligent and efficient approach to identity governance. These advanced capabilities enhance access review processes by offering peer group analysis to identify users with similar access privileges, detecting outlier access patterns that may indicate potential risks, and providing meaningful recommendations to reviewers. Access Governance can also automate micro-certifications triggered by specific events or timelines, thereby ensuring the continuous monitoring of access rights. This proactive and intelligent approach to governance can lead to an improved security posture and more efficient compliance management with less manual effort, compared to Identity Governance.

The simplified implementation and intuitive user experience of Access Governance represent a significant advantage. Access Governance is designed for quick configuration, and its business-friendly user interface enables nontechnical users to easily assume administrative capabilities. This ease of use extends to self-service interfaces for access requests and application onboarding, which increases end-user productivity and reduces the workload on IT help desks. In fact, the effort it typically takes to complete any IGA task in Access Governance is not more than five steps. In contrast, Identity Governance generally requires a steeper learning curve and often requires trained personnel for management and maintenance. The streamlined experience with Access Governance can lead to a faster time-to-value and broader adoption of governance processes across the organization.

Enhanced Security and Compliance

Access Governance offers a range of enhanced features designed to address modern security and compliance challenges. These features include access guardrails that enforce separation of duties (SoD) by implementing metadata-driven rules, such as not allowing an invoice approver to submit an invoice for payment. The platform also supports various types of access reviews, including identity access reviews, policy reviews, group reviews, and ownership reviews to verify accountability for digital assets. Furthermore, Access Governance provides deep integration capabilities with both Oracle and non-Oracle applications, which facilitates comprehensive lifecycle management and granular control over access rights. These advanced features enable organizations to implement more robust and adaptive access controls compared to Identity Governance.

Enhanced Visibility and Insights

Reporting and analytics are significantly enhanced in Access Governance, offering a wide set of ready-to-use reports and intelligent analytics. These capabilities provides better visibility into user access across the entire organization, so that managers and administrators can understand who has access to what resources and how that access was granted. The platform also offers interactive dashboards that provide valuable insights, which helps users focus on essential governance tasks.

In addition, Access Governance can publish event data, which is a process of exporting one-time data events and sequentially and continually publishing ongoing data events to external systems, such as an Oracle Cloud Infrastructure (OCI) Streaming. With Access Governance, you have the flexibility to export one-off events and continually publish data events, such as identity, identity collections, policies, resources, access to resources, and so on, and use this data for deriving insights, storing data for compliance, or for analyzing access management and governance data. In contrast, Identity Governance typically relies on Oracle Analytics Publisher for custom report generation.

Comprehensive Governance for Hybrid Environments

In today's complex IT environments, the ability to govern access across hybrid landscapes is crucial. Access Governance is designed to provide comprehensive governance across both cloud and on-premises environments. It can connect with various cloud applications and service providers through APIs and offers containerized agents for integrating with on-premises systems. This unified approach to governance simplifies the management of identities and access rights in organizations with diverse IT infrastructures, a capability increasingly important in modern enterprise architectures.

Transition Options

Transitioning from Oracle Identity Governance to Oracle Access Governance can be approached in several ways. Here are the two main options:

- **Option 1: Move “all at once” to Access Governance as the primary IGA system:** Make Access Governance your main system for all identity and access governance tasks, integrating it directly with all your data sources and applications.
- **Option 2: Gradually migrate from Identity Governance to Access Governance:** Slowly transition workloads from Identity Governance to Access Governance. In this approach, Identity Governance and Access Governance coexist till the transition is complete.

The two options are explained in the following sections.

Option 1: Move “All at Once” to Access Governance as the Primary IGA System

This option represents a complete transition where Access Governance becomes the single, unified platform for all your identity and access governance needs. This option aims to modernize and streamline your identity management processes by centralizing them within Access Governance. With this option, Access Governance directly integrates with all your authoritative sources for identity data and manages access to all applications and systems. In addition, Access Governance acts as the main governance system for creating certification campaigns and performing access reviews.

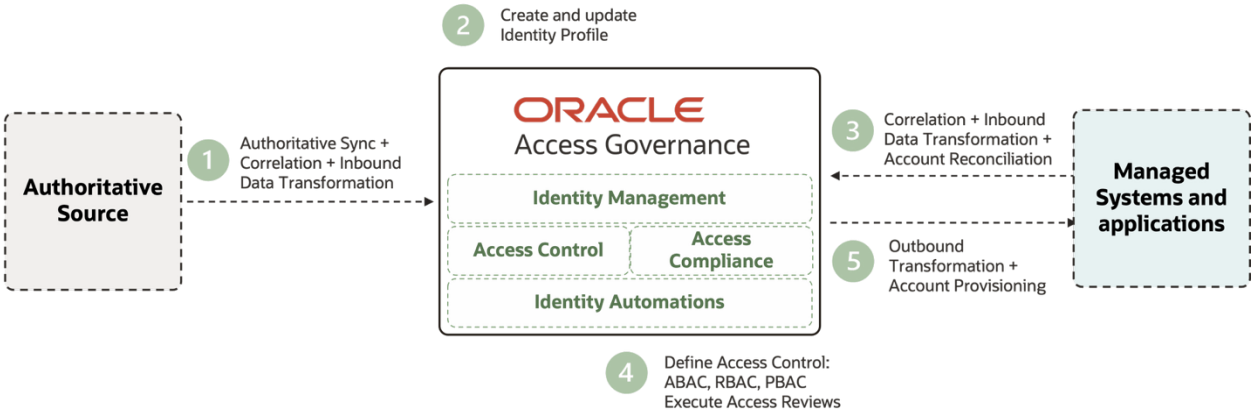

Figure 1. Oracle Access Governance as the Primary IGA System

This option provides the following benefits:

- **Unified identity management**: Access Governance directly integrates with all your authoritative sources of identity data, such as HR systems, directories (like Active Directory or LDAP), and flat files. This integration allows Access Governance to consolidate and manage all user identities within a single system.
- **Centralized access governance**: Access Governance manages access to and governance of all applications and systems, including account provisioning, account reconciliation, and access reviews. It also provides a comprehensive view of who has access to what across your entire IT landscape.
- **Modernized approach**: This option leverages the modern features and capabilities of Access Governance, offering benefits like no-code workflows, an intuitive user experience, AI/ML driven insights, and potentially more advanced access control models.

High-Level Steps for Setting Up Access Governance as the Primary IGA System

1. Integrate with the authoritative sources for onboarding and updating identity data through identity reconciliation.
2. Define correlation rules in Access Governance to link user identities from different sources and configure transformation rules as needed.
3. Review the identity-marking rules defined in the Access Governance instance to ensure that those rules take care of newly onboarded authoritative sources and their identities.
4. Create or review the codeless access review workflows in Access Governance.
5. Onboard the managed systems for governing access through account provisioning, account reconciliation, and reviewing access. If Identity Governance currently manages the application, disable this connection with Identity Governance.
6. Define account matching and outbound transformation rules in Access Governance to match user accounts from the application with identities and to define how account attributes are set during provisioning.
7. Remediate any unmatched user accounts that aren't automatically matched to identities.
8. Get a consolidated view of who has access to what across applications managed by both Access Governance and Identity Governance.
9. Create workflows in Access Governance for access requests and associate them with access bundles.

10. Manage the access permissions within your organization by using the access control framework that offers request-based, role-based, attribute-based, and policy-based access control permission models.
11. Users can request access for themselves or others through the Access Governance self-service portal. Approvers can view requests, review any compliance violations, and approve or reject requests. , After approval, access is automatically provisioned.
12. Configure default access control by using attribute-based access control (ABAC) and policy-based access control (PBAC).
13. Create campaigns and perform user access reviews.

Considerations

- **Immediate impact of advanced features**: Consider how your organization can immediately leverage Access Governance's modern user interface, streamlined workflows, enhanced reporting capabilities, and potentially more advanced access control models across the entire user base and application landscape.
- **Architectural simplification and maintenance**: Consider the benefits of a simplified architecture and reduced maintenance efforts after the migration to a single, centralized identity governance system is complete. Benefits include how it might streamline future upgrades and reduce the complexity of managing disparate systems.
- **Lower total cost of ownership (TCO)**: Consider the potential for a lower TCO by transitioning to a single, SaaS-delivered enterprise IGA solution like Access Governance, thereby eliminating the costs associated with managing multiple IGA systems.
- **Migration effort and change management**: Consider the level of effort and resources required for a complete migration, as well as the essential change management activities needed to prepare and support your organization and users throughout this transition.

Option 2: Gradual Migration from Identity Governance to Access Governance

This option involves a step-by-step migration of workloads from Identity Governance to Access Governance.

This option might involve multiple stages, with first integrating Access Governance with Identity Governance in a hybrid model. This hybrid approach uses Identity Governance as the foundational system for managing the core, day-to-day operations of user identities and access provisioning, thereby leveraging existing infrastructure and processes. Complementing this, the Access Governance system is employed specifically for the critical compliance function of conducting periodic access reviews or certifications, which allows organizations to potentially use a more specialized or modern tool focused solely on verifying the ongoing appropriateness of user permissions. This strategy effectively separates access control tasks from governance oversight, combining established management capabilities with focused review functionalities.

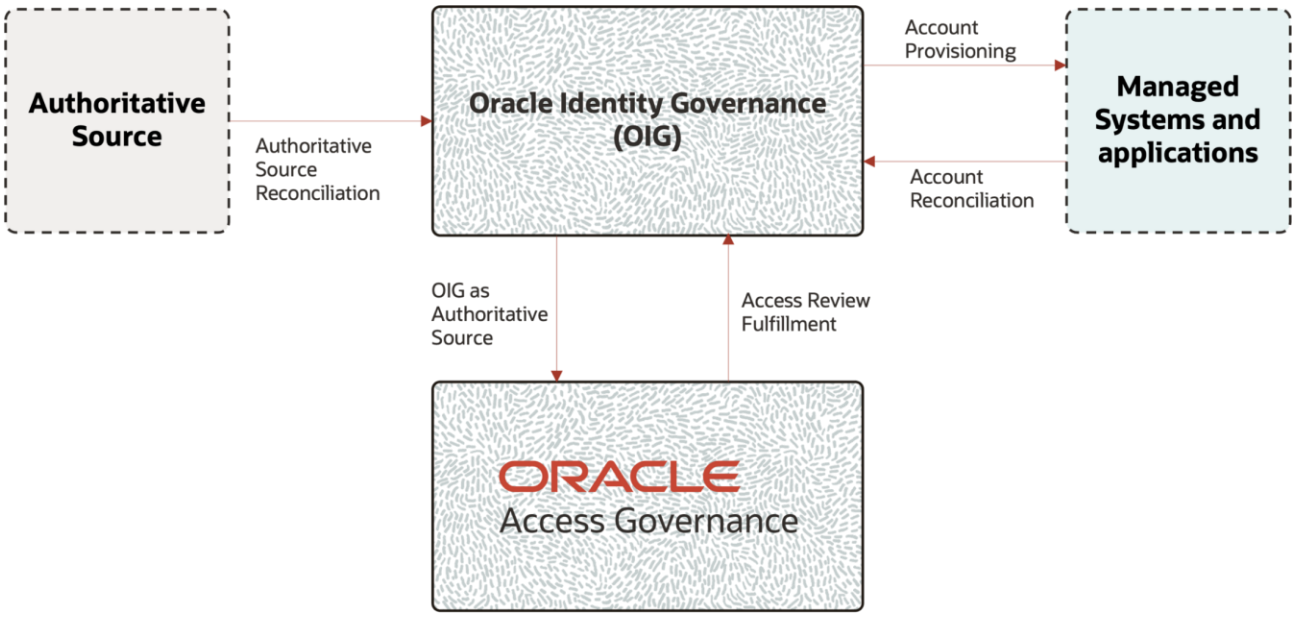

Figure 2. Hybrid Architecture with Identity Governance and Access Governance

High-Level Steps for Setting Up the Hybrid Architecture

1. Set up an Access Governance instance in Oracle Cloud.
2. Connect Access Governance to your existing Identity Governance system through agent-based integration.
3. Define rules in Access Governance to activate and categorize users.
4. Review the access profile of users onboarded in Access Governance. Oracle Access Governance offers complete visibility into who has access to what and how that access is granted to identities, and resources, through multiple access dashboards
5. Create workflows in Access Governance to manage the approval process for access reviews.
6. Schedule access review campaigns in Access Governance. User access reviews can be defined in Access Governance to certify request-based permissions assigned to the users in Identity Governance by running periodic access certifications and event-based micro-certifications.
7. Perform access review tasks within Access Governance.

Eventually, Access Governance can directly connect to your main data sources to manage identity information. Access Governance can also start managing access provisioning for some applications. The following diagram shows this state in which a set of authoritative sources and a set of managed systems and applications are moved over to Access Governance and are managed in parallel.

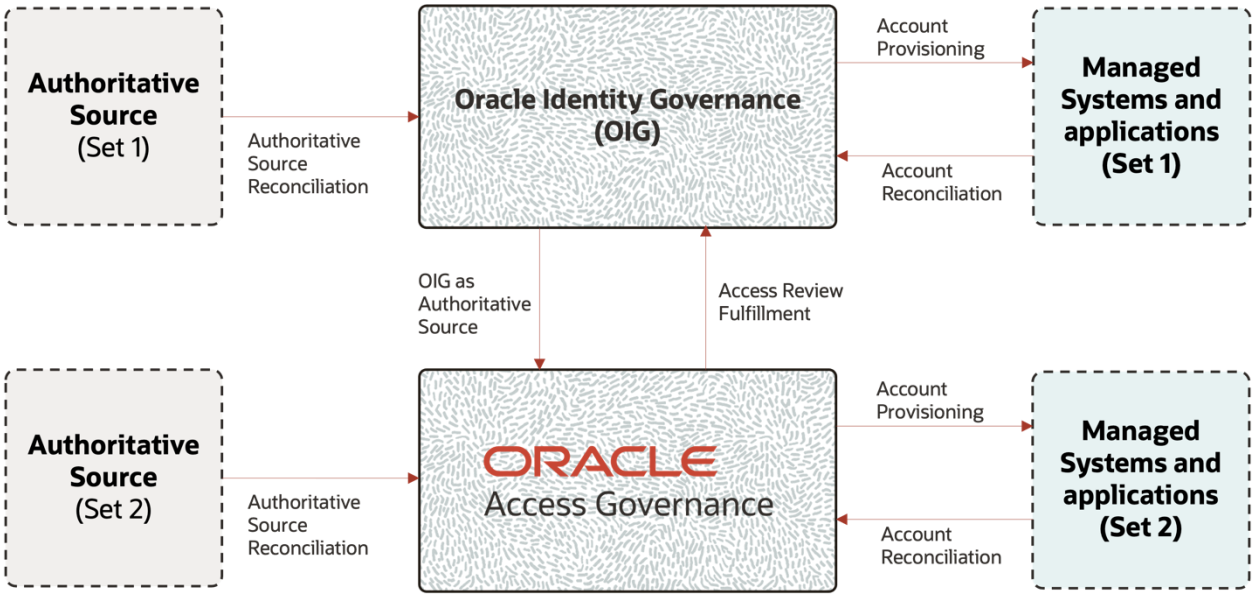

Figure 3. Transition State: Identity Governance and Access Governance Coexistence

High-Level Steps for Performing Access Reviews for Additional Managed Systems with Access Governance

1. Integrate with the authoritative source for onboarding and updating identity data through identity reconciliation.
2. Define correlation rules in Access Governance to link user identities from different sources and configure transformation rules as needed.
3. Review the identity-marking rules defined in the Access Governance instance to ensure that those rules take care of newly onboarded authoritative source and its identities.
4. Create or review the codeless access review workflows in Access Governance.

High-Level Steps for Using Access Governance as the Provisioning Engine for Managed Systems

1. Onboard the managed systems for governing access through account provisioning, account reconciliation, and reviewing access. If Identity Governance currently manages the application, disable this connection with Identity Governance.
2. Define account matching and outbound transformation rules in Access Governance to match user accounts from the application with identities and to define how account attributes are set during provisioning.
3. Remediate any unmatched user accounts from the application that are not automatically matched to identities.
4. Get a consolidated view of who has access to what across applications managed by both Access Governance and Identity Governance.
5. Create workflows in Access Governance for access requests and associate them with access bundles.
6. Manage the access permissions within your organization by using the access control framework that offers the request-based, role-based, attribute-based, and policy-based access control permission models.

7. Users can request access for themselves or others through the Access Governance self-service portal. Approvers can view requests, review any compliance violations, and approve or reject requests. After approval, access is automatically provisioned.
8. Configure default access control by using attribute-based access control (ABAC) and policy-based access control (PBAC).

Considerations

- **Minimizing risk and disruption**: Consider how a phased approach could minimize risk and disruption by allowing your organization to adapt to Access Governance incrementally, thereby reducing the impact on users and IT operations and providing opportunities for learning and adjustments.
- **Incremental benefits realization**: Consider the advantage of realizing benefits from Access Governance's features and functionalities in stages, as specific applications or user populations are migrated. This gradual approach can help demonstrate value incrementally and build confidence in the new system progressively.
- **Parallel testing and validation**: Consider the opportunity to conduct parallel testing and validation of Access Governance's capabilities (for example, by initially using it for access reviews and integrating it with Identity Governance) in a controlled manner, without immediately affecting core identity management processes.
- **Plan for long term**: Consider that a phased migration, with its multiple stages of planning, configuration, testing, and deployment for different workloads, might potentially extend the overall migration timeline and require sustained effort.
- **Planning and coordination**: Consider the critical importance of thorough planning and coordination for a successful gradual migration. This planning includes determining the migration order, ensuring proper integration between Identity Governance and Access Governance during the transition, and aligning efforts across various teams and stakeholders.
- **Potential for higher transitional TCO**: Consider the possibility of a higher total cost of ownership (TCO) during the transition period, which might arise from licensing costs and the effort involved in maintaining two systems concurrently.

Best Practices for Transitioning to Access Governance

A successful transition from Identity Governance to Access Governance requires careful planning and adherence to best practices to minimize risks and ensure a smooth migration process.

Plan and Assess

To ensure a successful migration to Access Governance, complete the following foundational planning and assessment activities:

- Define the specific goals and objectives that you want to achieve by migrating to Access Governance, such as improved efficiency, enhanced security, or better compliance.
- Thoroughly assess the existing Identity Governance environment to understand its complexities, including the number and type of integrated systems, the extent of customizations, the nature of existing workflows, and the volume of identity data being managed.
- Analyze the dependencies between Identity Governance and other critical business systems to avoid disruptions during the transition.

- Based on your organization's needs and risk tolerance, determine the most appropriate migration strategy: a phased approach or an "all at once" approach.
- Prioritize the migration sequence of interdependent systems to prevent operational disruptions.
- Establish a detailed project plan that outlines specific timelines, clearly defined roles and responsibilities for team members, and resource allocation.

Integrate Systems

A key aspect of the transition to Access Governance is ensuring that all systems currently integrated with Identity Governance are also properly connected to the new Access Governance environment. Identify all such integrated systems, which typically include target applications for provisioning and deprovisioning, and authoritative sources for identity data. Use Access Governance's native integration capabilities, such as prebuilt connectors and APIs, to streamline this process. Understand the differences in integration mechanisms between Identity Governance and Access Governance.

Planning for identity reconciliation and correlation is vital for maintaining a unified view of users and their access rights in Access Governance. Define how identities from various source systems are matched and linked within Access Governance. Use Access Governance's built-in correlation and transformation rules to help automate this process and improve accuracy.

After establishing the integrations with Access Governance, conduct thorough testing to verify that data flows correctly between Access Governance and all connected systems. Validate end-to-end workflows for provisioning, deprovisioning, and reconciliation to ensure that the new system effectively manages identities and access rights across the IT landscape.

Test and Validate

Thoroughly test and validate at every stage of the migration process to identify and resolve any issues before they impact the production environment. Use functional testing to validate that all features are working as expected, integration testing to verify seamless communication with other systems, and user acceptance testing (UAT) to confirm that the migrated system meets the needs of the users. Use sandbox environments for premigration testing to identify and resolve potential problems early.

Unlearn and Relearn

Migrating from Identity Governance to Access Governance requires a new approach because of their different architectures and operational models. Identity Governance's strength lies in its advanced customization capabilities through its service-oriented architecture (SOA), whereas Access Governance emphasizes configuration and leveraging prebuilt functionalities over extensive custom coding. Identity Governance administrators must adapt to Access Governance's configuration-driven paradigm and potentially unlearn the habit of relying heavily on custom code for achieving specific requirements. Access Governance, as a SaaS offering, requires Identity Governance teams to unlearn the complexities of manual upgrades and embrace the continuous delivery model inherent in cloud services. Users must familiarize themselves with the new navigation and functionalities to effectively perform their tasks.

Clean Up Data

The migration process from Identity Governance to Access Governance provide an opportunity to address and rectify existing data quality issues within the identity management system. Cleansing the data before migrating to Access Governance enables a more efficient and accurate implementation of the new system. This migration presents the following opportunities for cleaning up data:

- Verify and validate user identities before migrating them to Access Governance, to enhance the security and integrity of the identity data.
- Identify and remove rogue accounts, which include orphaned accounts, service accounts that are no longer in use, and other unauthorized or unnecessary accounts. Eliminating these accounts reduces the potential attack surface and improves overall compliance.
- Exclude any test data and nonproduction accounts from the migration, to ensure that the production Access Governance environment contains only relevant and necessary information.
- Establish robust data governance policies and procedures for the postmigration Access Governance environment, to help maintain the quality and accuracy of the identity data over time.

Train Users and Manage Change

The successful adoption of Access Governance relies on providing comprehensive training to all users who interact with the new system. Such users include administrators, managers who are involved in access reviews and approvals, and end-users who might use self-service portals. Tailor training plans to the specific roles and responsibilities of different user groups to familiarize them with the new Access Governance system and its functionalities.

Effective change management is equally important. Proactively communicate the benefits of transitioning to Access Governance to all stakeholders, highlighting the improvements in user experience, security, and efficiency. This information helps to manage expectations and foster a positive attitude towards the change. Provide ongoing support and readily available resources, such as documentation, FAQs, and a dedicated support team, after the migration to help enable users to effectively use the new system and address any questions or issues they might have.

Provide Post-Migration Monitoring and Support

Post-migration monitoring and ongoing support are essential to ensure the long-term success and stability of the migrated Access Governance environment. Establish a plan for continuously monitoring the performance and stability of Access Governance after the “go-live” date, allocate resources for ongoing support and troubleshooting, and gather user feedback to identify areas for optimization. Providing "hypercare" support immediately after migration can help address any initial issues quickly.

High-Level Project Plan

The transition from Identity Governance to Access Governance can be structured into several key phases, each with specific activities that compose a systematic and well-managed migration. The estimated durations provided in this section are typical but can vary based on the complexity of the specific environment. This plan is generic and applicable to both the options outlined previously.

Phase 1: Initiate and Plan

Estimated duration: 4–8 weeks

This initial phase focuses on defining the scope, objectives, and approach for the migration project. Key activities include the following ones:

- **Define project scope and objectives**: Clearly articulate what the migration should achieve and the boundaries of the project.
- **Conduct detailed assessment of existing identity governance environment**: Analyze the current Identity Governance setup, including integrations, customizations, workflows, and data.
- **Define target access governance environment and requirements**: Determine the necessary configuration and functionalities of the Access Governance implementation.
- **Develop a high-level migration strategy and timeline**: Outline the overall approach to the migration and create an initial project schedule.
- **Assess risks and plan mitigation**: Identify potential risks associated with the migration and develop strategies to mitigate them.
- **Plan and approve the budget**: Estimate the software and services costs. Define the financial resources required for the project and secure necessary approvals.

Phase 2: Analyze and Design

Estimated duration: 6–10 weeks

This phase involves a deeper look at the technical aspects of the migration and the design of the target Access Governance environment. Key activities include the following ones:

- **Analyze and map data**: Analyze the data structure in Identity Governance and map it to the Access Governance data model.
- **Design integration architecture**: Plan how Access Governance integrates with all necessary authoritative and managed systems.
- **Design correlation and transformation rules**: Define the rules that Access Governance uses to match and link identities from different sources.
- **Develop user training materials**: Create training resources for administrators and end users on how to administer and use Access Governance.
- **Develop test plans and scenarios**: Outline the testing procedures and specific test cases to validate the migration.
- **Finalize project plan and timeline**: Refine the project plan with detailed tasks, dependencies, and a realistic timeline.

Phase 3: Configure and Implement

Estimated duration: 8–12 weeks

In this phase, the Access Governance environment is set up and configured, and the migration processes are implemented. Key activities include the following ones:

- **Set up and configure the Access Governance service instance**: Provision and configure Access the Governance service instance.
- **Configure integrations with target systems**: Establish connections between Access Governance and other target systems.
- **Implement correlation and transformation rules**: Configure the rules defined in the design phase within Access Governance.
- **Configure codeless workflows**: Create any necessary codeless approval workflows in Access Governance.
- **Set up access controls and policies in Access Governance**: Configure identity collections, access bundles, policies, roles, and other security controls such as access guardrails in the new environment.
- **Prepare test environments**: Set up dedicated nonproduction environments to isolate production and nonproduction data and for testing the Access Governance solution.

Phase 4: Test and Validate

Estimated duration: 4–8 weeks

This critical phase involves rigorous testing to verify that the migrated Access Governance environment functions correctly and meets the defined requirements. Key activities include the following ones:

- **Conduct functional testing**: Test all core functionalities of Access Governance, such as access requests, approvals, and certifications.
- **Perform integration testing**: Verify that Access Governance integrates seamlessly with all orchestrated systems and that data loads are performed without any issues.
- **Initiate user acceptance testing (UAT)**: Allow end users to test the system and provide feedback.
- **Address and resolve identified issues**: Fix any bugs or issues identified during testing.
- **Perform performance and scalability testing**: Validate that Access Governance can handle the expected user load and data volume.

Phase 5: Deploy

Estimated duration: 2–4 weeks

This phase involves the final steps to deploy Access Governance into the production environment and transition users from Identity Governance. Key activities include the following ones:

- **Perform a final system review**: Review the Access Governance and agent configurations.
- **Cut over from Identity Governance to Access Governance**: After all functionality and users have been migrated to Access Governance, disable or decommission the old Identity Governance environment.
- **Provide initial go-live support and monitoring**: Provide immediate support to users and closely monitor the system for any issues.

Phase 6: Monitor and Optimize

Estimated duration: Ongoing

This final phase focuses on ensuring the continued success of the Access Governance implementation and identifying areas for improvement. Key activities include the following ones:

- **Monitor system performance and stability**: Continuously track the health and performance of the Access Governance environment.
- **Provide end-user support and training**: Offer ongoing assistance and additional training to end users and administrators as needed.
- **Address any post-deployment issues**: Resolve any problems that arise after the system has gone live.
- **Gather user feedback and identify areas for optimization**: Collect feedback from users to identify potential enhancements.
- **Regularly review and update the Access Governance configuration**: Periodically review and update Access Governance configurations to align with evolving business needs and security requirements.

Project Schedule Guidance

The time required to transition from Identity Governance to Access Governance depends significantly on the complexity of existing business and technical processes that are customized into the existing Identity Governance implementation. The following general estimates are based on collective experience, and assume that the organization has a clear understanding of its current Identity Governance environment, a well-defined scope for the Access Governance implementation, and dedicated resources available for the project. The assessment of complexity considers factors such as the number of orchestrated systems, the level of customization in Identity Governance, the volume of identity data, and the complexity of existing workflows and policies.

- A **small implementation** is characterized by less than 5 orchestrated systems, minimal customizations, a user base of less than 5,000, and standard workflows and policies. For a small implementation, the estimated duration for a transition to Access Governance is typically **3–6 months**. This timeframe allows for adequate planning, basic configuration, straightforward data migration, and sufficient testing. The limited number of integrations and customizations simplifies the analysis, design, and implementation phases.
- A **medium implementation** involves between 5 and 15 orchestrated systems, some level of customization, a user base between 5,000 and 30,000, and moderately complex workflows and policies. A medium implementation is likely to require a transition duration of **6–12 months**. The increased number of integrations and the presence of customizations necessitate more detailed planning and execution for integration, data migration, and testing. Managing a larger user base also adds to the overall timeline.
- A **large implementation** includes more than 15 orchestrated systems , significant customizations including custom code and integrations, a large and distributed user base of more than 30,000, and highly complex and bespoke workflows and policies. For a large implementation, the estimated duration for a transition to Access Governance can extend to **12 or more months**. Such complex environments demand time and effort for thorough analysis, detailed design, custom development (if required), rigorous testing across numerous scenarios, and careful data migration. Experienced personnel and meticulous planning are critical for managing projects of this scale. High numbers of users and managed systems result in creation and maintenance of many (sometimes thousands), of Access Governance objects such as identity collections and access bundles. However, automation capabilities such as access bundle recommendations can help reduce this complexity.

The following table summarizes the preceding information.

Table 1. Project Schedule Guidance

Criteria	Small Implementation	Medium Implementation	Large Implementation
Number of orchestrated systems	0–5	5–15	15 or more
Level of configuration	Minimal	Some	Significant
User base	0–5000	5,000–30,000	30,000 or more
Workflows	Standard and simple	Moderately complex	Highly complex and bespoke
Number of Access Governance objects (access bundles, identity collections, and so on)	Dozens	Hundreds	Thousands
Approximate duration (may vary based on the approach and complexity)	3–6 months	6–12 months	12 or more months

The complexity of the existing Identity Governance environment and the new requirements are primary determinants of the transition timeline. Organizations with highly customized and deeply integrated Identity Governance deployments should anticipate a longer and more involved migration process compared to those with simpler Identity Governance deployments. The migration approach also significantly influences the time duration of the project.

Conclusion

Transitioning from Oracle Identity Governance to Oracle Access Governance offers a strategic pathway for organizations to modernize their identity governance and administration capabilities. The cloud native architecture, AI/ML-driven insights, simplified administration, and enhanced security and compliance features of Oracle Access Governance provide compelling advantages over traditional on-premises solutions such as Oracle Identity Governance. A successful transition requires meticulous planning, a well-defined migration strategy, seamless system integration, effective user training, and thorough testing.

Organizations should carefully assess their current Oracle Identity Governance environment to understand its complexity and plan their transition strategy accordingly. While the duration of the project can vary significantly based on this complexity, a phased approach guided by best practices helps to enable a smooth and successful migration. Engaging with Oracle or experienced implementation partners can provide valuable expertise and support throughout this journey, and enable you to fully leverage the benefits of Oracle Access Governance and establish a future-ready identity governance and administration solution.

ORACLE

Appendix A: Identity Governance and Access Governance Feature Comparison

The following table provides a comparative overview of key features between Oracle Identity Governance and Oracle Access Governance.

Table 2. Identity Governance and Access Governance Feature Comparison

Feature	Oracle Identity Governance	Oracle Access Governance	Key Reasons to Move
Deployment model	On-premises, container-based	Cloud native SaaS (OCI)	Reduced infrastructure management, scalability
Maintenance	Customer-driven upgrades and patches, higher maintenance cost	Automatic updates, lower maintenance cost	Reduced IT burden, lower TCO
Scalability	Flexible, customer-driven architecture	Automated vertical and horizontal scalability, high performance	Adaptability to changing needs
Analytics	Custom reports through Oracle Analytics Publisher	Wide set of ready-to-use reports and intelligent analytics, AI/ML-driven insights, event data publisher	Proactive risk detection, real-time analytics, flexible data retention and reporting
Implementation	Requires trained personnel and learning curve	Simple to set up and implement, intuitive user experience, easy for business users to assume administrative capabilities	Faster deployment, reduced need for specialized skills
User experience	Primarily focused on technical users	Intuitive, conversational approach, designed for business users	Improved user adoption, enhanced productivity
Workflow automation	Customizable through Oracle SOA	Codeless business workflows	Simplified process automation, business user empowerment
Application integration	May require customization, integrations maintained by the customer	Wide range of specialized and generic integrations, low-code onboarding, Oracle connectors maintained by Oracle	Easy connectivity, reduced integration complexity
Cost of ownership	Higher due to infrastructure, licensing, and maintenance	Lower due to cloud services economics	More cost-effective in the long run

ORACLE

Appendix B: Oracle@Oracle Case Study: Oracle's Journey to Modernize IGA

Oracle is strategically migrating from the Oracle Identity Governance system to the cloud native Oracle Access Governance platform using the gradual migration approach outlined earlier in this document. The goal is to significantly improve usability, scalability, and security across Oracle's global enterprise, which spans more than 2,500 applications, millions of Oracle Cloud Infrastructure (OCI) tenancies, more than 170,000 employees, and more than 16 million customers. While Identity Governance continues to operate in containers on OCI, Access Governance runs as a native SaaS solution on the same platform.

Key Objectives Driving the Transition

Oracle set clear goals for its migration to Access Governance:

- **Empower business users:** Achieve 100% business-user-friendly self-regulation, enabling nontechnical staff to manage access more directly.
- **Reduce operational burden:** Eliminate the need for specialized skill development for managing the platform and significantly cut IT and DevOps deployment costs.
- **Increase efficiency:** Decrease identity-related helpdesk tickets by 70%, freeing up IT support resources.

A Phased Strategy for a Seamless Transition

Given the scale of the operation, Oracle adopted a gradual migration approach using a phased deployment strategy. This approach allowed Identity Governance and Access Governance to run concurrently during the transition, which minimized disruption. Access Governance was deployed in both staging and production environments.

- **Staging environment:** Used by application owners to test onboarding processes and configurations in a safe sandbox.
- **Production environment:** The live environment for governing access at scale across the enterprise after testing is complete.

The migration itself was divided into distinct, manageable phases:

1. **Self-regulation:** Focus on using Access Governance to visualize employee access across all connected systems and applications.
2. **Access reviews:** Transition manager-led access certification campaigns from Identity Governance to Access Governance's streamlined review process.
3. **Audit and compliance:** Establish Access Governance as the central system of record for audits and compliance reporting.
4. **New application onboarding:** Onboard all new applications directly into Access Governance, including governance for OCI itself.
5. **Existing application migration:** Methodically migrate the extensive portfolio of existing applications managed by Identity Governance over to Access Governance.
6. **Authoritative source switch:** Connect authoritative data sources directly to Access Governance to drive identity lifecycle management processes.
7. **Identity Governance decommissioning:** Fully retire the legacy Identity Governance system after all its functions are successfully transitioned to Access Governance.

Ensuring Success Through Enablement and Support

To handle a transition of this magnitude, Oracle developed a comprehensive suite of resources, including tools, documentation, and training programs to streamline this transition. These resources were tailored for the specific needs of application owners, IT staff, audit teams, and end users, which ensured a coordinated and smooth migration.

The Future: Intelligent, Always-on Governance

By migrating to Oracle Access Governance, Oracle is harnessing AI-driven onboarding, ML-powered analytics, and context-aware access enforcement to improve governance, proactively detect risks, and dynamically manage access at enterprise scale. This transformation aims to significantly enhance Oracle's internal governance capabilities, strengthen its security posture, and efficiently manage access at an enterprise scale.

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Author: Anbu Anbarasu

Contributors: Srinivas Rajaraman, Abhishek Juneja, Sandeep Banerjie, Pavana Jain, Balaji Suriyan, Kari Jyrala