OKERA

Okera & Collibra

An enterprise data catalog, like Collibra, is critical in transforming data into actionable intelligence. It also serves as a powerful tool for governance teams to document, curate, and classify data to adhere to the organization's policies and security classification standards and ensure they are enforced correctly.

However, enforcing data access policies is the responsibility of IT or the data platform team. The complexity of tools and use cases manifests into bespoke enforcement solutions for each tool, multiple copies of each dataset, and more of the data being locked down in an attempt to standardize access to the lowest common denominator.

This disconnect between the governance and the platform teams results in often-inconsistent policy enforcement and an operational bottleneck that ultimately slows down business agility at the last mile, where data must be consumed and quickly analyzed for competitive advantage.

How it Works

The Okera and Collibra integration closes the gap between business governance and central IT, enabling faster time-to-insight on new data and increased business agility. Enterprises gain a unified metadata layer that can act as a single source of trust for both their technical and business metadata, giving them the certainty that their governance policies are being enforced consistently throughout the organization.

Okera's **Collibra Connector** offers a two-way automated sync:

1. Imports business metadata such as data classification attributes from Collibra into Okera to enforce attribute-based access control (ABAC) policies.

2. Exports technical metadata from Okera's unified metadata layer back into Collibra to enhance the data catalog and help the governance teams understand their data.

Lack of Secure Data Access Impacts All Teams

DATA GOVERNANCE AND PRIVACY TEAMS

Set the organization's governance policies and security classification standards, but lack visibility into whether or not their policies are actually being enforced correctly and consistently.

### DATA OWNERS AND DATA STEWARDS

Must give access to their data for different purposes, but become overwhelmed with requests and cannot easily provision access across all the various systems in the data platform.

DATA PLATFORM TEAMS (IT)

The only users with the technical skills to interact with source systems and run policies. They typically lack context on the data and any relevant regulations and policies.

DATA ANALYSTS AND DATA SCIENTISTS

Disconnect between the first three groups means this group has to wait a long time to access the data they need. They associate data security with friction. Sometimes, with the best intentions, they attempt to bypass protective processes, opening the organization up to regulatory risk.

Okera exports technical metadata

Okera imports business metadata

PII PHI
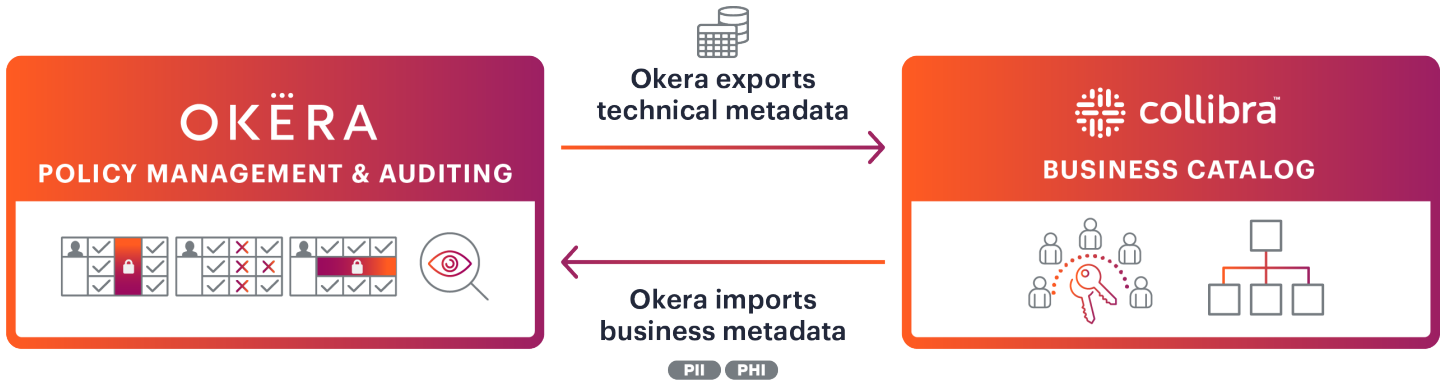
BENEFITS

The integrated solution improves governance, saves time, and eliminates repetitive work by:

Automating Policy Enforcement

Policies can be defined in Okera leveraging classification of attributes from Collibra. These policies will then be automatically enforced at query time. This allows the enterprise to leverage their pre-existing workflows and atttributes, and saves the governance team and/or data stewards from doing repetitive work.

Creating a Unified Metadata Layer

Collibra is a rich source of manually curated business metadata, while Okera focuses on technical metadata with automatic discovery and tagging of sensitive data. With the integrated solution, enterprises gain a single source of truth in Okera for all metadata, whether the data resides in legacy systems or in the cloud.

Improving Responsiveness to Regulatory Change

Because policy enforcement happens dynamically within Okera, any policy changes made in Collibra because of changes in regulations or internal governance standards are transparently enforced by Okera the next time an analyst runs a query.

Scaling Data Classification

Okera's automated tagging of sensitive data provides data stewards with a head start in classifying information. This enables them to quickly understand whether a dataset contains sensitive data and what type, so they can map it back to the organization's governance standards.

CASE STUDY

A leading US financial institution, was able to significantly shorten the time-to-value for their cloud-native data lake by integrating Okera and Collibra. Their governance team was already leveraging Collibra's catalog to classify data (e.g. highly confidential, confidential, sensitive, public) across all their existing data stores. As they built out their modern data platform, they deployed Okera as the foundation for their unified access layer.

Instead of having to create a new governance strategy for the data lake, they were able to use Okera's Collibra Connector to automatically sync classifications from Collibra in order to define and enforce ABAC policies on their cloud-native data lake.

Together Okera and Collibra were able to deliver agile data governance with minimal change management, which allowed the customer to hit the initial milestones for their data lake initiative significantly faster, enabling access to new data in a matter of hours rather than weeks.

Learn more at **www.okera.com** or contact us at **info@okera.com**.