ORACLE

Securing Higher Education Institutions with Oracle Access Governance

July 2025, Version 1.0

Public

ORACLE

Purpose Statement

This document provides an overview of the features of Oracle Access Governance and how it can provide a framework for robust identity management and risk mitigation in higher education. It is intended solely to help you assess the business benefits of Oracle Access Governance and plan for implementation of the product features described.

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

Overview

The higher education sector presents a complex and high-risk environment for identity management. The potential for identity-based breaches of sensitive student records, research data, and financial systems is significant. Threat actors increasingly target educational institutions, exploiting vulnerabilities that stem from fragmented identity data and inconsistent access controls. The severity of data breaches within the sector emphasizes the urgent need for comprehensive Identity Governance and Administration (IGA) solutions. This document examines how Oracle Access Governance addresses these critical security challenges by providing a framework for robust identity management and risk mitigation in higher education.

Current Implementation Topology in Higher Education

Universities and colleges operate a diverse IT ecosystem composed of the following types of systems, applications, and services:

- **Student information systems (SIS)**: Platforms like Oracle PeopleSoft Campus manage student records and academic information.
- **Human resources management systems (HRMS)**: Systems like Oracle Fusion App or PeopleSoft Human Capital Management (HCM) manage employee data and payroll.
- **Learning management systems (LMS)**: Tools such as Canvas or Blackboard facilitate course delivery and management.
- **Cloud applications**: Services like Microsoft Office 365 or Google Workspace support communication and collaboration.
- **Directory services**: Microsoft Active Directory, Oracle Unified Directory, or LDAP systems handle authentication and authorization.

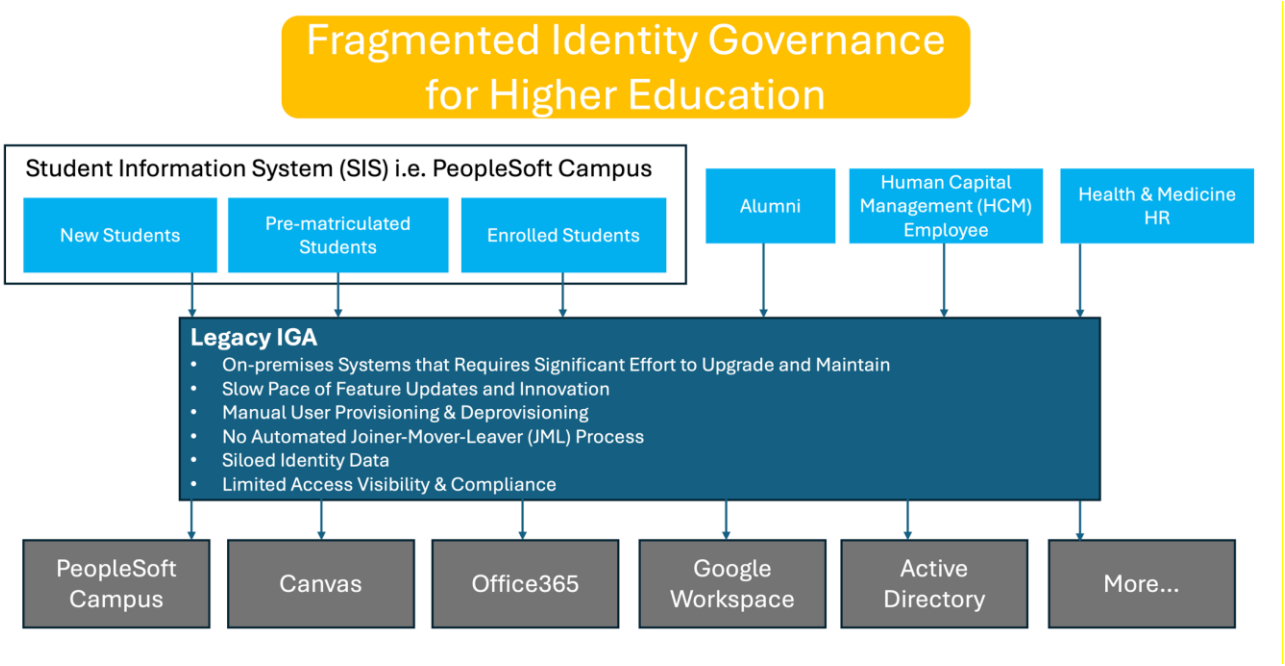

Figure 1. Fragmented Identity Governance for Higher Education

University campuses often maintain separate authoritative systems, leading to identity duplication challenges. Students and faculty frequently move between campuses, requiring identity records to be duplicated or temporarily placed "on hold" until consolidation is possible.

The inherent complexity of this landscape leads to data silos and inconsistent access provisioning. For example, a student taking a teaching assistant role may experience delays in updates to their access, or worse, retain excessive privileges after leaving the teaching assistant role, creating potential security gaps. These fragmented systems increase the attack surface and complicate audit trails, making a unified identity management solution like Oracle Access Governance essential.

Higher Education Use Cases and Specific Requirements

Beyond standard Joiner-Mover-Leaver (JML) processes, higher education institutions encounter unique IGA use cases:

- **Multiple roles per user**: Some individuals might simultaneously hold multiple roles, such as a student who also serves as a teaching assistant or research associate. Others might have concurrent enrollment at different campuses. These scenarios require nuanced access controls.
- **Seasonal access**: Access requirements that change with academic terms or special projects demand dynamic provisioning and deprovisioning.
- **Guest access**: Temporary access for visiting scholars, external collaborators, or conference attendees must be managed securely and efficiently.
- **Auxiliary staff**: Distinct access controls are needed for full-time staff versus auxiliary staff, based on role and affiliation.
- **Compliance and audit**: Compliance and audit procedures are often complex and burdensome.

Higher education institutions must also adhere to various regulatory standards, such as the following ones:

- **Family Educational Rights and Privacy Act (FERPA)**: Protects the privacy of student education records.
- **Health Insurance Portability and Accountability Act (HIPAA)**: Protects the confidentiality of health information and is pertinent to institutions with medical centers or health services.

In addition to adhering to FERPA and HIPAA, universities must protect personally identifiable information (PII), such as Social Security numbers (SSNs) and dates of birth. This protection requires strict encryption and controlled distribution. Health records are managed separately and are not typically integrated into identity systems.

Introduction to Oracle Access Governance

Oracle Access Governance is a comprehensive solution designed to streamline identity governance processes within organizations, particularly in complex environments like higher education. Oracle Access Governance offers centralized management of user identities and access rights, which gives institutions the tools they need to automate provisioning and control, help with compliance goals, and improve operational efficiency. Cloud-based IGA solutions like Oracle Access Governance eliminate the need for costly on-premises system upgrades and enable rapid adoption of new features.

How Oracle Access Governance Addresses Higher Education Needs

Oracle Access Governance addresses governance challenges in higher education in the following ways:

- **Centralizing identity management**: Integrates disparate systems to provide a unified view of user identities and access rights.
- **Automating access provisioning**: Enables timely and accurate assignment of access based on predefined roles, attributes, and policies, which reduces manual intervention and errors.
- **Enhancing compliance**: Offers tools for continuous monitoring, access certification, and auditing to help meet regulatory requirements. Oracle Access Governance provides comprehensive auditing and reporting capabilities, which allows institutions to conduct regular, automated access reviews. These controls can help reduce FERPA compliance risks.
- **Mitigating separation of duties (SoD) risks**: Implements access guardrails and SoD checks to prevent and detect conflicting access rights, which safeguards institutional integrity.
- **Real-time provisioning**: Provides policy-based and attribute-based real-time provisioning and deprovisioning capabilities that specifically address higher education requirements. Batch provisioning is inadequate for timely access management.

Typical Deployment of Oracle Access Governance for Higher Education

Oracle Access Governance typically integrates with hybrid environments that connect on-premises systems (such as PeopleSoft HCM and Campus Solutions) and cloud applications (such as Office 365 and Google Workspace). For on-premises systems, Oracle Access Governance employs a secure, agent-based architecture, which allows for seamless and secure communication with platforms like PeopleSoft. For cloud-based applications, Oracle Access Governance leverages API integration to efficiently manage identities and access controls.

Oracle Access Governance also reconciles multiple identities sourced from diverse authoritative systems into a unified identity profile. This approach helps verify accurate, consistent identity data across all integrated systems, which reduces duplication and administrative overhead.

Additionally, Oracle Access Governance supports automated provisioning to managed targets such as Canvas, Office 365, Google Workspace, and other essential higher education systems. Using role-based, policy-based, and attribute-based access control, Oracle Access Governance automates the provisioning process, so users can receive timely and appropriate access aligned with their roles and responsibilities. Figure 2 shows the typical Oracle Access Governance deployment architecture for higher education institutions.

Note: Although Oracle Access Governance supports role-based access control (RBAC), many universities historically have not widely adopted RBAC. Universities are now starting to adopt Oracle Access Governance's SaaS model to more rapidly and effectively implement flexible role-based, policy-based, and attribute-based access control.

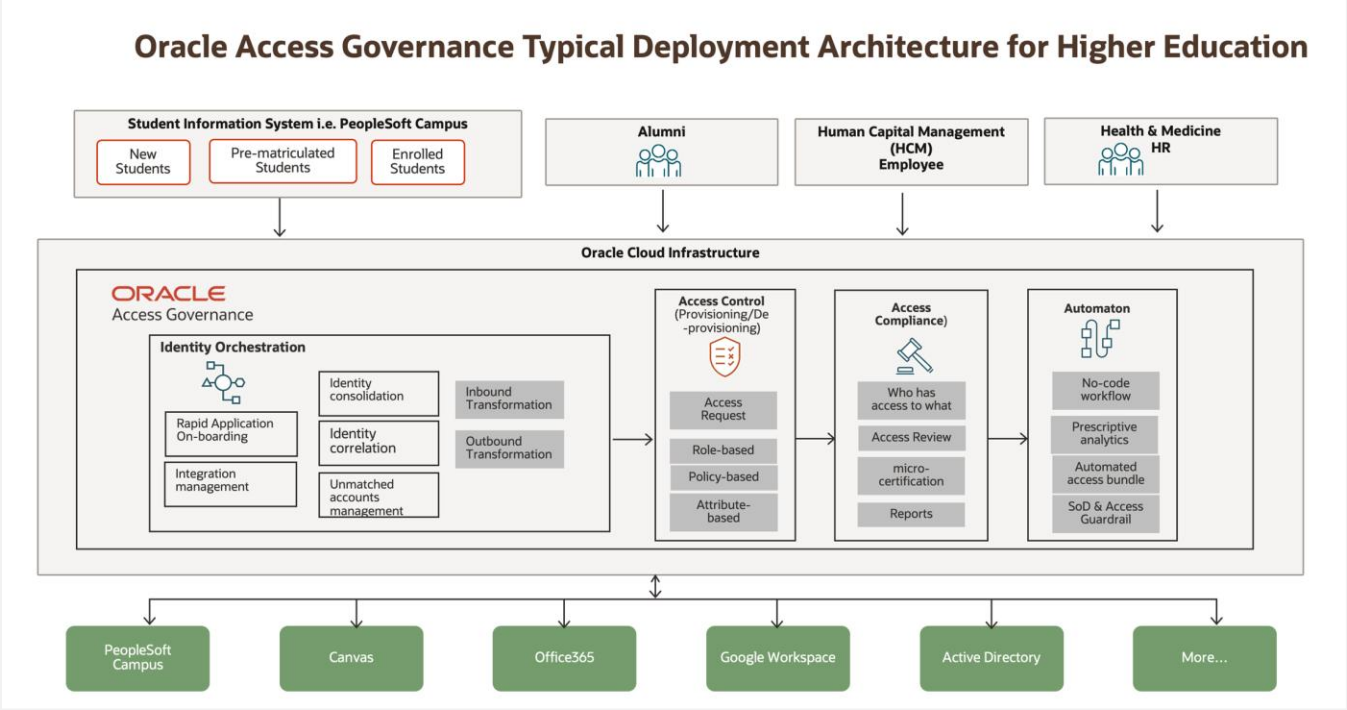

Figure 2. Oracle Access Governance Typical Deployment Architecture for Higher Education

Oracle Access Governance's Unique Capabilities for Addressing Higher Education Identity Management Challenges

Higher education institutions often grapple with fragmented identity data and inconsistent access controls because of disparate systems that manage student, faculty, and staff information. Oracle Access Governance offers targeted capabilities to address these challenges.

Identity Reconciliation and Correlation

Oracle Access Governance connects seamlessly to various student information systems (SIS), human resource management systems (HRMS), and other authoritative sources, to consolidate and correlate identity information across platforms. This integration facilitates the detection and management of rogue accounts, which enhances security. The inbound and outbound transformation capabilities of Oracle Access Governance ensure that multifaceted identities are uniquely represented across systems, thereby maintaining data integrity and consistency.

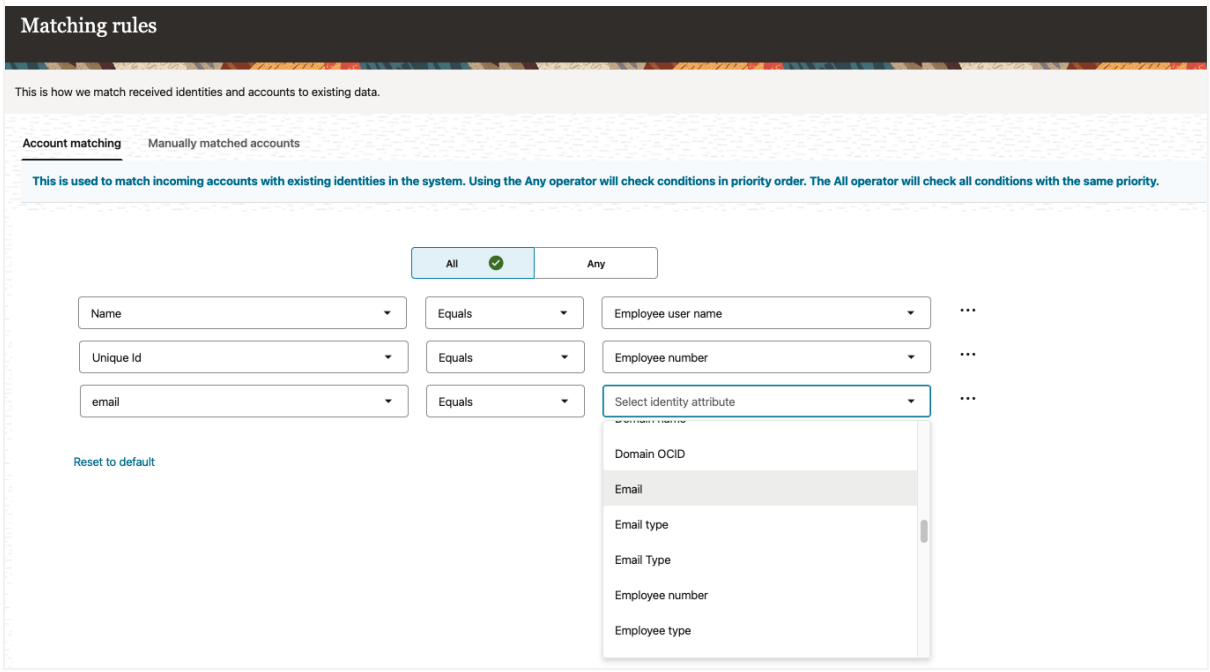

Figure 3. Identity Matching in Oracle Access Governance

Automated Provisioning

Oracle Access Governance automates the provisioning process to essential applications like Oracle PeopleSoft Campus Solutions and Office 365. By using codeless workflows, Oracle Access Governance simplifies access provisioning, which reduces manual interventions and associated errors. This automation helps faculty and student users receive timely and accurate access that's aligned with their roles and responsibilities, thereby enhancing operational efficiency. Oracle Access Governance provides role-based, policy-based, and attribute-based access control that's tailored to the unique needs of universities and colleges.

- **Roles**: Supports students, faculty, researchers, staff, and alumni by dynamically adjusting access for users with multiple concurrent roles (for example, students who are also teaching assistants).
- **Policies**: Enforces access based on academic standing, employment status, department, and compliance (for example, faculty access to grading systems that is limited to assigned courses).
- **Attributes**: Uses real-time factors like enrollment status, contracts, and research involvement to automatically adjust access as roles change.

The ability of Oracle Access Governance to handle real-time provisioning and support campus-specific rules provides essential flexibility that enables central IT to establish governance templates with 10-20% variation tailored for individual campuses.

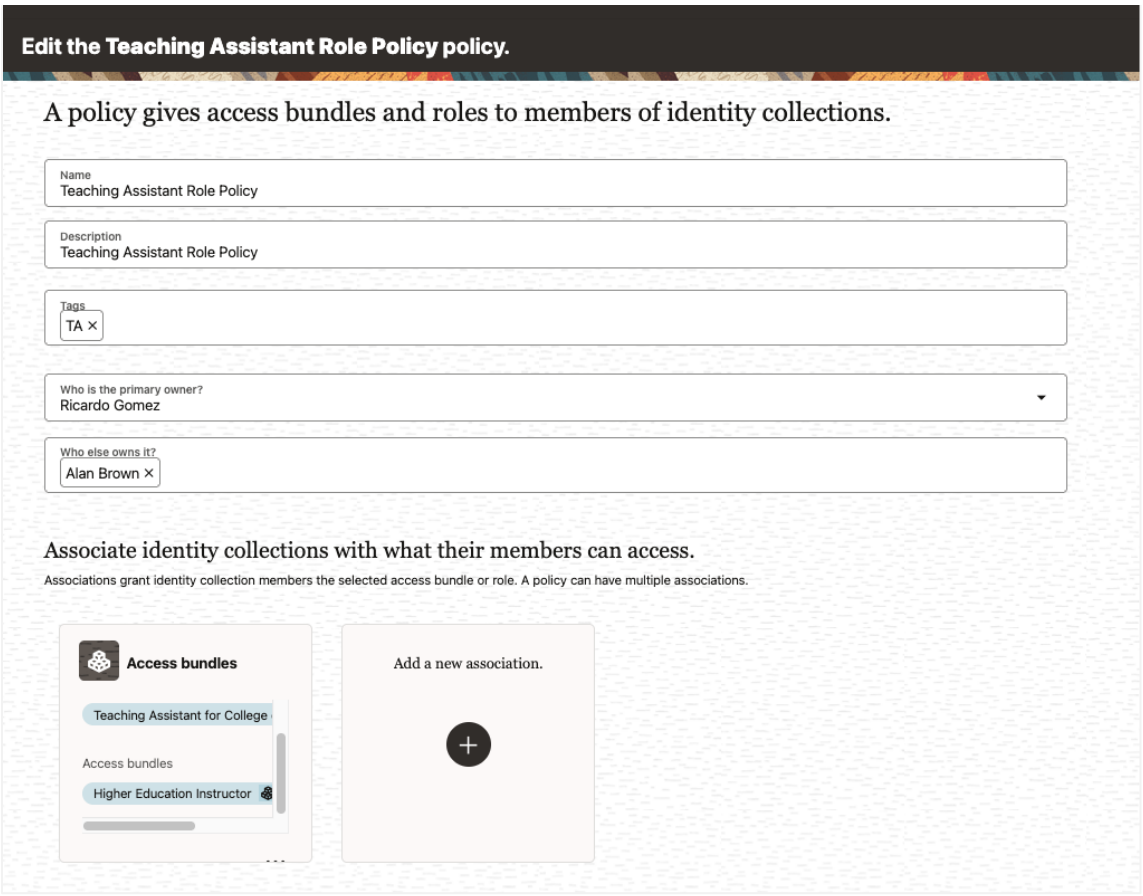

Figure 4. Policy-Based Access Control in Oracle Access Governance

Access Review and Compliance Reporting

Oracle Access Governance provides robust tools for conducting access reviews and generating compliance reports. Through prescriptive, analytics-driven processes, Oracle Access Governance automates access review campaigns, which offer insights into access permissions and identifying anomalies. This functionality helps institutions meet regulatory requirements and internal policies, streamline audit processes, and mitigate compliance risks.

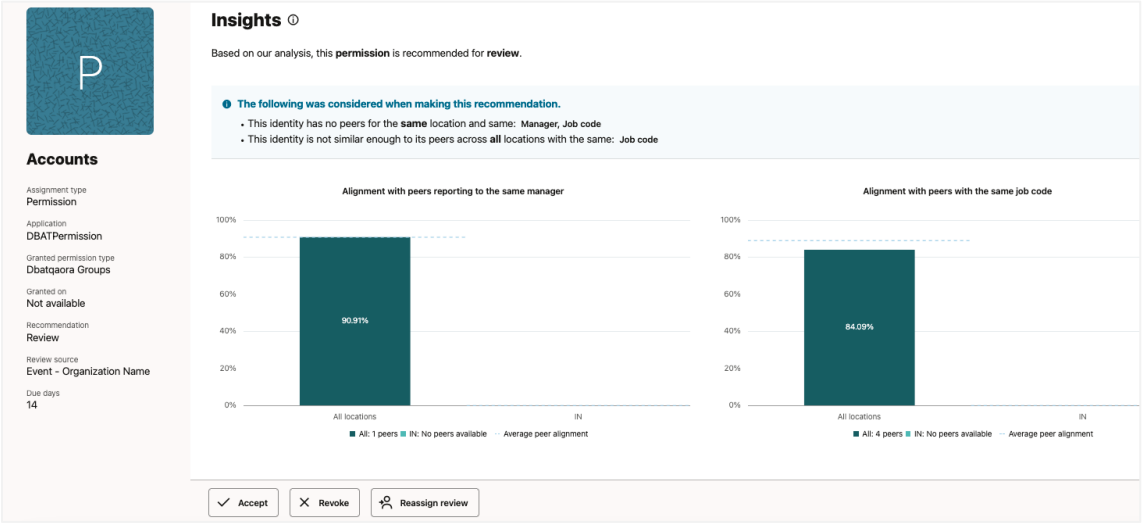

Figure 5. Insight-Driven Access Review in Oracle Access Governance

Access Guardrails for Separation of Duties

Oracle Access Governance incorporates access guardrails to enforce separation of duties (SoD) policies, which prevents users from obtaining conflicting roles that could lead to fraud or policy breaches. For example, an access guardrail may be implemented in which a user who maintains teaching staff records is unable to also approve payroll processing. These guardrails serve as preventive controls by verifying whether access requests violate SoD policies and ensuring that they are flagged and reviewed before approval. This proactive approach helps maintain the integrity of institutional processes by mitigating risks associated with conflicting duties.

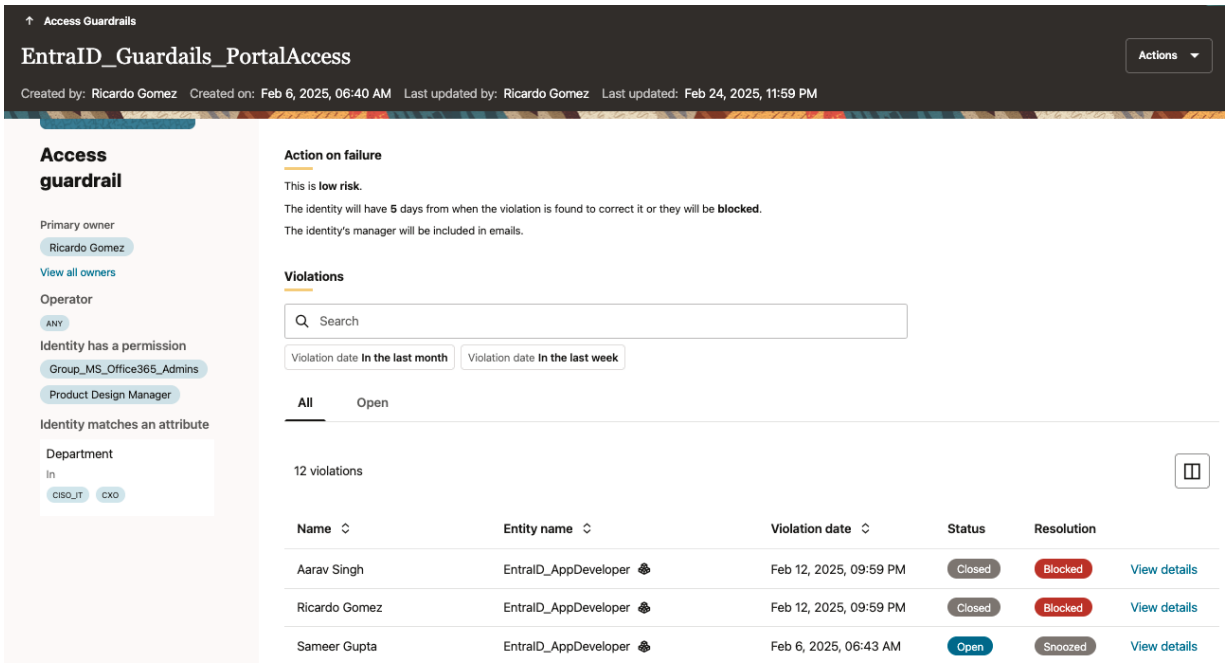

Figure 6. Access Guardrail in Oracle Access Governance

Case Study: Transforming Identity Governance at ABC University

In this case study, a prominent institution with over 30,000 students and 5,000 staff members, referred to here as "ABC University," faced significant identity management challenges:

- **Fragmented systems**: Multiple standalone applications led to inconsistent and inefficient identity management processes.
- **Compliance pressures**: Increasing regulatory requirements necessitated more rigorous access controls and reporting capabilities.
- **Security concerns**: Incidents of unauthorized access highlighted vulnerabilities in the existing IAM infrastructure.

To address these challenges, the university adopted an incremental migration to the cloud. They started with identity reconciliation and basic data migration and then moved to advanced cloud functionalities such as automated access reviews and provisioning.

Implementation of Oracle Access Governance

As part of its cloud migration to address the challenges, ABC University implemented Oracle Access Governance and used the following features:

- **Unified identity repository**: Reconciles identity data from various systems into a single authoritative source to improve data accuracy and consistency.
- **Automated workflows**: Streamlines provisioning and deprovisioning processes, which reduces administrative burden and minimizes errors.
- **Real-time monitoring**: Continuously monitors access rights and user activities to enable prompt detection and response to anomalies.

Example Identity Orchestration Scenario for ABC University

Oracle Access Governance facilitates robust identity and access management for universities by integrating seamlessly with systems like PeopleSoft Human Capital Management (HCM) and PeopleSoft Campus Solutions. This integration ensures secure and efficient management of user identities and access rights across the institution. This section describes such an integration at ABC University.

Integration Architecture Overview

Oracle Access Governance integrates with PeopleSoft applications by using an agent-based connection. An Oracle Access Governance agent is set up on-premises. The agent performs outbound calls to Oracle Access Governance to get provisioning and data-loading activities to initiate against the PeopleSoft HCM target. The agent then performs the relevant operations on the target and returns relevant data back to Oracle Access Governance.

The integration supports two primary configurations:

- **Authoritative Source mode**: Oracle Access Governance retrieves identity data from PeopleSoft HCM, treating it as a trusted source. Inbound transformation is done based on multiple inbound HR attributes before identity data is loaded into Oracle Access Governance. This mode ensures that any additions or changes to employee records in PeopleSoft HCM are reflected in Oracle Access Governance, which maintains up-to-date identity information.
- **Managed System mode**: Oracle Access Governance manages user profiles within PeopleSoft Campus and Office365 applications, including role and permission assignments. This configuration allows for provisioning new accounts, updating existing ones, and revoking access as necessary.

Common University Use Cases

The following are common use cases that Oracle Access Governance can help universities such as ABC University accomplish.

Automated Access Control for Faculty and Staff

When a new faculty member is hired, their details are added to PeopleSoft HCM.

Oracle Access Governance detects the new record and automatically provisions access to university systems (for example, research databases, faculty portals, email, and campus solution systems) based on access bundles and policies. Access is automatically assigned based on the job role and department, which reduces manual effort.

If a faculty member moves from one department to another, their HR record is updated in PeopleSoft and attributes, such as department and job code, are synchronized with Oracle Access Governance. Oracle Access Governance automatically adjusts their access by revoking permissions no longer needed and granting new ones, which maintains the principle of least privilege access.

When a faculty member retires or their contract ends, their HR record is deactivated in PeopleSoft. Oracle Access Governance detects the event and automatically disables access to sensitive university systems, thereby preventing security risks.

University Compliance and Security with Access Review

Periodic and event-based access reviews for faculty members, administrators, advisors, and financial aid officers help verify that only authorized personnel can access sensitive student data.

With Oracle Access Governance, ABC University has an option to create an access review campaign for unmatched accounts. Through the campaign, identities can be matched to an existing identity, or unmatched accounts can be removed.

"Who has access to what" reports enable comprehensive audit reporting and access certifications, which are helpful for compliance with federal regulations such as FERPA and HIPAA and help with PII data protection for students and faculty.

Cost Savings Through License Optimization

Higher education institutions frequently encounter licensing cost challenges with cloud services like Office 365 or Google Workspace. Oracle Access Governance helps institutions identify overprovisioned or unused entitlements through automated, periodic access reviews. By highlighting unnecessary licenses, universities can reduce licensing costs.

Outcomes

After a successful Oracle Access Governance implementation, ABC University realized substantial business benefits:

- Duplicate accounts were eliminated, significantly reducing user confusion and helpdesk workload.
- Authentication issues decreased because of accurate role-based and policy-based access control.
- Access reviews and compliance audit campaigns were streamlined from days to just minutes. Likewise, policy reviews went from hours to minutes.
- Detailed visibility and prescriptive analytics regarding "who has access to what" provided deep and actionable insights.
- Rapid onboarding of new cloud and on-premises applications improved operational agility.
- Necessary tools with user-friendly interfaces were implemented to help the university adhere to audit and compliance goals while securing access across the university.
- Costs related to hardware and software for on-premises system upgrades and maintenance were reduced, the latest service and feature updates were implemented quickly, and the system scaled without any performance degradation.

Conclusion

Oracle Access Governance provides higher education institutions with a robust, centralized cloud IGA solution for managing complex identity governance challenges. Institutions adopting Oracle Access Governance enjoy enhanced security, simplified compliance-related operations, and improved operational efficiency, which ultimately empowers them to focus more effectively on their core mission of education and innovation.

For more information about Oracle Access Governance, see the following resources:

- Oracle Access Governance product page
- Oracle Access Governance datasheet
- Oracle University: Introduction to Oracle Access Governance
- Hands on: Oracle Access Governance LiveLabs
- What's New for Oracle Access Governance
- Oracle Identity Governance and Administration Integrations Exchange
- Blog: Oracle Access Governance introduces next-gen access dashboard and more integrations
- Blog: Oracle Access Governance optimizes identity orchestration and enables unlimited integrations with generic connectors
- Blog: Oracle Access Governance adds support for OCI group membership reviews, orphan account management, and more integrations
- Blog: Oracle Access Governance adds identity lifecycle management and expanded targets
- Developer Coaching: Oracle Access Governance (video)

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