Mastering the Security Maze: Navigating OBS and Security Rights

Your Guides:
Chris Ciavarella and David Zywiec

Agenda

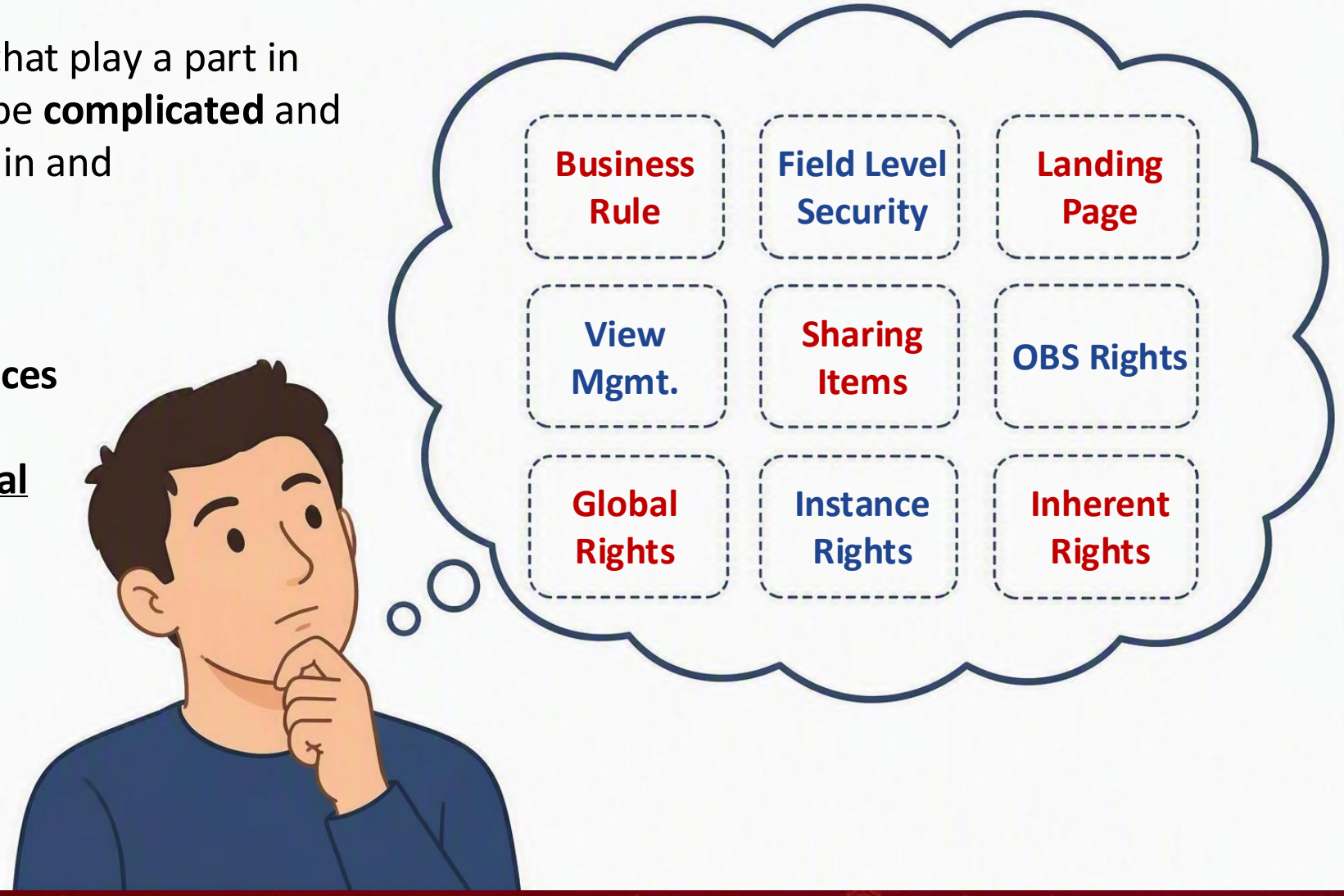
- Introduction to Security
- Security Rights
  - Global Rights
  - OBS Rights
  - Instance Rights
  - Inherent/Automatic Rights
  - Psuedo-Security: Blueprint Rules
- Organizational Breakdown Structures (OBS)
  - OBS Demo / Live Session
- Security Best Practices

Introduction to Security

Complex Security & Rego's Value

Navigating all of the components that play a part in securing something in Clarity can be **complicated** and **challenging** to understand, maintain and troubleshoot.

Following Rego/Broadcom **recommendations** and **best practices** will guide you in forming a model that is **optimized**, will have **minimal potential impact to performance**, and will have the *least* amount of **administrative overhead**.



Security Considerations

- Can be assigned at group or individual level
  - Best practice is group level
  - Define groups based on needed functionality (e.g., PM Group, RM Group, Admin group)
  - Provides option to restrict access to menu options, pages, etc.
  - Provides option to secure sub-objects and sub-pages (Classic PPM)
  - Provides option to notify everybody in a group (e.g., Results of Job execution)

- **NOTE – the rights you grant can impact your licensing costs!**

Security Rights

Overview

regoUniversity
SAN ANTONIO·2026

Security Rights – Overview

Security Rights can be applied at the **Global**, **OBS**, or **Instance** level.

GLOBAL RIGHTS

Access to ALL Projects in the organization

OBS RIGHTS – Marketing OBS

Access to all **Marketing** projects

- **Omnichannel Campaign Manager**
- **AI Content Generator for Social Media**
- **Real-Time Influencer ROI Tracker**
- **Voice-of-Customer Sentiment Analyzer**
- **Hyper-Personalized Email Engine**

INSTANCE RIGHTS
Access to these specific projects only

OBS RIGHTS – Finance OBS

Access to all **Finance** projects

- **Expense Reconciliation System**
- **Cash Flow Forecasting AI Model**
- **Digital Audit Trail Platform**
- **Vendor Payment Optimization Tool**
- **Financial Risk Heatmap Dashboard**

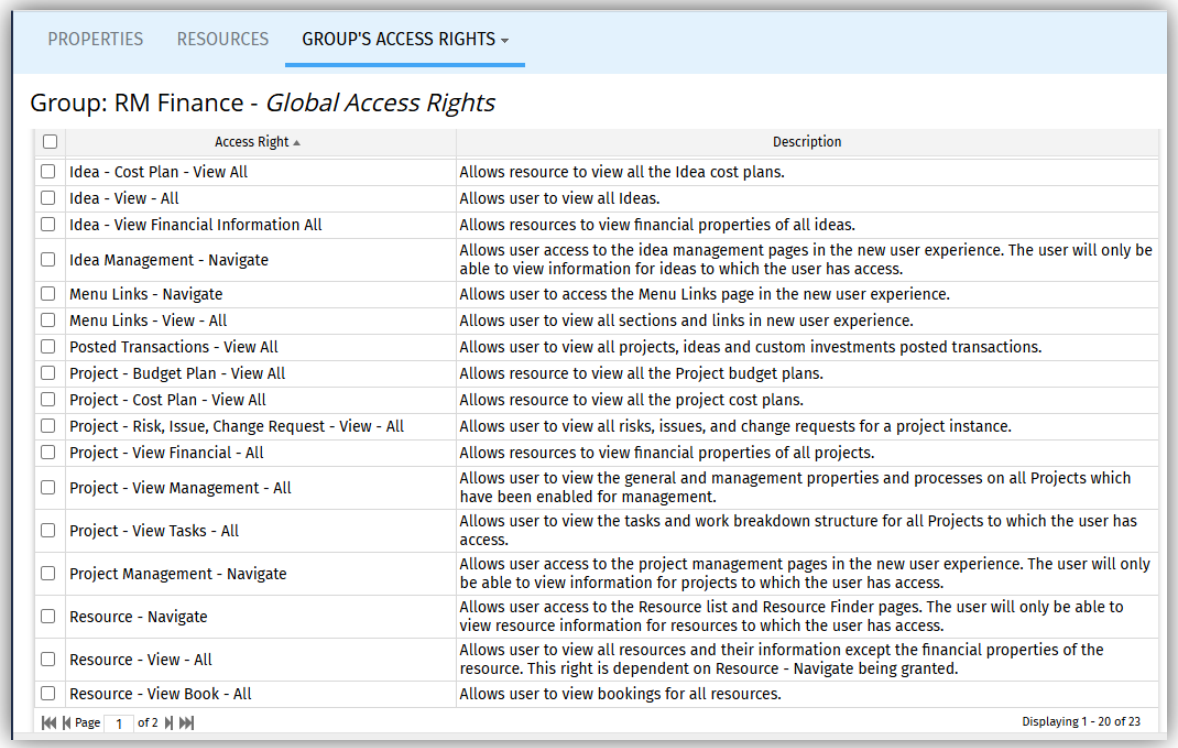
INSTANCE RIGHTS
Access to these specific projects only

Security Rights

Global Rights

Security Rights – Global Rights

- Global Rights have the broadest scope
- Overrides any other associated instance or OBS level rights
- Provides broad access to objects of a particular type
- Allows users access a general area of the application to perform a specific function or to all instances of an object
- A common global right is Resource – View All
- Recommended where possible for performance reasons



PROPERTIES | RESOURCES | GROUP'S ACCESS RIGHTS

Group: RM Finance - *Global Access Rights*

Access Right	Description
Idea - Cost Plan - View All	Allows resource to view all the Idea cost plans.
Idea - View - All	Allows user to view all Ideas.
Idea - View Financial Information All	Allows resources to view financial properties of all ideas.
Idea Management - Navigate	Allows user access to the idea management pages in the new user experience. The user will only be able to view information for ideas to which the user has access.
Menu Links - Navigate	Allows user to access the Menu Links page in the new user experience.
Menu Links - View - All	Allows user to view all sections and links in new user experience.
Posted Transactions - View All	Allows user to view all projects, ideas and custom investments posted transactions.
Project - Budget Plan - View All	Allows resource to view all the Project budget plans.
Project - Cost Plan - View All	Allows resource to view all the project cost plans.
Project - Risk, Issue, Change Request - View - All	Allows user to view all risks, issues, and change requests for a project instance.
Project - View Financial - All	Allows resources to view financial properties of all projects.
Project - View Management - All	Allows user to view the general and management properties and processes on all Projects which have been enabled for management.
Project - View Tasks - All	Allows user to view the tasks and work breakdown structure for all Projects to which the user has access.
Project Management - Navigate	Allows user access to the project management pages in the new user experience. The user will only be able to view information for projects to which the user has access.
Resource - Navigate	Allows user access to the Resource list and Resource Finder pages. The user will only be able to view resource information for resources to which the user has access.
Resource - View - All	Allows user to view all resources and their information except the financial properties of the resource. This right is dependent on Resource - Navigate being granted.
Resource - View Book - All	Allows user to view bookings for all resources.

Page 1 of 2 — Displaying 1 - 20 of 23

Global Rights will provide access to "All" records of a given type, as denoted in the Access Right name and description

Global Rights

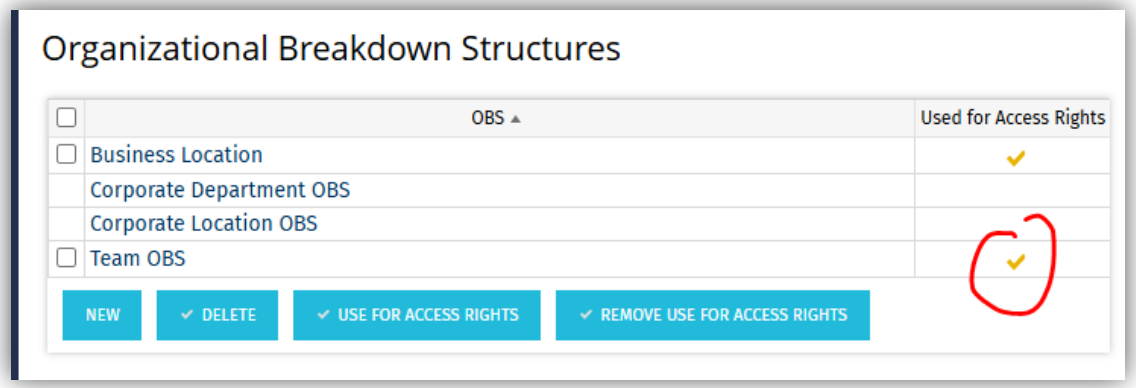
Demo

Security Rights

OBS Rights

Security Rights – OBS-Level Rights

- OBS-Level Rights define access to a logical grouping of items
  - Investments grouped by Department
- More limited access based on the OBS that a record is associated with
  - e.g., Project – View access to all projects where Department OBS = Corporate/Marketing
- Common use case is to isolate resources or projects for discrete organizations



If an OBS will be used to define access to a logical grouping of instances, ensure that it is selected for **Use for Access Rights.**

***Note**: When an OBS is **not** used for access rights, its purpose is more suited for tagging (organizing data into logical groups) and then reporting/filtering on those selections only.*

OBS Rights

Demo

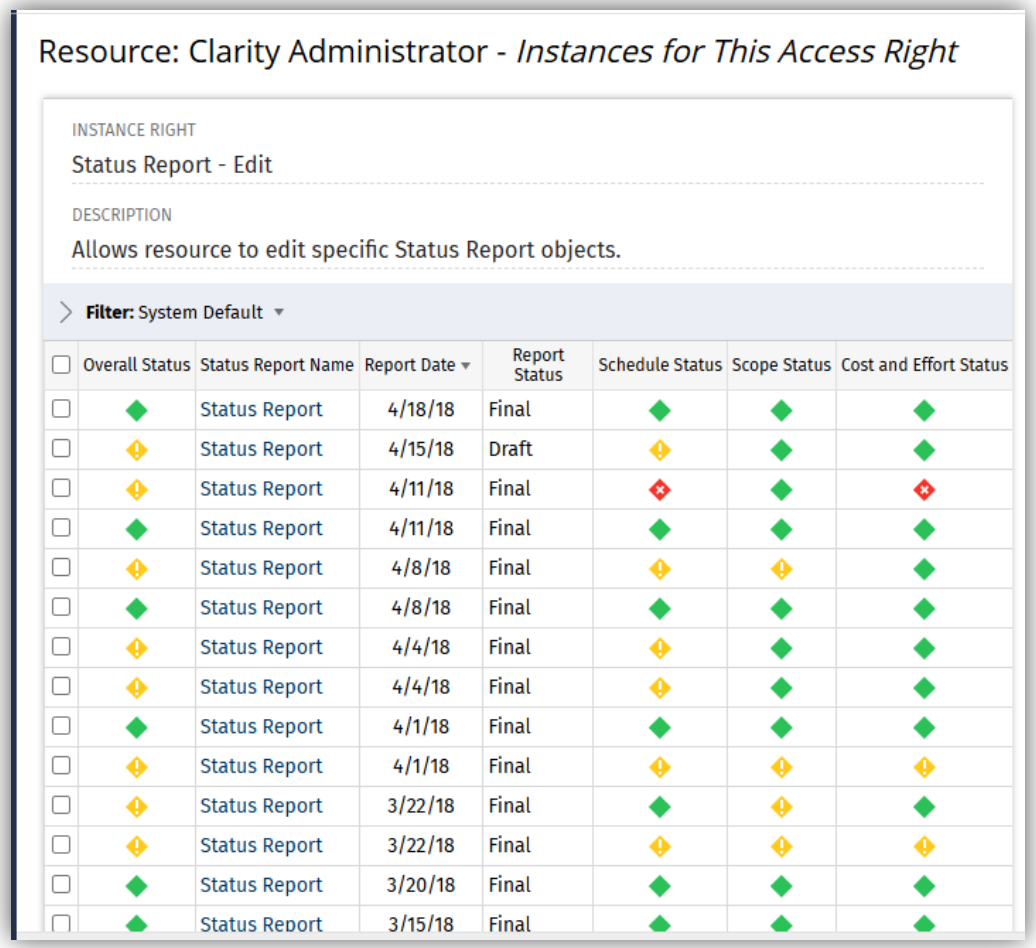
regoUniversity
SAN ANTONIO·2026

Security Rights

Instance Rights

Security Rights – Instance Rights

- Provide access to a specific instance of an object (one project, one resource, etc.)
- Can be assigned to an individual or a group
- Can lead to performance issues if not managed carefully
- ***Difficult to manage*** **-** minimal use is recommended

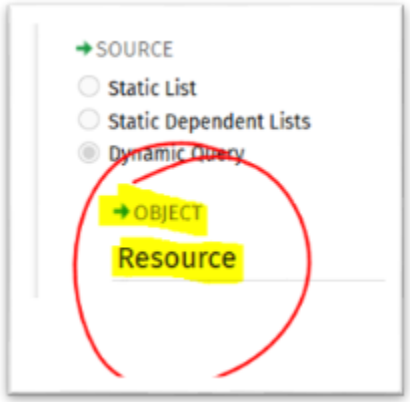


Overall Status	Status Report Name	Report Date	Report Status	Schedule Status	Scope Status	Cost and Effort Status
◆	Status Report	4/18/18	Final	◆	◆	◆
⚠	Status Report	4/15/18	Draft	⚠	◆	◆
⚠	Status Report	4/11/18	Final	✖	◆	✖
◆	Status Report	4/11/18	Final	◆	◆	◆
⚠	Status Report	4/8/18	Final	⚠	⚠	◆
◆	Status Report	4/8/18	Final	◆	◆	◆
⚠	Status Report	4/4/18	Final	⚠	◆	◆
⚠	Status Report	4/4/18	Final	⚠	◆	◆
◆	Status Report	4/1/18	Final	◆	◆	◆
⚠	Status Report	4/1/18	Final	⚠	⚠	⚠
⚠	Status Report	3/22/18	Final	◆	⚠	◆
⚠	Status Report	3/22/18	Final	⚠	⚠	⚠
◆	Status Report	3/20/18	Final	◆	◆	◆
◆	Status Report	3/15/18	Final	◆	◆	◆

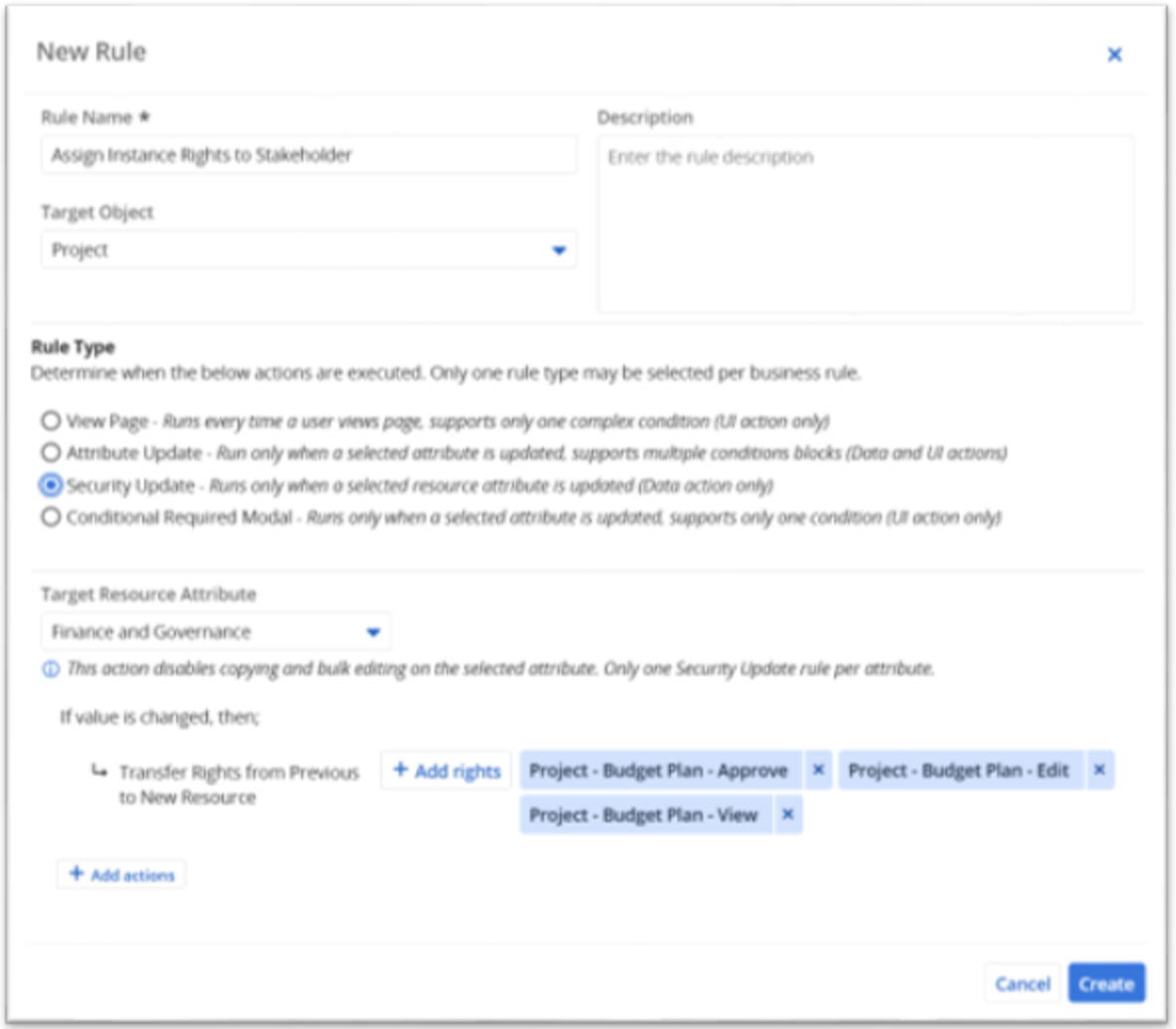
Security Rights – Instance Rights Cont'd

- Granting Instance rights to Stakeholders is now a much easier than it used to be

- A **Security Update** rule will allow you to add, remove, or transfer rights to stakeholders in Resource Attributes



A **Resource Attribute** is one that is associated to a lookup which is associated to the **Resource** object

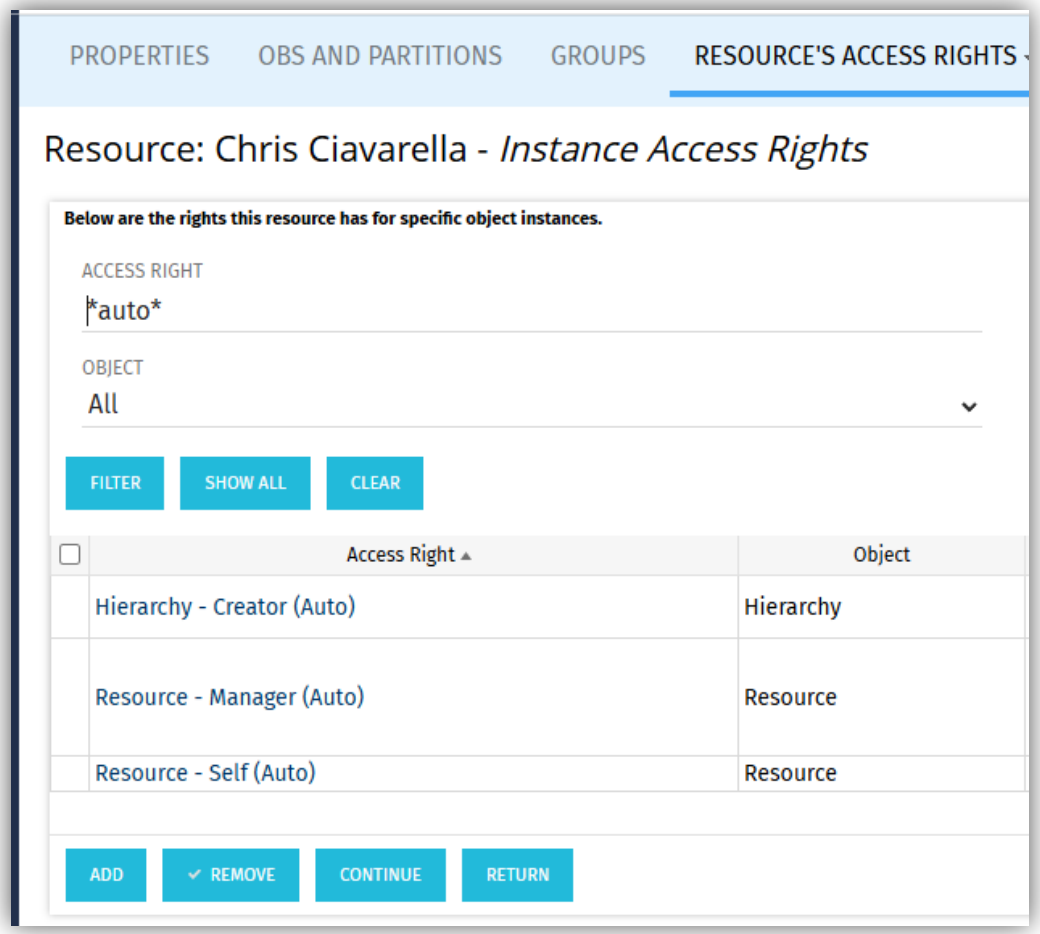


Instance Rights

Demo

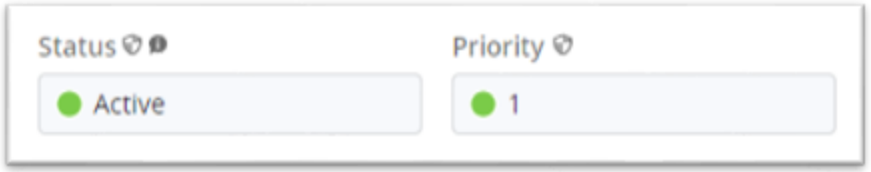
Security Rights – Inherent/Automatic Rights

- Automatically applied when user is first added to Clarity or the user is associated with a particular field on an object (e.g., Resource Manager)
- **Irrevocable**
  - User Favorites Menu – Edit
  - Project – Manager (Auto)
  - Resource – Manager (Auto)
- **Revocable**
  - Resource – Enter Time (for themselves)

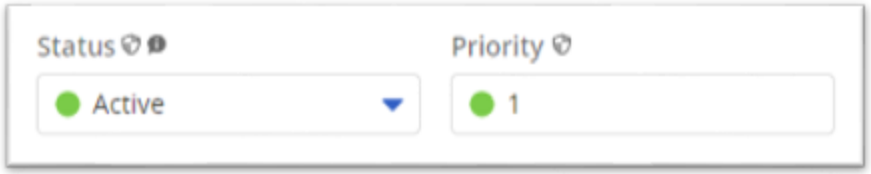


Security Rights – Field-Level Security (FLS)

- Controls access to a specific attribute of an object
- Available in Modern UX under:
  Administration -> Attributes
- Can grant view and edit rights or hide a field entirely
  - *When inaccessible secured fields comprise an entire blueprint section, that section is not rendered.
- Can lead to performance issues if not managed carefully
- Is denoted by a "shield" icon in the field label 
- ***Difficult to manage*** **-** minimal use is recommended



When a secured field is read-only for the current logged-in user, it appears greyed-out.



When a secured field is editable for the current logged-in user, it renders normally but the "shield" is still denoted in the label

Best practice: Prioritize Group and OBS access rights over Field-Level Security

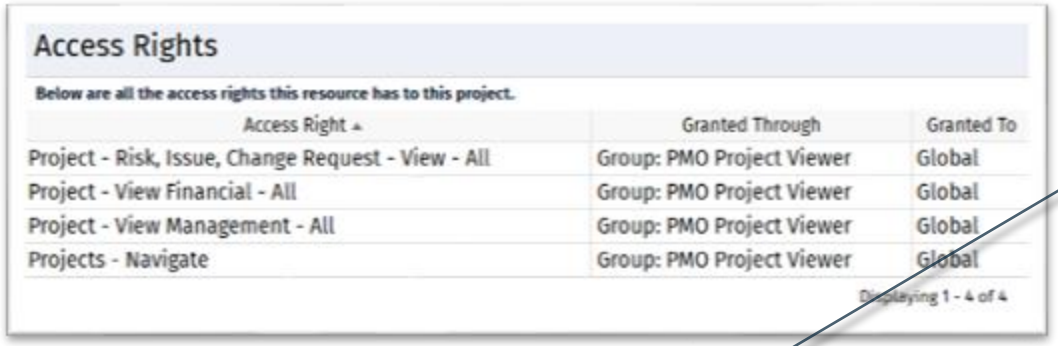
Security Rights – Field-Level Security (FLS)

The **Prioritize Access Rights Over Attribute Level Security** system option under **Administration -> System Options (Classic UI)** controls the behavior of Field-Level Security.

Sample Security Configuration:

Access Rights

- User is a member of the **PMO Project Viewer** group and has global view-only access to all projects



Access Rights

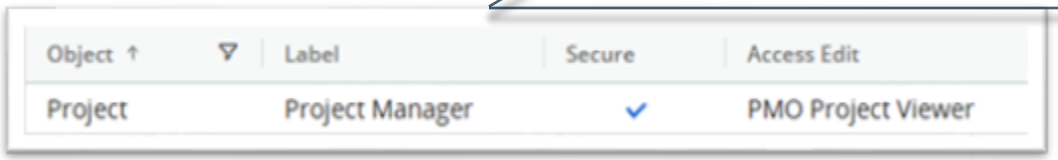
Below are all the access rights this resource has to this project.

Access Right	Granted Through	Granted To
Project - Risk, Issue, Change Request - View - All	Group: PMO Project Viewer	Global
Project - View Financial - All	Group: PMO Project Viewer	Global
Project - View Management - All	Group: PMO Project Viewer	Global
Projects - Navigate	Group: PMO Project Viewer	Global

Displaying 1 - 4 of 4

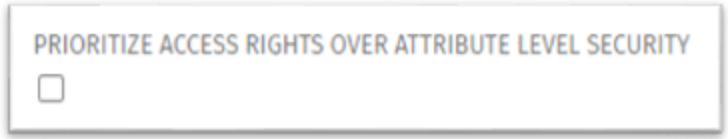
Field Level Security

- **Edit** rights have been granted to the **PMO Project Viewer** group



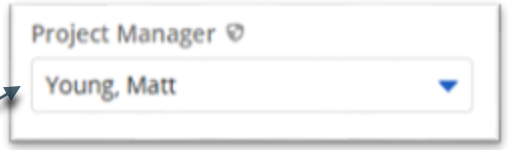
Object	Label	Secure	Access Edit
Project	Project Manager	✓	PMO Project Viewer

Scenario 1 (Disabled - Default)



PRIORITIZE ACCESS RIGHTS OVER ATTRIBUTE LEVEL SECURITY

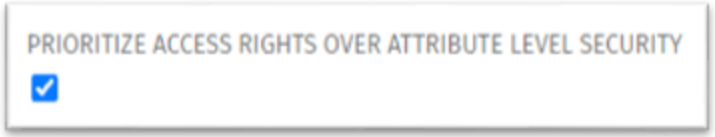
Result: FLS takes effect and field is ***Editable***



Project Manager

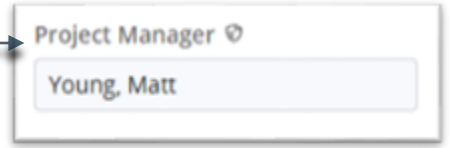
Young, Matt

Scenario 2 (Enabled)



PRIORITIZE ACCESS RIGHTS OVER ATTRIBUTE LEVEL SECURITY

Result: Access Rights prioritized, field remains ***Read-Only***

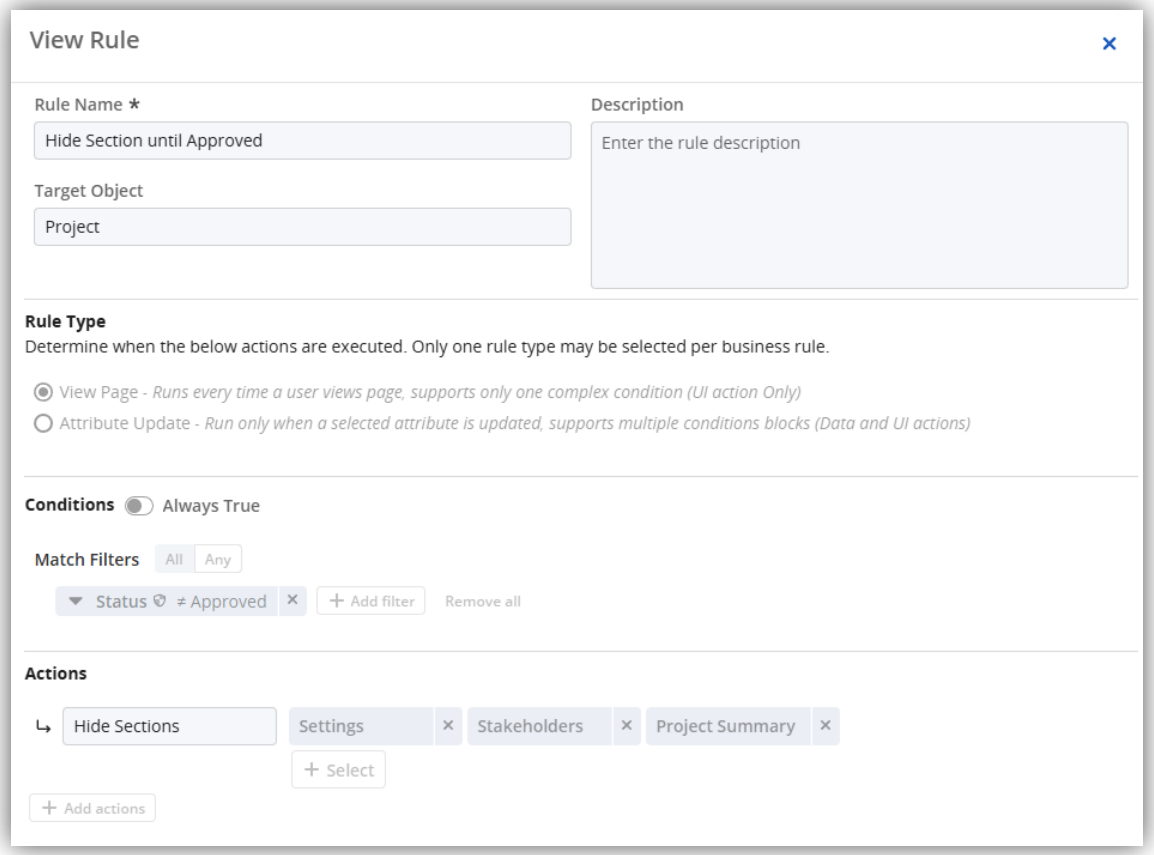


Project Manager

Young, Matt

Pseudo-Security: Blueprint Rules

- Records (instances), attributes, sections and modules (tabs) of a Blueprint in the MUX can be conditionally “secured” or hidden using Blueprint-based Business Rules
- This type of security can still be circumvented by Classic PPM, XOG, REST APIs or Processes
- Read-Only Blueprint rules always take precedence over Field-Level Security ‘Edit’ access



Blueprint Rules vs. FLS

Individual attributes in Clarity can be conditionally secured or hidden using either Blueprint-based Business Rules or using FLS (field level security) at the attribute-level. Some initial considerations to help determine the optimal approach given the requirements:

Feature \ Requirement	Business Rule	Field Level Security
Securing Logic	Can be aligned to both group membership and other attribute conditions and triggers	Relies strictly on group membership
Real-Time Application	May require a screen refresh if business rules is triggered based on real-time condition being met	Always active
User Experience	Applies to Modern UX only.	
Evaluation Priority	Most restrictive takes priority.	
Priority Against Security Rights	Most restrictive takes priority.	FLS takes priority over security rights, unless “Prioritize Access Rights over Attribute Level Security” is selected in system options.

Blueprint Rules vs. FLS

Individual attributes in Clarity can be conditionally secured or hidden using either Blueprint-based Business Rules or using FLS (field level security) at the attribute-level. Some initial considerations to help determine the optimal approach given the requirements:

Feature \ Requirement	Business Rule	Field Level Security
Supported Number of Attributes	**Users can define any number of rules but only 50 rules can be active simultaneously.**	**No restriction**
Supported Attribute Types	**Cannot be used to secure time-scaled attributes.**	**A minimal number of attributes are flagged as "Not Securable."**
Performance	**Not formally evaluated**	**Not formally evaluated**
Visual Indicator	**Field is "greyed out" with hover message that indicated field is locked by a business rule**	**Field is "greyed out" with shield icon visible to the right of the attribute label**

Organizational Breakdown Structures (OBS)

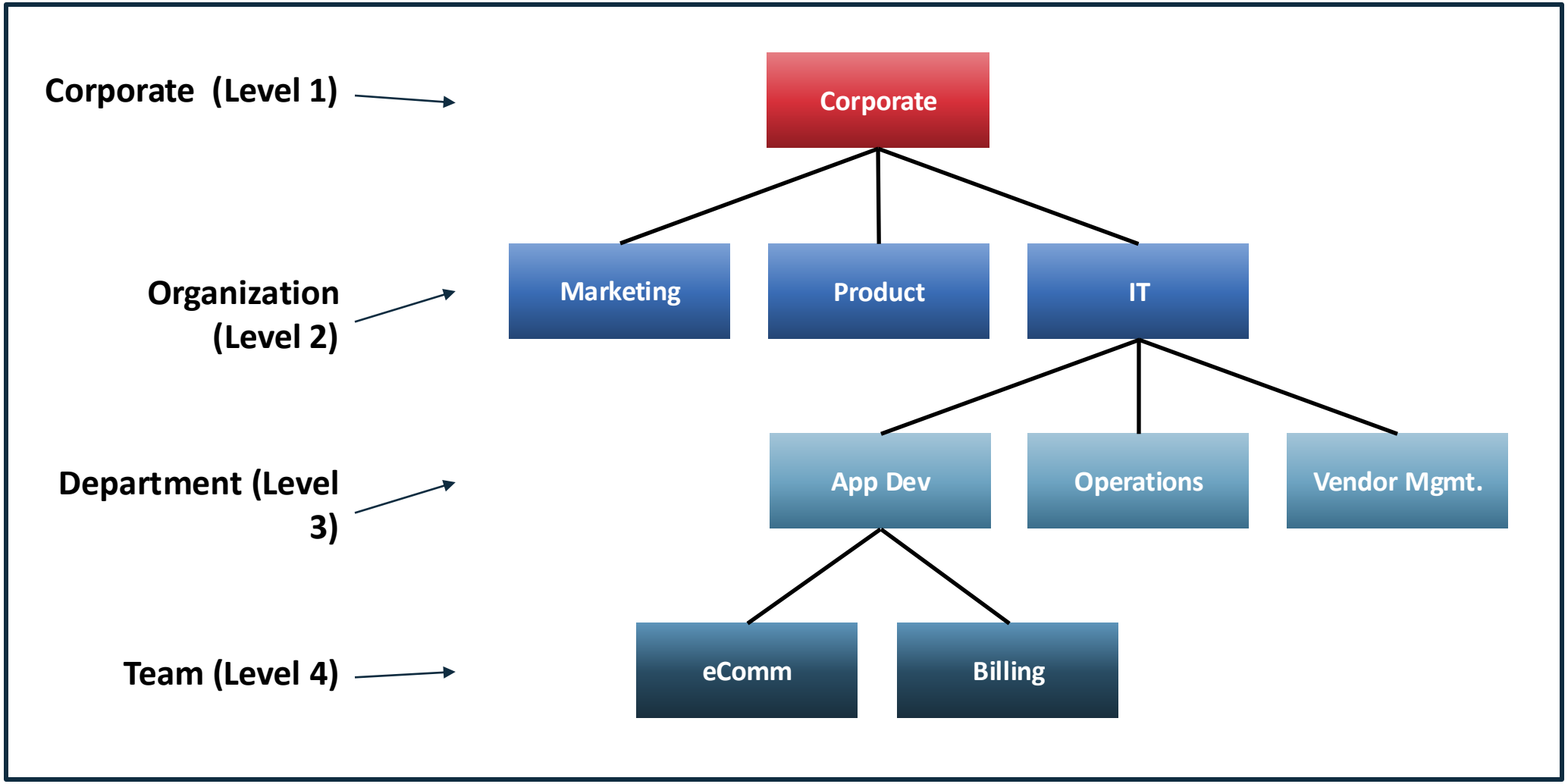
Organizational Breakdown Structure (OBS)

- An OBS is a company-defined hierarchical structure
- Can be used for filtering, reporting, and security (OBS rights)
- You can create any number of OBSs with up to 10 levels
- Security can be enabled for any OBS
  - Department OBS and Location OBS only on initial creation (until tied to Entity)
- Remember that every OBS created will need to be maintained which can be a time-consuming task depending on complexity
- OBS is a default filter parameter on most out-of-the-box reports

OBS Types

- Identifying what your business needs are is the first step in determining what types of OBS structures to build
  - In what ways do we need to group data for portlets and reports?
  - Are there other fields that can be used to accomplish this? (e.g., Sponsoring BU)
  - Is there a need for multi-level filtering or roll-up reporting?
- Some OBS Examples:
  - Organizational (like HR org chart)
  - Financial Departments / Cost Centers
  - Functional Organizations and Teams
  - Product or Product Teams

OBS Example: Functional / Team OBS



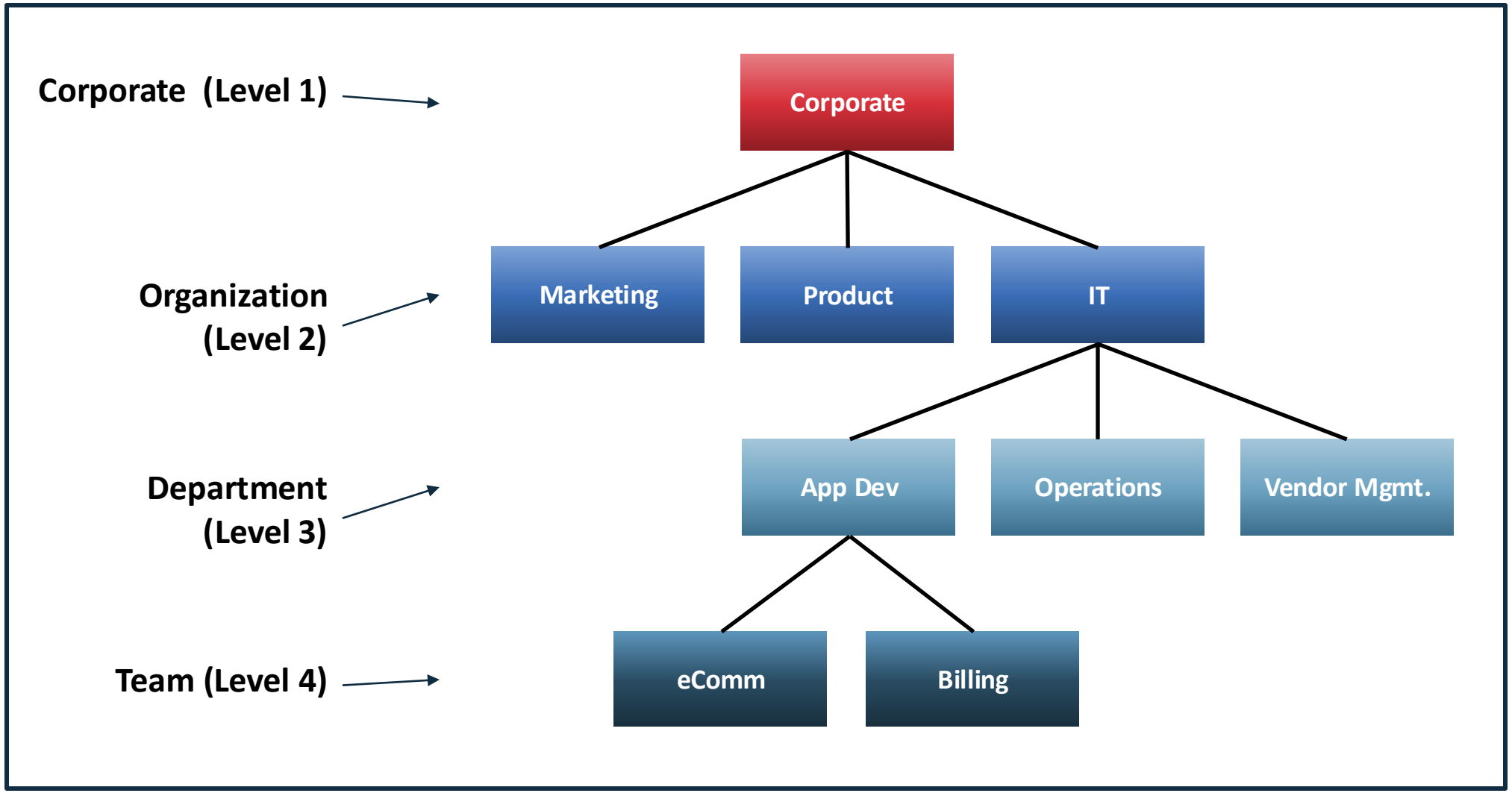
OBS Maintenance

- Maintaining an OBS and associated records can be time-consuming
- Keep the number and complexity of OBSs to a minimum
- Changing the structure and/or labels in an OBS can affect reporting
- Deleting an OBS unit will also delete all child units under that level
- Any record tied to a deleted OBS unit will be “orphaned” (null value in OBS field)
- Units can be moved from one parent to another within a specific OBS and all child units will follow
- OBS associations can be done using a list/grid view, but the fastest method could be from the Admin menu (OBS Unit tab “Attached Instances”)
- Look for automation opportunities (e.g., do associations via GEL script)

OBS Demo: Let's Build this OBS!

Steps:

1. Create the OBS
2. Enable Security
3. Define the Levels
4. Add Units
5. Attach Instances



Security Best Practices

Security Best Practices

- Assign people their rights only once
  - Granting the same rights at different levels or through multiple groups can slow down performance in some pages/views
- Only use Instance rights as a last resort and try to keep at a Group level
- Minimize security maintenance
  - It’s better to create more Groups with a relatively small number of rights than to create a few Groups with rights to many different objects.
  - This approach makes it easier to add and remove rights when people change roles, you can simply add them or remove them from the appropriate groups
- Understand what each right means
  - Know the definition of each right
  - Understand the licensing implications of different rights

Security Best Practices

- Think about security “roles” or user “personas”
  - Not the same as Primary Role
  - Theoretical, not in the system (examples: Timesheet user, Project approver)
- Document your security model design before building it
  - Use OOTB groups as a reference but most likely you will create your own groups
- Set up the model in Clarity
  - Create dummy data
  - Create generic test users – one per functional “role”
- Use the MUX’s “Impersonate” feature to verify the model is working as designed
  - Can you see and do what you expect for each role?
  - Can you see or do anything that shouldn’t be allowed?

Security and Group Design

There tends to be two general design philosophies, one organized around personas and one around capabilities.

#1 Persona

- One "function" group established for each persona (e.g., Project Manager, Portfolio Manager). This group establishes access to capabilities.
- Multiple "data" groups are established for each persona that grants access to data records, usually driven by OBS.
- Blueprints, Blueprint Rules, and FLS are used to support department, team, or organizational variations.
- Ideally, a given user is associated with only one persona group for simplified provisioning.
- This model often requires that security rights are included in multiple groups. For example, a project view right may need to be included in the PM, PfM, RM, and Executive persona groups. Maintenance is the tradeoff here.
- A variation in which personas are stacked (i.e., a PfM must be a member of the Team Member and PM groups) can help rationalize rights, but results in overly complicated provisioning.

Security and Group Design

There tends to be two general design philosophies, one organized around personas and one around capabilities.

#2 Capability

- Security groups are aligned to high-level capabilities (e.g., Idea Management, Schedule Management).
- Users are provisioned based on what they need to do in the system, with each user potentially have a different set of groups.
- This model reduces maintenance overhead, but provisioning can be complicated.
- The model can also leverage the "data" group concept, though they tend to be more broadly defined than when established for individual personas.

Security and Group Design

Establish and communicate "Guiding Principles" during initial design sessions:

- Lean towards an open model, locking down data only when required.
- Don't assume malicious intent. Security is enabled to support the user experience and meet visibility, compliance, or regulatory requirements.
- Configure auditing as an enabler to an open security model, mitigating the risk of accidental updates.
- Favor Global rights over OBS and favor OBS over Instance.
- Continuously look for opportunities to automate provisioning (e.g., expand inherent rights).
- Limit the number of security groups per resource. Minimize overlapping rights; try to have resources receive their rights from one source only.

Security Groups

Groups

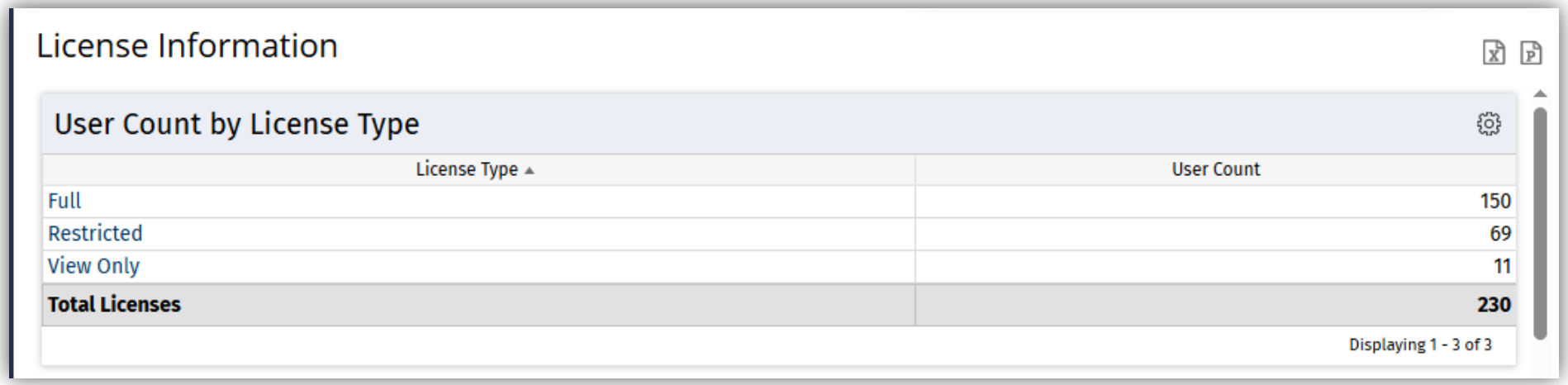
- A set of users who perform similar functions or roles in the tool
- Contains a collection or combination of rights applicable to each member of that group
- Can associate a single resource with any number of groups
- Can contain a collection of Instance, OBS, and Global level rights
- Quickest way to assign multiple rights to several people at once
- Much easier to manage than assigning rights to specific individuals

Other Uses for Groups

- Can be used to determine what users see in the application
  - Menu options
  - Pages, Portlets and Tabs
- Groups can also be created for things other than granting rights
  - e.g., notifications from a workflow

Security and Licenses

- The rights assigned to an individual or group determine the type of license consumed and counted by Clarity
- Use the License Information portlet (Administration->License Information) to monitor usage and maintain compliance
- Audit this usage periodically



Questions?

Survey

Please take a few moments to fill out the class survey.
Your feedback is extremely important for future events.

Earn Rego University Certifications and Professional Specializations

Your participation in this class may count toward Rego University certification progress.

Certifications

Build recognized Clarity expertise.

Complete 10 eligible learning units within a certification track.

Best Practice Clarity Administrator

Best Practice Clarity Lead

Professional Specializations

Deepen your skills in focused topic areas.

Complete 4 eligible learning units within a selected specialization, with the option to earn multiple specializations.

Artificial Intelligence (AI)

Reporting & Analytics

Technical

Important: ***Complete the class survey in the app after each session so your credits can be tracked.***

More info: https://regouniversity.com/certificates

Earn PMI credit

Eligible Rego University sessions qualify for Professional Development Units (PDUs)

- Access your account at pmi.org
- Click on **Certifications**
- Click on **Maintain My Certification**
- Click on **Visit CCR's** button under the **Report PDU's**
- Click on **Report PDU's**
- Click on **Course or Training**
- Class Provider = **Rego Consulting**
- Class Name = **Rego University**
- Course **Description**
- Date Started = **Today's Date**
- Date Completed = **Today's Date**
- Hours Completed = **1 PDU per hour of class time**
- Training classes = **Technical**
- Click on **I agree** and **Submit**

Let us know how we can improve!
Don't forget to fill out the class survey.

Phone
888.813.0444

Email
info@regoconsulting.com

Website
https://regouniversity.com/pmi-credits/