Applying Effective Access Level Controls for Informatica Data Quality
Abstract
Successful data quality efforts rely on the expertise of many contributors from many parts of the enterprise. These contributors serve in different roles to manage the quality of the data across the enterprise. Informatica Data Quality users can define roles that grant different levels of access to different users. This article describes the factors to consider when you define roles in a data quality project.

Supported Versions
• Informatica Data Quality 9.5.1

Table of Contents
Challenge ......................................................................................................................................... 2
Description ....................................................................................................................................... 5
Logical Model: Access Management ........................................................................................... 6
Approach ...................................................................................................................................... 6
Configuring Roles ........................................................................................................................ 7
Configuring Groups ................................................................................................................... 11
Configuring Connections ............................................................................................................ 13
Configuring Projects ................................................................................................................... 15
Author ............................................................................................................................................ 18

Challenge
For many organizations, privacy and regulatory requirements, as well as internal controls on information sharing, dictate that only certain users are granted access to certain data and functions. Each function denotes a certain level of responsibility. Users and Groups may be permitted different levels of access to data and artifacts based on Published, Internal, and Secured classifications.

The types of role that you might define in a data quality project include the following:
• Administrator:
  Platform or Effort
• Developer
• Operator
• Analyst:
  Data Subject Matter Expert, Business User/Data Owner, or Staff
• Human Task Participant:
  Data Reviewer/Remediator, Data Manager, Business User/Data Owner, Data Steward
• Reporting User:
  Upper Management, Mid-Level Management, Business User/Data Owner,
  Data Manager, and Data Reviewer
• Pro-Active Monitoring Alert Recipient:
  Data Manager, Business User/Data Owner

You might also need to differentiate access between service user accounts and personal user accounts.
To further refine the data access needs for groups of users, it is probable that information access is compartmentalized on a need-to-know basis to meet confidentiality, privacy, and security regulations and policies along a Line of Business, Department, or Level of Management.

As examples, a shipping department may have access to account numbers but not Social Security or credit card numbers. The warehouse may know inventory levels but not pricing or customer data. The Commercial Loans Department has no need to access Residential Loan Department data and vice versa. Upper management needs summary data across all lines of business and departments that they are responsible for.

The Informatica Data Quality platform provides this role based environment, enabling all the contributors to seamlessly work together to ensure good quality data is made available to the enterprise.

To do so, these users need differing levels of access to the functions and features of the Informatica Data Quality platform, as well as to the underlying data. The appropriate level of access is governed by what they are vetted for as well as what they need to know to effectively manage the quality of the data as well as use the data quality artifacts given to their assigned role.

The features of the Informatica platform that provide access level controls include function privileges, roles, services, projects, connections, and groups.

Within an Informatica domain, access level controls can be assigned at the user and/or group level, with the most flexible practice being to assign them at the group level. A user can be assigned to any number of groups. A group can have any number of users. A group may contain several other groups arranged in a hierarchy that inherit the function privilege set and access level of the containing group at a minimum.

An Informatica platform role consists of a set of privileges to functions made available from a service that can be enabled or disabled. Not only can a specific function privilege be enabled or disabled, so can the entire service. A user or group can be assigned one or more roles.

An Informatica project contains a collection of data quality artifacts such as physical data objects, logical data objects, mappings, workflows, rules, and transformations as well as folders and subfolders. Access to this collection of artifacts is made available to users and groups at the project level. A user or group can be given the permission to read, write, or execute artifacts within the project. Currently there are no features that further restrict access within the project as you would find with a UNIX file system. Access to all or nothing in the project is managed at the project level.

An Informatica connection provides access level controls on a credentialed data store such as a database source or target. Access to the credentialed data store is made available to users and groups at the connection level. A user or group can be given the privilege to read, write, execute, and grant other users access on the connection.

Data owners and source system DBAs have an interest in the data they permit you to access. They are responsible for its appropriate care. They normally require that assurances and controls that they can manage are put in place to avoid unauthorized disclosure and to minimize impact to their platforms before they agree to trust you with the data.

One of the concerns when using the Informatica Data Quality platform is how to enforce column-level and row-level data access controls for personal accounts, service accounts, and group accounts. This type of access is normally handled by the underlying database role that controls access to the data for a logged in user. That Database role would restrict user access to certain views.

In Informatica 9.5.1, you can configure a connection to pass in the credentials of the user from the Developer tool. Unfortunately, that is not the case with the Analyst Service. As such, the Analyst Service uses the credentials explicitly set on the connection, or the credentials for the operating system user account that the service runs under. The Data Director Service operates in a similar way to the Analyst Service. The assumption with the Data Director Service is that you will employ one or more people as a team to review and remediate the exceptions and duplicate records on the exception model connection. The Reporting and Dashboards Service uses the
explicit database credentials configured at the data source for the reports at that level of access. Informatica Data Services, if licensed, can be used to limit access to the data based on the credentials provided. Dynamic Data Masking, if licensed, can be used to mask the data to provide limited access based on the credentials provided.

To further complicate access management, when it comes to files loaded to the server, there is no credentialed level of access. A sophisticated user in the Analyst Service can configure access to any file on the server that the underlying operating system account for the service has access to. If such access level control is required, the data must be loaded into a database — or, consider that Informatica Data Services can apply a virtual database layer complete with credentialed access to your file-based source data through a connection.

Another nuance is how to protect interim data files from non-vetted access in production, given a sophisticated user can gain access to it if left unprotected. One approach would be to encrypt this temporary data upon writing it to temporary storage and decrypt it upon reading it from temporary storage. The default approach is to delete it after use. Some clients find it sufficient to encrypt the file system and not leave data files on the server. Encrypting the data at temporary rest during execution of a job can bring with it a performance impact.

Informatica Data Quality provides a platform that enables users to rapidly prototype and implement solutions. When it comes to managing all these artifacts on a project basis, some controls and procedures should be followed. Each effort undertaken may have needs for multiple effort project folders to support shareable artifacts, deliverable artifacts, and sensitive data. These project folders can reuse published artifacts from other shared projects but should only do so in a manner that can be promoted across the migration landscape.

Once work in personal projects has been unit tested and vetted in development, they can be exported from the personal project and imported into the effort project where regression testing can be performed. Safe promotion (that is, with tested and working artifacts and established service connections) via export and import should then be possible across the landscape. It is in the best interest of the administrator to enforce appropriate project access privileges to simplify the migration effort. Note: If any services fail on the platform, the administrator and operator may need to police the interim file storage areas. If so, they will want to know where to look, as the user could configure an alternate location for temporary storage.

Given the widespread use of the internet by business today, you can protect the confidentiality and proprietary nature of the organization’s data by encrypting it while in transit. Access to the Informatica domain can be configured for Transport Layer Security and HTTPS with a certificate authority. Creation and management of users and groups can be external to the Informatica domain, notably via Lightweight Directory Access Protocol (LDAP) or Active Directory.

The challenge for the enterprise, and specifically for the Informatica platform domain administrator, is to apply all of these access control features in an manner that appropriately constrains access to those who need it while maintaining a secure but easily modified and organized set of controls that meet the needs of the business. It take pre-planning. You need to understand how the enterprise intends to use the product(s).
Management concerns include:

- Personally Identifiable Information
- Proprietary and Confidential Information
- Aggregated Information
- Ability to modify
- Ability to accept
- Ability to alert
- Masking and Scrambling
- Lower level environment security policies – Dev/Test/QA/UAT
- Obsolete data
- Trustworthiness - vetted access
Logical Model: Access Management

Approach

1. Build data access plan spreadsheet.
   - Request corresponding LDAP/Active Directory groups.
2. Configure roles.
3. Configure groups in native domain
4. Assign roles to groups
5. Assign groups to services
6. Create service database Connections
7. Assign groups to service database connections
8. Create effort projects
9. Assign groups to effort projects
10. Create personal projects
11. Create users in native domain
12. Assign users to groups
13. Assign users to personal projects
14. Assign users to the appropriate reporting and dashboards level
15. Configure LDAP/Active Directory
16. Assign all LDAP groups in similar model created for native domain.

**Configuring Roles**

The roles defined in this section correspond to what is likely for an enterprise data quality initiative. Your needs may vary, but it is best to make a plan for what you need. Roles will vary based on your licensing and intent. You may only need to support a subset of the products and roles listed herein. There may be additional roles needed. A person may serve in multiple roles in your effort as well as on multiple efforts. By recognizing there are multiple roles, you add the ability to more cleanly manage the work and provide vetted access to perform the tasks.

**Platform Administrator**

The Platform Administrator manages the applications installed. The Platform Administrator installs the software and any version upgrades, Hot Fixes and Emergency Bug Fixes. The Platform Administrator is responsible for maintaining and keeping current any subscription content.

The Platform Administrator needs operating system level access to the server platform. On a Windows platform this should be an administrator. On UNIX, they may need to work with the UNIX administrator to prepare the platform for the application.

The Platform Administrator may need to work with the network support team to resolve firewall and port provisioning as well as encryption requirements. The Platform Administrator will need to work with the Database Administration team to appropriately configure the database to support the application as well as specify the application-specific service accounts and passwords.

The Platform Administrator needs to have a thorough understanding of the policies for handling data to avoid unauthorized data breaches that were put in place for the organization.

The Platform Administrator configures the services and implements the data access plan for data quality. The Platform Administrator will create projects for the out-of-the-box content.

**Effort Administrator**

The Effort Administrator usually serves as the Project Lead. The person who serves in this role is usually the front-line manager for the project. This person can either grant access or approve access for staff assigned to the project in any capacity. With LDAP or Active Directory implemented, the Effort Administrator may not need access to the Security tab of the domain. Allocation of personnel to groups can be performed externally to managing security.

The Effort Administrator is also responsible for project migration throughout the platform landscape. The Effort Administrator exports completed and unit tested work from personal projects and imports the work into the base project. The Effort Administrator may verify the work and perform some regression testing, as well as grant the developer or analyst the ability to further test the work in the project folder before promotion to the next level in the platform landscape.

The Effort Administrator will create projects for specific efforts and assign the appropriate groups and permissions to the projects and connections. The Effort Administrator will work closely with the Platform Administrator to accomplish this in a manner that verifies secure data access in conformance with the policies of the enterprise.

The Effort Administrator is likely to have some access to Metadata Manager with Business Glossary, if licensed.

**Read-Only Analyst**

For some customers there is a need to provide a Read-Only Analyst role. The users in this role are those who want to see deliverable artifacts through the Analyst Service, reflecting summary
results, but do not want to drill down into the data or change it by re-running the profile or scorecard.

This role is more common in organizations that have not implemented the Dashboards and Reports template for enterprise-wide data quality reporting. It gives upper and middle management the ability to review the work in progress and learn about data quality issues.

**Basic Analyst**
The Basic Analyst role provides the ability to drill down and export results as well as to create profiles and scorecards from data objects and access mapping specifications. It is an enhanced version of the Read-Only Analyst role for those users who need to review detailed data and create simple data quality checks. It provides hands-on managers like the Data Manager with the ability to create simple metrics.

More sophisticated rule development may require engaging an Analyst, Power Analyst, or a Developer.

**Analyst**
The Analyst role includes all the capabilities of the Basic Analyst as well as the ability to manage mapping specifications, reference tables, and scorecard notifications. Most Data Analysts will have this role.

The Analyst is primarily responsible for identification of all data quality issues and composition of simple rules with out-of-the-box rule content to identify them as well as propose possible corrections to the data. More sophisticated rule development (multiple or complex transformations) may require engaging a Developer.

The Analyst usually reports to the Data Owner.

The Analyst is likely to have some access to Metadata Manager with Business Glossary, if licensed.

**Power Analyst**
The Power Analyst includes all the features of the Analyst as well as the ability to manage connections, load flat-file data objects, create profile models (with an Informatica Data Explorer License), and Manage the Data Domain Glossary (with an Informatica Data Explorer license). This role represents a fully-functional Analyst Service user.

The Power Analyst will also need the Developer tool installed to support some Informatica Data Explorer features, such as Profile Models.

The role of the Power Analyst is not to develop mappings or web services. More sophisticated rule development (including multiple or complex transformations) may require engaging a Developer.

The Power Analyst usually reports to the Data Owner.

The Power Analyst is likely to have some access to Metadata Manager with Business Glossary, if licensed.

**Developer**
The Developer role supports the Basic Analyst, Analyst, and Power Analyst with sophisticated rule development on request.

The Developer builds **data quality-specific** mappings, workflows with Human tasks, and web services in support of data quality initiatives such as a Data Warehouse, Marketing Data Mart, Object Data Store, Data Quality Monitoring Dashboard Star Schema, Master Data Management, ERP, MRP, Shipping, Mail Room, and other initiatives.

The Developer is the full-featured Model repository user. The Developer is likely to be configured as a Power Analyst as well.

The Developer is likely to use only the service connections provided by the Effort Administrator.

The Developer will create deliverables to be run in the background by the Operator.
The Developer is likely to have some access to Metadata Manager with Business Glossary, if licensed.

**Operator**

The Operator will manage the operational effort on the platform to run, on a regular frequency, the deliverable data quality artifacts in published and internal project folders, such as profiles, scorecards, mappings, and workflows, for all efforts undergone by the enterprise within expected service-level agreements (SLAs).

The operator is the front-line reviewer of the results and verifies that the SLAs are met. When SLAs are not met, the Operator is responsible for engaging the Platform Administrator, should any platform issues crop up on the platform, and the Effort Lead.

**DataReviewer**

The Data Reviewer or Data Remediator is the front-line data entry person responsible for entering the data correctly. The role includes the first-line staff who report to the Data Manager to review or fix exceptions. The Data Reviewer will use the Data Director Service to perform Human tasks. Fully-configured workflows with e-mail notifications for Human tasks should alert the appropriate members of the Data Team (Data Reviewer, Data Manager, Data Owner, Data Steward) about the exceptions.

**Data Manager**

The Data Manager reviews and approves the work of Data Reviewer/Remediator. The Data Manager will use the Data Director Service to review the work done in the Human tasks.

The Data Manager is also likely to be a Basic Analyst, so that they can create profiles and scorecards to highlight issues in the data with Pro-Active Monitoring for Data Quality (if licensed) before the problems in the data make it downstream and affect the business.

The Data Manager manages staff to handle exceptions or unresolved duplicates.

The Data Manager is likely to have some access to Metadata Manager with Business Glossary, if licensed.

**Data Owner**

The Data Owner (that is, the Business Owner or Business Data SME) reviews the work of the Data Team with a focus on business value. The Data Owner is responsible for the use of the data as applied to the business need. The Data Owner is usually the driving manager or champion for the use of an application by the business.

The Data Manager is also likely to be a Basic Analyst, so that they can create profiles and scorecards to highlight issues in the data with Pro-Active Monitoring for Data Quality (if licensed) before the problems in the data can affect the business.

The Data Owner works closely with the Data Manager to determine the priorities for handling exceptions and unresolved duplicates.

The Data Owner is likely to have some access to Metadata Manager with Business Glossary, if licensed.

**Data Steward**

The Data Steward is primarily an overseer who reviews the handling of exceptions and unresolved duplicates from an effort or enterprise standards perspective.

Multiple Data Stewards may have an interest in the data. They can come from an IT discipline, Data Governance team, or they can be a specific business data subject matter expert. Their interest can reflect enterprise, line of business, middle management, or effort perspectives.

They are likely to have advanced access to Metadata Manager with Business Glossary, if licensed.
The Data Steward reviews the work of the Data Team with respect to standards conformance. The Data Steward is likely to also be a Power Analyst.

Reports Consumer
The Reports Consumer role covers anyone in the enterprise who needs to view data quality reports and dashboards. The specific data quality reports they may view depend upon the level and department of the organization they belong to.

The user with the Reports Administrator role configures the access level for users with the Reports Consumer Role within the business intelligence reporting tool (out-of-the-box Jaspersoft). The Reports Consumer role is used by Unit Managers, Line of Business Managers, Middle Managers, C-Level Managers, Unit Managers, Data Stewards, Data Reviewers/Remediators, Reports Developers, and all flavors of Analysts. The dashboards and reports that they view reflect the data in the Dashboards and Reports Template.

The Reports Consumer accesses the artifacts available from the business intelligence reporting tool (out-of-the-box Jaspersoft).

Reports Developer
The Reports Developer role involves the use of the Developer tool and iReportsDesigner. The Report Developer role is used by developers to create and modify reports (including out-of-the-box reports) that point to the Dashboards and Reports Template Star Schema. The Developer tool and the iReportsDesigner are thick clients.

Reports Administrator
The Reports Administrator manages user and group access to the vetted set of reports and data sources based on the levels in the organization. The business intelligence reporting tool (Jaspersoft) can integrate with LDAP or Active Directory, so user assignment to specific groups can be managed at another level within the organization.

The Reports Administrator differs from the Platform Administrator and Project Administrator. The Platform Administrator installs the out-of-the-box reports and dashboards. The Platform Administrator may assist the Project Administrator to migrate developer reporting artifacts. The Project Administrator would be responsible for establishing the service-level passwords. Individuals can be moved around externally via LDAP or Active Directory changes.

Alert Recipient
The Alert Recipient Role is included here for consideration in future applications. The Alert Recipient Role would be used with Pro-Active Monitoring of Data Quality. Pro-Active Monitoring is not fully integrated into the current domain. Once it is, this role will likely include Data Managers and Data Owners. Currently, it would include these users insofar as these reflect the e-mail addresses used in most alert configurations for data quality issues. Other roles used by Pro-Active Monitoring for Data Quality would include the RulePoint and Real-Time Alert Management (RTAM) Administrator roles, as well as specific configuration roles. Pro-Active Monitoring differs from the e-mail generated with Scorecard notifications or with Human task notifications, as it filters the notifications by issue and priority.

Business Glossary User
The Business Glossary User role is represented in the domain configuration with the View Glossary, Draft/Propose Terms in Glossary, and Manage Glossary feature privileges under the Metadata Manager Service Configuration. The Business Glossary Desktop is a service tray-based popup installed on the client. It communicates with the Metadata Manager Service to provide end users with easy search capabilities based on the metadata contained in the Metadata Manager repository.
MM Advanced User
The Metadata Manager Advanced User is essentially the Administrator for the Metadata Manager Service. This role is not intended for installations but for ongoing configuration as metadata sources are added or removed. All features of the Metadata Manager Service are available with this role. This includes all features of Load, Model, Catalog, and Security. The Metadata Manager Advanced User role is normally included as a function of a Data Steward as well as Platform Administrator and Effort Administrator.

MM Intermediate User
The Metadata Manager Intermediate User role reflects the needs of the typical business analyst. It includes the ability to View the Glossary, Load and View a Metadata Resource, View Model, Catalog, Lineage, Related Catalogs, Reports, Profile Results, Relationships, Comments, and Links, as well as Post and Delete Catalog Comments and Manage Links. Both hands-on Developers and Analysts are normally given this role. Data Owners and Data Managers are often given this role also.

MM Basic User
The Metadata Manager Basic User role reflects the needs of the limited user who would have no need to propose specific changes to the architecture but may need to identify the impact of changes or exception data, such as a Read-Only Analyst, Basic Analyst, Reports Consumer, Data Reviewer or Operator. It includes the ability to view the Model, Catalog, Related Catalogs, Lineage, Relationships, Comments, and Links through the Metadata Manager Service.

Configuring Groups
Note: nesting can reduce the keystrokes required to grant permissions and privileges on services, connections, and projects within the domain.

Enterprise-Effort Hierarchy
Most Enterprise Data Quality initiatives consist of several complimentary but distinct efforts. There usually remains a need at the enterprise level to specify access across all the efforts for enterprise purposes, including auditability, reusability, and providing support for common standards. In addition there can be subordinate efforts within an effort.

The effort reflects the use by the business. Common efforts include support for Sarbanes-Oxley, Basel, fraud avoidance, privacy management, enterprise data governance, data quality monitoring, data warehousing, and marketing data marts.

There is a hierarchy and need to share certain artifacts between the efforts and the enterprise. The hierarchy can be reflected in the creation of nested groups.

LDAP and Active Directory
Creating the appropriate LDAP or Active Directory groups for the enterprise usually involves making a request to the network security group. The process can take time to complete. In the interim, configure what you have designed in the Native domain, so you can verify that it will meet the needs of the business and the enterprise policy for data access security.

You can verify the configuration with temporary accounts that you create and distribute to the data quality effort team until the LDAP/Active Directory Manager can make the change required for you to use LDAP/Active Directory.

There are numerous examples of how to configure LDAP and Active Directory user and group filters online. From past experience, there appear to be differences in setup at every company, most likely for security purposes. However, once you have LDAP or Active Directory configured in the security domain, you can replicate the roles as appropriate to the new groups as you modeled in the Native Domain.
Figure 3: Informatica Administrator Security, LDAP Configuration – LDAP Connectivity

Figure 4: Informatica Administrator Security, LDAP Configuration – Security Domains
Figure 5: Informatica Administrator Security, Privileges tab – Edit Roles and Privileges

Configuring Connections

Groups can be assigned to Connections and configured for Read, Write, Execute, or Grant access on the connection. Execute access is needed for drilldown. Read access is needed to view the data.

Figure 6: Informatica Administrator Connections
Database Service Accounts Level

If users in specific groups have the same level of access to a connection that points to a database, they can be granted access via a single database service account.
This level of access makes sense for operational purposes in producing deliverables as well as in some development and testing efforts. It may or may not be applicable for production data—typically it is not used for production data, as most production sources contain both sensitive and non-sensitive data. Enterprise applications are also used by different departments for different purposes.

Individual/Personal Database Account Level

There are two ways to configure a connection to further restrict access to a data source based on database role. You can create a specific connection that only the individual user may be granted access to, or you can enable pass through security. If pass through security is enabled and operating as intended, the user login credentials to the domain may be used to further restrict access to just the database role of the individual user.

When the artifacts are explored from individual/personal projects on the designated ad-hoc profiling platform for production data, separate connections are an appropriate solution. When the artifacts are explored from a shared project folder, data access restrictions may be better served with the enterprise level LDAP domain access to the database. When the database credentials differ from the user login credentials to the domain, use SSO (Single Sign On) to implement user credentialed data access controls.

Configuring Projects

As previously mentioned, access to artifacts in Informatica Data Quality is controlled at the IDQ Project level. A project may contain additional folders and subfolders, but these are not like folders in a directory on UNIX. Access is granted at the Project level only. As a result, you are likely to use several projects to meet the needs of the effort.

The standardized use of folders can assist with integration. What works best is to export and import objects from the Effort Project folder to your personal folder to work on them. When unit development and testing are complete, export the work from your personal folder and import it to the Effort Project folder. The Effort Project folder then becomes an integration project and goes through integration testing.
Some reasons for additional projects in an effort include:

- Enterprise-effort reusability of common artifacts like transformations, rules, mapplets, profiles, and physical or logical data objects.
- The need to provide published deliverables that may be shared.
- The internal team integration folder contains artifacts that may not be shared.
- Separate projects compartmentalize access to sensitive data.

As it takes people to work on a project, individual or personal projects need to be created. It is not good practice for multiple people to work on the same set of artifacts at the same time, which usually happens if individual or personal projects are not present.

**Enterprise-Effort Reusability**

Reusability of standard artifacts reduces development and testing efforts. In order to promote the reuse of standard artifacts, they need to be made accessible to groups (or the nested overseeing group) at the project level.

The out-of-the-box Informatica_DQ_Content project contains content that everyone should have read access to. Each effort, including the enterprise, should also have a project containing those artifacts that it wants to share with other Efforts or with the enterprise. In support of profiling efforts with the Analyst Service, this typically includes reusable rules that can be leveraged. It can also include reusable transformations, reference tables, sample physical data objects, sample profiles, and scorecards. For Developers, it may even include sample mappings, mapplets, applications, and workflows with Human tasks. With a license for Informatica Data Explorer, it may include custom data domains. Profile models would not likely be kept in this project.

To reduce maintenance, reusing artifacts from this project should be done by reference and not by copy.

**Shared/Published**

The Shared or Published project for an effort (including the enterprise) would include deliverable artifacts that are updated on a regular basis to meet SLAs. These would normally be shared with groups further up in the organizational hierarchy. The level to which they are shared would depend on the needs of the reporting or auditing level.

This project may contain profiles, scorecards, and physical and logical data objects that point to connections that those groups with the Operator role may read, write, and execute. Other roles and groups with vetted and relevant access may only have read access to the artifacts (or perhaps read and execute access for drilldown to detailed data). The connections available from this project point to actual data and not to the mockup data sets that can be made available in the Effort Reusable Artifacts project.

This project may also contain applications, web services, mappings, mapplets, transformations, reference tables, workflows, and Human tasks reflecting deliverable items for operational use. Reusable artifacts from the Effort Reusable Artifacts project should be used by reference to the maximum extent possible. Additional rules and other artifacts contained therein are not intended for distribution outside the project, and they should not be leveraged in any way by other efforts, as they are subject to change to support existing deliverables. They can still be made visible to those users vetted with access to the published folder.

**Internal/Team/Integration/Private**

The Team project contains artifacts that are not intended for sharing outside the team, such as work in progress. Work in progress may include logic undergoing integration testing and past versions of artifacts. It may include exploratory work intended for use only by the team, such as profile models and specific profiles. This is essentially an Integration project where groups with the Project Administrator role can import and export project work. Groups with the Operator role can run and verify integrated developed artifacts. Depending on your security and data access policies, the artifacts can include physical and logical data objects that are reused by reference by team members from individual or personal projects where development or analysis is being
performed. Once the work is integrated and verified, it can be packaged and exported for use in the Published project to meet SLAs or the Effort Reusable Artifacts project to promote reusability.

**Personal/Individual Workspace**

The Personal or Individual project is specific to a user. This is where development and analysis is performed. This insulates the artifacts produced by the effort from getting unintentionally stepped on and changed when there are multiple people involved in the effort with access to the Effort Projects. The folder structure of this project should reflect the folder structure of the Integration project, e.g.

```
Enterprise_Integration
  Dashboards_And_Reports
    ADDRESS
    CONTACTS
  BASEL_II
    SOURCEA
    SOURCEB
    TARGETC
  MDM

z_mgagnon
  Enterprise_Integration
    Dashboards_And_Reports
      ADDRESS
      CONTACTS
```

This approach permits the Project Administrator to export the current relevant set of artifacts from the Integration project and then add them to a version control system. The export should be named in a standard way with the Project and Folder being worked on. Then the exported file can be imported to the personal project of the individual working on it. Anyone who wants to work on it can see who has checked it out, and they can either wait for it or move onto other work. When the individual has completed the work, it can be exported and checked back in to the version control system. The Project Administrator can then import it to the Integration project at the relevant level. The individual can organize work into multiple folders under the personal or individual project.

**Sensitive Data**

The three types of Effort project folders described above are further complicated by regulatory requirements to protect sensitive data. Some reusable artifacts, some deliverables, and some integration projects need to be separated according to whether they are relevant to sensitive data or non-sensitive data. There is a need to prevent sensitive data breaches as well as to ensure vetted access. In essence the needs for the four types of projects depicted above can be duplicated.

For example: