Role-Based Access Control to the Data Owner Level in Zubin

One of the core aspects of **data democratization** is the need to be able to control access to all data in your environment so that any given user can only manage or view information about their data, the specific set of files, folders, objects, shares, exports, or data stores for which they are responsible.

Zubin does this with a robust **role-based access control (RBAC) system**, which ensures that users are given access to only the areas of the product and areas of the data they need to be able to access. This system enables granular control over user access, which then improves overall data security and compliance with internal and external rules.

The platform's RBAC system is tied into **your organization's own identity management system**, whether that is Microsoft Active Directory or another Lightweight Directory Access Protocol (LDAP) application. In practical terms, this means that once Zubin is installed and configured in your environment, all of your users can be easily added to Zubin and assigned a role.

Built-in Zubin Roles

Zubin includes the following built-in roles:

- Data Owner/Data Owner Custodian
- Storage Administrator
- Policy Administrator
- Security Officer (CISO)
- Infrastructure Officer (CIO)
- System Administrator

Each role has its own set of responsibilities and access to different features and parts of Zubin flow from those responsibilities:

- **Data Owner:** By default, all Zubin users are assigned the **Data Owner** role, which lets them access only the data they own in your organization's storage environment. Zubin operates on the principle that **users own their own data,** and they should therefore be able to access that data, manage that data, and act on that data. Data Owners are **"non-administrative" users,** without the permissions necessary to configure Zubin, manage data stores, or manage policies or workflows, although they can run workflows to which they have access. Some Data Owner users are also **Data Owner Custodians;** these users are responsible for managing not just their own data but also data owned by their respective team or department. Data Owner Custodians are very similar to lower-level Data Owners in terms of what they can do in Zubin, but they are able to see more of a "roll-up" view of data that includes all of their reports.

- **Storage Administrator:** Users assigned the **Storage Administrator** role are responsible for setting up the data infrastructure for your Zubin installation, including adding and managing databases, adding and managing data stores, and deploying data engines. Storage Administrators can configure some areas of the product but cannot run workflows or policies. In effect, they are **"non-data" users.**

- **Policy Administrator:** Users assigned the **Policy Administrator** role **provide the tools used by other users** to work with and view information about your enterprise's data. This type of user can **create policies and workflows** that can then be used or run by other users and can also run those policies and workflows themselves. However, Policy Administrators cannot configure most of Zubin's settings; their responsibility is to build out the overall data management flow.

Click here for a demo

- **CISO (Security Officer)/CIO (Infrastructure Officer):** Users assigned the **CISO (Security Officer)** or **CIO (Infrastructure Officer)** roles are more powerful users than either Data Owners or Policy Administrators but cannot configure settings in Zubin. Instead, they primarily need **high-level views** of the whole enterprise in terms of **security** or **storage.**

- **System Administrator:** Users with the **System Administrator** role assigned are responsible for **installing and configuring Zubin** in your environment. System Administrator users are "non-data" users like Storage Administrators and are tasked with setting up the product for other users with other roles to use.
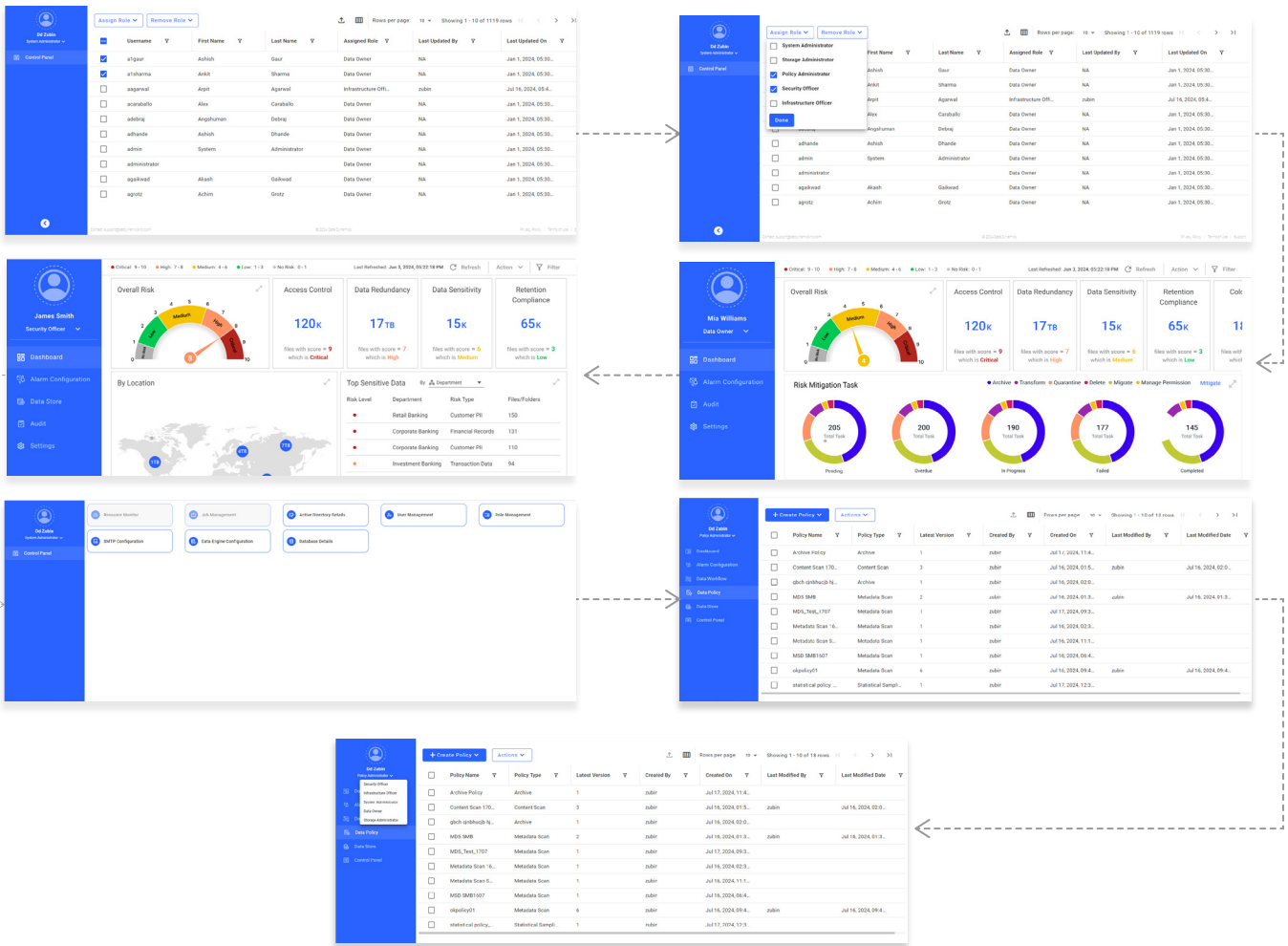
Data Access

As previously mentioned, users can only access the data to which they have access, on any data store added to Zubin. With that said, users with Executive-level functions within a company need to have access to more data than just their own specific set of files – a CISO, for example, may not care about the details of individual files but needs to be able to see an overview of potential risks related to those files.

At the lowest level, if you are a **Data Owner** user with access to only a certain set of shares on **Windows Server-1** when your Storage Administrator adds **Windows-Server-1** to Zubin, you can then access only those shares or information about those shares.

You could, however, be a Data Owner user who is responsible for more than just your files – managing a department, for instance, or in charge of a particular application and all the files associated with that application.

In either of those cases, you would still be assigned the **Data Owner** role, but because of the permissions assigned outside of Zubin, either on the application level or in Active Directory, you would be able to access all the data for which you are responsible, as a **Data Owner Custodian** user.

Security Officer or **Infrastructure Officer** users, on the other hand, have access to a much wider range of data, across entire networks or organizations, only at a higher level. If you are assigned one of these roles, you can view analytical information about the data in your enterprise in the Dashboard, but you cannot access the files themselves.

Click here for a demo

Feature/Functional Area Access

The following table displays all the features and functional areas of Zubin with the different roles that do and do not have access to those features and areas:

| Functionality	System Admin	Storage Admin	Policy Admin	Sec Officer	Data Owner	Infra Officer
Dashboard	N	Y	Y	Y	Y	Y
Data Workflow, View	N	Y	Y	Y	Only Applicable WFs	Y
Data Workflow, Update	N	N	Y	N	N	N
Data Workflow, Delete	N	N	Y	N	N	Y
Data Workflow, Execute	N	N	Y	Y	Only Applicable WFs	Y
Data Policy, View	N	N	Y	Y	N	Y
Data Policy, Update	N	N	Y	N	N	N
Data Policy, Delete	N	N	Y	N	N	N
Data Policy, Execute	N	N	Y	Y	N	Y
Data Store, View	N	Y	Y	Y	N	Y
Data Store, Update	N	Y	N	N	N	N
Data Store, Delete	N	Y	N	N	N	N
Alarm Configuration, View	N	N	Y	Y	Y	Y
Alarm Configuration, Update	N	N	Y	N	N	N
Alarm Configuration, Delete	N	N	Y	N	N	N

Click here for a demo

Functionality	System Admin	Storage Admin	Policy Admin	Sec Officer	Data Owner	Infra Officer
Logs	Y	Y	Y	Y	Y	Y
Audit	Y	Y	Y	Y	Y	Y
Control Panel, Active Directory, View Update, Delete	Y	N	N	N	N	N
Control Panel, User Management, View, Activate, Deactivate, Force Logout	Y	N	N	N	N	N
Control Panel, Role Management, View, Assign, Unassign	Y	N	N	N	N	N
Control Panel, SMTP Configuration, View, Update	Y	N	N	N	N	N
Control Panel, Email Template Configuration, View, Add, Update	Y	N	Y	N	N	N
Control Panel, Data Engine Configuration, View	Y	Y	Y	N	N	N
Control Panel, Data Engine Configuration, Add, Install, Uninstall	N	Y	N	N	N	N
Control Panel, Database Details, View	Y	Y	Y	N	N	N
Control Panel, Database Details, Update	N	Y	N	N	N	N
Settings	System	Storage	Policy	Sec	Data	Infra
API, Control Panel, AD, User Management, Role Management, SMTP Configuration	Y	N	N	N	N	N

Click here for a demo

Functionality	System Admin	Storage Admin	Policy Admin	Sec Officer	Data Owner	Infra Officer
API, Control Panel, Data Engine Configuration	N	Y	N	N	N	N
API, Control Panel, Database Details	N	Y	N	N	N	N
API, Data Store	N	Y	N	N	N	N
API, Data Policy	N	N	N	N	N	N
API, Data Workflow	N	N	Y	N	N	N
Control Panel, Resource Monitor	Y	N	Y	N	N	N
Control Panel, Job Management	Y	N	Y	N	N	N

Process Flow
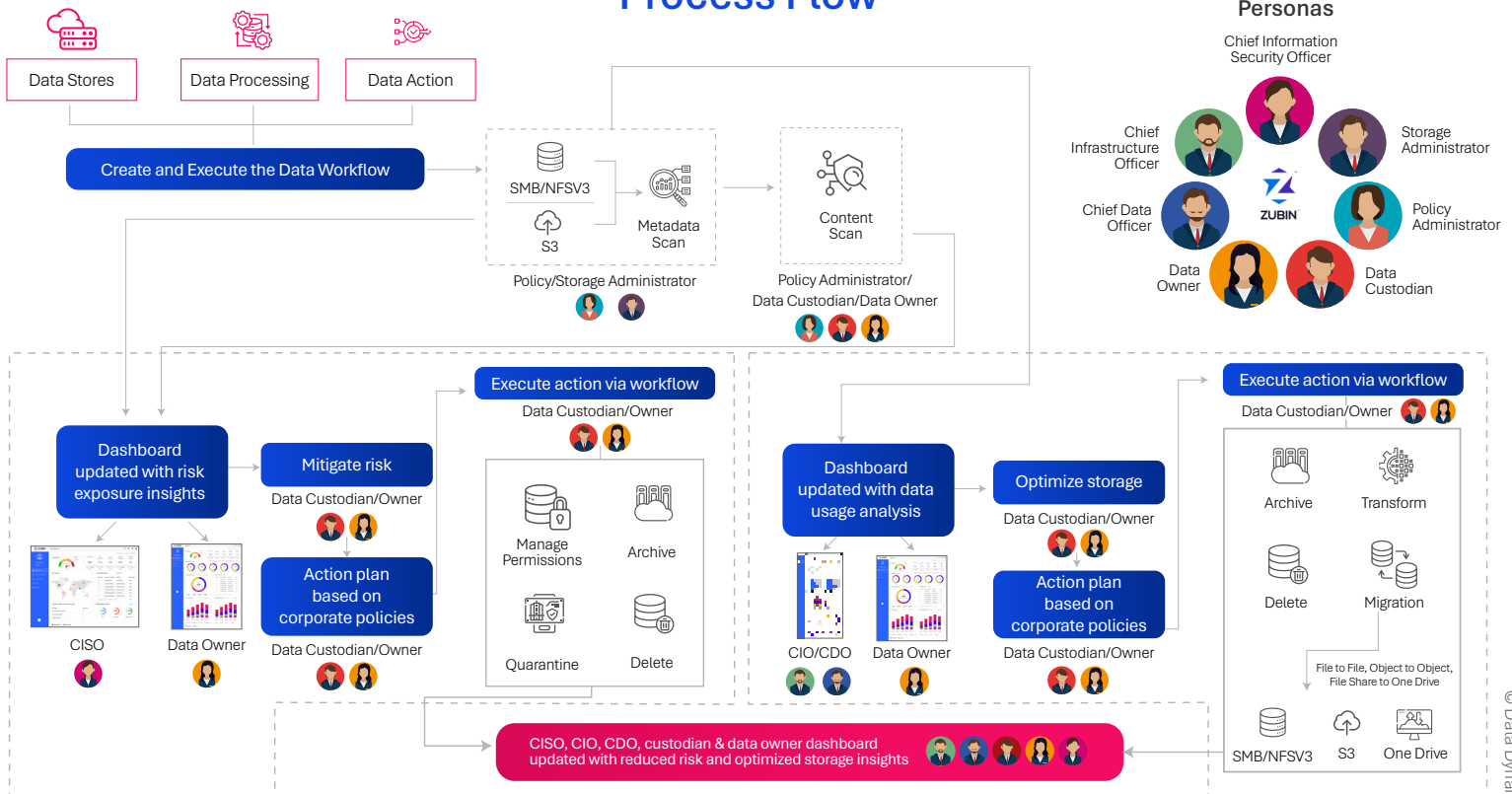
Your next chapter of success awaits; let's write it together with Zubin. **Click here for a demo**