Informatica

01 Apr, 2025

Leveraging Metadata Access Control for Security and Regulatory Compliance in Data Governance

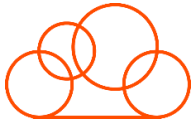
- Puneet Dudeja, Sr. Customer Success Architect, CSA
- Naveed Haider, Principal Customer Architect, CSA
- Susruth Chunduru, Sr. Customer Success Architect, CSA

Where data & AI come to LIFE

Housekeeping Tips

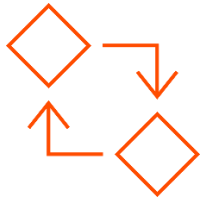
- Today's Webinar is scheduled for 1 hour
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via the Q&A option and we will respond at the end of the presentation
- The webinar is being recorded and will be available on our Success Portal - where you can download the slide deck for the presentation. The link to the recording will be emailed as well.
- Please take time to complete the post-webinar survey and provide your feedback and suggestions for upcoming topics.

Feature Rich Success Portal



Bootstrap trial and POC Customers

Enriched Customer Onboarding experience



Product Learning Paths and Weekly Expert Sessions

Informatica Concierge

Tailored training and content recommendations

More Information

Success Portal

https://success.informatica.com

Communities & Support

https://network.informatica.com

Documentation

https://docs.informatica.com

University

https://www.informatica.com/in/services-and-training/informatica-university.html

Safe Harbor

The information being provided today is for informational purposes only. The development, release, and timing of any Informatica product or functionality described today remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision.

Statements made today are based on currently available information, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products or functionality in the future.

Agenda

1. Introduction
2. Overview of Metadata Access Control in IDMC
3. Building Policies and Asset Groups
4. Functional Use Cases
5. Demo
6. Q&A

Informatica: Intelligent Data Management Cloud (IDMC)

Data Integration

Data Integration Developer creates *mappings* that infuse Data Privacy

Users, User Groups
User Roles
Data Connections

Administrator

Metadata Command Center

Data Classifications
Metadata Access
Data Catalog Scan

Glossary Terms
Classify Assets
Data Access

Data Governance and Catalog

Consumer Self-Service users may directly access protected data

Data Marketplace

snowflake
databricks

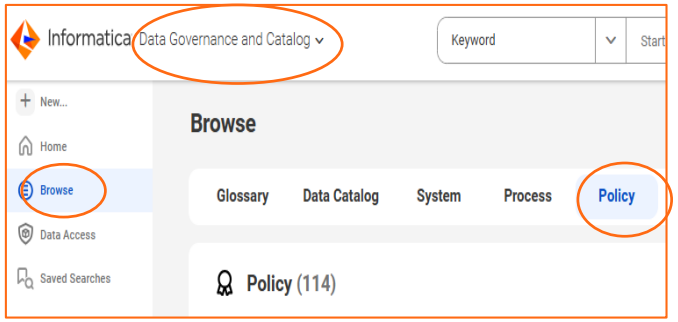
Data is natively restricted for the user

Informatica

Types of **Policies** in Intelligent Data Management Cloud

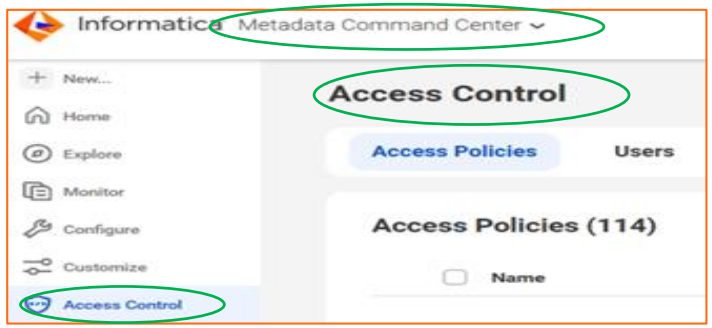
Data Governance Policy

A Policy asset in DG Catalog represents an internal collection of rules and guidance on how to conduct business and manage data



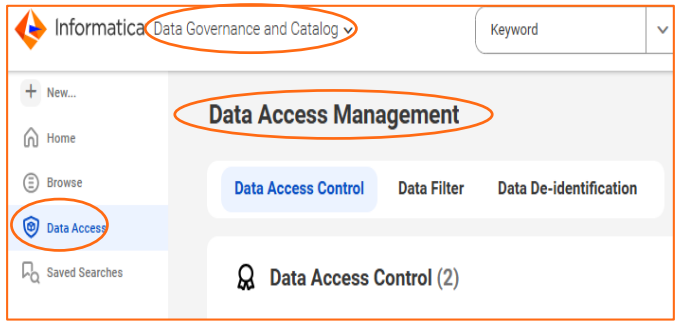
Metadata Access Policy

Metadata access control allows you to manage how users interact with assets in Catalog **Access Control,** control the level of access that users have on catalog assets..



Data Access Policy

A data access policy is a set of rules that you can use to protect data and control access to your data



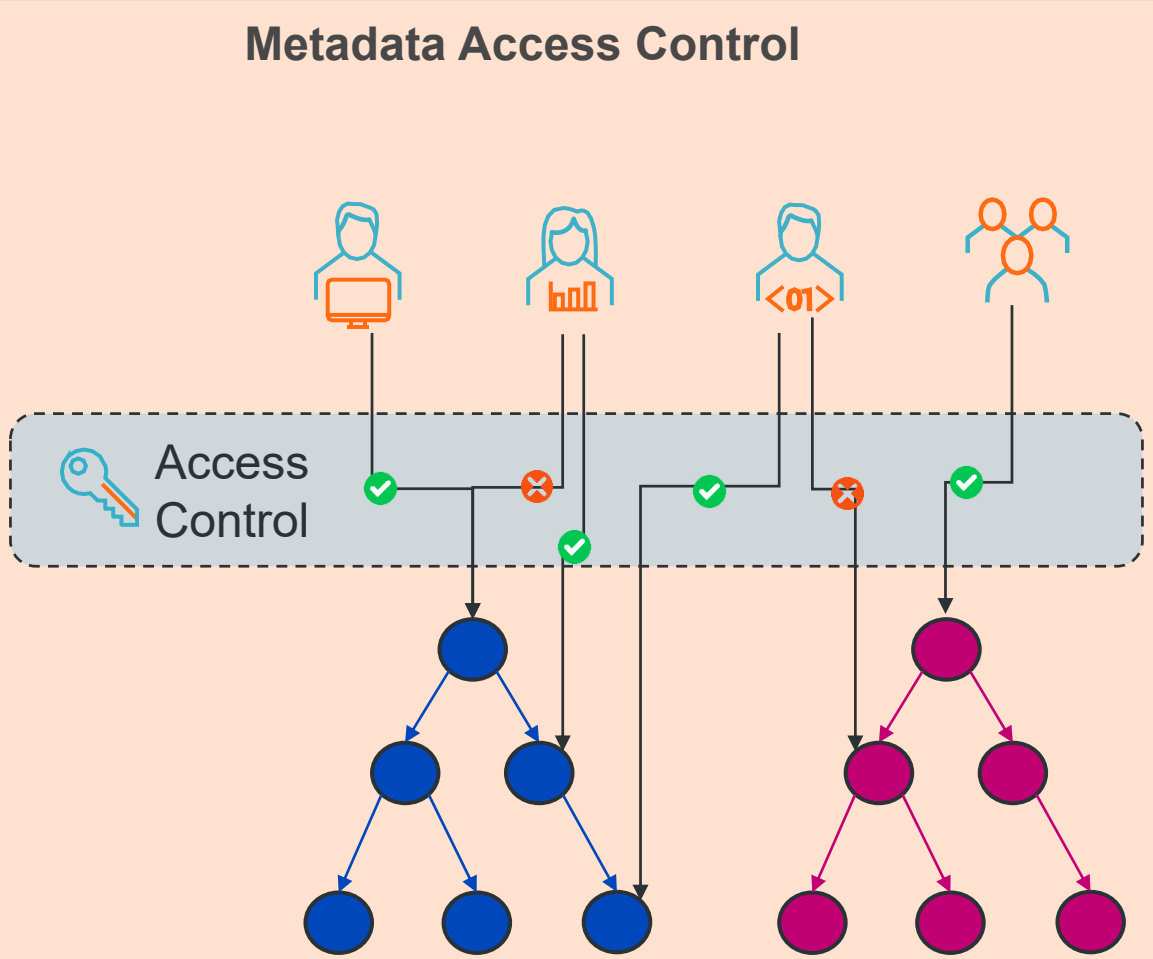
Metadata Access Control

Key Highlights

- Easy and efficient metadata access control extending IDMC user roles definition
- Attribute value driven metadata access control for all asset at any level of the hierarchies
- Granular metadata access control for any asset of the metadata platform via asset specific roles (stakeholders) definition

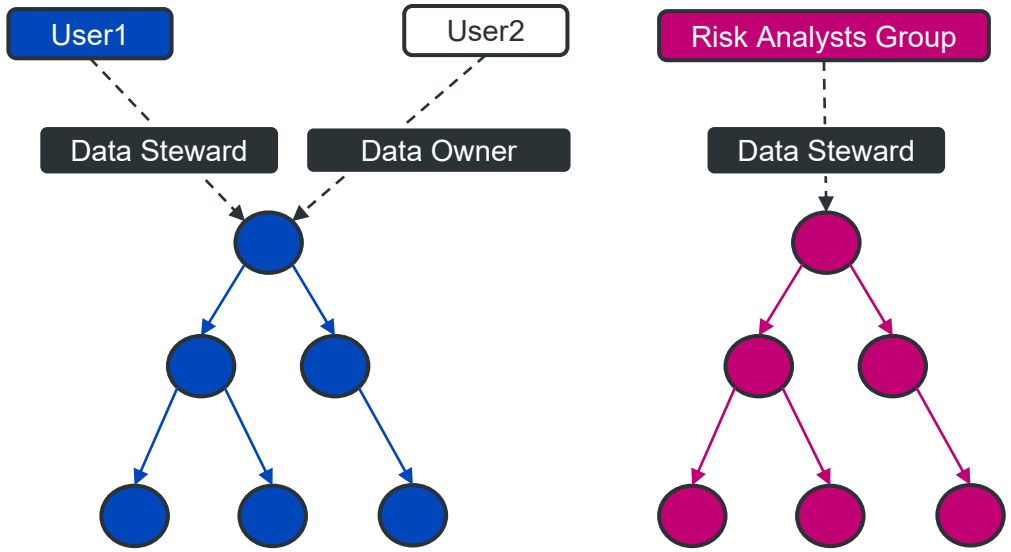
Benefits

- Provide full control to customers to control access to dataset information at an enterprise level
- Allow customers to catalog the entire data landscape securely and manage asset ownership at scale
- Allow customers to open consuming application (CDGC, CDMP, CLAIRE GPT) to their entire organization



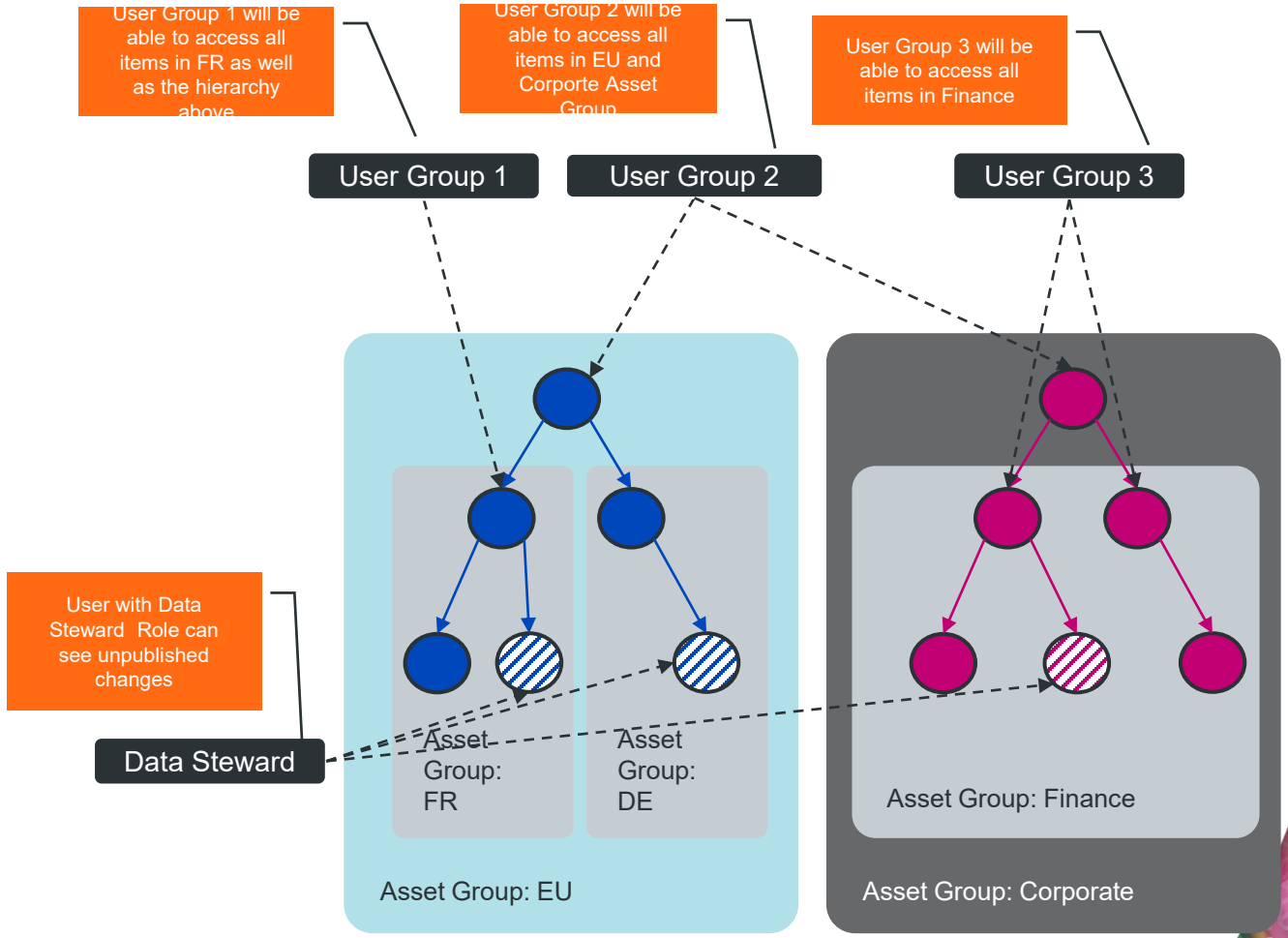
Enhanced control of permissions based on roles

- **User roles** grants access to asset types based on their roles.
  - Permissions can be granted at the abstract types level (Business assets, marketplace assets, and technical assets).
  - Permissions can be granted at individual type level
  - Technical assets: Different access controls can be defined for the same class type based on **catalog source type**.
- **Stakeholder roles** are used to control who gets to edit or make changes to an asset.
  - Presence of a stakeholder on an asset activates non-stakeholder policies to grant permission to other users.
  - In case of Tech Asset, Stakeholder assignment are inherited from parent asset unless overridden.



Control permissions on assets based on attribute

- Access to assets can be restricted based on attribute value of specific attribute
  - **Lifecycle**: Visibility based on Lifecycle values
    - For published asset, access to ongoing changes can be restricted as well
  - **Reference**: to reduce the scope permissions on technical assets
  - **Asset Group**: Parameters on an Asset that drives visibility of the asset for the user
- Permission on specific information on the Asset with attribute groups:
  - **Profiling:** base profiling statistics
  - **Data:** Value frequencies, Min/Max values
  - **Code:** Code definition (SQL, Calculation expressions…)
  - **unpublished changes:** Changes made to an asset published at least once



Access control policies

Collection of Rules

- Policy contains rules which grant permissions to users through
  - User roles
  - User groups
  - Or role performed on an asset (stakeholder roles)
- Scope based on
  - Assets filtered by type
  - Assets filtered based on attributes
  - Attribute groups
- Effective permissions are determined by the intersection of all applicable policies
- Once a user or stakeholder role policy with asset group filter is enabled, visibility of asset is effectively enforced and read permission must be granted for asset to be accessed

Access Control

Policy 1

Rule 1	**User Set**	Org-level Role : Business Asset Manager
	Resource	Technical Assets
	Actions	read

Rule 2	**User Set**	Org-level Role : Business Asset Manager
	Resource	Business Assets
	Actions	Create, read, update, delete, manage-access

Policy 2

Rule 1	**User Set**	User Group : Risk Analyst
	Resource	Assets in EU group
	Actions	Create, read, update, delete, manage-access

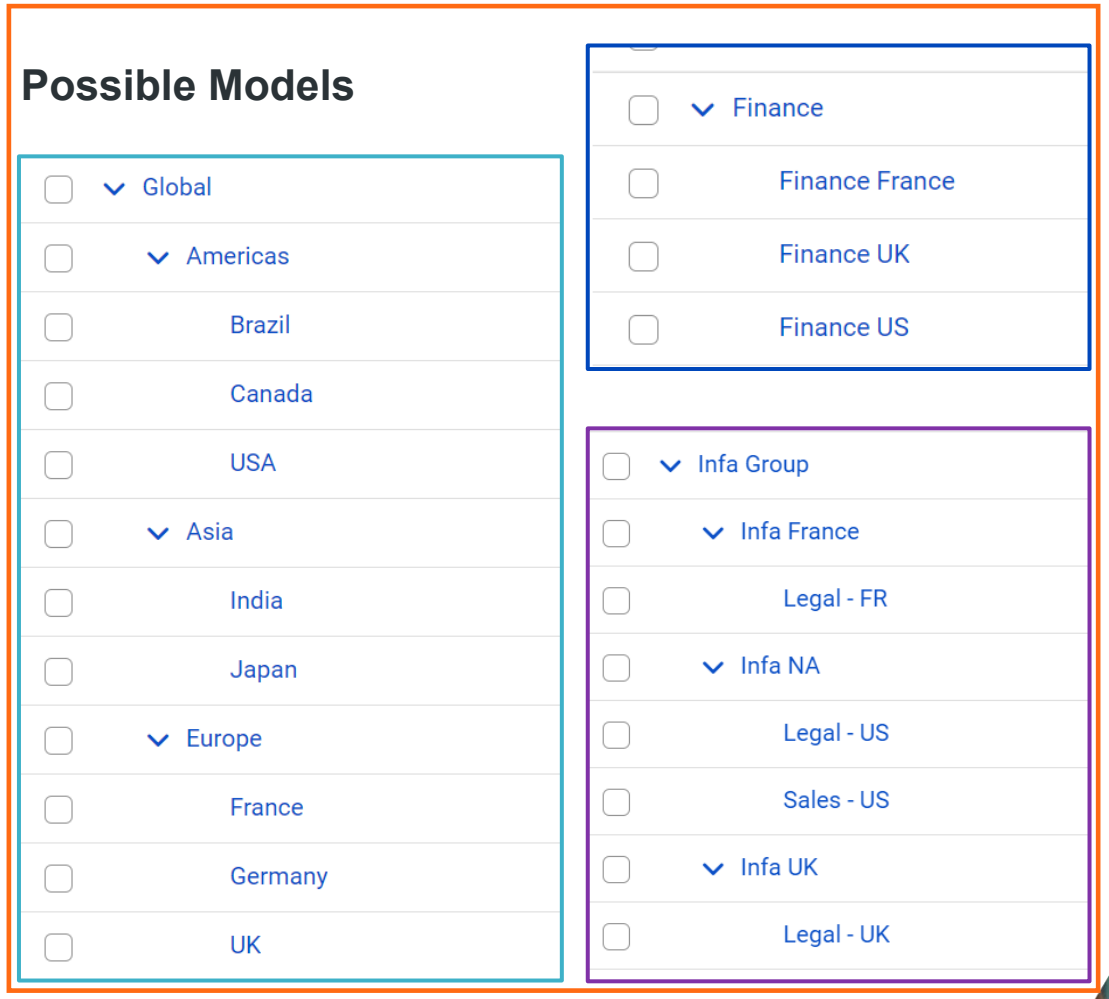
Policy 3

Rule 1	**User Set**	Stakeholder Role : Data Owner
	Resource	Business Assets with Lifecycle == drafts
	Actions	Create, read, update, delete, manage-access

MCC: Asset Group Structures

Asset Groups can be organized hierarchically – here's why

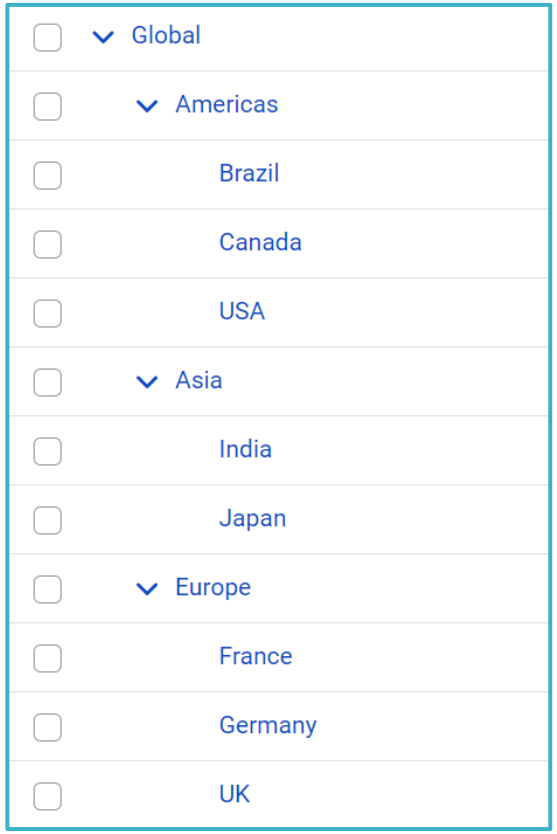
- Permission required: **Manage Asset Groups**
- Not everything needs to be protected, so we need to create scenarios that protect the right things, share the right things
  - E.g. shared enterprise glossary but each business units' assets protected for those employees only
- To achieve this, asset groups can be nested in a Parent/Child structure: Max 4 levels
- To simplify MAC policy creation there is a certain amount of visibility up and down this hierarchy

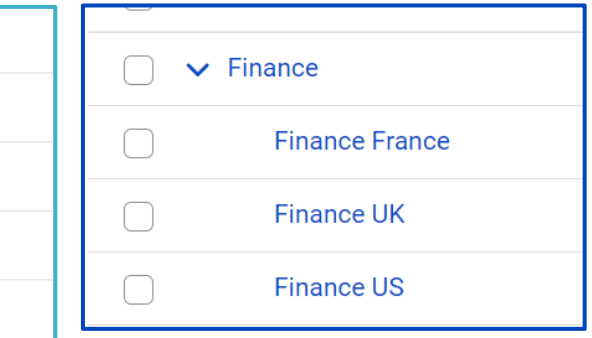


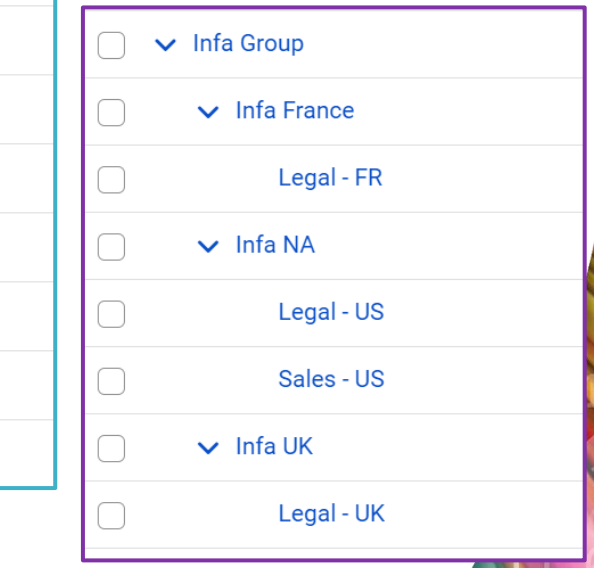
Asset Group – Different Ways to Organise

Different customers will choose different structures

- You only need to add an asset to the most restrictive group(s) required
- How should asset groups be organised?
  - There's no right/wrong answer – depends on customer model
  - Hierarchy will affect how policies impact viewer access
- Less is more – simpler to understand
  - Dozens / 100s of Asset Groups is unmanageable
- MCC: you can't edit Asset Group parent *after publish*



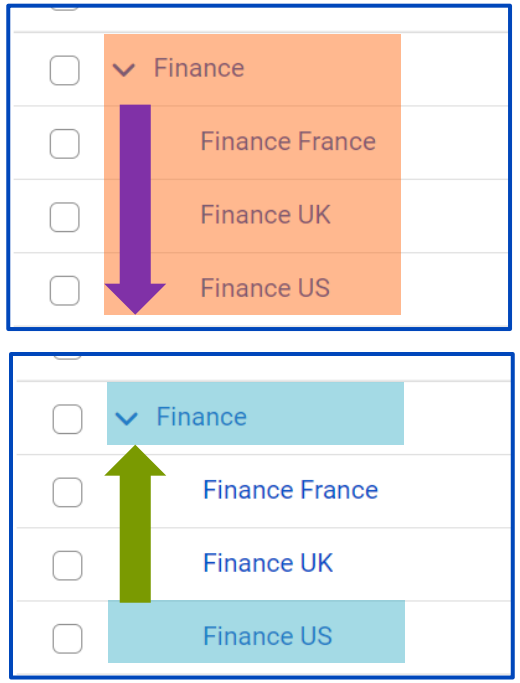




MCC: Asset Group Structures: Most Likely

Single Parent, Multiple Children

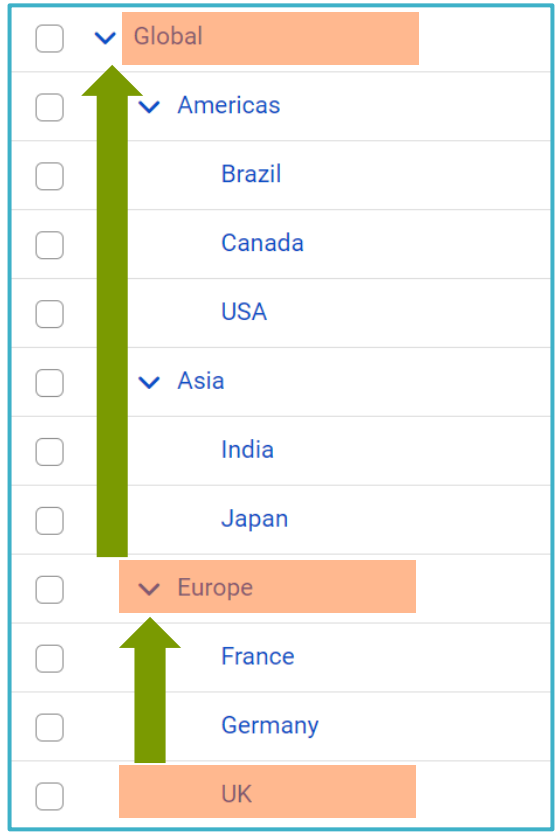
- A multinational company has organised its finance function across three territories – France, UK and USA
- They want all Finance employees to see some content, and keep the remainder protected for users in specific country locations.
    - Some senior users will require access to all Finance assets
- A policy written to permit access for different Asset Groups will have the following effect
    - Senior users granted access to **Finance** asset group will see
        - All assets marked with Finance asset group
        - All assets marked with any child asset group (France, UK and US)
    - Policy granting users access to **Finance US** will permit those users to see
        - All assets marked with Finance US asset group
        - All assets marked with Finance asset group
        - **No access to peers** (Finance France, Finance UK)



MCC: Asset Group Structures

Global / Region / Territory model

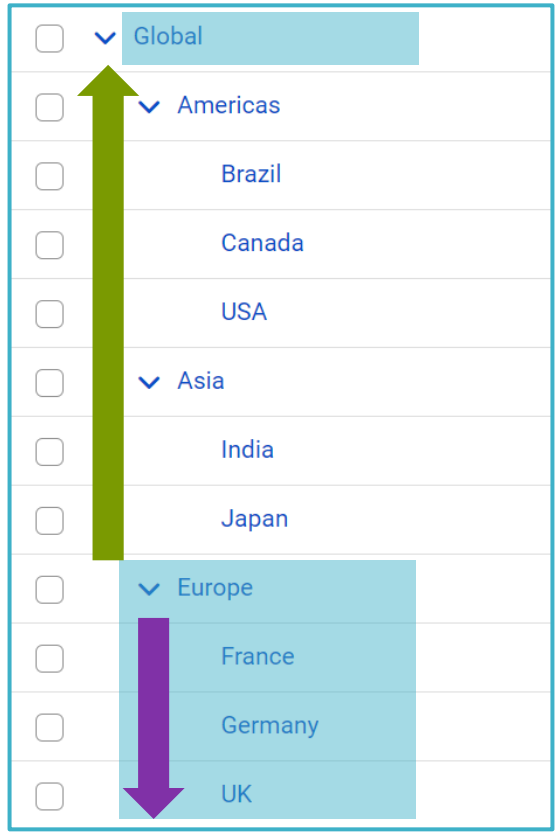
- More complex version of the previous example with 3 levels and more asset groups available. Same principles:
  - In CDGC allocate the assets to the most restrictive Asset Group they need
  - In MCC write polices to say who can access at which level
- A policy written to permit access to the **UK Asset Group** will have the following effect
  - UK
  - Europe
  - Global
  - No access to:
    - Peers (France, Germany)
    - Asia and Americas



MCC: Asset Group Structures

Global / Region / Territory model

- A policy written to permit access to the **Europe Asset Group** will have the following effect
  - Parent: any asset marked with Global
  - Any asset marked with Europe
  - All assets with children of Europe – France, Germany, UK
- They will **not see** content for
  - Peers: Americas, Asia



Informatica

Use Cases and Demo

Where data & AI come to LIFE

Business Drivers and Use Cases

- Story 1 >> Control Access to Unpublished Data Assets
- Story 2 >> Restrict Access to Sensitive Employee HR Data
- Story 3 >> Control Access to Data Access Policies
- Story 4 >> Cross Unit Glossary Collaboration

Demonstration

Story #1: Control Access to Unpublished Data Assets

Challenge

Ensure the Data Stewards can only access the published glossaries, so they are aware of the up to date and finalized glossary definitions.

Today:

- Some of the Draft and In-Review definitions often end up Data Stewards finding the multiple versions and some of them could be either outdated or not approved
- Follow up with stakeholders lead to additional time and effort

Solution

1.) In Administrator, define 2 roles as Glossary Steward and Stakeholders. (Re-use if existing already)

2.) In Metadata Command Center, create user role-based policy :

Data Steward :

Provide read, create, update, delete and manage access permissions along with read permission on

Condition		Permissions
Asset Type	**Is Any** Business Asset	Create, Delete, Manage Access, Read, Update
Attribute Group	**Is** Unpublished Changes	Read
Asset Type	**Is Any** Asset	

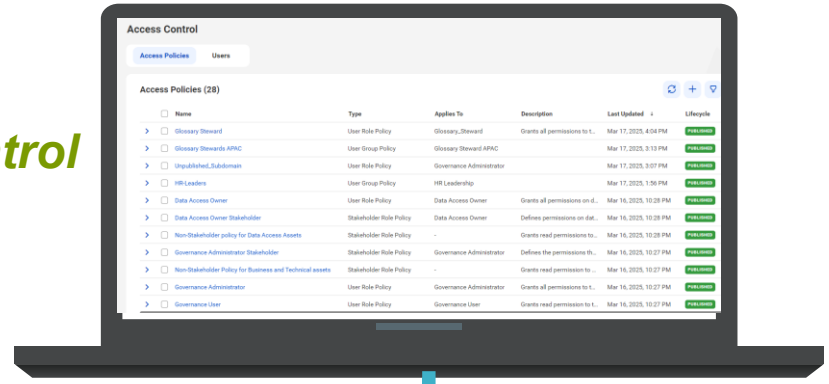
Stakeholders :

Provide read, create, update privileges along with lifecycle as **Published**

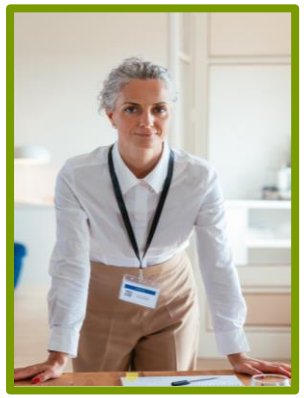
Condition		Permissions
Asset Type	**Is Any** Business Asset	Manage Access, Read, Update
Lifecycle	**Is** Published	

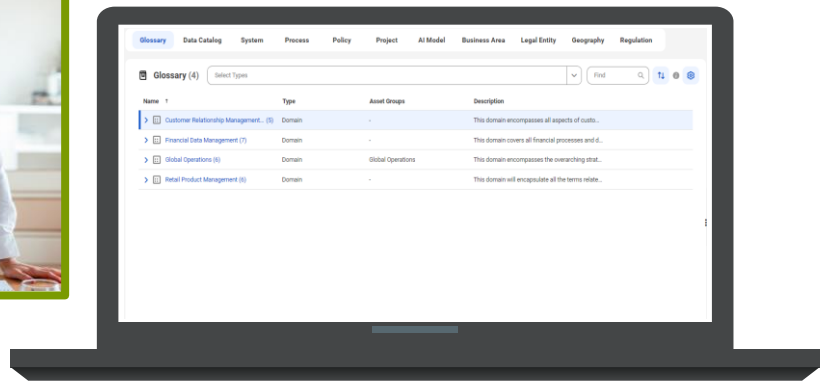
Result

Access Control

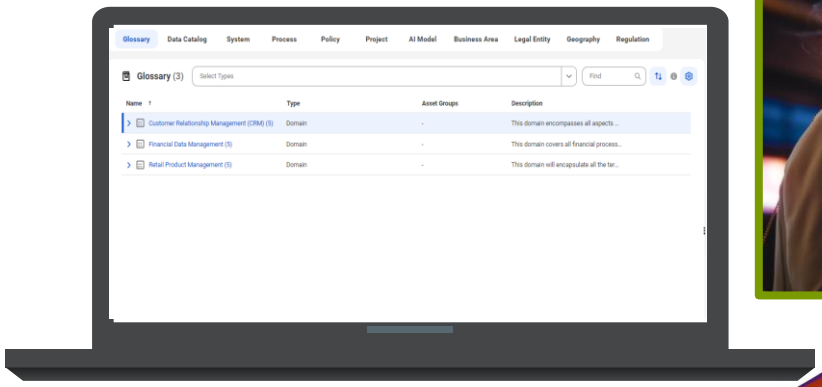


Glossary Stewards



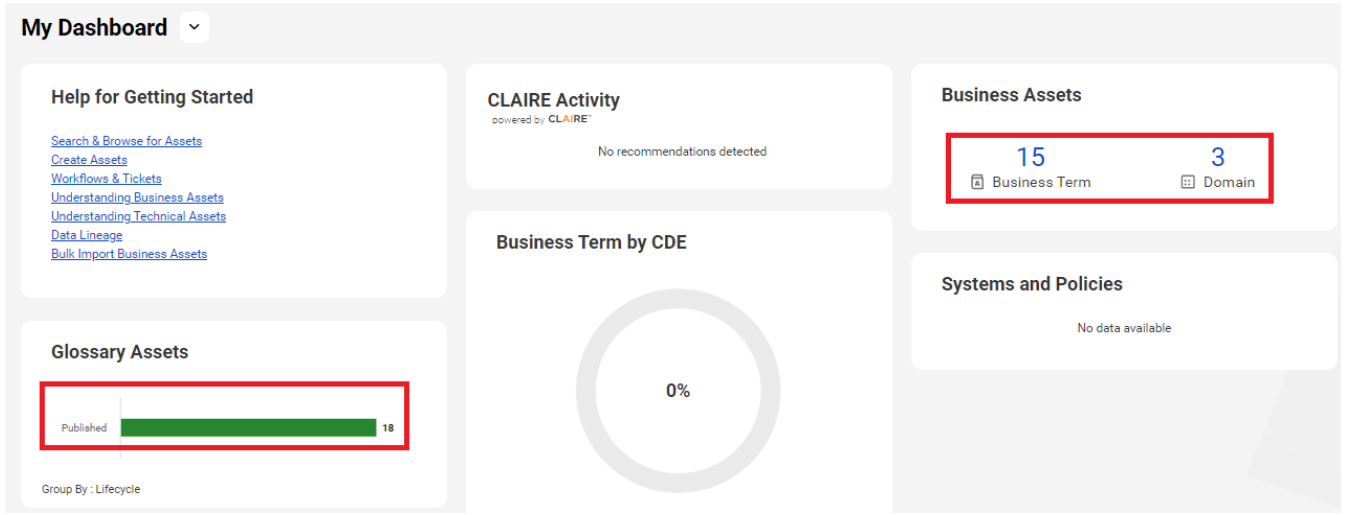


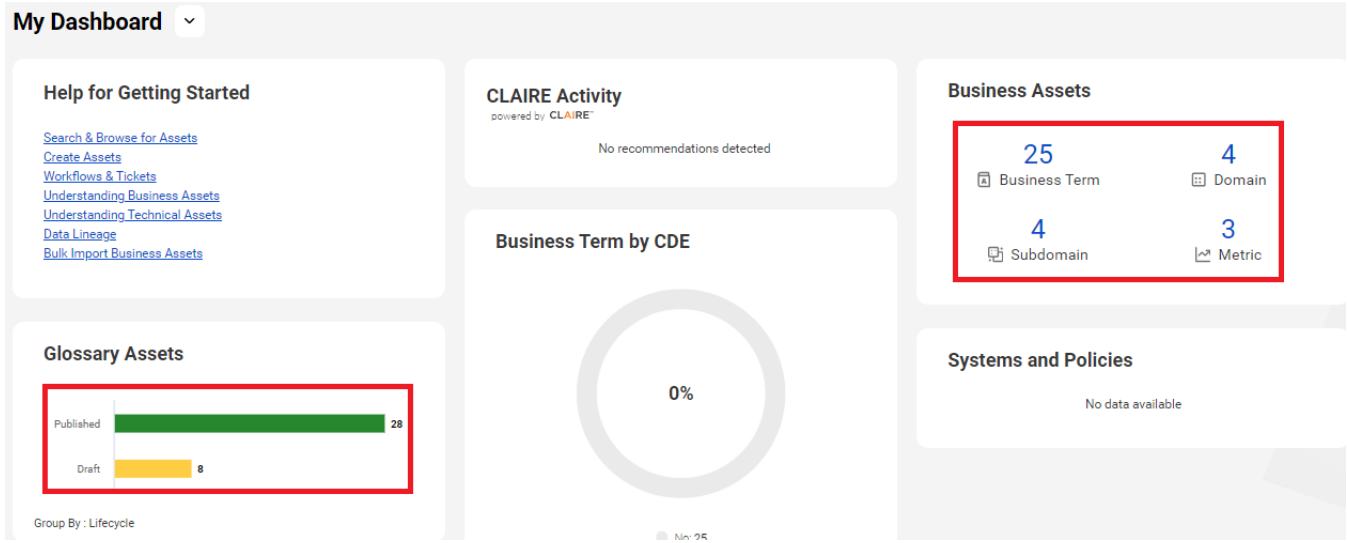
Stakeholders



CDGC: What will users from different personas see ?

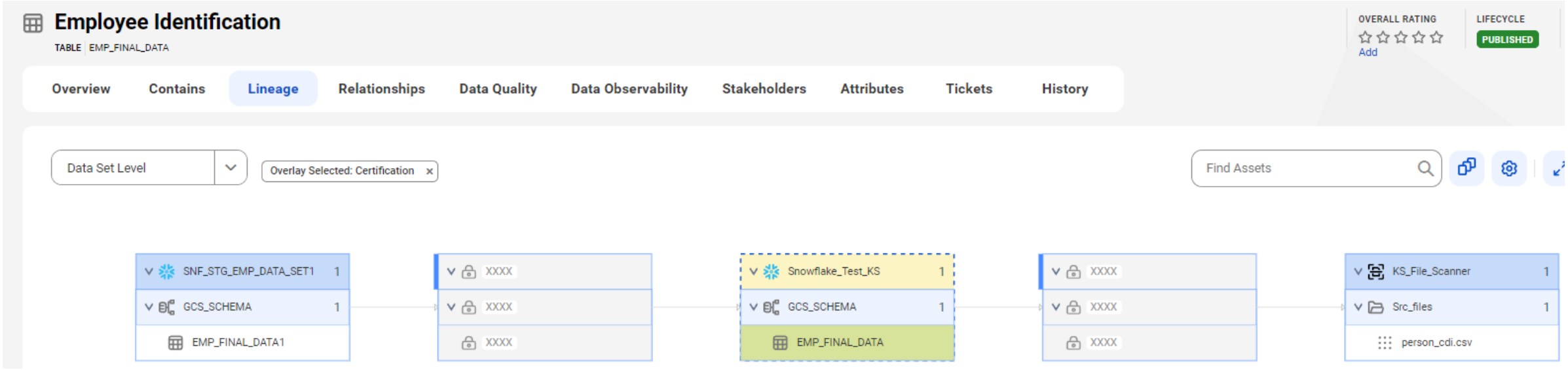
Users would see different # of assets depending upon the Metadata Access Control policies :





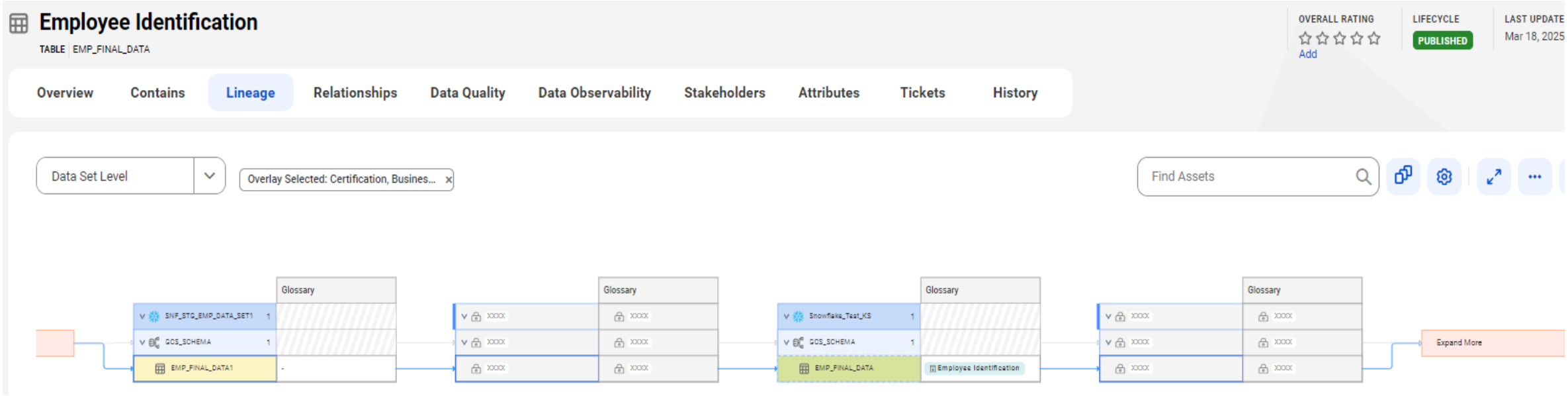
CDGC: What a technical lineage could look like ?

Technical Data Lineage Example



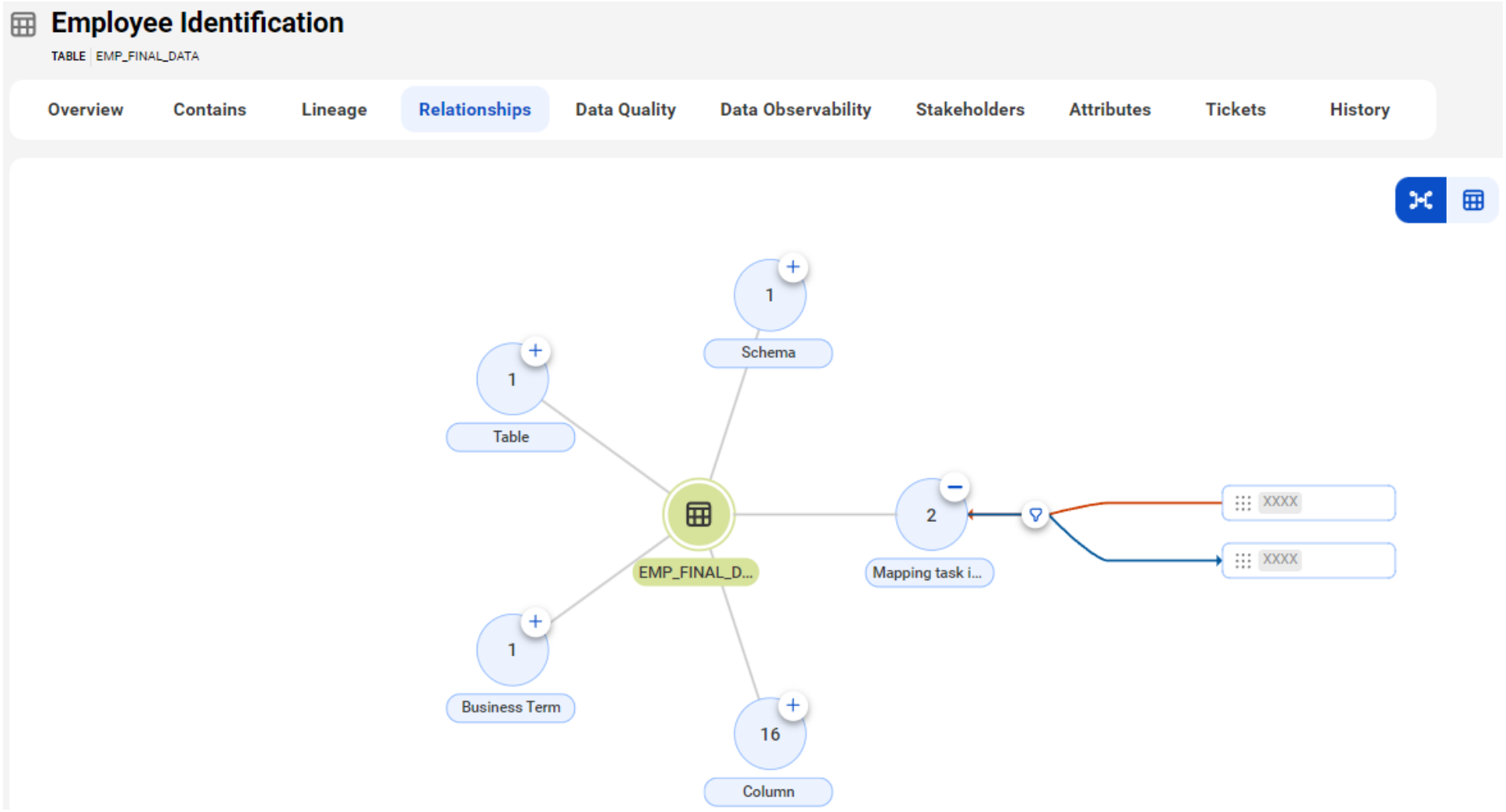
CDGC: What a technical lineage could look like ?

Technical Data Lineage Example with an overlay



CDGC: What a relationship diagram could look like ?

Relationship map



Informatica

DEMO

Where data & AI come to LIFE

Demonstration

Story #2: Restrict Access to Sensitive Employee HR Data

Challenge

Ensure that Data Stewards belonging to HR Department only can access the Data Marketplace categories and collections, so as to have a greater control around sensitive data for HR related decisions.

Today:

- Current setup allows the Data Stewards across the organization to access all the Data Marketplace categories and collections present, thus, limited security control.
- Data Owner manually needs to validate the department details & authorization of the requester while approving accesses.

Solution

1.) In Administrator, define a user group specific to Data Steward - HR and add the users who requires access to employee sensitive data. (Re-use if existing already)

2.) In Metadata Command Center, create an asset group such as HR – Data Stewards and assign to

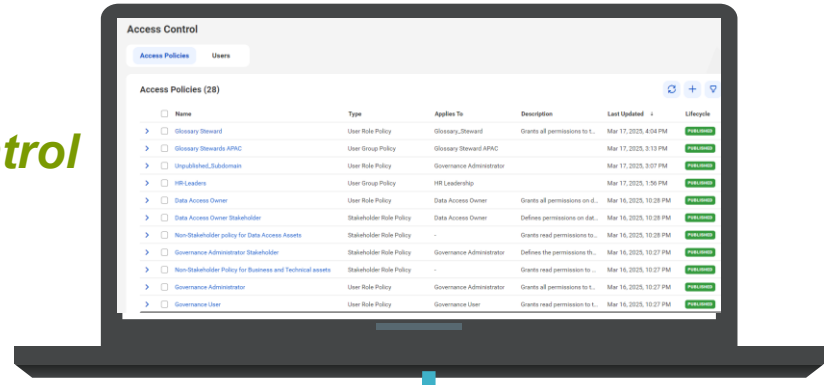
Asset Groups (5)

Name	Description	Updated On	Updated By	Lifecycle
Global Operations		Mar 17, 2025, 12:23 PM	Admin MAC	PUBLISHED
HR-Data Stewards		Mar 18, 2025, 10:23 AM	Admin MAC	PUBLISHED

3.) In Metadata Command Center, create a user group-based access policy for Data Steward – HR group with a rule granting read permissions on assets with HR – Data Stewards asset group.

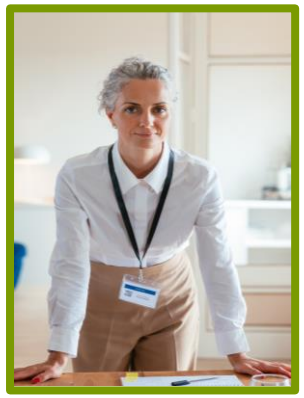
Condition		Permissions
Asset Type	**Is Any** Asset	Read
Asset Groups	**Is** HR-Data Stewards	

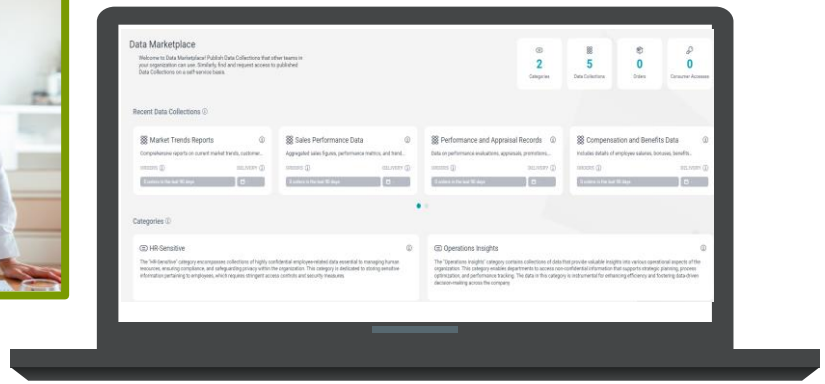
Result



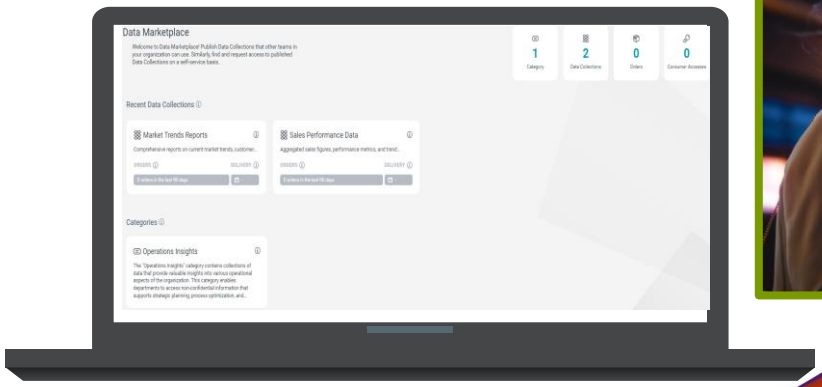
Access Control

Data Steward - HR





Data Steward - Finance



Informatica

DEMO

Where data & AI come to LIFE

Demonstration

Story #3: Control Access to Data Access Policies

Challenge

Governance users can access the Data Access Management policies irrespective of the roles within the organization they belong to.

Today:

- All users can view the Data Access polices and data protection standards applied.
- Data Access Owners from various business units or geographies may have overlapping or conflicting sets of use cases/requirements.

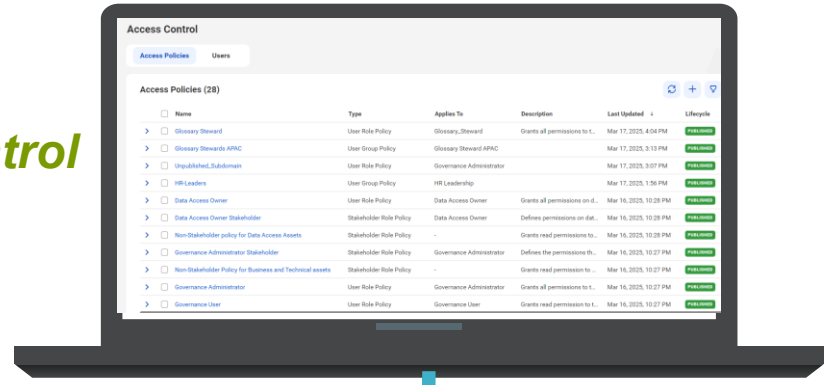
Solution

1.) In Administrator, define a user role for Data Engineering and assign to the users. (Re-use if existing already)

2.) In Metadata Command Center, create a user role policy for above Data Engineering role with grant read permissions on Data De-identification, Data Protection and Precedence Tier asset types.

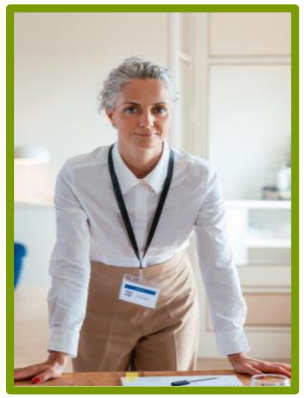
Condition		Permissions
Asset Type	**Is Any Of** Data De-identification, Data Protection, Precedence Tier	Read

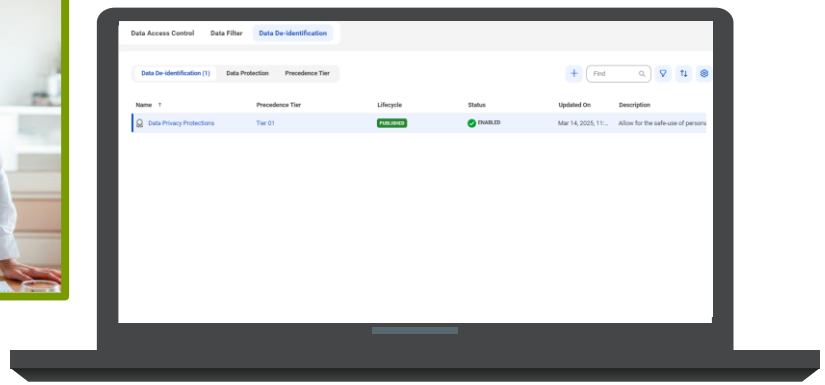
Result



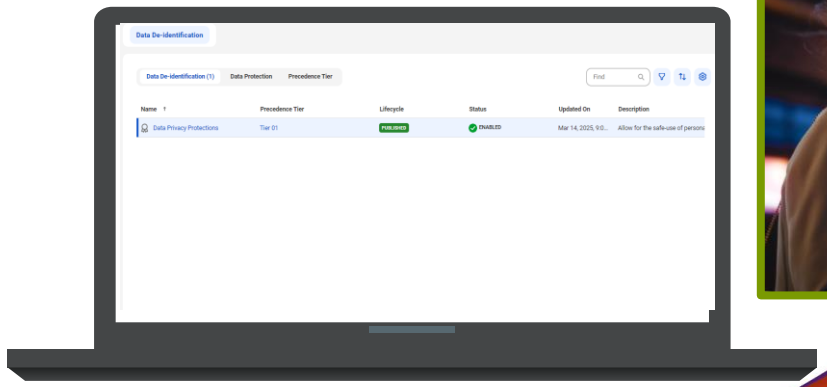
Access Control

Data Access Owner





Data Engineer/Governance User



Informatica

DEMO

Where data & AI come to LIFE

Demonstration

Story #4: Cross-Unit Glossary Collaboration

Challenge

Enterprise operates across geographies and thus, has an enterprise glossary that everyone should utilize and then, each geographical unit has its own assets that must stay separate from other units for security, legal and compliance reasons.

Today:

- Though there is a logical differentiation of glossary assets based on separate domains but still everyone has read-access to all assets across geographical units.
- Not that simple or straight forward to maintain such a glossary structure

Solution

1.) In Metadata Command Center, create a Global Operations assets group followed by 3 child asset groups for America, APAC and EMEA operations respectively.

Asset Groups (5)

Name	Description	Updated On	Updated By	Lifecycle
Global Operations		Mar 17, 2025, 12:23 PM	Admin MAC	PUBLISHED
Americas Operations		Mar 17, 2025, 12:23 PM	Admin MAC	PUBLISHED
APAC Operations		Mar 17, 2025, 12:24 PM	Admin MAC	PUBLISHED
EMEA Operations		Mar 17, 2025, 12:24 PM	Admin MAC	PUBLISHED

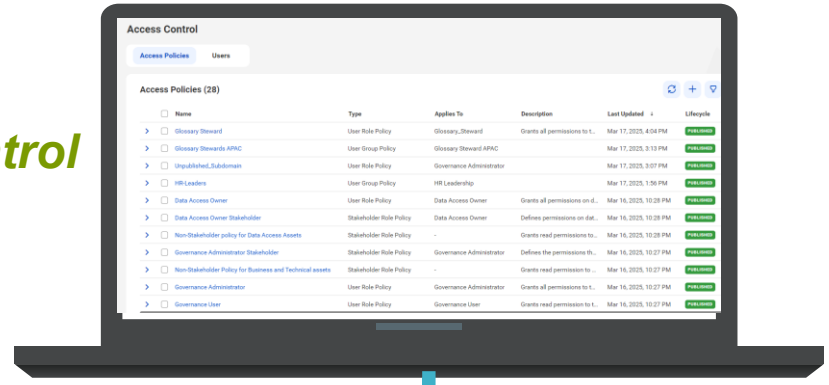
2.) Assign each child asset group to corresponding business units and global asset group to enterprise glossary assets that all users can collaborate on.

3.) Use these asset groups in access policies to grant different levels of user accesses to each asset group.

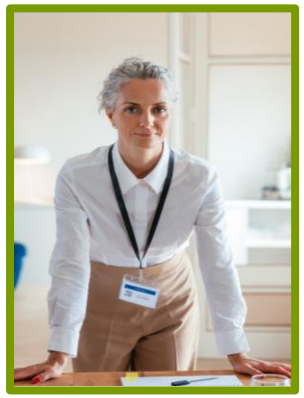
Condition		Permissions
Asset Type	**Is Any** Asset	Create, Delete, Execute, Manage Access, Read, Update
Asset Groups	**Is** APAC Operations	

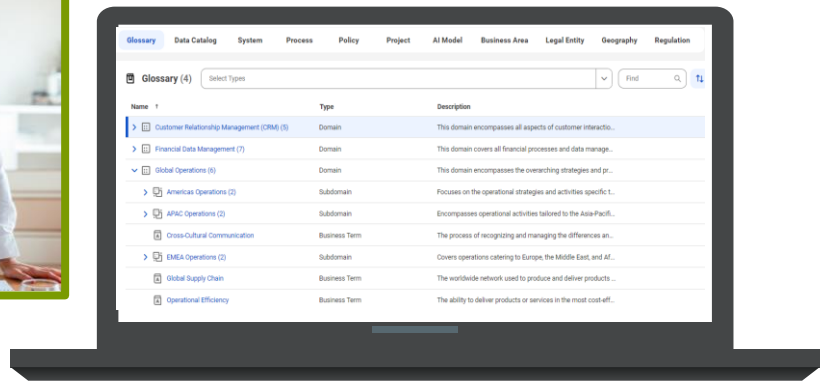
Result

Access Control

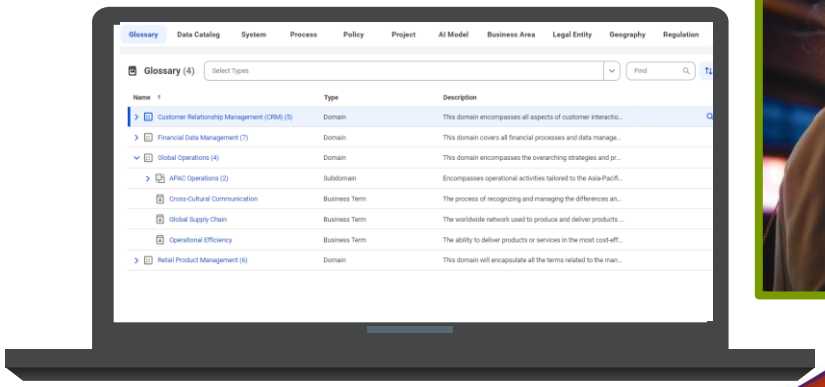


Data Steward - Global





Data Steward - APAC



Informatica

DEMO

Where data & AI come to LIFE

Metadata Access control

Out-Of-The-Box definitions

- CDGC Predefined Roles
  - **Governance Administrator** : access MCC and CDGC and has most of the administrator privileges
  - **Governance Owner** : manage business assets in CDGC application
  - **Governance User** : access CDGC with limited privileges
- CDMP Predefined Roles
  - **Data Marketplace Administrator :** perform administrative tasks related to Data Marketplace
  - **Data Marketplace Technical Administrator :** manage delivery options and various settings, specifying the general terms of use
  - **Data Marketplace Category Owner :** responsible for managing the category and data collections in your category
  - **Data Marketplace Delivery Technical Owner :** manage delivery options that is used to deliver the data collections
  - **Data Marketplace Collection Owner :** publish/unpublish the collections responsible for. Manage data assets within the collection.
  - **Data Marketplace Technical Owner :** provision data to Data Owners whose orders are approved by Data Owners
  - **Data Marketplace User :** can search for and order Data Collections that are published
- Data Access Management Predefined Roles
  - **Data Access Owner :** manage assets in Data Access Management

Metadata Access Control

Summary

More Control

- Greater control over different asset types
  - Who can access
  - Who can be a stakeholders
- Write your own rules
- In Metadata Command Centre (MCC)

Attribute Based

- Lifecycle
- Reference Technical Assets
- Asset Groups

Attribute Group Based

- Profiling
- Data
- Code
- Unpublished Changes

References :

- Metadata Access Control in CDGC - 2024.11 Release – Webinar
- Metadata Access Control - Docs
- Informatica Cloud Data Marketplace -Introduction and Getting Started
- TT Webinar - Data Discovery Best Practices in Cloud Data Governance and Catalog
- TT Webinar - Enabling Self-Service Analytics using CDMP, CDGC and CDQ
- Experience Lounge – IDMC

Thank You

Where data & AI come to LIFE