

Oracle Access Governance

Oracle Access Governance is a cloud native identity governance and administration (IGA) service that provides customers a simple, easy-to-understand view of what resources individuals can access, whether they should have those accesses at all, and how they're using the entitlements. Businesses are challenged every day to enforce appropriate just-in-time access user rights to manage control of their information and address regulatory compliance requirements of least privileged access. With immediate and prescriptive guidance about the types of access identities should have, Oracle Access Governance makes it easier for administrators to provision new users and deprovision departing users quickly. In addition, machine learning intelligence in Oracle Access Governance can monitor all types of access for anomalous behavior patterns and automate remediation actions as required. Instead of big, manual, periodic reviews, Oracle Access Governance allows continuous compliance with the proper access management where risk is constantly evaluated and alerted. Events and access at risk are being reviewed regularly and informed by built-in intelligence. This continuous compliance model significantly reduces the cost and effort of audit response. Oracle Access Governance continuously adds target systems, providing strong insights into access controls across new applications, cloud, and on-premises environments.

Background

Traditionally, organizations of all sizes and across industries have encountered challenges in effectively managing access levels for users, devices, bots, and services, aiming to enhance productivity while minimizing potential risks. Additionally, maintaining visibility into who has access to which digital asset and verifying the validity of such access in accordance with company compliance guidelines is another significant challenge.

Organizations typically rely on manual processes to assign permissions to users and other identities. This often involves users contacting other individuals through emails or multiple collaboration tools to request access. However, manual processes pose challenges in terms of scalability and compliance verification. Organizations also depend on periodic manual reviews across access rules, entitlements, permissions, roles, and policies.

The global increase in cloud adoption and digital transformation has made organizations aware of security risks associated with access and entitlements. With the prevalence of multicloud and hybrid environments, organizations face challenges of effectively managing accurate and automated provisioning or deprovisioning for user access. Additionally, the complex and time-consuming nature of access reviews and the lack of necessary context make it difficult for reviewers to make informed decisions about an individual's access. The lack of clarity leads many organizations to take a "rubber stamping approval" approach, causing blanket approvals that don't revoke overprivileged access. These issues make it hard for organizations to minimize or eliminate risks associated with



Oracle Access Governance continuously discovers identities, monitors their privileges, learns usage patterns, and automates access review and compliance processes with prescriptive recommendations to provide greater visibility into access across an organization's entire cloud and on-premises environment.

“As we steer our path towards the adoption of a cloud native governance architecture, Oracle Access Governance rises as a critical player in this arena. Its strategic design, emphasizing intuitive user access review, prescriptive analytics powered by data insights, and automated remediation, echoes our commitment to fostering a secure IT environment. This cloud native service aligns perfectly with our forward-looking IT security strategy, and we are eager to explore its potential.”

Chinna Subramaniam
 Director, IAM & Directory Services, Department of Technology, City and County of San Francisco

identity access to digital assets, overprivileged access to critical data, prove compliance with corporate policies, and reduce governance costs.

Overview

To leverage advanced identity governance and administration (IGA) capabilities, organizations should evaluate solutions that offer flexible access control measures to improve productivity. These solutions should incorporate real-time capabilities, such as prescriptive analytics, to identify anomalies and mitigate security risks effectively. By evaluating and implementing such solutions, organizations can bolster their security posture and streamline identity governance processes.

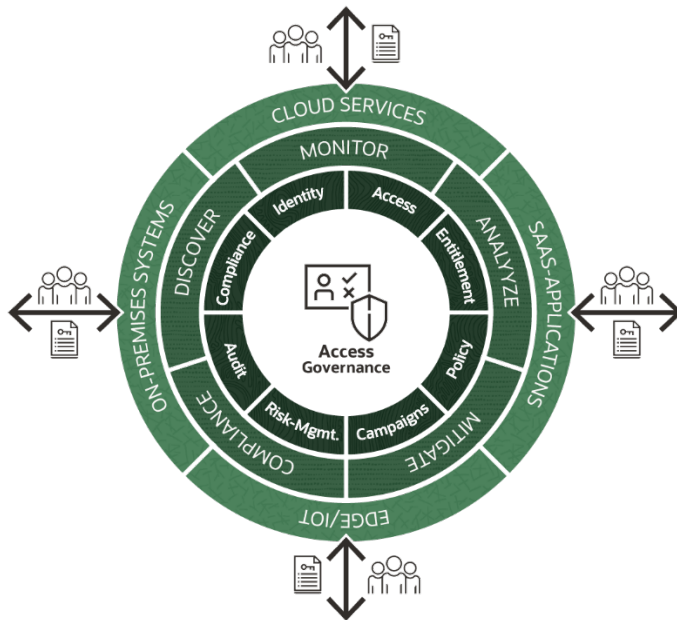


Figure 1. Oracle Access Governance—Governance that’s always on

[Oracle Access Governance](#) delivers a comprehensive governance solution that encompasses various provisioning methods like access request and approvals, role-based access control, attribute-based access control, policy-based access control. This service features a conversation-style user experience, offering deep visibility into access permissions across the entire enterprise. It facilitates ad hoc, periodic, and automated event-based microcertifications, such as an access review triggered by a job code or manager change. Additionally, it enables near real-time access reviews, providing detailed recommendations with options for reviewers to accept or review an entitlement based on the identified level of risk. Oracle Access Governance can also run with [Oracle Identity Governance \(OIG\)](#) in a hybrid deployment model. Organizations that opt for a hybrid model can take advantage of advanced capabilities available from cloud native services, while retaining parts of their on-premises Identity and Access Management Suite for compliance or data residency requirements.

“With our transition to a cloud-based governance solution, Oracle Access Governance presents an appealing option for streamlining user access reviews, providing enterprise-wide visibility into access permissions, ensuring zero migration effort, and offering insight-driven analytics. We believe it has the potential to enhance our IT security and efficiency, making it a worthwhile solution for organizations exploring cloud governance platforms.”

Monica J. Field

IT Director, Identity and Access Management, Cummins Inc.

“We see tremendous value when leveraging identity-as-a-service solutions, such as Oracle Access Governance, to integrate more powerful, analytics-driven security for organizations moving to the Cloud. This solution enables Deloitte professionals to deliver enhanced security with agility, scale, and analytics, all while helping clients protect their existing investments in governance and supporting multicloud environments.”

Kashif Dhatwani

Advisory Senior Manager
Cyber and Strategic Risk
Deloitte & Touche LLP

Key Benefits

- **Simplified self-service:** Oracle Access Governance provides self-service that empower users to request access bundles or roles for themselves or others. This streamlined process enhances efficiency and empowers users to actively participate in access governance activities.
- **Automated access control:** Oracle Access Governance supports identity collections which enable attribute-based access control. This capability allows for fine-grained control over access bundles based on specific attributes associated with identities. Furthermore, Oracle Access Governance incorporates role-based access control (RBAC), a feature that enables access rights to be defined and managed based on specific roles. These identity collections and roles can be further utilized by policy-based access control for granting and managing access rights.
- **Flexible delegated access control:** Oracle Access Governance facilitates delegated ownership, allowing businesses to manage identity collections, while application owners can oversee access bundles including accounts and entitlements. This delegation enables efficient and streamlined management of access rights within Oracle Access Governance, promoting collaboration and accountability among stakeholders.
- **Visibility into access map:** Oracle Access Governance offers visibility into user access across the entire organization, providing insights into which users have access to specific applications, resources, and services. Managers can review the access map of their teams, enabling them to understand and oversee the access privileges of their team members. Individual users can also view their own access permissions, giving them transparency and awareness of their own access rights.
- **Enhance regulatory compliance:** Oracle Access Governance helps enforce and attest to regulatory requirements, such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and GDPR, associated with identifying who has access privileges to sensitive, high-risk data.
- **Improve certification efficiency:** Oracle Access Governance empowers organizations with actionable insights and prescriptive analytics, facilitating a comprehensive understanding of the necessary access required to expedite user productivity. Organizations gain visibility triggered by event-based certifications like a job or organization change, so access reviewers can quickly take the necessary actions to update access privileges.
- **Reduce costs:** Oracle Access Governance allows organizations to use a cloud native identity governance service that helps reduce IT costs and save time through efficient, user-friendly dashboards, code-less workflows, and wizard-based application onboarding.

Key features

- **Cloud native service:** It's an OCI native subscription service.
- **Intuitive user experience:** It offers an intuitive user experience using a conversational approach.
- **Interactive dashboard:** It includes dashboards that offer valuable insights to enable users to focus on essential tasks.
- **Identity orchestration:** It supports rapid application onboarding based on its innovative orchestration capabilities with a no-code, wizard-based integration approach.
- **Simplified access request:** It provides a simple user experience for self-service based requests.

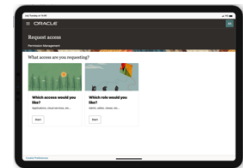


Figure 2. Simplified self-service

- **Automated access control:** It provides multiple access control measures that can be leveraged to automate accesses in various scenarios.

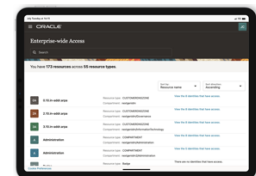


Figure 3. Visibility into enterprise-wide access

- **Actionable access Reviews:** It simplifies the access review process and provides actionable insights based on prescriptive analytics so managers can make informed decisions.

Summary

Oracle Access Governance helps organizations to automate access control, gain visibility, make informed access decisions, and support their overall compliance objectives. Organizations can extend their current Identity Governance and Administration capabilities with a cloud native service to begin with deeper insights. For more information, review the Oracle Access Governance [product documentation](#) or visit the [Oracle Access Governance webpage](#).



Figure 4. Enforce access controls with prescriptive analytics

- **Event-based microcertifications:** It facilitates intelligent event-based access reviews triggered only when there are changes in the system of record.
- **Codeless workflows:** It provides lightweight codeless workflows for access control and governance.
- **Comprehensive IT audit, monitoring, and reporting:** It includes simplified auditing, monitoring, and flexible reporting capabilities.

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](#)

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120