



# INDIANA UNIVERSITY

## **ENTERPRISE BUSINESS INTELLIGENCE CONSOLIDATED BUSINESS INTELLIGENCE AND BUSINESS INTELLIGENCE MANAGEMENT PORTAL**

## **USER'S GUIDE**

## Table of Contents

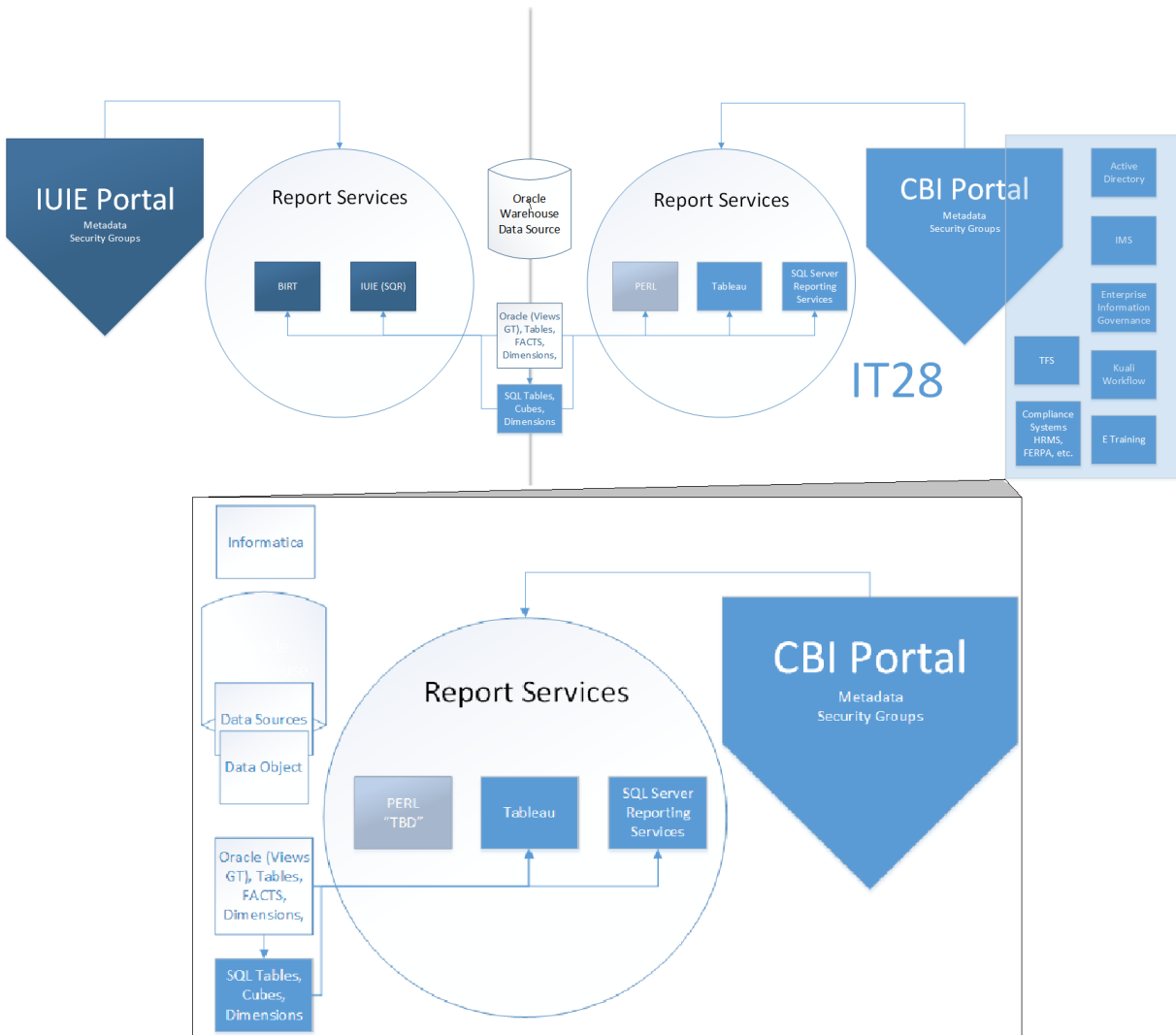
1	Enterprise Business Intelligence .....	4
2	Consolidate Business Intelligence Reports Catalog (Consumer) .....	6
2.1	Access to the CBI .....	6
2.2	CBI Catalog Functionality .....	7
2.3	CBI Interface .....	8
2.3.1	Catalog Panel .....	8
2.3.2	Request Access to Report or Data .....	9
3	Business Intelligence Management Portal (Publisher) .....	11
3.1	Access to the BIM .....	11
3.1.2	Test Environment .....	13
3.1.3	Tester Access to Test Reports .....	13
3.2	BIM Catalog Functionality .....	14
3.3	BIM Interface .....	14
3.3.1	Catalog Folders and Reports Details .....	15
3.4	Manage Options Interface .....	18
3.4.1	User and Group Search .....	18
3.4.1	Manage Access .....	19
3.4.2	Publishing Reports .....	22
4	Business Intelligence Work Flow (Data Manager) .....	29
4.1	Workflow Routing Business Rules .....	29
4.1.1	Publishing a Report and Approval Workflow .....	30
4.1.2	Request Access to a Report or data Object and Approval Workflow .....	31
4.2	Data Manager Role and Kuali Workflow .....	31
4.2.1	Receiving a Request .....	32
4.2.2	E-mail Business Rules and Functionality .....	32
4.3	Data Manager CBI Approval .....	33
4.3.1	Reports Approval .....	33
4.3.2	Security Groups Approval .....	34
5	Security Access .....	35
5.1	Data Classifications, Roles, and Compliance .....	35
5.1.1	Data Classifications .....	35
5.1.2	CBI Roles .....	35

5.1.3	Data Compliance .....	37
5.1.4	Former and Position Change of University Status .....	38
5.2	Authentication and Authorization .....	38
5.3	Security Access Developers/Publishers .....	39
5.3.1	BI Center Access .....	39
5.3.2	Reports Catalog Access for Publishing – BIM.....	39
5.3.3	Data Access .....	40
5.4	Active Directory.....	40
5.5	Rights Management Services .....	41
5.6	Enterprise Business Intelligence Naming Standards (EBI) .....	42
5.6.1	CBI\BIM NAMING PROCEDURE .....	42
5.6.2	BI CENTER NAMING.....	43
5.6.3	CUBE NAMING .....	44
6	Release Tracking, IT Training, CBI Tutorial .....	46
6.1	Release Tracking.....	46
6.2	IT Training and Documentation .....	46
6.3	CBI Tutorial and Quiz.....	46
7	Report Environments .....	47
7.1	Report Services Proxy/Service Accounts.....	47

# 1 Enterprise Business Intelligence

Indiana University's Enterprise Business Intelligence (EBI) consists of many services. Such services include the dimensional SQL Server Analysis services (Cubes), SQL Server Reporting Services, and Tableau Server Services. The Indiana University Consolidated Business Intelligence (CBI) portal is one component of a much larger set of Enterprise Business Intelligence services which provides the one stop location to access the various reports and the publishing services.

The Indiana University Consolidated Business Intelligence portal is a web application developed by the Indiana University using foundational Microsoft technologies. The framework of the CBI will continue to evolve and adapt to university business rules and requirements. The application is a centrally maintained, enterprise-wide, web-based business intelligence report portal environment. It provides a central repository of all enterprise reports, metadata, tools for provisioning of access to institutional reports, and workflow routing and compliance for all Enterprise Business Intelligence reports and data access.



The Indiana University CBI provides access to the new modern report services which includes dimensional data from SQL Server Analysis services (Cubes), SQL Server Reporting Services, and Tableau Server Services. The CBI does not replace Indiana University Information Environment (IUIE), it does however provide access to the modern analytics reports services and provides enterprise management functionality for data access. The CBI provides minimal steps to complete tasks and allows quick access to features and complete actions with substantially less clicking.

As a part of the Enterprise Business Intelligence ([EBI](#)) environment, the CBI features functionality to deliver reports, self-service functionality for management of security groups and roles, access requests to data, advanced data stewardship of the reporting and data access environment using Quali workflow, and surfacing metadata. Report Publishers (Developers) can manage security and publish reports, and Data Managers can approve security and report requests which are routed to your action list in OneStart.

The CBI environment consists of two web application portals:

- **The (CBI) Consumer portal:** The CBI Consumer portal provides an interface for anyone on the internet to view institutional Public reports. Consumers have access to the reports and data catalog and have the ability to favorite reports and share reports with other university colleagues. Consumers whom CAS into to the CBI can perform :
  - Add reports to their Favorites folders.
  - Share reports with colleagues; access to the reports content may still require Data Manager Approval.
  - Search the reports and data catalog using advanced options including the ability to search.
- **The BIM Administration portal:** The Business Intelligence Management (BIM) Administration portal is accessible to report Publishers and Data Managers facilitating the publishing and management of reports, data, and associated metadata. The BIM provides Data Managers the ability to steward security access to reports and data in the Enterprise Business Intelligence environment such as Cubes.

*For documentation and training for the report tools and services see section 6.2 in the User's Guide.*

## 2 Consolidate Business Intelligence Reports Catalog (Consumer)

### Video Tutorial

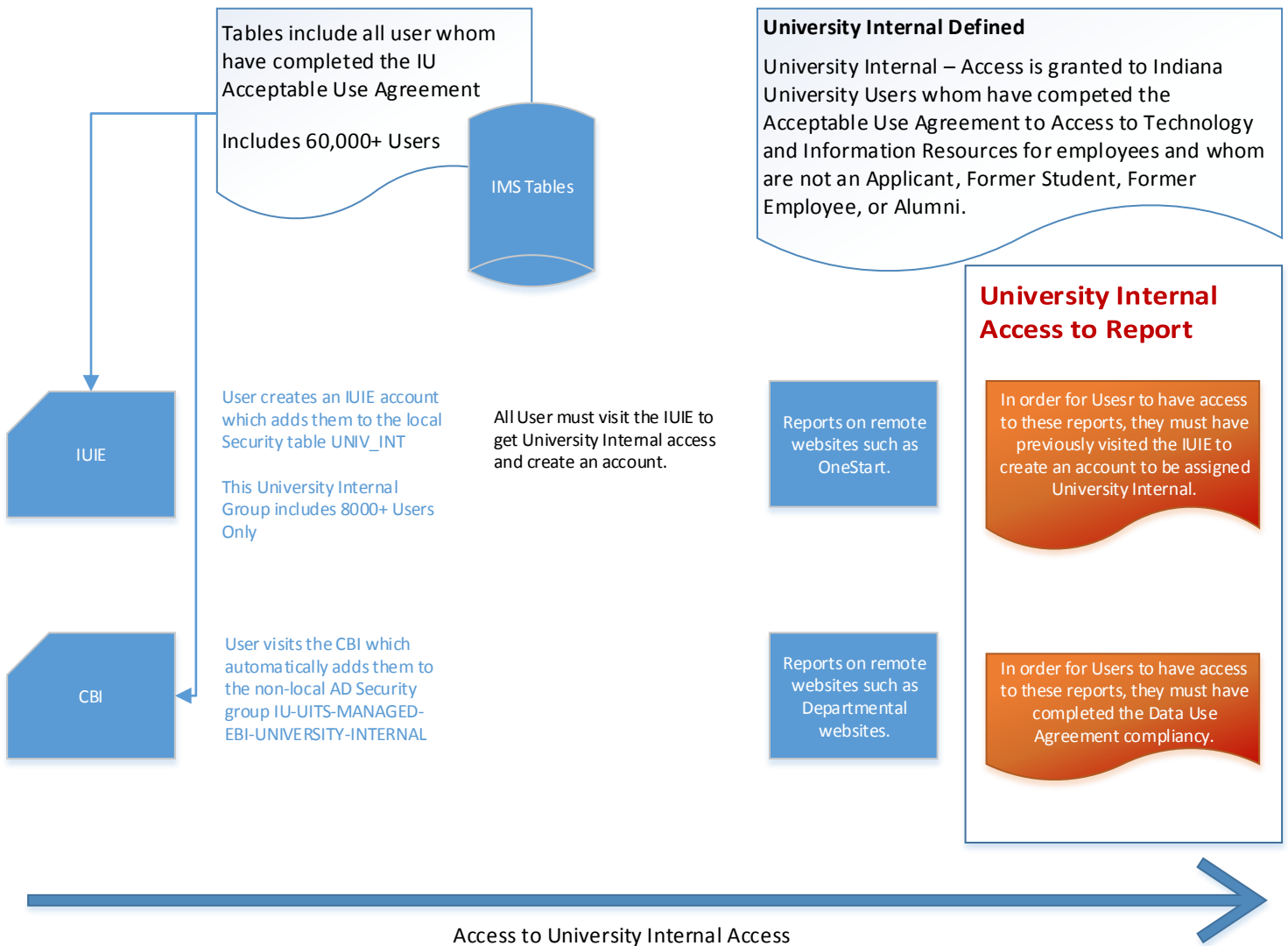
The Consolidated Business Intelligence Portal (CBI) is a web application used to access analytical reports and access to data. The CBI consumer portal provides a common catalog to navigate reports and data, add favorites, share reports with colleagues, organize favorite reports, and view most popular reports. The catalog provides personalization's features that allow grouping of reports and data by campus, department, data classification and other useful groupings. CBI Consumers can search the Reports and Data Catalog using standard and advanced options including the ability to search from within catalogs or only in favorites.

### 2.1 Access to the CBI

Access to the by CBI is gained by navigating to <https://bi.iu.edu> and then by selecting the CBI button to Login. For those whom do not have a domain account use the **"Click here for Public Access"** to access Public reports. You can also gain access by navigating to <https://one.iu.edu> and typing "CBI" into search which will display the CBI and the Decision Support Results.

In order to access any reports when signed into the CBI, policy requires that all Users have agreed to the IU [Acceptable Use Agreement for access to institutional data and applications](#). Similar to the way the IUIE functions (with the exception of account creation) when a user visits the CBI a check is performed which verifies whether the user has completed and verified the Data Use Agreement and is a valid user sourced from IMS (Active Directory Users). If the User has not completed the Data Use Agreement they are redirected to the Data Use Agreement form and must electronically read/sign before access is granted to the CBI.

- Compliancy requires that the User is not an Applicant, Former Student, Former Employee, or Alumni which is sourced from the Identity Manage Services at Indiana University. The below flow depicts this process further.



## 2.2 CBI Catalog Functionality

The CBI reports catalog portal is accessible to all university faculty and staff. It allows users to:

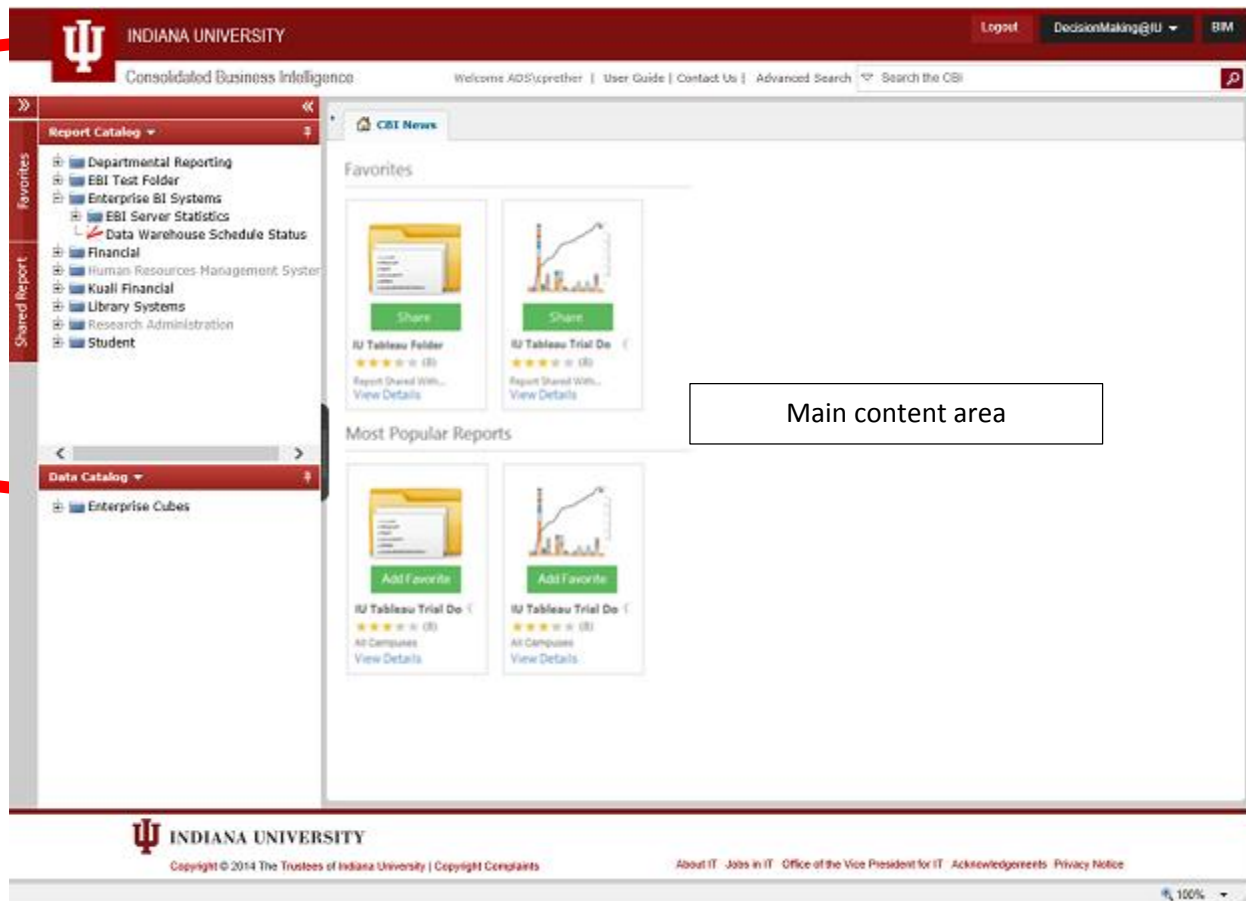
- Navigate University reports
- View reports metadata
- Share reports
- Create favorite reports
- Search for reports using advanced search functionality
- Group reports catalog by security group, business group, campus, etc.

## 2.3 CBI Interface

The portal interface is divided into two main parts, the Catalog and Metadata panels on the left, and the main content area which provides your favorites and popular reports in addition to personal feature functionality.

### 2.3.1 Catalog Panel

The Catalog Panel contains a list of folders and reports to which the user has access. Subfolders can be displayed by clicking the plus sign to the left of a folder name.

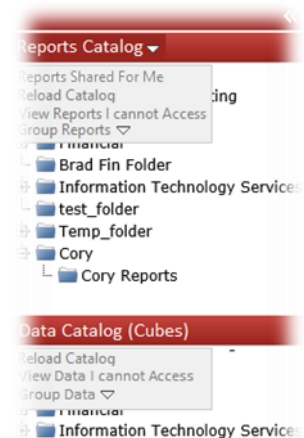


#### 2.3.1.1 Right-Clicking a Folder: The Contextual Menu

Right-click on a folder to activate the contextual menu.



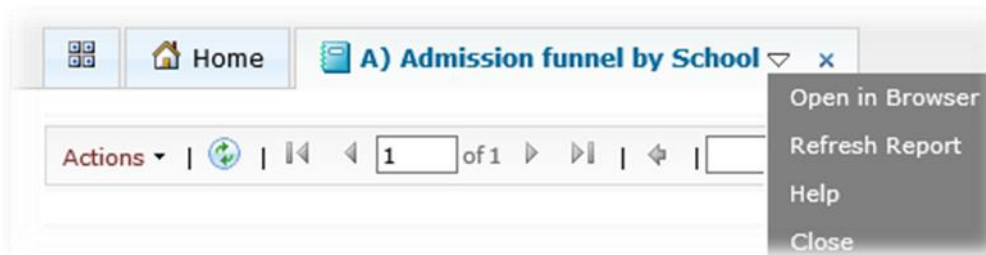
- Right clicking a folder or report in the catalog panel provides option to Add to favorites, Share, Open, Open in Browser, Help, and View Details....
- Right clicking a folder or report in the Shared Report panel provides options to Add to Favorites, Open, Delete, and View Details...
- Right clicking a folder or report in Favorites panel provides options to Open, Open in Browser, Share, Move Report to..., Delete, and View Details...



### 2.3.1.2 Viewing a Report

When a report is selected by clicking it in the Catalog panel, the report will open in the main area of the screen.

At the top of each report are dropdown options to select Open in Browser, Help, and Close. Selecting Help will redirect you a help page or e-mail of the reporting group that created the report.



### 2.3.1.3 Schedule, Push, Snapshots, etc...

Report functions beyond those listed in the CBI are specific to each report type, two of several types which are listed below. For example, the reporting type service provides the below functionality, not the CBI.

Scheduling or Push Reports

Reporting Services - [http://technet.microsoft.com/en-us/library/bb283320\(v=sql.105\).aspx](http://technet.microsoft.com/en-us/library/bb283320(v=sql.105).aspx)

Tableau - <http://community.tableausoftware.com/thread/107973>

Create E-mail Using Query Results

<http://technet.microsoft.com/en-us/library/ms160334.aspx>

## 2.3.2 Request Access to Report or Data

The CBI provides functionality to request access to reports and data objects such as cubes. In the catalog, reports which a User does not have access is indicated by a light gray color and a no access icon. Click the report you wish to open and a dialog box will open to request access, provide your business need and justification for access.. This request is sent to the Data Mangers for approval.

To view reports and cubes which you do not have access you must **login** (upper right area of the page) if your name does not appear you are not logged in.

Requests are routed accordingly by the Subject and Campus assigned to the resource, this was designated when the report was added to the cataloging. This justification will be reviewed by the assigned Data Manager and Approved or Disapproved.

# 3 Business Intelligence Management Portal (Publisher)

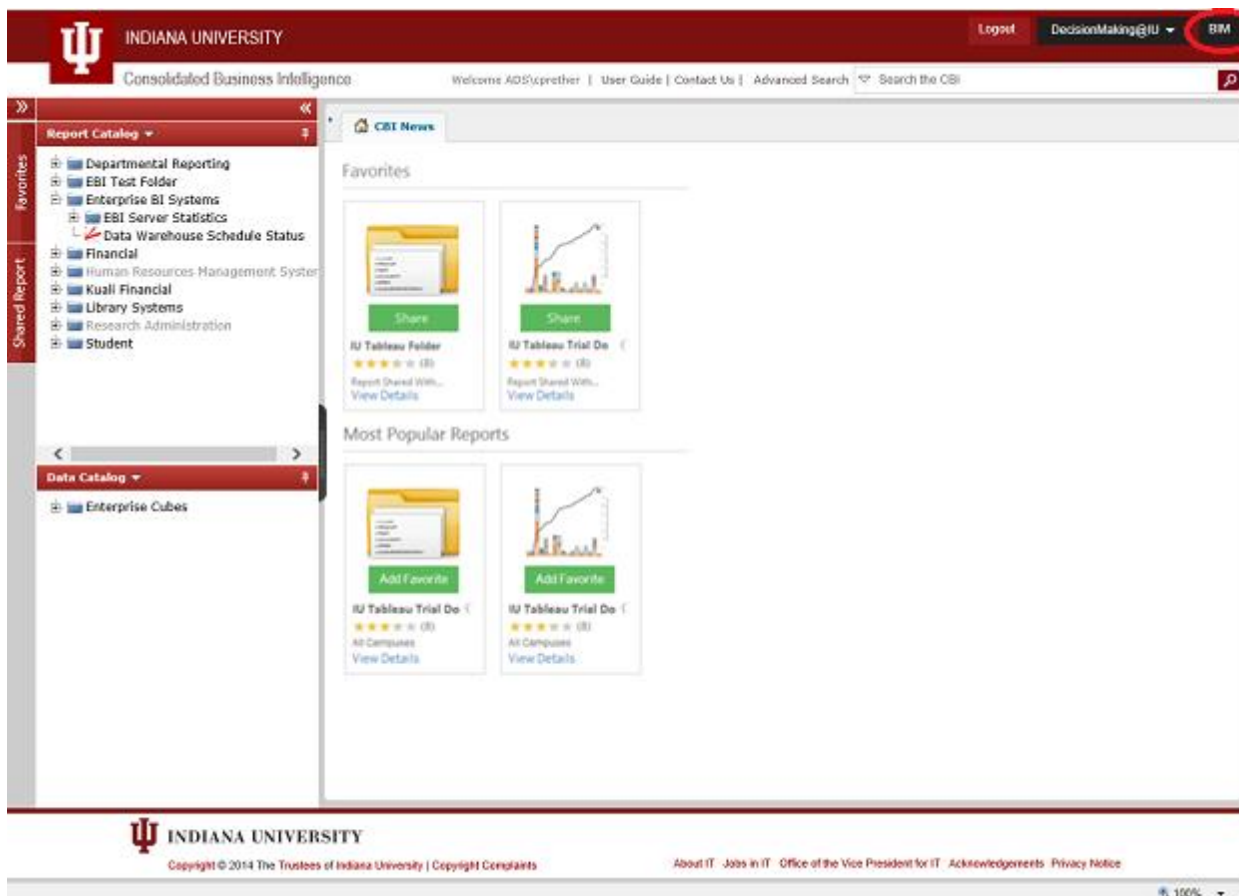
## Video Tutorial

The Business Intelligence Management (BIM) Portal is a centrally maintained, enterprise-wide, web-based business intelligence and reporting management environment. It provides functionality for Publishers and Data Managers to manage access for reports publishing tools and security stewardship to manage access resources such as cubes and reports.

### 3.1 Access to the BIM

To access and use the Business Intelligence Management “BIM” tools, first complete the eTraining CBI Tutorial Quiz as mandated by the University Committee of Data Stewards, see section 6.3 for more details and to complete this process. Once completing and passing the quiz access will be granted to the access the BIM.

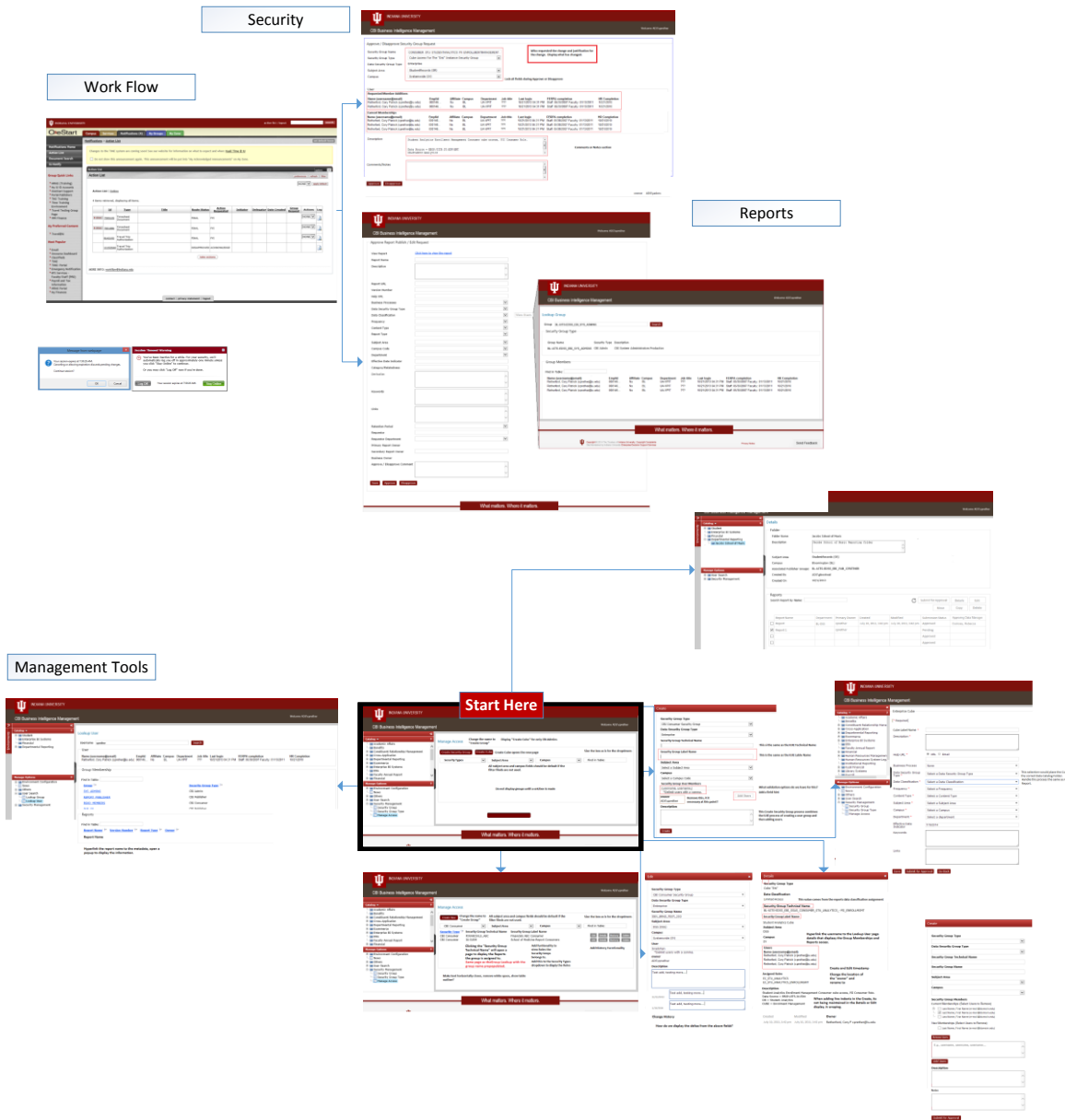
Access the BIM administration portal via the consumer portal by clicking the **BIM** link in top right-hand corner of the screen. The admin button is only available if you are authenticated through CAS and have the Publisher Role (BI Center Access).



The BIM (Business Intelligence Management) portal is accessible to only University Data Managers and Publishers whom have access to a BI Center (Tableau or Microsoft). It provides functionality to:

- Add and publish reports with metadata
- Add metadata to reports and security groups
- Search users/groups/reports access
- Create Consumer and Test Security Groups
- Approve user access to groups
- Data manager approval to access reports
- Manage BI Center memberships access

### 3.1.1.1 Business Intelligence Site Map



### 3.1.2 Test Environment

The CBI <https://cbi.bi.iu.edu> or the Decision Support <https://ds.iu.edu/> does not provide a test catalog, however testers can access reports in their respective reports environments directly.

#### 3.1.2.1 Tester Access to Test Reports

Publishers that develop preproduction reports in SQL Server Reporting Services and Tableau and require Users have test access should follow the following steps.

To create a Security test group, refer to **section 3.3.4 Publishing and Assigning User Access** to create a Test Security Group for the test report located on the [tst.tableau.bi.iu.edu](http://tst.tableau.bi.iu.edu) and [tst.rs.bi.iu.edu](http://tst.rs.bi.iu.edu) Tableau and SSRS servers. After creating the security group send a request to the Help Desk at <http://mailform.kb.iu.edu/email.php?cid=1221> requesting the new security group be assigned to the report object.

Once a Test Security Group has been assigned to the report, the individual whom created the group and their delegate will have the ability to manage the security groups memberships.

## 3.2 BIM Catalog Functionality

The Business Intelligence Management Portal (BIM) is accessible to Publishers and Data Managers.

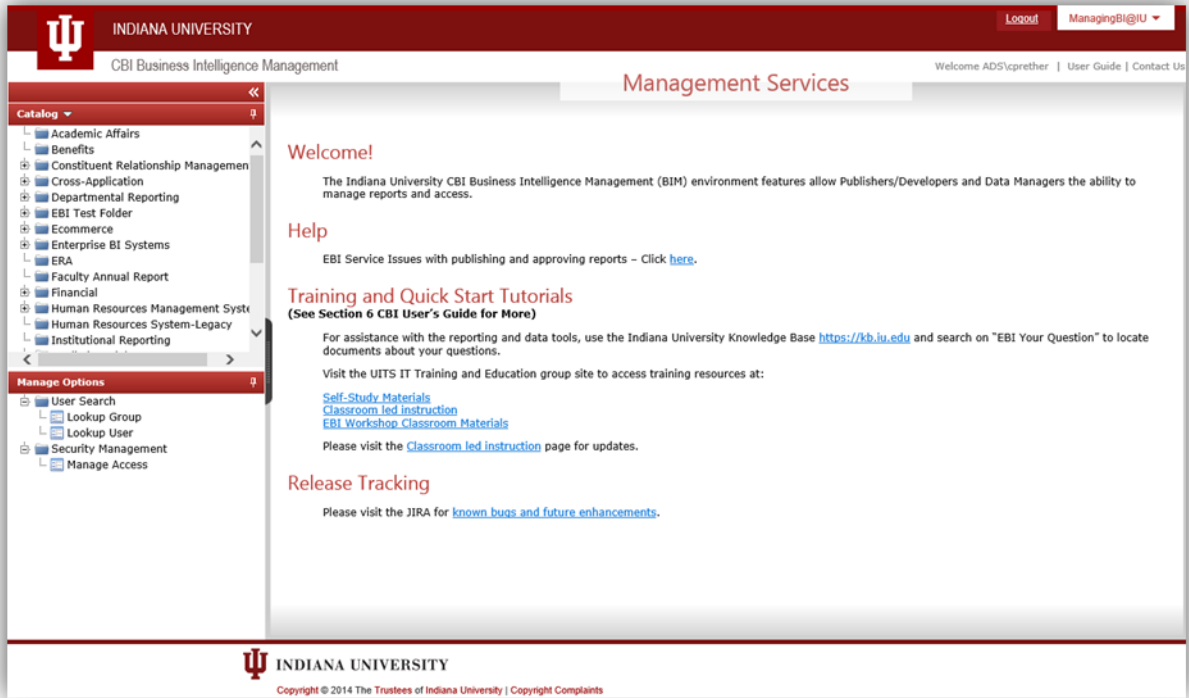
It allows Users to:

- Save and Publish reports with metadata
- Data manager approval to access reports
- Search for Users, Security Groups, Data Objects, and Reports
- Create and manage Consumer Security groups
- Create and manage Testers Security Groups
- Stewardship of User access to group Security Types
- Manage BI Center Memberships
- Refine Filter Searches on Security Types, Campus, Subject Area, and Data Security Group Types.

## 3.3 BIM Interface

The BIM interface is divided into two main parts, the Catalog and Manage Options side panels and the main area of the screen located to the right of the panels.

Catalog and Manage Options Panels



Clicking on the **ManagingBI@IU** option at the top right will drop down valuable resources such as Publishing reports steps and Publishing Security Groups.



The Catalog Panel contains the catalog of folders which reports can be added.

Right-click on a folder to activate the contextual menu to access various functionality. Left-clicking a folder displays folder details in the main area of the screen.

When an option is chosen from the contextual menu, options will appear to complete a task or operation.

### 3.3.1 Catalog Folders and Reports Details

Folders in the BIM provide functionality to edit, delete, or move folders and add reports to a folder in the BIM catalog.

Each folder contains details such as name, description, the date the folder was created, the date the folder was modified, and who modified it for example.

Selecting a folder will display a page which provides Details for the folder and reports details. If there are reports in the folder they will be listed at the bottom of the Details page under the Reports section as shown in the below graphic.

The Reports section shows the report name, owners, published state, and provides other advanced features such as copy as depicted below.

The screenshot displays the 'Management Services' page for the 'UIRR Admissions' folder. The interface includes a navigation catalog on the left, a header with the university logo and name, and a main content area. The folder details section shows the folder name, description, and creation information. Below this is a table of reports associated with the folder, each with its own set of action buttons.

**Folder Details:**

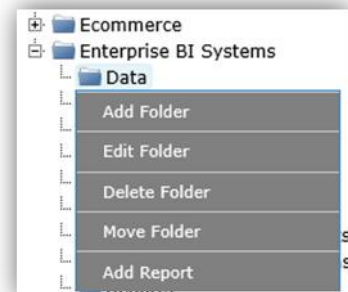
- Folder Name: UIRR Admissions
- Description: UIRR Admissions CBI Reporting Folder
- Created By: ADS\cstine
- Created On: 3/18/2014

**Reports Table:**

Report Name	Primary Owner	Secondary Owner	Action
UIRR Admissions Undergraduate Weekly Snapshot	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete
UIRR ADMS Point in Cycle Multi-Campus Summary	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete
UIRR ADMS Point in Cycle Duplicated Summary	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete
UIRR ADMS Point in Cycle Campus Details	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete
UIRR ADMS Point in Cycle Comparison Graph	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete
UIRR ADMS Point in Cycle Trend	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete
UIRR ADMS Point in Cycle Breakdown	cstine	tsanders	Edit, Details, Copy, Unpublish, Delete

### 3.3.1.1 Folder Functionality

To Add, Edit, Delete a folder in the catalog you must be in the BIM. Do this by Right clicking an existing folders and selecting the appropriate option. Only Add Folder and Add Report are options at the highest folder level. Note - A folder will not appear in the CBI (Consumer) catalog until a report is published and approved in the folder.





### 3.3.1.2 Reports Functionality

The BIM provides reports Publishing functionality and Actions to Submit for Approval, Edit the report, view Details, Copy report metadata, and Delete the report.

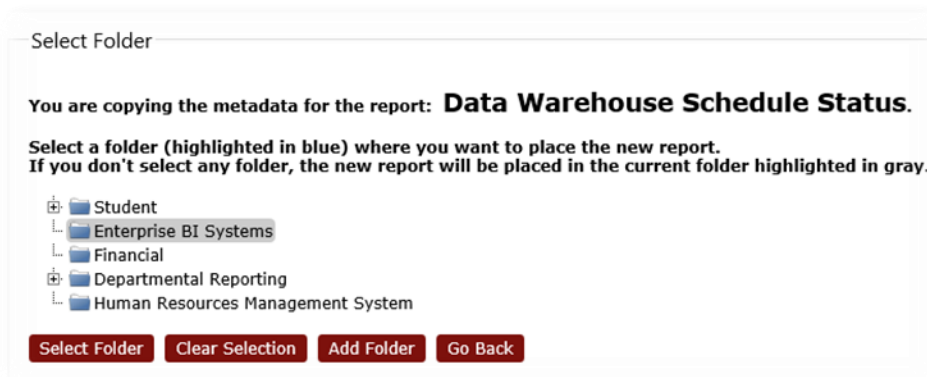
**Submit for Approval** – Selecting Submit for Approval initiates a Quali workflow which routes an Approve or Disapprove request to the Data Manager for the Enterprise report for that Area of Responsibility (AOR).

**Details** – Selecting Details will display a page which includes all report metadata.

**Edit** – Selecting Edit provides functionality to change existing metadata.

**Move** – Selecting Move provides functionality to move reports.

**Copy Reports “Metadata”** - Selecting the Copy function for an existing report allows options to copy the metadata to exiting folders or to create a new folder (See Section 3.4.2 for Adding a Report). Copy functionality provides the ability to select a report and Copy existing report metadata to be used to publish a new report. This process is commonly used when publishing several reports with similar report metadata.



Select Folder

You are copying the metadata for the report: **Data Warehouse Schedule Status.**

Select a folder (highlighted in blue) where you want to place the new report.  
If you don't select any folder, the new report will be placed in the current folder highlighted in gray.

- Student
  - Enterprise BI Systems
  - Financial
  - Departmental Reporting
  - Human Resources Management System

Select Folder Clear Selection Add Folder Go Back

Select a choice and folder and the Add Report screen will open for you to complete the report publishing. Many fields will be prepopulated with the report metadata you copied from.

- **Metadata not copied**
  - Report Name
  - Report URL
  - Version Number
  - Effective Date Indicator - This is auto-set along with Created On and Created By.
  - Requestor
  - Primary Report Owner – automatically set to the user doing copying
  - Secondary Report Owner
- **Metadata copied:**
  - Description
  - Help URL
  - Business Process
  - Data Security Group Type

- Data Classification
- Security Groups
- Frequency
- Content Type
- Report Type
- Subject Area
- Campus
- Department
- Category/Relatedness
- Derivation
- Keywords
- Links
- Retention Period
- Business Owner

**Delete** – Selecting the Delete button will delete the reports metadata permanently. Note \* There currently no undo action.

### 3.4 Manage Options Interface

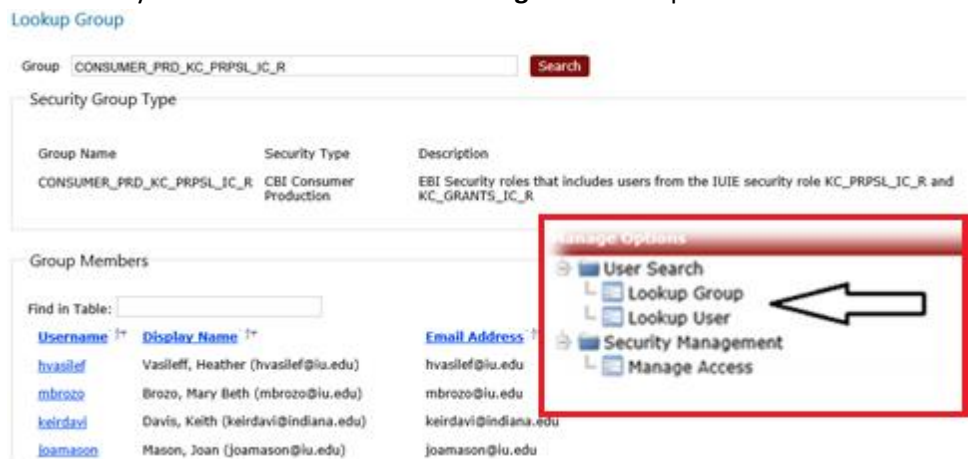
The BIM Manage Option Panel provides options to manage Security and User and Security Group Lookup options.



#### 3.4.1 User and Group Search

The BIM provides various self-service functionality for **Publishers** and **Data Managers** to lookup User Access details and Security Group details. The information provided by the lookup functionality includes user memberships to security groups, reports access, and cube access (See image).

You can access this functionality by navigating to the BIM and choosing **Manage Options > User Search**.



Selecting Lookup User will provide lookup functionality to search on domain network username. Add the username and select search. This will display the Users information including group memberships and reports the User has access to. From top to the bottom of the page will display the User information, Groups Memberships, and Reports. Each of the three sections provides details about the User and their access.

Lookup User

Username

---

User

Username	Name	Email Address
cprether	Retherford, Cory Patrick	cprether@iu.edu

---

Group Membership

Find in Table:

<a href="#">Group Technical Name</a>	<a href="#">Group Name</a>	<a href="#">Security Group Type</a>
<a href="#">PUB_SR_IR_IMIR</a>	-	CBI Publisher
<a href="#">PUB_SR_APPLICATION</a>	-	CBI Publisher
<a href="#">PUB_DEV_R</a>	-	CBI Publisher
<a href="#">CONSUMER_PRD_AAD_ADMIN</a>	Academic Advising Admin	CBI Consumer Production
<a href="#">CONSUMER_PRD_EDSS_TEAM</a>	EDSS Team	CBI Consumer Production
<a href="#">PUB_PUB_R</a>	-	CBI Publisher
<a href="#">CONSUMER_PRD_UITS_SURVEY</a>	UITS Survey	CBI Consumer Production
<a href="#">CONSUMER_PRD_BRADS_GROUP712</a>	brads group	CBI Consumer Production
<a href="#">CONSUMER_PRD_TEST_GROUP</a>	ebi test group	CBI Consumer Production
<a href="#">CBI_TSTR_PRD_TEST_TAM_MNMNMMN_GROUP</a>	Test TAM MNMNMNMN Group	CBI Consumer Tester
<a href="#">CBI_TSTR_PRD_TAM_TEST_AGAGAG_GROUP</a>	Test AGAGAG Group	CBI Consumer Tester

### 3.4.1 Manage Access

The BIM provides various functionality for **Publishers** and **Data Managers** to create Consumer and Tester User Groups as well as manage and modify security groups.

#### 3.4.1.1 Publishing and Assigning User Access

Assigning Security Groups (User Groups) to reports is similar to existing IU report systems. The BIM security authoring tools provide functionality to create a Security Group which are then available to apply to a report object once published.

Data Managers and Publishers can assign Security Groups in the BIM. It is the responsibility of each units group to employ procedural and operational policy for the creation and assignment of security to reports from within the BIM, this discretion is of the unit. The BIM services facilitates a repeatable process, you however must make the appropriate decisions for your business requirements which are potentially different for each organization.

You can access this functionality by navigating to the BIM and choosing **Manage Options > Manage Access**.

On the Manage Access page the option to **Create Security Group** is available to the Publisher and the Data Manager. Publishers and Data Managers have the ability to **Create, Edit, and View** any Security Group Type, however only the owner and delegate owner have the ability to edit these groups. If the Security Group is an Enterprise group it will generate a workflow approval request to the Data Manager for that Area of Responsibility.

[Manage Access](#)

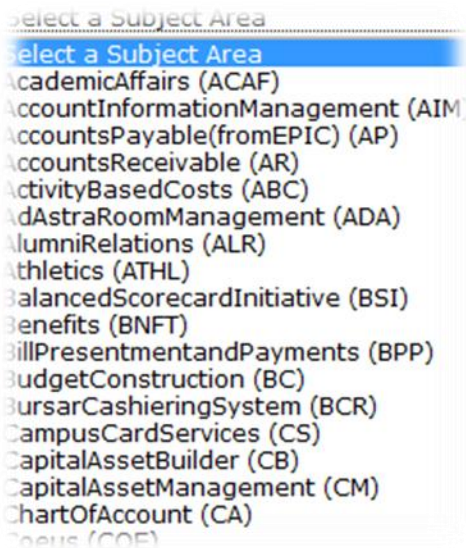
Create Security Group

When **Create New** is selected a popup dialogue will open allowing Publishers and Data Managers the option to select a Security Group Type such as **Consumers**, among others to create Security Groups.

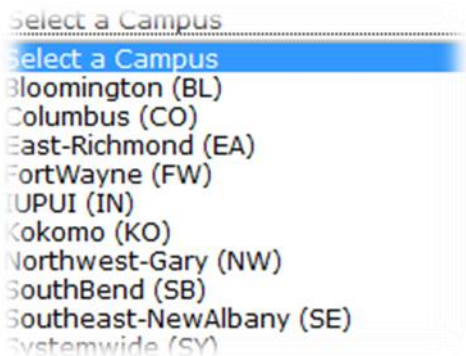
**Create Security Group** - The following field values are available listed below:

- **Security Group Type** = Options such as (BI Center, Consumer, Tester, and Cube) are available based on your role. The most common option will be to create a Consumer group.
- **Data Security Group Type** = This field provides a selection for Enterprise or Departmental.
  - When designating the Security Group as an Enterprise Security Group Type, a workflow action will be generated to the approving Data managers for the Area of Interest (AOR) to approve or deny.
  - When designating the group as a Departmental Security Group Type, any owner modifying the group is auto approved and should be explicitly used for reports not sourcing from DSS1PRD or EBIP\ENT data which in most cases is considered Enterprise.
- **Security Group Technical Name** = Any technical name can be given to the group, however all technical names are additionally prefixed with BL-UIITS-EDSS\_EBI\_XXXX as detailed below. Space in the text will append an underscore and lowercase characters will be capitalized automatically.
  - BI Center = BL-UIITS-EBI\_BICENTER\_PUB\_PRD\_CAMPUS\_DEPT
  - Consumers = BL-UIITS-EDSS\_EBI\_CON\_PRD\_NAME
  - Testers = BL-UIITS-EDSS\_EBI\_TSTR\_PRD\_NAME
  - Cube
    - Orgunit = BL-UIITS-EDSS\_EBI\_DB\_OWNER\_CAMPUS\_DEPT
    - Ent = BL-UIITS-EDSS\_EBI\_DB\_READ\_SUBJECT\_DATA

- **Security Group Name** = Any friendly name can be given to the group, however consider obvious and friendly names. For example, a consumer group used for reports which provide IR reporting access to Admissions reports could use the name “IR Admission Reports” as the friendly name.
- **Subject Area** = Specify subject area, only used for Enterprise Data Security Group Type. These values are populated from the University Enterprise Information Governance (EIG) system.



- **Campus** = Specify a campus, only used for Enterprise Data Security Group Type. These values are populated from the University Enterprise Information Governance (EIG) system.



- **Security group Members**
  - **Add Users** = This field provides functionality to add valid domain usernames (networkID).
- **Description** = Provide an obvious description of how the security group is utilized and the types of report(s) it is securing.
- **Group Owner**
  - User creating the group is by default the Owner.
- **Owner Delegate** (*Multiple Owners*)
  - Add a delegate to be the owner of the Security Group, this can be delegated infinitely.
- **Notes of Justification**
  - Add notes for each Edit which a version is created.

### 3.4.1.2 BI Center Management

A request will need to be made to the EBI Helpdesk (<http://mailform.kb.iu.edu/email.php?cid=1221>) to have a BI Center initially created. After the initial creation, an Owner and Delegate owner for those groups can Edit and manage Users whom have BI Center access. To do so navigate to the Business Intelligence Management (BIM) <https://bim.bi.iu.edu>. Select **Manage Options > Security Management > Manage Access** > Select **BI Center** from the **All Security Types** dropdown menu > Locate your group > click **Edit**. As an owner of the group the ability to add and remove users and make edits for most of the field options. Some fields will be in gray and indicate those options cannot be edited.

### 3.4.1.3 Routing for Approval and Data Manager Lookup

Once an “Enterprise” **Data Security Group Type** has been Submitted for approval, a Kualo workflow is initiated for Data Manager routing, locking the ability to edit the Group until an approve or disapprove action occurs. Once the request has completed the editing lock is removed.

When you Publish you are indicating a decision to implement a request which initiates a Kualo Workflow request, the same process used for many Enterprise systems. Once an Enterprise group has been Submitted for approval, a Kualo workflow eDoc is initiated for Data Manager routing, locking the ability to edit that group until an approve or disapprove action occurs. The Data Manager is the role which will have the ability to review the metadata and security previous to approving or disapproving, there is no FYI. Once the request has completed the editing lock is removed. See section 4.1 for more information about Workflow.

Groups that have been previously Published only provides ability to Submit for Approval/Publish and Go Back. There is no save option after a group has been published, as any edit/change will have to be approved again.

Once a “Departmental” **Data Security Group Type** has been Submitted, the creation is immediate since there is no approval workflow request generated since Departmental data does not have assigned a Data Manager.

**LATER FUNTIONALITY IMPROVEMENT** – At a later time Departmental requests may be routed to an appropriate data steward using workflow.

### 3.4.1.4 Lookup Data Managers Routing for Approval

In order to determine the Data Manger(s) that will receive a request for Enterprise approvals use the OneStart Data Manager Lookup tutorial.

- Job Aid - [https://onestart.iu.edu/dp-prd/resources/Data\\_Stewards\\_eDoc\\_job\\_aid\\_05.22.13.pdf](https://onestart.iu.edu/dp-prd/resources/Data_Stewards_eDoc_job_aid_05.22.13.pdf)
- Data Manager (Lookup) Job Aid Tutorial - [https://onestart.iu.edu/dp-prd/resources/Data\\_Stewards\\_eDoc\\_job\\_aid\\_05.22.13.pdf](https://onestart.iu.edu/dp-prd/resources/Data_Stewards_eDoc_job_aid_05.22.13.pdf)

Contact [ricereq@indiana.edu](mailto:ricereq@indiana.edu) for assistance.

## 3.4.2 Publishing Reports

The BIM provides functionality to initially Save and/or Publish reports from various reporting services such as Tableau and Reporting Services. Adding a report to the catalog is managed from within in the Business Intelligence Manager (BIM) site.

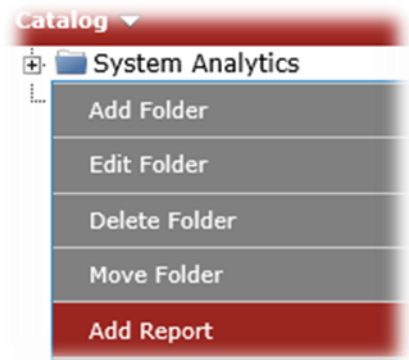
To add and finalize the publishing of an Enterprise report so that consumers can access reports through the CBI catalog, a Publisher or Data Manager will need to right click a folder from within the BIM catalog to add reports. Right clicking provides several options one of which is **Add Report**. When selecting this option a new window will be displayed to add required report metadata for the enterprise catalog.

**Departmental Reports** – Departmental reports are typically reports that are only operationally valuable to those departments' and/or source data from departmental data sources. To add a departmental report into the CBI catalog use the appropriate folder within the Departmental Reporting folder, and use the directions above to add your report. If you're Department does not have its own folder, right-click the "Departmental Reporting" folder and select "Add Folder" fill in the required folder information and click "Create". This folder will now be available under the "Departmental Reporting" folder.

Only report sources that include a URL using HTTPS can be added to the CBI catalog.

To add and publish a report:

1. Right-click a folder in the BIM catalog and select the **Add Report** option.
  - a. If a folder does not exist for you use see section 3.4.1.1.
2. In the report metadata window, enter all required data and select from the available options.



Publishing a report requires a common set of Metadata requirements detailed below. The definitions for each metadata field are displayed in the web browser when adding the report metadata by selecting or hovering over the item.

### 3.4.2.1 Required Metadata for Initial Publishing of Reports

**Metadata Required Fields** [*\* Required for Initial Publish*] – Additional information or questions about intent for use of the following metadata requirements is available at <https://bi.iu.edu/BI-Governance/Pages/Metadata.aspx>.

- Report Name \*
  - Provide a report name to be identified by users. Hint - make the name short and friendly.
- Description \*
  - Provide a description of the reports use such as what information is being provided through the report and other important information for your consumers.
- Report URL \*
  - This is any URL that is in an <https://reporturlpath> format, most of these URL's will be direct links to your Tableau or Microsoft BI reports.
    - For example: Hover over the link to view the URL or by clicking.  
[Reporting Services URL](#)  
[Tableau Services URL](#)
- Help URL \*
  - This is the URL that you want to provide your consumers when a report is not working properly so that data errors can be resolved. This URL or e-mail is typically a Helpdesk website form or an e-mail distribution account to a group and not to an individual.
- Data Security Group Type \*
  - This field indicates if the report is considered Enterprise or Departmental data.



- Data that is sourced from DSS1PRD or EBIP is considered Enterprise data and will require Data Manager approval which is routed based on the selections from the Campus Code and Subject Area selection criteria which are available by choosing Enterprise.
  - If the report is sourced from a departmental SQL server for example that does not contain Enterprise data, select Departmental.
  - If a combination of Enterprise and Departmental data is used, then Enterprise should be selected.
    - In the Derivation field its recommended that you provide these sources to better inform the Data Manager for approval decision making and to better inform consumer's about data origination.
- Data Source
  - This field determines if the report is considered Enterprise or Departmental data. Data that is sourced from DSSPRD or EBIP is considered Enterprise data.
  - If the report is sourced from a departmental SQL server for example that does not contain Enterprise data then select **Other** and specify the data source.
  - If a combination of Enterprise and Departmental data is used, then **EBIP\DSSPRD and Departmental Data** should be selected. *This should be selected even if the data is sourced from these data sources and cleansed and housed in a departmental database, this is still considered Enterprise data.*
- Data Classification \*
  - This field contain the four Indiana University Data Classifications. Choose the appropriate classification. Choosing Public and University Internal will automatically assign the correct security group used for these groups.
    - Choosing Restricted or Critical will provide the next field named Security Groups.
- Security Groups \*
  - This group is only displayed when choosing Restricted or Critical Data Classification groups from the previous step. In this list you will have access to select among security groups already available for this data classification. In many business cases, you will want to create this group previous to report publishing. See section 3.4.4 for more information.
- Frequency \*
  - This is how often your report data will be refreshed from the source. For example if your report is census information, Quarterly may be an appropriate choice. If the data is sourced from DSS1PRD or EBIP then the daily option would be more appropriate. As is the case with many reports data that is sourced from DSSPRD, EBIP, and other sources may use a data extract model sourced from these systems. Such reports will only be updated when the actual data extract is updated in the reporting system replacing the underlying data. Although data from DSSPRD which its data is refreshed daily, many reports may source from snapshots which only get updated when the snapshots are taken. Take these examples into consideration when setting tis option.
- Report Type \*
  - This field defines the type of reporting services being used to display the report. For example if the report is a tableau report, choose this selection criteria so that the CBI handles the report properly when displayed. Choosing an incorrect Report Type may improperly display the report and this can be changed later if necessary.
- Subject Area \* (Available When Data Security Group Type is selected)
 

A subject area is how the resource is assigned to a particular Area of Responsibility (AOR) for data stewardship. This field in addition to Campus Code determines which Data Manager(s) receives communications for approval of the report selection criteria.
- Campus Code\* (Available When Data Security Group Type is selected)



- A campus is how the resource is assigned to a particular area of data stewardship. This field in addition to Subject Area determines which Data Manager(s) receives communications for approval of the report selection criteria.
- Department \*

  - This selection includes the campus and department organizational unit which is generally the 3-4 character code. This field selection should be the group that created the report, in most cases this is the BI Center name.

- Effective Date Indicator \* Auto generated
  - Sets the date the report metadata is added to the CBI.
- Category/Relatedness
  - High level group to which this resource belongs and its relationship with other entities such as Course/Class reports.
- Derivation
  - Logic for any derivations present in the resource. This can either be as the data transforms from the source system into the data warehouse or any additional derivations that are completed at the report level. For example derived ethnicity combines data on visa status and primary ethnic field in SIS to determine whether students are international or a U.S. minority.
- Keywords
  - Words selected by the author from a pre-defined lexicon to help others find the resource. For example enrollment, headcount, etc.
- Links
  - This could provide links to appropriate related reports and data dictionaries for a particular report and its contents. For example links from contextual data about a report to individual data elements and their metadata.
- Retention Period
  - How long data in this particular report should be kept before the report needs to be refreshed or retained for reporting needs.
- Requestor \*

  - Person who initially requested the resource. For example if a user in your group or another department requests the report creation, this is the user who should be identified. This can be the developer/Publisher or any user deemed appropriate.

- Requestor Department \*

  - Department requesting the resource, by default this selection will default to the Department selection from previous fields and can be changed. For example BL-EDSS builds the report however IN-IMIR requested the report, in this scenario IN-IMIR would be selected as the requestor.

- Primary Report Owner \*

  - Domain username who is the primary contact for the report.

- Secondary Report Owner \*

  - Domain username who is the backup contact for the report.

- Business Owner\*

  - This field is auto selected from the previous choice Department is chosen. This field represents the department owner of the report.

When adding the reports initial metadata a Publisher has the functionality to **Save** the data to later return to complete the request. A Publisher also can **Submit for Approval** which initiates a Kuali workflow which is then routed to the Data Manager for the Area of Responsibility (AOR) for approval when using the Enterprise Data Security Group Type choice.

During the original creation of a report, Publishers can save reports metadata as many times as necessary before they are ready to submit. When saving the original report metadata previous to any Publishing requests three buttons are available depending on whether the data is enterprise or departmental.

Reports that have been previously Published only provides ability to Submit for Approval/Publish and Go Back. There is no **Save** option after a report has been published, certain metadata edit(s)/change(s) will require an Approval.

- Enterprise: ‘Submit For approval’, ‘Save’, ‘Go Back’
  - Submit For approval – Initiates Data Manager workflow approval, locking editing capability until the approval or disapproval has completed.
  - Save – Saves a copy of your publishing for later use/editing, only available previous to any Publish.
  - Go Back – Directs you back to the folder view wiping any changes/edits you have made
- Departmental: ‘Publish’, ‘Save’, ‘Go Back’
  - Publish – Publishes the report immediately. Departmental data does not have assigned Data Managers, so no approval workflow request is generated.
  - Save – Saves a copy of your publishing for later use/editing, only available previous to any Publish.
  - Go Back – Directs you back to the folder view wiping any changes/edits you have made

### 3.4.2.2 Required Metadata for Subsequent Publishing of Reports

#### SECTION UNDER DEVELOPMENT...

**Metadata Required Fields** [*\* Required for Subsequent Edits*] – Additional information or questions about intent for use of the following metadata requirements is available at <https://bi.iu.edu/BI-Governance/Pages/Metadata.aspx>.

- Report Name \*
  - Provide a report name to be identified by users. Hint - make the name short and friendly.
- Description \*
  - Provide a description of the reports use such as what information is being provided through the report and other important information for your consumers.
- Report URL \*
  - This is any URL that is in an <https://reporturlpath> format, most of these URL’s will be direct links to your Tableau or Microsoft BI reports.
    - For example: Hover over the link to view the URL or by clicking.  
[Reporting Services URL](#)  
[Tableau Services URL](#)
- Help URL \*
  - This is the URL that you want to provide your consumers when a report is not working properly so that data errors can be resolved. This URL or e-mail is typically a Helpdesk website form or an e-mail distribution account to a group and not to an individual.
- Data Security Group Type \* **Cannot be changed on subsequent edits.**
  - This field indicates if the report is considered Enterprise or Departmental data.
    - Data that is sourced from DSS1PRD or EBIP is considered Enterprise data and will require Data Manager approval which is routed based on the selections from the Campus Code and Subject Area selection criteria which are available by choosing Enterprise.

- If the report is sourced from a departmental SQL server for example that does not contain Enterprise data, select Departmental.
  - If a combination of Enterprise and Departmental data is used, then Enterprise should be selected.
    - In the Derivation field its recommended that you provide these sources to better inform the Data Manager for approval decision making and to better inform consumer's about data origination.
- Data Source
  - This field determines if the report is considered Enterprise or Departmental data. Data that is sourced from DSSPRD or EBIP is considered Enterprise data.
  - If the report is sourced from a departmental SQL server for example that does not contain Enterprise data then select **Other** and specify the data source.
  - If a combination of Enterprise and Departmental data is used, then **EBIP\DSSPRD and Departmental Data** should be selected. *This should be selected even if the data is sourced from these data sources and cleansed and housed in a departmental database, this is still considered Enterprise data.*
- Data Classification \* Changing this will require "Security Groups" Approval again.
  - This field contain the four Indiana University Data Classifications. Choose the appropriate classification. Choosing Public and University Internal will automatically assign the correct security group used for these groups.
    - Choosing Restricted or Critical will provide the next field named Security Groups.
- Security Groups \*
  - This group is only displayed when choosing Restricted or Critical Data Classification groups from the previous step. In this list you will have access to select among security groups already available for this data classification. In many business cases, you will want to create this group previous to report publishing. See section 3.4.4 for more information.
- Frequency \*
  - This is how often your report data will be refreshed from the source. For example if your report is census information, Quarterly may be an appropriate choice. If the data is sourced from DSS1PRD or EBIP then the daily option would be more appropriate. As is the case with many reports data that is sourced from DSSPRD, EBIP, and other sources may use a data extract model sourced from these systems. Such reports will only be updated when the actual data extract is updated in the reporting system replacing the underlying data. Although data from DSSPRD which its data is refreshed daily, many reports may source from snapshots which only get updated when the snapshots are taken. Take these examples into consideration when setting tis option.
- Report Type \*
  - This field defines the type of reporting services being used to display the report. For example if the report is a tableau report, choose this selection criteria so that the CBI handles the report properly when displayed. Choosing an incorrect Report Type may improperly display the report and this can be changed later if necessary.
- Subject Area \* (Available When Data Security Group Type is selected)
 

A subject area is how the resource is assigned to a particular Area of Responsibility (AOR) for data stewardship. This field in addition to Campus Code determines which Data Manager(s) receives communications for approval of the report selection criteria.
- Campus Code\* (Available When Data Security Group Type is selected)
  - A campus is how the resource is assigned to a particular area of data stewardship. This field in addition to Subject Area determines which Data Manager(s) receives communications for approval of the report selection criteria.

- Department \*
  - This selection includes the campus and department organizational unit which is generally the 3-4 character code. This field selection should be the group that created the report, in most cases this is the BI Center name.
- Requestor \*
  - Person who initially requested the resource. For example if a user in your group or another department requests the report creation, this is the user who should be identified. This can be the developer/Publisher or any user deemed appropriate.
- Requestor Department \*
  - Department requesting the resource, by default this selection will default to the Department selection from previous fields and can be changed. For example BL-EDSS builds the report however IN-IMIR requested the report, in this scenario IN-IMIR would be selected as the requestor.
- Primary Report Owner \*
  - Domain username who is the primary contact for the report.
- Secondary Report Owner \*
  - Domain username who is the backup contact for the report.
- Business Owner\*
  - This field is auto selected from the previous choice Department is chosen. This field represents the department owner of the report.

### 3.4.2.3 Routing for Approval and Lookup Data Manager

Publishing a report indicates a decision to implement a request initiated as a Quali Workflow request, the same process used for many Enterprise systems. Once an Enterprise report has been Submitted for approval, a Quali workflow eDoc is initiated for Data Manager routing. Until an Approve or Disapprove has occurred, the record will be locked. The Data Manager is the role which will have the ability to review the metadata and the actual report previous to approving or disapproving; there is no FYI. Once the request has completed the editing lock is removed. See section 4.1 for more information about Workflow.

Once a “Departmental” **Report** has been Published, the report (Lazy Approval) is immediate available since there is not a concept of a Departmental Data Manager.

*LATER FUNTIONALITY IMPROVEMENT* – At a later time Departmental requests will be routed to the department Information Technology Manager, LSP, or Fiscal Officer for approval.

In order to determine the Data Manger(s) that will receive a request for Enterprise approvals use the OneStart Data Manager Lookup tutorial.

- Job Aid - [https://onestart.iu.edu/dp-prd/resources/Data\\_Stewards\\_eDoc\\_job\\_aid\\_05.22.13.pdf](https://onestart.iu.edu/dp-prd/resources/Data_Stewards_eDoc_job_aid_05.22.13.pdf)
- Data Manager (Lookup) Job Aid Tutorial - [https://onestart.iu.edu/dp-prd/resources/Data\\_Stewards\\_eDoc\\_job\\_aid\\_05.22.13.pdf](https://onestart.iu.edu/dp-prd/resources/Data_Stewards_eDoc_job_aid_05.22.13.pdf)

Contact [ricereq@indiana.edu](mailto:ricereq@indiana.edu) for assistance.

# 4 Business Intelligence Work Flow (Data Manager)

The following sections overview the Data Manager Approval process and functionality only available to the University assigned Data Manager Role. This Role and responsibility is assigned and maintained by the Enterprise Information Governance Data Provisioning services available through <https://onestart.iu.edu> > **Services** > **Administrative Systems** > **Data Governance**. Contact [ricereq@indiana.edu](mailto:ricereq@indiana.edu) for additional information.

The Role of the [Data Manager](#) includes the stewardship of all Enterprise request for access to reports and data. As result you will receive e-mails delivered by the Kuali Enterprise Workflow services as result of reports and data requests for the modern reporting services. These requests facilitate decision making by providing a preview for access requests to reports and data services.

Data Managers will have access to reports which list all Publishers with access to the Business Intelligence Management services and also Developers for the area that you are Data Manager.

New University Data Managers will receive an e-mail from the EBI Helpdesk which will include assignment details as a Data Manager for the **Subject** for the **Campus** and additional KB documentation relevant to your position.

What is a Data Manager - <http://kb.iu.edu/data/ddou.html>

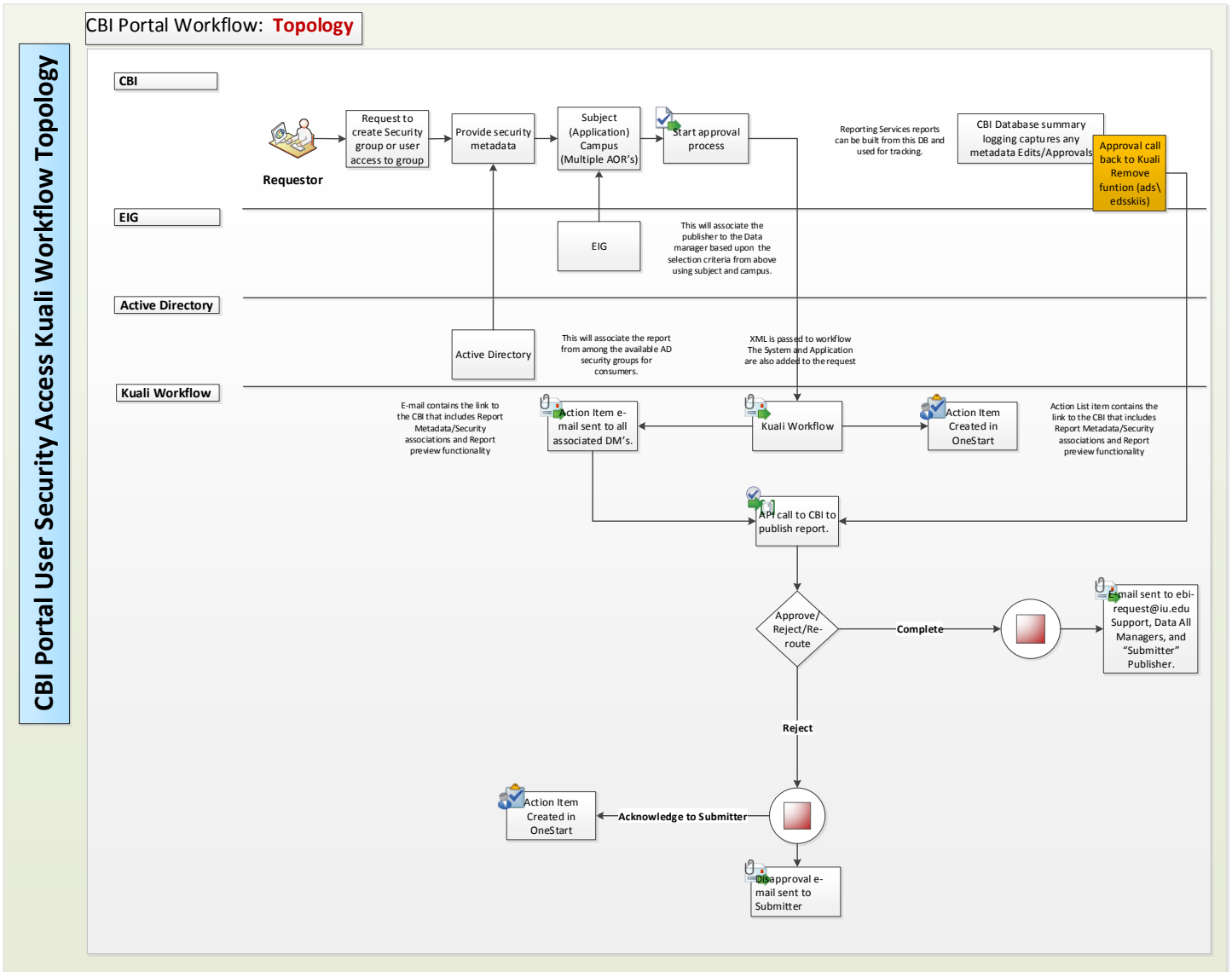
## 4.1 Workflow Routing Business Rules

Access requests for reports and data objects “cube” access is routed to the appropriate Data Manager for approval. If the data resource requested includes multiple areas of responsibility (cross-modular data) the approval request will be routed to all Data Managers in those areas which require that at least one Data Manager approves the request. If a Data Manager from one of the multiple areas of responsibility does not approve the request, the overall request is disapproved. If a Data Manager in an AOR approves the request and then later another Data Manager in the same AOR denies the request, the system has already approved the request or vice-versa. When this occurs the Data Managers in that AOR must reconcile the request and contact the EBI Helpdesk to request any change to the approval if required.

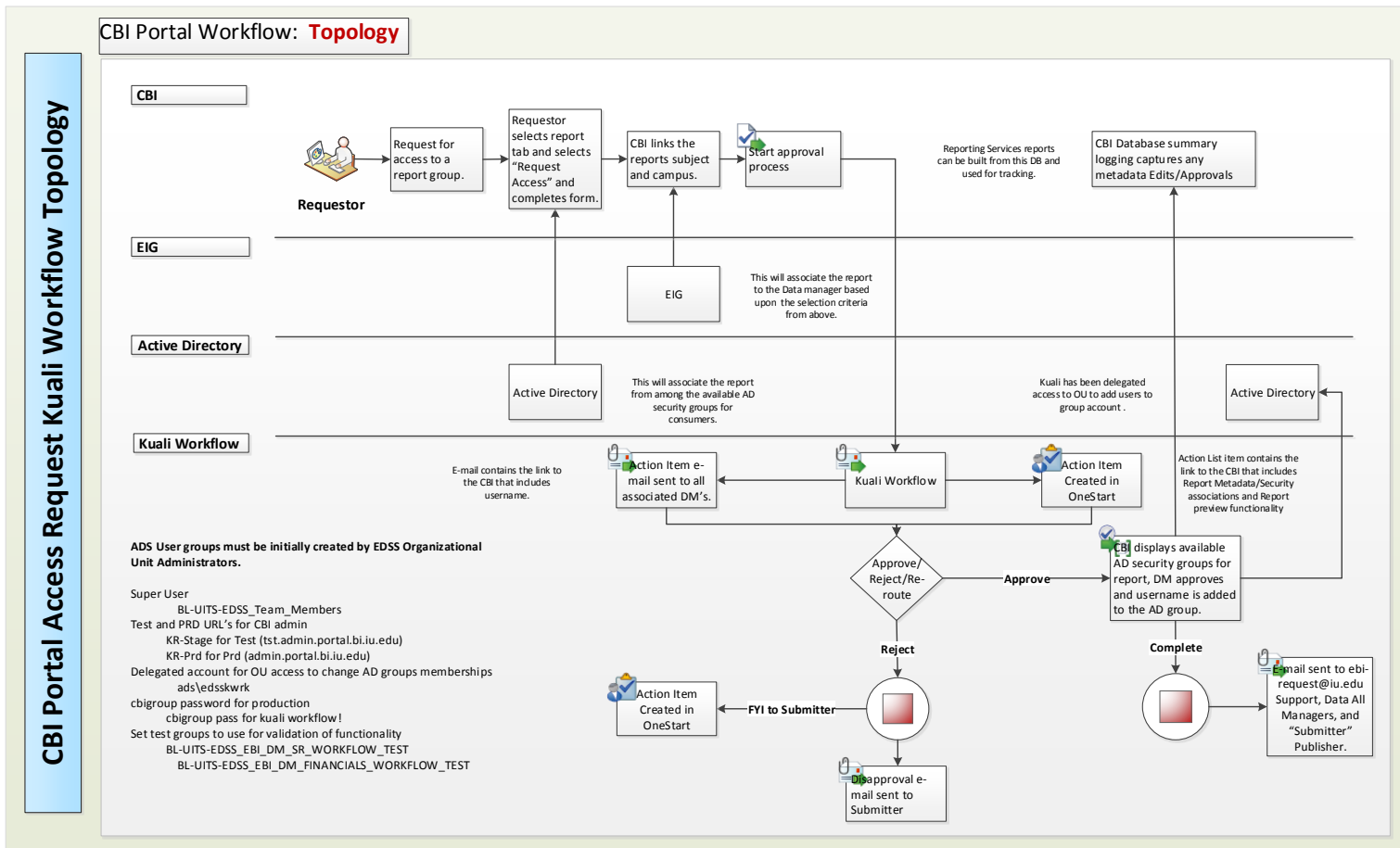
Report access must be approved through this Data Manager Approval process using the CBI, e-mail requests received through the EBI Help Desk for access will be denied since we are unable to make data access decisions.

All enterprise reports and cubes have assigned Subject Area and Campus codes as result of the publishing process. This information provides the necessary information to appropriately route the Kuali Workflow which will initiate an e-mail and appear as an Action Item in the OneStart Portal. The Data Manager will have the ability to review the metadata and the report when it is submitted for review and Publishing. The Data Manager can only Approve or Disapprove a request, there is no FYI.

## 4.1.1 Publishing a Report and Approval Workflow



## 4.1.2 Request Access to a Report or data Object and Approval Workflow



## 4.2 Data Manager Role and Kualif Workflow

The Business Intelligence Management services utilizes the Indiana University Kualif Enterprise Workflow which provides all workflow routing for reports and security group requests to data resources. Report Data is not stored in the BIM, it is sourced from the Report Systems such as SQL Server Reporting Services and Tableau. More information about the Kualif Workflow service can be found at <http://kb.iu.edu/data/aqgg.html>.

As a Data Manger you are expected to have knowledge of data classifications and requirement for university staff interacting with university data as overviewed in the [IU Acceptable Use Agreement](#) for access to institutional data and applications. Data Managers are also responsible for ensuring that users receive orientation and training as dictated by the requirements of the particular data subject area to which they are assigned.

To learn more about the Data Manger(s) Data Provisioning services use the OneStart Data Manager tutorials.

- Job Aid - [https://onestart.iu.edu/dp-prd/resources/Data\\_Stewards\\_eDoc\\_job\\_aid\\_05.22.13.pdf](https://onestart.iu.edu/dp-prd/resources/Data_Stewards_eDoc_job_aid_05.22.13.pdf)

- Data Manager (Lookup) Job Aid Tutorial - [https://onestart.iu.edu/dp-prd/resources/Data\\_Stewards\\_eDoc\\_job\\_aid\\_05.22.13.pdf](https://onestart.iu.edu/dp-prd/resources/Data_Stewards_eDoc_job_aid_05.22.13.pdf)

Contact [ricereq@indiana.edu](mailto:ricereq@indiana.edu) for assistance.

## 4.2.1 Receiving a Request

When a User submits an Enterprise request for approval for a report or security group a Kuali Workflow action will be initiated. This request will contain the required metadata and assigned memberships.

The Publisher or Data Manager will select Submit for Approval and be presented with a Loading screen.

**Submit for Approval**

After this approval submission completes the request is immediately sent. The Kuali workflow service initiates and routes the request to the Data Managers for the area of responsibility (AOR) which is routed using Campus code and Application Code and was supplied by the requestor during the creation of the report metadata. The combination of the two codes defines whom the request is routed using Kuali and the Enterprise Information Governance data provisioning services.

## 4.2.2 E-mail Business Rules and Functionality

As a Data Manager one of the common interfaces to routing is the use of e-mail and in addition the BIM Data Manager Web interface. All e-mail is sent by the Kuali Onestart Workflow services and uses the following business logic and document types for the following business conditions.

### Report

- Access Requests.
  - Reports access notice uses KR Workflow (CBI.ReportGroupAccessRequest).
- Creates and Edits.
  - Reports edit notice uses KR (CBI.PublishReport).

### Security Group (*User Group*) (includes Cubes)

- Access Request and Edits.
  - Security request notice uses a single KR Workflow type (CBI.AddRemoveSecurityGroupUsers).
- Creates.
  - Security request notice uses a single KR Workflow (CBI.CreateSecurityGroupRequest).



The following content details the e-mail notification content details for the above business logic.

- Create and Edit a report - should receive e-mails from Workflow showing user info, resource details, details for security groups; should get same sort of an e-mail from CBI for the initiator
- Create and Edit a security group - should receive e-mails from Workflow showing user info, resource details, security group details; should get same sort of an e-mail from CBI for the initiator
- Disapprove and Approve a report - should receive e-mails from CBI for you as DM and one should go to the initiator; disapproval should also send a standard acknowledgement e-mail from Workflow to the initiator
- Disapprove and Approve a security group – should receive e-mails from CBI for you as DM and one should go to the initiator; disapproval should also send a standard acknowledgement e-mail from Workflow to the initiator
- Request access to a report - should receive e-mails from Workflow showing user info, resource details, security group details to the DM's; should get an e-mail sent from CBI to the initiator

For a disapproval, and e-mail is sent to the Initiator.

#### 4.2.2.1 Data Manager as the Initiator

The Data Managers for the Area of Responsibility (AOR) as routed by the Publisher (Subject and Campus) will receive an e-mail following the business rules for e-mail as detailed in the previous section.

When a Data Manager initiates their own request, report approvals will still generate an e-mail which will be sent to the AOR Data Managers whom is the initiator (i.e. requestor). As result if the Data Manager initiates the change to a Report or Security Group in their AOR an e-mail will also be sent to all Data Managers for the AOR.

## 4.3 Data Manager CBI Approval

The BIM services uses the Quali Workflow for all actions to reports. A Quali workflow e-mail and Action Item in the OneStart Action List will be generated for all Enterprise requests.

### 4.3.1 Reports Approval

Data Managers approving or disapproving reports will receive an e-mail or an Onestart Action item. These e-mail and Action Item links will direct the Data Manager to a Data Manager Approval page from within the BIM facilitating a preview of the report previous to publishing and will display the initial metadata or edits which will display changes to previous requests and can be overviewed and an informed decision made to Approve or Disapprove.

The image below depicts the Data Manager screen seen during the approval process and displays the popup functionality provided when looking at the security assigned to the report.

## 4.3.2 Security Groups Approval

Data Managers approving or disapproving security group requests will receive an e-mail or an Onestart Action item. These e-mail and Action Item links will direct the Data Manager to a Data Manager Approval page where a review of the requests or changes to previous requests can be overviewed and a decision made to Approve or Disapprove as depicted in the following image.

The following depicts an edit request for a security group. Green highlight indicates new metadata and removed metadata with red highlight with a strikethrough.

# 5 Security Access

The Enterprise Business Intelligence Services provides several methods to secure data that facilitate access to the reporting environments reports, data objects such as cubes, and development tools.

What is sensitive data, and how is it protected by law? <http://kb.iu.edu/data/augs.html>

## 5.1 Data Classifications, Roles, and Compliance

The following overviews IU Data Classification, Security Groups, CBI Roles, and Compliance as it pertains to the Enterprise Business Intelligence Services.

### 5.1.1 Data Classifications

At Indiana University classifications of institutional data are characterized into a data classification which provides the context and sensitivity of data. The CBI requires that any data added to the Reports Catalog or Data Catalog are tag with appropriate metadata which includes its data classification. All university data classifications are approved for use in the Enterprise Business Intelligence services, you can read more about Data Classifications at <http://datamgmt.iu.edu/classifications.shtml>.

### 5.1.2 CBI Roles

The Consolidated Business Intelligence services provides several web application “task-based” roles which permit access to report tools and management functionality; some of which are listed below.

#### Application “Task-Based” Roles

- BI Center Role
  - Role provides access to a departmental set of resources to store and use tools to create reports.
- Developer Role
  - Role provides access to enterprise warehouse data application areas. This role is required to use enterprise data for reports. This role is not necessary for Publishing departmental data.
- Publisher Role
  - Role provides individuals access to various resources such as a BI Center storage, report tools, and CBI catalog crud functionality. Role does not provide access to Enterprise data.
- Administrator Role
  - Role which provides highest level of access to all CBI and EBI services (UITS Enterprise Administrators).
- Access Coordinator Role **(Not Yet Implemented)**
  - Role responsible for receiving and assessing requests for access to departmental information (non-enterprise data) and databases in accordance with policies and guidelines established by the Committee of Data Stewards. This role is not yet used within the business intelligence services, it is awaiting proper guidance by the Committee of data Stewards and identification of source systems for this role.
- Data Manager Role
  - Role responsible for receiving and assessing requests for access to university information systems and databases in accordance with policies and guidelines established by the Committee of Data Stewards.
- Test Application Release Role

- Role which includes functional testers for software version releases of the CBI and participate in SFRUM testing.
- Report Tester
  - Role which provides access to Report Test instances, typically individuals which vet and QA reports.

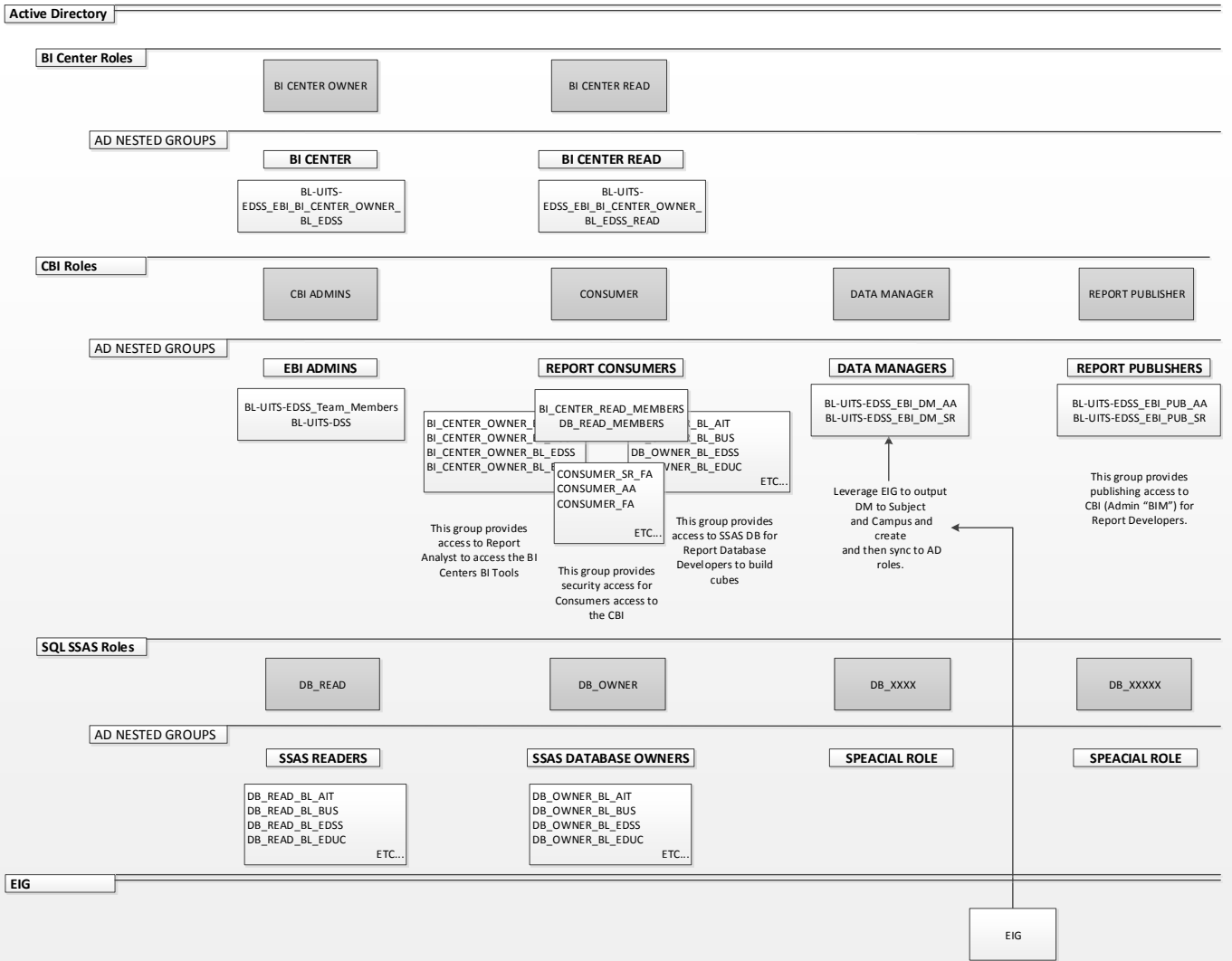
#### Individual Data Roles

- Security Group(s) for the Restricted and Critical data classifications.

#### High-Level Data Roles

- Anonymous Data Role – Anonymous, no authentication required to access to reports.
- Domain Users Data Role – Provides all Indiana University domain Users access to reports, however authentication is invoked.
- University Internal Data Role – Access is granted to Indiana University Users whom have completed the Acceptable Use Agreement to Access to Technology and Information Resources for employees and whom are not an Applicant, Former Student, Former Employee, or Alumni. ***Please note that the University “Data Classification” is different from the University Internal “Data Role” which is a security group managed by the Identity Management Services team.***

Enterprise Business Intelligence Active Directory Services Security: **Topology**



### 5.1.3 Data Compliance

In addition to the approval process to data, the services further verify that compliance requirements have been satisfied before permitting access to reports or data such as cubes.

When a User requests access to data a popup Access Request form is displayed which indicates the compliancy requirements to view the data. If the User has not completed the compliance requirements to view the data they will need to do so before the CBI will permit access.

When the User's request has been approved by a Data Manager access to the data is granted only if the compliancy requirements have been satisfied. In some situations the User accessing the report may be redirected to the compliancy resource such as the User Agreement form or the FERPA tutorial.

Compliance for data is determined during the development specifications for the data and is added during the data publishing process.

University Internal requires that users have agreed to the IU [Acceptable Use Agreement for access to institutional data and applications](#). When a user visits the CBI a check is performed which verifies whether the user has completed and verified the Data Use Agreement. If the User has not completed the Data Use Agreement they are redirected to the Data Use Agreement form and must electronically read/sign before access is granted to the CBI.

ePHI and HIPPA - <http://kb.iu.edu/data/ayzm.html>

HIPPA - <http://kb.iu.edu/data/ayyy.html>

## 5.1.4 Former and Position Change of University Status

When a User leaves Indiana University or a Position change occurs it is the responsibility of the Data Manger to stay informed by following best practices for auditing User access to University data resources as defined by the CDS and Policy Office.

The report services employs a security model leveraged by the Identity Management Services and leverages network accounts (ads\username). As result the networkID (ads\username) status will be inherited be changes as result of the eDoc/HR process and will flag Users as former and regardless if their access is assigned to a group, they will still be denied access to these resources which at a minimum require University Internal access.

This provides the Data Manager or their delegated security coordinators additional opportunities to remove access.

**LATER FUNTIONALITY IMPROVEMENT** – At a later time the CBI will provide functionality to inform Data Managers of User status changes providing additional procedural opportunities to remove the user from the group. How this approach is ultimately decided is in the hands of the Steering Committee / Advisory Council.

To further comply with university policy Identity Finder is used to scan SSRS and Tableau Reports. This utility searches for, protects, and dispose of personal information stored on inappropriate locations containing information which includes credit card numbers, bank account numbers, Social Security numbers, birthdates, passwords, driver's license numbers, addresses, passports, employee identification numbers, maiden names, or other data further prevent incidental and inappropriate use of data.

## 5.2 Authentication and Authorization

The CBI provides flexibility to assign Roles based on Subject and Campus Area and granularly applied security roles. When applying a 1:1 security group to a report, only those members of the security group have access to the data. When applying Role access, Users are assigned permissions to a report or cube through their access defined by the role(s). Individual user rights are assigned the appropriate roles to the user's account which provides added flexibility to reassign common operations such as adding a user or changing a User's department.

Note \* The CDS are defining long-term objectives to identify Job Function role assignment.

Indiana University's report and security environment is a centrally maintained, enterprise-wide, web-based business intelligence portal and set of services.

## 5.3 Security Access Developers/Publishers

The Business Intelligence Management application allows the management of access to many of the Enterprise Business Intelligence resources. In addition to access to reports and cubes, the CBI allows the access management for Developers/Publishers to access resources such as BI Centers, the BIM, reports tools, and Publishing.

### 5.3.1 BI Center Access

The Enterprise Business Intelligence services accommodates many types of reporting that are necessary for federal and state reporting as well as university reporting. A BI Center provides departments the tools and flexibility to provide institutional reporting to manage the mission and operational requirements of the department. A BI Center includes storage and folder space in the reporting services such as Tableau and SQL Server Reporting Services, access to tools and resources, a secure location to build reports, and access to the BIM to create security groups and publish reports.

Publishers use the BI Center to access the advanced tools provided in the Enterprise Business Intelligence services which permit the development of reports.

In order to use the Enterprise Business Intelligence (EBI) services a BI Center request must be made. A BI Centers name is defined using the Organization code <http://kb.iu.edu/data/bdbc.html>. The [Indiana University Organization Hierarchy Report](#) lists all the Organizational Units, locate your Org Code and provide this detail with your BI Center request.

To request access to the tools submit a BI Center Request <http://kb.iu.edu/data/bdbc.html> using the online request form and supplying the Organization Code and Users whom should have access (Domain\username). Requesting access to this resource is the first step to leverage the advanced capabilities of the Enterprise Business Intelligence reporting environment. Requestors must also provide the departments Information technology Manager (ITM) or Fiscal Officer contact details. This process is similar for when assigning technology access for technology professionals (LSP) at Indiana University. This will be verified using the UITS LSP Database to correctly verify or identify the ITM or Fiscal Officer assigned to the department.

Departments that require project area for internal divisions have the ability to create reporting folders from within each reporting library type to further organize projects and to align organization reporting needs.

**Note\* BI Centers provide access to the tools for a Publisher (developer), not data.**

### 5.3.2 Reports Catalog Access for Publishing – BIM

When a Publisher is assigned a BI Center they are added to the BL-UITS-EDSS\_EBI\_PUB\_PUB\_R Role which provides access to the BIM Manage Access and Publishing features. The Publisher Role provides the ability to publish reports to the report and data catalog.

The PUB\_R Role includes all BI Center Owners “Publishers” by default. In the EBI, Publishers are not the same as Developers are in the Warehouse, developers have access to Enterprise Warehouse data (See Section 5.1.2 for more detail). Publishers may not have access to the Enterprise Data Warehouse (Developer), however a Publisher is granted access to the services.

**Note\* BI Centers (PUB\_R) provide access to the tools for a Publisher, not data.**

### 5.3.3 Data Access

Developers (Publishers) request access to many data sources such as Oracle data and SSAS (cubes).

For a Developer to request access to Oracle data, contact the data warehouse team to request access to the security group that provides access to the data requested.

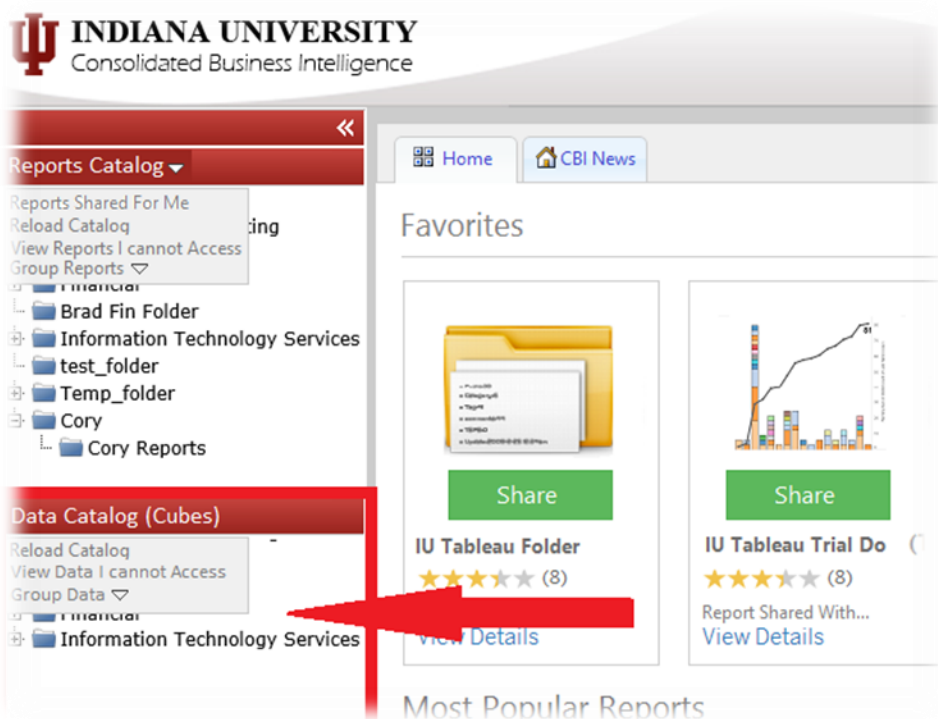
Consumer's requests access to Oracle data by completing a request using the following pages as guidance:

<http://kb.iu.edu/data/allk.html>

<http://kb.iu.edu/data/arhc.html>

#### 5.3.3.1 Cube Request CBI

The CBI provides Publishers the ability to request access to reports and cubes by clicking the report or data object within the Data Catalog folder structure. When a User selects a resource they do not have access to, a popup window will open to provide a justification for the access. A Quali workflow action will be generated on submission and routed to the Data Manger(s) for the Area of Responsibility (AOR) managed by the Enterprise Information Governance (EIG) system.



Data Managers review the request approval page and Approve or Deny the request. If the Data Manager Approves the request then that Publisher is added to the corresponding Roles and security groups for the requested data.

## 5.4 Active Directory

The UITs Identity Management Systems group centrally manages the creation and life of all domain user accounts provisioning. The Identity management process uses a set of business processes, and a supporting infrastructure, that provides identity-based access control to systems and resources in accordance with established policies.

<http://kb.iu.edu/data/aptr.html>



The use of Active Directory for security rather than local SQL or Oracle security management of User or Groups management provides many advantages. Using Active Directory allows central management of access to most enterprise systems. Identity Management uses a central metadirectory to facilitate lifecycle identity management. The metadirectory connects to all key enterprise systems and then aggregates and synchronizes identity information across all systems, including enterprise directories. This provides a consistent and accurate representation of each person within the entire organization. As data is changed in one system, it automatically updates in all other connected systems.

UNIX integration with varying levels of interoperability with Active Directory can be achieved on most UNIX-like operating systems through standards-compliant LDAP clients.

In Microsoft Active Directory, when you create a new group type for security groups which allow you to manage user and server access to shared resources. This methodology simplifies administration by allowing reusable access control on many systems which all inherit membership changes of Groups and Users. The change in group membership automatically takes effect everywhere.

For example the local SSAS Dimensional Group or User management does not enable a reusable model to easily apply security changes broadly to all SSAS Dimensional or Tabular services and local Groups and Users must be created in each instance.

Active Directory security groups enables User access to all network resources with a single desktop login. The scope of Active Directory can range from storing all the resources of a small computer network to storing all the resources of several wide areas networks (WANs). Fundamentally the choice to leverage a third party application to manage security such as Active Directory or use local management of Groups and Users is driven by many factors such as business process or technological constraints.

#### **Additional Resources:**

Best practices for computer security - <http://kb.iu.edu/data/akln.html>

Principle of Least Privileges - <http://kb.iu.edu/data/amsv.html>

Store Password (Vaults) - <https://protect.iu.edu/cybersecurity/safeonline/passphrases/vaults>

Active Directory and Oracle - [http://docs.oracle.com/html/B13831\\_01/active\\_dir.htm](http://docs.oracle.com/html/B13831_01/active_dir.htm)

## 5.5 Rights Management Services

The Enterprise Business Intelligence Services utilizes various report services that are vended. Using these tools an authorized user can export report data such as Excel or on storage media not approved for data storage. This data could then later be obtained by non-authorized users accessing a file server or printed copies.

The Microsoft and Tableau vendors are creating additional technologies to mitigate the unauthorized user created Excel files or unauthorized printing of these materials, however these Rights Management Services to protect these types of data to the "BI to the masses" is still unavailable for the systems used.

The Indiana University Policies located at <http://policies.iu.edu/policies/categories/information-it/index.shtml> provide guidance and policy for handling data which should be followed.

## 5.6 Enterprise Business Intelligence Naming Standards (EBI)

A friendly name is an English phrase with a specific construction and length that describes the subject matter of the data contained in the cube. Each business name comprises one or more prime words, optional modifying words, and one class word. It cannot exceed 64 characters in length. Systems developers assist end users in the construction of meaningful business names.

Friendly cube names should meet the following guidelines:

- as meaningful as possible
- self-documenting
- easily distinguishable

### 5.6.1 CBI\BIM NAMING PROCEDURE

When creating a security group name, any departmental or subject area request must be captured either in the EBI Helpdesk <http://mailform.kb.iu.edu/email.php?cid=1221> Footprints incident/request tracking system or created through the Business Intelligence Management (BIM) tools through Manage Access. In order to best support and maintain best practice, use the following guidelines.

Naming Logic Definition

**BL-UIITS-EDSS\_SYS\_R\_I\_DEFINED**

SYS = System (i.e. SSAS, SQLDB, TAB, BICenter, CBI.)

R = Role = Job function or title which defines an authority level

PUB = Developer Role Access

CON = Consumer Role Access

TSTR = Consumer Role Access

I = Instance

SND

DEV

TST

QA

STG

PRD

DEFINED = Publisher Defined Value

#### 5.6.1.1 CBI REPORT CONSUMER NAMING

*Example of Enterprise CBI Consumer Role*

- Consumer Role
  - Consumers = BL-UIITS-EDSS\_EBI\_CBI\_CON\_PRD\_DEFINED

#### 5.6.1.2 CBI PUBLISHER NAMING

*Example for Enterprise CBI Publisher Role*

- Publisher Role
  - Consumers = BL-UIITS-EDSS\_EBI\_CBI\_PUB\_PRD\_DEFINED



**INDIANA UNIVERSITY**

Consolidated Business Intelligence Original Author Retherford, Cory Patrick

ENTERPRISE BUSINESS INTELLIGENCE | INDIANA UNIVERSITY

### 5.6.1.3 TESTER ROLE NAMING

*Example for Enterprise CBI Tester Role*

- Tester Role
  - Consumers = BL-UIITS-EDSS\_EBI\_CBI\_TSTR\_PRD\_DEFINED

### 5.6.2 BI CENTER NAMING

A friendly name is an English phrase with a specific construction and length that describes the subject matter of the data contained in the cube. Each business name comprises one or more prime words, optional modifying words, and one class word. It cannot exceed 64 characters in length. Systems developers assist end users in the construction of meaningful business names.

Friendly cube names should meet the following guidelines:

- as meaningful as possible
- self-documenting
- easily distinguishable

Naming Logic Definition

BL-UIITS-EDSS\_EBI\_SYS\_R\_I\_S\_P\_DEFINED

SYS = System (i.e. SSAS, SQLDB, TAB, BICenter, EBI.)

R = Role = Job function or title which defines an authority level

PUB = Developer Role

CON = Consumer Role

TSTR = Consumer Role

I = Instance

SND

DEV

TST

QA

STG

PRD

S = Subject or Org = A person, subject area, organization “Campus-Department”, or automated agent

P = Permissions approval or access to a resource (-PII = Access denied to Personal Identifiable Information, etc.).

Access Denied = D

Test = T

Read = R

Owner = O

DEFINED = Publisher Defined Value

*Example of Enterprise BI Center Role*

- BI Center Role
  - BL-UIITS-EDSS\_EBI\_BICENTER\_PUB\_PRD\_BL-EDSS\_R\_STUANA
  - BL-UIITS-EDSS\_EBI\_BICENTER\_PUB\_PRD\_BL-EDSS\_O

### 5.6.3 CUBE NAMING

A friendly name is an English phrase with a specific construction and length that describes the subject matter of the data contained in the cube. Each business name comprises one or more prime words, optional modifying words, and one class word. It cannot exceed 64 characters in length. Systems developers assist end users in the construction of meaningful business names.

Friendly cube names should meet the following guidelines:

- as meaningful as possible
- self-documenting
- easily distinguishable

#### CUBE SECURITY NAMING

The following are security group naming standards for SSAS cubes in the Enterprise Business Intelligence (EBI) environment. The following guidelines have been established so that a structured security group and role naming convention is consistent so that systems interacting with EBI

Naming Logic Definition

BL-UIITS-EDSS\_EBI\_SYS\_R\_I\_S\_DB\_P\_CU

SYS = System (i.e. SSAS, SQLDB, TAB, BI\_Center, EBI.)

R = Role = Job function or title which defines an authority level

PUB = Developer Role

CON = Consumer Role

TSTR = Consumer Role

I = Instance

SND

DEV

TST

QA

STG

PRD

S = Subject or Org = A person, subject area, organization "Campus-Dept", or automated agent

DB = SQL Analysis Services Database

P = Permissions approval or access to a resource (-PII = Access denied to Personal Identifiable Information, etc.).

Access Denied = D

Test = T

Read = R

Owner = O

CU = Cube name

*Example of Enterprise and Departmental Cubes*

- Org Unit

- BL-UIITS-EDSS\_EBI\_SSAS\_CON\_TST\_IU-IUSM\_IU-IUSM\_R\_GL
- Enterprise
  - BL-UIITS-EDSS\_EBI\_SSAS\_CON\_TST\_STU\_SA\_D\_PII\_ENRLMNT
  - BL-UIITS-EDSS\_EBI\_SSAS\_CON\_PRD\_STU\_SA\_R\_PII\_ENRLMNT

**Additional Resources:**

<http://kb.iu.edu/data/bctf.html>

<http://www.indiana.edu/~dss/Services/Naming/nameDisplay.pl?table=ab>

# 6 Release Tracking, IT Training, CBI Tutorial

This CBI User's Guide does not provide documentation on the use of dimensional data access from SQL Server Analysis services (Cubes), SQL Server Reporting Services, SharePoint BI, Tableau Server Services, or PERL which will become widely available 2015. For assistance with these services see section 7.

## 6.1 Release Tracking

The EBI development team uses Footprints for incident tracking and JIRA for development project management for CBI and BIM releases. A list of all backlog projects can be viewed in the [JIRA Enterprise Business Intelligence Services Project](#) (CAS required). For access issues to JIRA use the KB for assistance <http://kb.iu.edu/data/baxx.html>.

## 6.2 IT Training and Documentation

For assistance with the reporting and data tools, use the Indiana University Knowledgebase <https://kb.iu.edu> and search on "EBI" to locate documents about your questions.

For training documentation the UITS IT Training and Education group has coordinated with EBI staff to create comprehensive training resources at:

- [Self-Study Materials](#)
- [Classroom led instruction](#)
- [EBI Workshop Classroom Materials](#)
- Training and documentation continues to evolve and in addition to the KB documentation, IT Training Resources, the CBI User's Guide, and additional classroom led instruction is under development for Publishers and Data Managers. Please visit the [Classroom led instruction](#) page for updates.

## 6.3 CBI Tutorial and Quiz

At a later phase of development, in order to receive access, a short quiz will be required. This process is the same as the FERPA tutorial requirements to receive access to Student Data (<https://ferpa.iu.edu>).

In an effort to provide the best support and experience using the tools to Publish reports, it is required that the services adopt the recommendations for policy and standards on training and continuing education as provided and approved by the BI Governance Working Group and mandated by the University Committee of Data Stewards. More can be read at <https://bi.iu.edu/BI-Governance/Pages/Training-and-Education.aspx>

Data Managers are also responsible for ensuring that users receive orientation and training as dictated by the requirements of the particular data subject area to which they are assigned. More information available at <http://datamgmt.iu.edu/dm.shtml>.

# 7 Report Environments

Indiana University's Enterprise Business Intelligence (EBI) consists of many services. Such services include the dimensional SQL Server Analysis services (Cubes), SQL Server Reporting Services, SharePoint BI, and Tableau Server Services. Each of these services including the Business Intelligence Management portal is one component of a much larger set of Enterprise Business Intelligence services which provides the one stop location to access the various report services.

To read more about the new modern report tools and services which includes dimensional data from SQL Server Analysis services (Cubes), SQL Server Reporting Services, SharePoint BI, and Tableau Server Services refer to the following resources. You can also search “[EBI...](#)” using the Knowledge base at <http://kb.iu.edu>.

SQL Server Analysis services (Cubes) - <http://kb.iu.edu/data/bcvp.html>

SQL Server Reporting Services - <http://kb.iu.edu/data/bdbd.html#2>

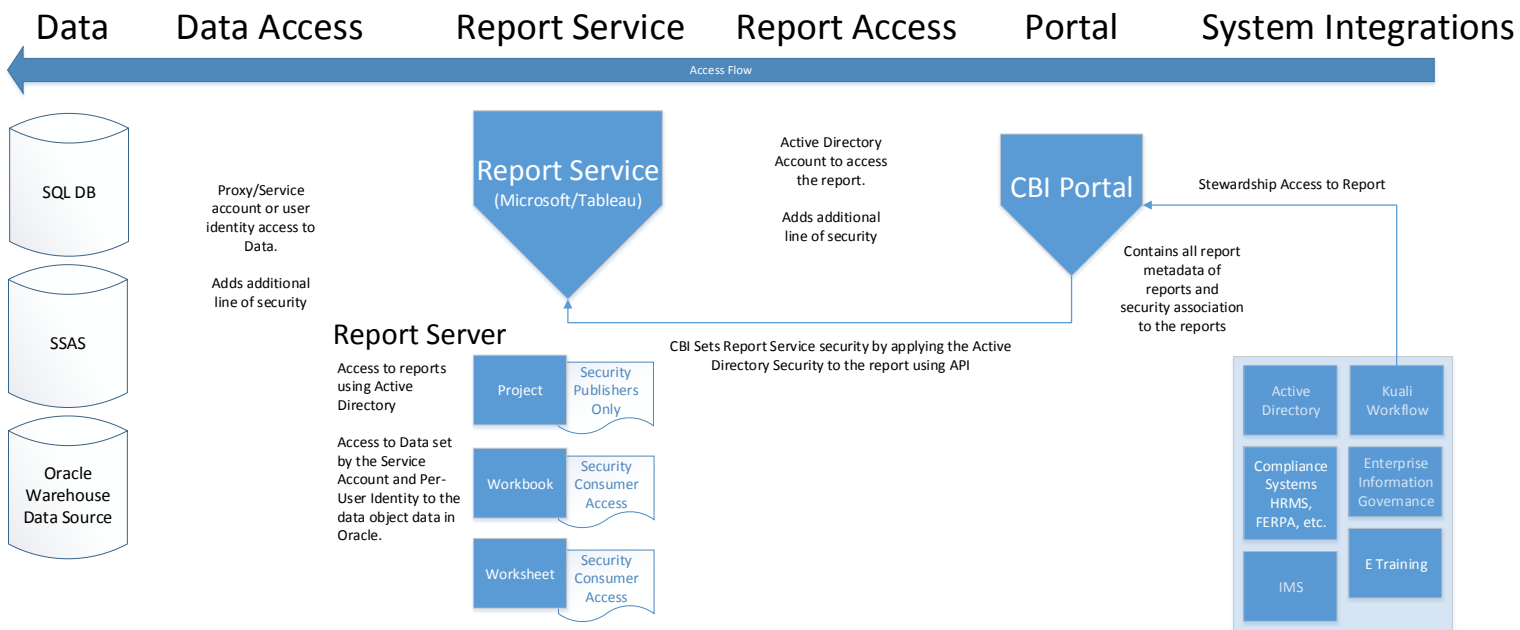
Tableau Server Services - <http://kb.iu.edu/data/bdbd.html#2>

The new portfolio of modern reporting tools allows for a less technically driven (non-programmatic) process to build and publish reports. As result in addition to Developers whom have Enterprise access to the Oracle Warehouse, a new group of report Publishers require additional education and guidance for the use of reporting tools and BIM Publishing features and an awareness of each Unit’s operational procedural and policy how to best facilitate and manage reports creation and security assignment. Additionally Developers whom have published reports will need to be familiar with the new services.

Visit the [E Training](#) services to take the CBI Tutorial and Quiz.

## 7.1 Report Services Proxy/Service Accounts

The following section overviews concept of service/proxy accounts and their applicability to the EBI SQL Server Reporting Services and Tableau (Proxy) Service Accounts.



### 7.1.1.1 UIIE Report Services (Proxy) Accounts

The UIIE is both the portal and reporting service as result when a data extract (GT) report or pre-defined query (PDQ) report is executed from the UIIE, it connects to DSS1PRD to gather the appropriate data for the report results. The connection to DSS1PRD needs to provide the same level of data access for that person, independent of what UIIE report type they run. It also needs to be the same level of access if they connect directly to DSS1PRD instead of querying the data through the UIIE. While we give control over the direct-login account to the user, the EDSS team retains control of the connection mechanism for UIIE reports.

To accomplish all this, each user has multiple DSS1PRD accounts, one for their direct connections and two “proxy” accounts for different UIIE report types. These accounts are:

- <Oracle username> (aka “**base**” account) - the user has control over the password and can connect directly to DSS1PRD with this account.
- <Oracle username>\_BATCH (aka “**\_BATCH**” account) – proxy account for data extract report connections to DSS1PRD. The password is stored and maintained by the UIIE. The user has no direct access to this account.
- <Oracle username>\_PDQ (aka “**\_PDQ**” account) – like the \_BATCH accounts, but used for PDQ reports.

The UIIE \_PDQ and \_Batch accounts are proxy accounts having broad access to all GT and PDQ’s. Access to these for general User access is restricted by the User account has permissions to. The proxy accounts are used as an internal process as in the EBI (See KB <http://kb.iu.edu/data/bcu.html>) and the typical Consumer, Developer/Publisher, or Data Manager can use these, however are not able to manage credentials.

The three DSS1PRD Oracle accounts are created when a user creates their UIIE account. As **object-level** data access is granted to the UIIE user account, the corresponding Oracle access is granted to the base and \_BATCH account. Object-level data access is handled differently for PDQ’s. From the beginning, the **\_PDQ** account has extremely broad object-level data access, but the user is limited in its use based on UIIE report security assigned to the user.



For application areas which have **row-level** secured data, it is enforced strictly in the database and not in the IUIE. Developers create views in DSS1PRD which join the full dataset to a security table which defines the allowed rows for the username used in the connection. Since all three accounts start with the same username, the view can use just the first portion of the connection name and apply the same row-level security.

IUIE departmental proxy accounts, are requested by Developers and used by IU Departments for automated data queries against DSSPRD, DSSTST, and DSSDEV. The security of these accounts is handled similar to regular user accounts, (via the IUIE), however, the account itself cannot/should not access the IUIE directly. The name/Oracle password for this account is embedded into the queries as a service/proxy for that department. A department as a whole may need access to a wider or narrower range of data than the individual members of that team and service/proxy accounts are not owned an individual.

IUIE departmental accounts are requested and used by the Developers in the IUIE from various Indiana University departments for automated data queries against DSSPRD or DSSTST. This is a proxy account that typically has broader access to data than the individual Developers. This provides the Department as a whole broader access to data than the individual members of that team allowing access to the report data. Additionally this approach provides access to the report regardless if the individual Developer leaves the University, Developer account is disabled, and automated data pulls will function regardless the Developers status using a departmental “proxy” account.

The \_PDQ, \_BATCH, and departmental accounts are accounts that give restricted access to users/departments that do not necessarily have that access with their own accounts.

Oracle Proxy Accounts - <http://www.oracle.com/technetwork/database/security/index-092912.html>

### 7.1.1.2 SQL Server Reporting Services and Tableau (Proxy) Service Accounts

The Enterprise BI Reporting Services provides the ability to store Credentials similar to the way a PDQ and GT creates a username\_serviceaccount. From within each report tool a developer creates a data source connection which provides the report the connection string to the data surfaced in the report. **Service/Proxy accounts are not set in the CBI, it's completed in the Report Tools.**

For each reporting type a developer selects any of the following options for the report to access this data.

- Windows authentication
- Prompt for credentials to access Oracle or Windows resources (This option will require the consumer to provide their Oracle username and passphrase to access the data source).
- Stored credentials provides a mean to store a usernames credentials which are encrypted in SharePoint or Tableau and provide the report service access to the data for the report such as the same process that the IUIE uses to create the username\_PDQ or username\_batch process. **Unlike the IUIE, the developer provides this service account** until a means has been determined to pass a username\_CBI level of access to the various tools. This method could be used to provide the same access as do the BT and PDQ do. In the reporting tools the serviceaccount\_username is passed to the data source which is the same process as the IUIE.

Read more about using proxy/service accounts at <http://kb.iu.edu/data/bcu.html>.