Oracle® Enterprise Governance, Risk and Compliance

Security Implementation Guide

Release 8.6.4.7000

Part No. E40662-01

May 2013

ORACLE

Oracle Enterprise Governance, Risk and Compliance Security Implementation Guide

Part No. E40662-01

Primary Author: David Christie

Contents

A Appendix

Preface

This Preface introduces the guides and other information sources available to help you more effectively use Oracle Fusion Applications.

This *Implementation Guide* is meant to provide helpful guidance on the usage of the product. Think of this document as a combination FAQ and helpful "Tips and Tricks."

It is a supplement to the official product documentation (such as the *User Guide* and *Installation Guide*), and is not intended to replace it. If discrepancies exist between this *Implementation Guide* and the official product documentation, the guidance and functional commentary provided by official documents supersede any that may be written here.

Disclaimer

The information contained in this document is intended to outline our general product direction and is for informational sharing purposes only, and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided life cycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository

Oracle Enterprise Repository provides visibility into service-oriented architecture assets to help you manage the life cycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Publishing other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

The Oracle Fusion Applications information is provided as a solution pack that you can upload to your own deployment of Oracle Enterprise Repository. You can document and govern integration interface assets provided by Oracle with other assets in your environment in a common repository.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww@oracle.com. You can use the Send Feedback to Oracle link in the footer of Oracle Fusion Applications Help.

1

Enterprise Governance, Risk and Compliance Security Overview

Oracle Enterprise Governance, Risk and Compliance (GRC) is a set of components that regulate activity in business-management applications:

- Oracle Application Access Controls Governor (AACG) and Oracle Enterprise Transaction Controls Governor (ETCG) enable users to create models and "continuous controls," and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk. These applications are two in a set known collectively as "Oracle Advanced Controls."
- Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's strategy for addressing risk and complying with regulatory requirements. In enables users to define risks to the company's business, controls to mitigate those risks, and other objects, such as business processes in which risks and controls apply.
- Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in EGRCM, AACG, and ETCG.

These GRC components run as modules in a shared platform. AACG and ETCG run as a Continuous Control Monitoring (CCM) module. EGRCM provides a Financial Governance module by default, and users may create other EGRCM modules to address other areas of the company's business.

Because these components share a common platform, they also share a system for securing GRC functionality and data. In this system, duty roles define narrowly focused sets of privileges and are then combined into broader job duty roles. Primary data roles specify narrowly focused sets of data and are then combined to form broader composite data roles. Finally, job roles combine job duty roles with composite data roles, and are assigned to users.

Moreover, administrators can define perspective hierarchies, each of which is a set of related values. Users can associate individual perspective values with individual objects (such as EGRCM risks or models in AACG or ETCG). A composite data role may be associated with perspective values, and if so would grant access only to data concerning objects associated with those perspective values. Assuming, for example, that a Region perspective includes a US value, and a Business Process perspective

includes an Order to Cash value, it would be possible to create roles that permit access only to data associated with the Order to Cash process in the US region.

Preparing the Web Browser

Either the Internet Explorer or Firefox web browser can display the GRC user interface. If multiple users share a single computer, and web browser security settings on that computer are not configured properly, the browser cache may provide each user with access to other users' privileged data. To prevent this from happening, configure web browser security settings as follows.

Internet Explorer Security Settings

To configure Internet Explorer for shared access to GRC:

1. Open Internet Explorer and select Internet Options from the IE Tools menu.
2. Select the General tab of the Internet Options window.
3. In the Browsing History section, select the "Delete browsing history on exit" check box.
4. If the GRC application is set as a favorite site in IE, click the Delete button in the Browsing History section of the Internet Options window. A Delete Browsing History window opens. In it, clear the "Preserve Favorites website data" check box. Click the Delete button.
5. Optionally, limit the amount of data stored in the temporary internet files directory when GRC is run. Select the Security tab of the Internet Options window; select the Trusted Sites icon. Then do either of the following:
   - Click the Sites button and, in a Trusted Sites window, look for the GRC URL in the Websites field. If it exists there, select it and click the Remove button. Then click the Close button. (This makes GRC a member of the more restrictive "Internet" zone.)
   - If removing GRC from the Trusted Sites zone is not feasible, select the Enable Protected Mode check box in the Security tab of the Internet Options window. (This assumes that the Trusted Sites zone is set to its default security level, Medium. This limits the amount of data cached locally for all Trusted sites, not only for GRC.)
6. Select the Apply button to record your changes, and then to OK button to close the Internet Options window.
7. Restart Internet Explorer.

To test the security settings, start Internet Explorer and use the GRC application. Log off of GRC and go to the temporary internet files location. (Once again, select Tools > Internet Options. In the Browsing History section of the General tab, select the Settings button. A Temporary Internet Files and History Settings window opens; select its View Files button.) The location should contain no files.

As they log on to GRC, users may also select the Internet Explorer "InPrivate Browsing" feature.

Firefox Security Settings

To configure Firefox for shared access to GRC:

1. Open Firefox and select Options from the Tools menu.
2. Select the Privacy tab of the Options window.
3. In the History section, select "Use custom settings for history" in the "Firefox will" field. Then select the "Clear history when Firefox closes" check box.
4. Click the Settings button. A Settings for Clearing History window opens. In it, select the "Offline Website Data" check box, and click the OK button.
5. In the Options window, click the OK button.
6. Restart Firefox.

To test the security settings, start Firefox and use the GRC application. Log off of GRC and close Firefox. Go to the temporary internet files location and confirm that it is empty.

Security Checklist

To set up security in GRC, complete the steps in the following checklist. You must complete the steps identified as required. Complete the optional step only if you want to use the functionality implemented by that step.

Each step is described in further detail later in this document. In addition, the description for each checklist step includes a reference to a section and chapter of related documentation, or the current document, where you can find full information about the procedures for completing each step.

☐ 1 **Required:** Review delivered duty roles and, if you deem it necessary, create new duty roles.

The application is delivered with a set of duty roles that are collections of functional tasks to be performed within the various areas of the application. The functionality included in each duty role represents work the user can perform within a job role. What is delivered may or may not align with how your organization segregates work responsibilities, or a delivered duty role may have functionality you do not wish to use. If you need to make changes, create a new duty role by copying one that was delivered, and then removing or adding functionality.

See the "Security Administration" chapter (page 2-1), as well as "Managing Roles" in the *GRC User Guide*.

☐ 2 **Required:** Review delivered data roles, and consider using them as foundations for new roles that add perspective filters.

Data roles define the data to which users have access within their job roles. A primary data role selects data associated with a module, one or more object states, and an action that can be performed at the specified states. A composite data role combines primary data roles and may be associated with one or more perspective values; if so, it grants access only to data also associated with those perspective values.

For AACG and ETCG, three system perspectives — CCM Type, Business Object, and Datasource — are seeded in composite data roles for the CCM module. So by default, seeded CCM job roles for managing models, controls, conditions, and incident results allow access to Transaction and Access (CCM Type) data, as well as all datasources and business objects. Consider creating new composite data roles with additional perspective filters that define appropriate security access.

For EGRCM, no perspective filters are delivered with the data roles, since they are totally dependent on the perspectives you choose to use for each module. The product is delivered with a set of composite data roles for the Financial Governance module for each of the delivered job roles. Consider creating new custom data roles that reference the seeded composite data roles and add the perspective filters necessary to define appropriate security access.

Perspective hierarchies must be defined prior to the creation of data roles, since they form the criteria used in the data roles.

See the "Security Administration" chapter (page 2-1), as well as "Managing Roles" and "Managing Perspectives" in the *GRC User Guide*.

☐ **3** **Required:** Review delivered job duty roles and, if necessary, create new job duty roles.

A job duty role is a collection of duty roles, and it defines the tasks performed by a user assigned a job. GRC is delivered with a set of job duty roles for each delivered job role that align with the best practices of the functionality performed with each job. However, as with the duty roles, these job roles may not match your organization's requirements. If you need to make changes, create a new job duty role by copying one that was delivered, and then removing or adding functionality. Or, create a new job duty role from scratch.

See the "Security Administration" chapter (page 2-1) as well as "Managing Roles" in the *GRC User Guide*.

☐ **4** **Required:** Review delivered job roles and, if necessary, create new job roles.

A job role combines the functional privileges of the job duty role with data roles to define what tasks are performed against which set of data. The job role is assigned to users. The product is delivered with a set of job roles, but as with the duty roles and job duty roles, these job roles may not meet the requirements of your organization. If you need to make changes, create a new job role: Copy a delivered job role, then remove or add functionality. Or, create a new job role from scratch.

See "Job Roles" (page 2-6) and "Constructing Job Roles" (page 2-19), as well as "Managing Roles" in the *GRC User Guide*.

☐ **5** **Required:** Define users and grant them roles.

You can import users from LDAP or define them directly in the application. Functionality can be granted to the user only through the addition of job roles to the user's profile.

The product is seeded with one user, called admin, which has been granted all functional job roles except those for reviewing and approving job roles, or viewing GRCI dashboards. It's recommended that you create a new user by copying the admin user, and that you update this user to have access to all the operational data for all modules — i.e., a super user.

See "Define a User with Access to All Operational Data," page 2-21, as well as "Managing Users" in the *GRC User Guide*.

☐ **6** **Optional:** Run security administrative reports to review users and roles:

- Review the Role Assignment report to ensure users are assigned the correct roles.
- Review the Unassigned Perspective Values report to verify that all the appropriate perspectives are referenced within a data role.
- Review the Record Assignment report to see what records a particular user might have access to.
- Review the Inaccessible Records report to see what records may be orphaned based on the security setup.

2

Security Administration

GRC security employs a standard role-based access control (RBAC) model. You can combine security components — privileges, data roles, duty roles, and job roles — to define "who can do what on which set of data." The "who" is a user assigned a job role. Within the job role, two types of duty role (which ultimately invoke sets of privileges) determine the "what," and data roles determine the "which set of data."

This structure supports reusability: To define new job roles, you can use a given functional-access definition (set of duty roles) over and over again with varying data-access definitions (sets of data roles). Likewise you can use a given data definition with any number of functional definitions. Keep the concept of reusability in mind as you build out duty and data roles.

Security Components

GRC assigns individual users distinct combinations of rights to data and to functionality. To define access to functionality, it uses these components:

- A "privilege" is a specific feature GRC can make available to users.
- A "duty role" is a set of privileges. Each duty role defines one or more tasks a user can complete in the application — for example creating controls, or approving changes to them.
- A "job duty role" is the conceptual name for a job role that selects a set of duty roles. It encompasses the functionality a user needs to do a large-scale job such as Control Manager or Risk Manager.

To define access to data, GRC uses these components:

- A "primary data role" defines a narrowly focused set of data — at a minimum, that which exists at one or more specified states and is subject to a specified action. If a primary data role is to grant access to Financial Governance or CCM data, it also specifies the appropriate module.

  If a primary data role supports assessment activities in EGRCM, it further selects data associated with a specified value for a seeded perspective called Activity Type.

  If a primary data role supports work with CCM models, continuous controls, or incident results, it specifies a value for a seeded CCM Type perspective, which distinguishes between data for use by AACG and data for use by ETCG.

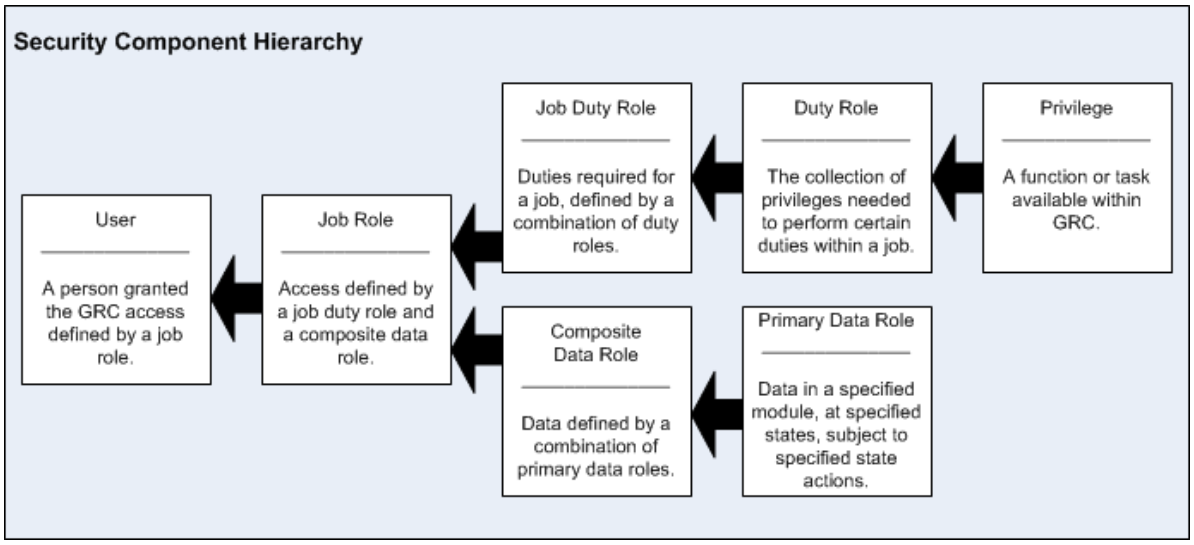
- A “composite data role” defines a more broadly focused set of data, to which a user can apply the functionality granted in a job duty role. It may specify primary data roles, or other composite data roles, to combine the access granted by them.

  There are specialized composite roles: A “custom perspective data role” limits the access defined by its constituent roles to data associated with specified perspective values. A “module data role” limits the access defined by its constituent roles to data belonging to a specified custom module. (Such a role would be created only for a custom module. For Financial Governance or CCM roles, the module is specified in a primary data role.)

To combine functionality and data access, GRC uses these components:

- A “job role” comprises a job duty role and a composite data role (or custom perspective data role).
- Each EGRCM user is assigned one or more job roles.

The following figure illustrates the relationships among these components.



Privileges

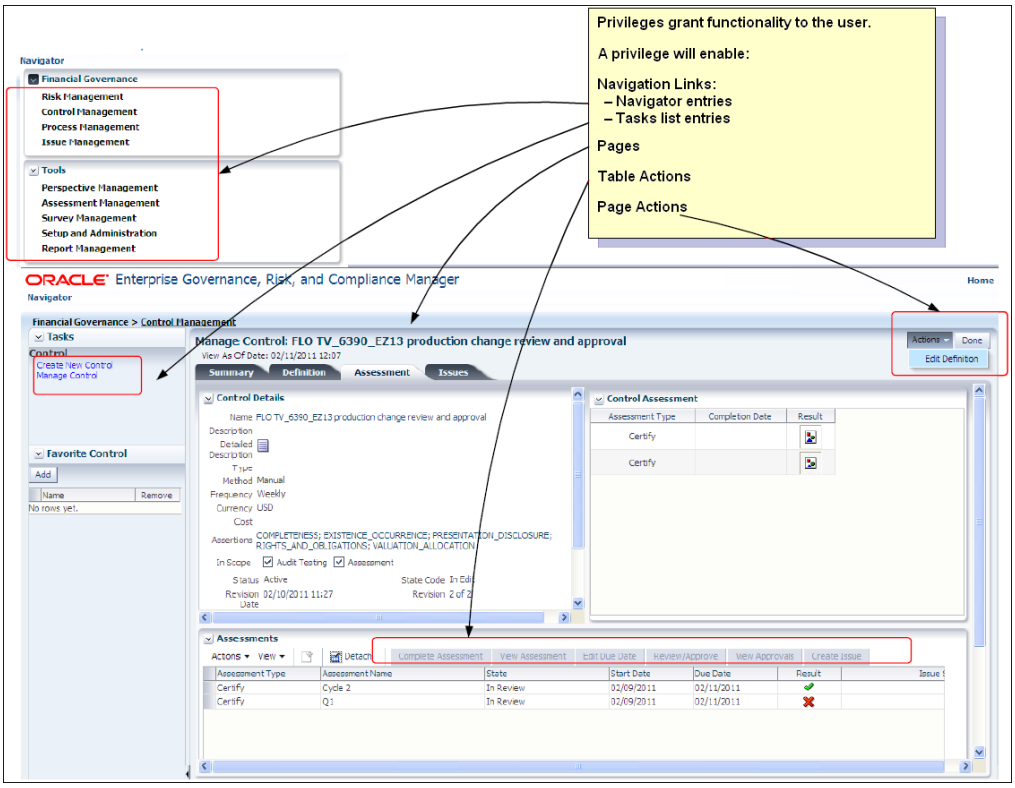
A privilege is the most granular aspect of functional access — a reference to a specific application resource, and the means to grant functional access to the user. Each privilege has a name that describes its functionality, a navigator entry identifying the navigator component in which it is included, and an activity identifying the type of activity it is part of. The following table contains a few privileges for EGRCM controls:

Navigator	Activity	Privilege
Control Management	Control Management	View Control
		View Control Approval History
		View Control Assessment Approval History
	Control Maintenance	Create Control
		Delete Control
		Create Control from Related Components
		Edit Control

Navigator	Activity	Privilege
Control Management	Control Maintenance (continued)	Create Issue for Control Definition
		Review Control Changes
		Approve Control Changes
	Control Assessment	Create Control Adhoc Assessment
		Create Issue for Control Assessment

Privileges are seeded within the application and cannot be created by the user.

A privilege grants the user access to a page, but it also enables navigation links as well as page and table actions. The following diagram illustrates elements of the user interface that can be enabled by a privilege.



Duty Roles

A duty role is a collection of privileges. Each represents a set of functional tasks needed for a unit of work within the application — a particular aspect of work to be performed. The following list presents a few EGRCM control duty roles, and their privileges:

- Create New Control: Privileges include Create Control and Delete Control.
- Control Management: Privileges include Create Control, Create Control from Related Components, and Edit Control
- Control Viewing: Privileges include View Control, View Control Approval History, and View Control Assessment Approval History.
- Review Control: Includes the Review Control Changes privilege.
- Approval Control: Includes the Approve Control Changes privilege.

Job Duty Roles

The job duty role is a type of job role that defines the functionality for a job, but does not contain the data access roles. It is a collection of duty roles. The job duty role represents the full set of functionality a user needs to be granted to perform a large set of integrated tasks.

For example, in EGRCM the Control Manager Job Duty Role contains the following duty roles: Create New Control, Control Management, Create Issue for Control within Control Management, Create Issue for Control Assessments, Control Viewing, Control Assessment Result Viewing, and Control Reporting.

Primary Data Roles

The primary data role is the most granular level of data access. It contains filters that select operational data according to its base attributes:

- The module with which the data is associated.
- The state of the data within the application workflow.
- The state action that can be performed against the data in its identified sate — for example, Create/Edit, Delete, or View.

There is a primary data role for each basic action for each of the objects.

For example, an Edit Control Primary Data Role contains three filters, and the role grants access to data for which all three filters evaluate to true:

- A filter selects data for which a Module attribute is set to Financial Governance.
- A filter selects data for which a State attribute equals any of New State Control, In Edit State Control, Rejected State Control, or Approved State Control.
- A filter selects data for which an Action attribute equals Edit.

Oracle has provided a complete set of primary data roles for all the core entities. The naming convention for primary data roles is: *"State Action" "Entity Name" Primary Data Role* (for example, Edit Control Primary Data Role). This distinguishes them from other data roles.

Assessment Activity Primary Data Roles

In EGRCM, a primary data role that supports assessment activity contains a filter to identify the type of activity the role supports; each grants access only to data appropriate to its type of assessment activity. The filter specifies a value for a system perspective called Activity Type. A primary data role that includes any Assessment Results state must include a filter for the Activity Type perspective.

The Activity Type perspective is not available within Perspective Management and is used only for the definition of assessment activity primary data roles.

For example, Control supports four types of assessment activity: Operational Assessment, Design Review, Audit Test, and Certification. So in the Financial Governance module, instead of one primary data role for Complete Control Assessment, there are four, one for each assessment activity type.

All four contain three identical filters:

- A filter selects data for which a Module attribute is set to Financial Governance.
- A filter selects data for which a State attribute equals any of the following: New State Control Assessment Results, In Edit Assessment Results, Rejected State Assessment Results.
- A filter selects data for which an Action attribute equals Edit.

But each of the four contains a distinct Activity Type filter:

- Complete Control Operational Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Operational Assessment.
- Complete Control Design Review Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Design Review.
- Complete Control Audit Test Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Audit Test.
- Complete Control Certification Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Certification.

Model, Continuous Control, and Incident Result Primary Data Roles

In CCM, each primary data role that supports models, controls, and incident results contains a filter that selects a value for a system perspective called CCM Type. The value — Access or Transaction — determines the type of CCM object the role supports; each grants access only to data appropriate to its type. A primary data role that includes any model, control, or incident result state must include a filter for the CCM Type perspective.

The CCM Type perspective is not available within Perspective Management and is used only for the definition of model, continuous control, and incident result primary data roles.

For example, models support four types of access: Create, Edit, View, and Delete. This same access is needed for either Access or Transaction type models. So instead of one primary data role for both Access and Transaction for each type of access, there are two, one for each CCM type. In essence, there are eight combinations of primary data role:

- Create Access Model Primary Data Role
- Edit Access Model Primary Data Role
- View Access Model Primary Data Role
- Delete Access Model Primary Data Role
- Create Transaction Model Primary Data Role
- Edit Transaction Model Primary Data Role
- View Transaction Model Primary Data Role
- Delete Transaction Model Primary Data Role

Filters differ for each object — model, continuous control, and incident result — because the states available to each vary. Models and controls can exist only in an

Approved or Invalid state. Incident result states vary depending on the state action. For instance, when an incident result is being viewed (versus edited), it may be in any of the following states: In Investigation State for Result, Approved State for Result, Closed State for Result. When an incident result is being edited (versus viewed), incidents in a closed state cannot be accessed.

As primary data roles are created for each object (model, control, incident result), each state (Create, Edit, Delete, and View), each CCM Type (Access and Transaction), and the variations of each state and state action allow for extremely granular data-level security that may be assigned to users to control their access.

Composite Data Roles

A composite data role is a collection of primary data roles needed for a particular job. It contains filters, each of which sets a Data Role attribute equal to one of the constituent primary data roles. Thus the composite role collects the data access provided by the primary roles.

As an example, for EGRCM the Control Manager Data Role contains eight filters that specify the Edit Control Primary Data Role, View Control Primary Data Role, View Control Operational Assessment Results Primary Data Role, View Control Design Review Assessment Results Primary Data Role, View Control Audit Test Assessment Results Primary Data Role, View Control Certification Assessment Results Primary Data Role, Create Control Primary Data Role, and Delete Control Primary Data Role.

When a composite role cites more than one primary role, it uses OR logic. In other words, the composite role grants access to data when that data matches criteria specified for any one of its constituent primary roles.

Each seeded composite data role bears the name of the job duty it supports, but ends with the suffix *Data Role*.

Job Roles

The job role is the combination of functional access and data access. It references one or multiple job duty roles and a composite data role, defining the complete set of functional and data access needed for a job.

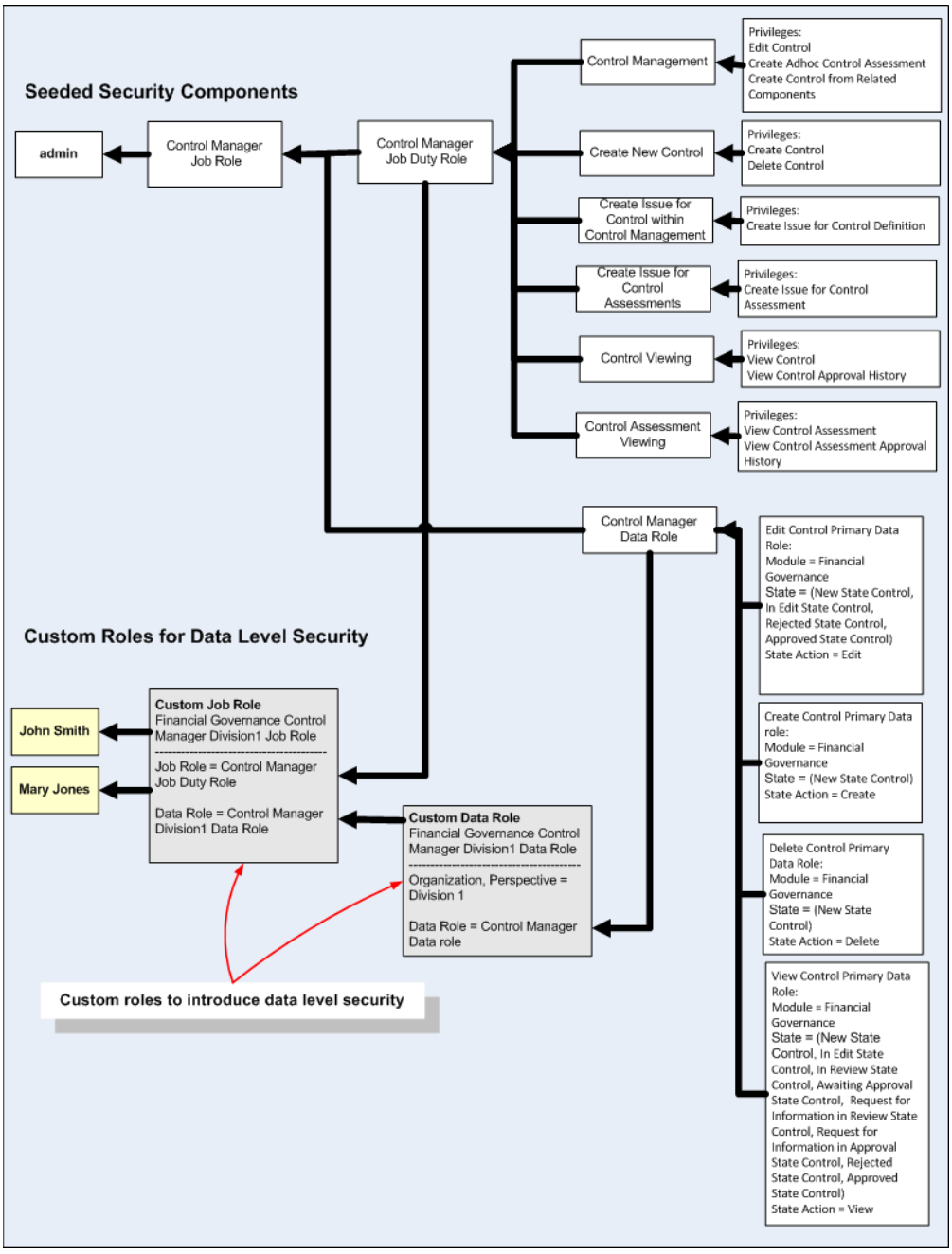
As an example, for EGRCM the Control Manager Job Role includes the Control Manager Data Role and the Control Manager Job Duty Role.

User

The user is the actual person using the application. Each user has a security profile that includes identifying information and defines the user's access to the system. A user can have one or multiple job roles. When signing into the application, the user is granted access that is the combination of all the job roles the user is given.

How to Introduce Data Level Security

The following example illustrates how to leverage the seeded security components to define data-level security for the user community. The example is based on objects used in EGRCM, but the concept is the same for CCM.



The unshaded components are seeded, and represent the Control Manager job role, which grants the ability to create, edit, delete, and view controls. You can define data access so that users can perform these actions only on controls associated with a perspective value. To do so, you create a custom perspective data role, and then include that role within a custom job role.

In the example, it's assumed that the Organization perspective includes values that divide a company into divisions, one of which is Division 1. Your purpose is to create custom roles that focus a Control Manager on controls associated with Division 1.

First, create a custom perspective data role. The role might look like this:

Name: Financial Governance Control Manager for Division1 Data Role

Description: Access to create and maintain controls in Division1

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
Division1	Perspective	Organization	Equals	Division1	Include
Control Manager	Data Attributes	Data Role	Equals	Control Manager Data Role	Include

The role contains two filters:

- A Control Manager filter sets a Data Role attribute equal to Control Manager Data Role. This provides access to data defined by the seeded Control Manager composite data role.
- A Division1 filter specifies that the Organization perspective be equal to Division1, thus limiting access to data associated with the Division1 value of the Organization perspective.

The system uses AND logic to combine the perspective criterion with the Control Manager Data Role criteria, and so grants access only to data for which both filters evaluate to true. In other words, data must meet all of these conditions:

- The perspective value associated to a control must equal Division1 (the condition of the Division1 filter).
- The control must exist in the Financial Governance module (a condition of the Control Manager filter).
- The control must be in one of the following state/action combinations (a condition of the Control Manager filter, because each combination is defined in one of the primary data roles that belong to the Control Manager Data Role):
  - Control State equals any of New State Control, In Edit State Control, Rejected State Control, or Approved State Control, AND Action equals Edit.
  - Control State equals New State Control AND Action equals Delete.
  - Control State equals any of New State Control, In Edit State Control, In Review State Control, Awaiting Approval State Control, Request for Information in Review State Control, Request for Information in Approval State Control, Rejected State Control, or Approved State Control AND Action equals View.

Second, create a custom job role that references the new custom perspective data role: Copy the seeded Control Manager job role (and give the copy a new name), remove the seeded data role from the copy, and add in the new data role.

Name: Financial Governance Control Manager for Division1 Job Role

Description: Maintain controls for Division1

Role Type	Role
Job Role	Control Manager Job Duty Role
Data Role	Financial Governance Control Manager for Division1 Data Role

Impact of Defining the Perspective Filter in a Separate Data Role

To implement data-level security, you created a data role that combines a perspective filter with an existing composite data role definition; you then included that data role (and a job duty role) in a job role. Do *not* instead include a perspective filter in its own data role, then create a job role that consists of a job duty role, a composite data role, and the perspective-filter data role. This would produce completely different results, because the application uses OR logic to evaluate a job role that contains multiple data roles.

For example, suppose you create a data role containing only one filter, which specifies the Division1 value of the Organization perspective:

Name: Division1 Data Role

Description: Access to Division1

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
Division1	Perspective	Organization	Equals	Division1	Include

Suppose also that you include this role along with seeded job duty and data roles in a job role:

Name: Financial Governance Control Manager for Division1 Job Role

Description: Maintain controls for Division1

Role Type	Role
Job Role	Control Manager Job Duty Role [seeded]
Data Role	Control Manager Data Role [seeded]
Data Role	Division1 Data Role

This configuration would produce results that differ from the data-level-security example illustrated on page 2-7, granting access to all controls for which either of the following is true:

- A control is associated with the Division1 perspective value, even if it does not satisfy conditions defined in the Control Manager Data Role.
- A control satisfies conditions defined in the Control Manager Data Role, even if it is not associated with the Division1 perspective value: It exists in the Financial Governance module AND in one of the following state/action combinations:
  - Control State equals any of New State Control, In Edit State Control, Rejected State Control, or Approved State Control, AND Action equals Edit.
  - Control State equals New State Control AND Action equals Delete.
  - Control State equals any of New State Control, In Edit State Control, In Review State Control, Awaiting Approval State Control, Request for Information in Review State Control, Request for Information in Approval State Control, Rejected State Control, or Approved State Control AND Action equals View.

Because the Division 1 Data Role criterion is not included with the Control Manager Data Role criteria, the user has access to view, but take no other actions on, controls whose perspective value is equal to Division1.

Manage Roles

Before you begin setting up your roles, consider who will use GRC and for what purposes. This will be the foundation for job duty roles. Examples include:

- Control Manager. A user in this role is responsible for the administration aspects of the compliance program. As an administrator, the user creates and maintains controls, issues, perspectives, and process.
- Model Manager. A user in this role is responsible for the creation and management of CCM models, which may ultimately serve as the basis of a continuous control, deployed to detect or prevent organizational risk from being realized. Or, a model may be used by auditors to test controls and do temporary analysis of user access and transaction data.
- Continuous Control Manager. A user in this role is responsible for the creation and management of controls to detect or prevent organizational risks from being realized.
- Control Assessor. A user in this role works independently of management to perform testing against the controls. A user in this role can also create and review issues, as well as participate in the assessment activities against controls.
- Risk Manager. A user in this role is responsible for the management aspects of risk management. This user is responsible for creating and maintaining definitions of risk, events, and consequences and the various risk models.
- Line of Business Manager. A user in this role is a manager (a line of business head, senior manager, or departmental manager) who leads a group of business process owners. This user makes sure the team provides necessary information to the audit/compliance group on time, and makes sure that related documentation is up to date. The user may be involved in periodic rollup certifications or surveys against the entire area, but does not operate at the process level.
- Process Manager. A user in this role owns one or more processes that are in the scope of the financial compliance program and may impact the accuracy of the financial reports. This user is responsible for maintaining the accuracy of the process documentation, evaluating risks to the processes, and identifying controls necessary to mitigate the risks; performs quarterly attestations for management on the state of the processes he owns; and participates in the annual assessment of the design and operational effectiveness of processes.
- Internal Auditor. A user in this role is responsible for executing the internal audit plan for financial compliance; works independently of management to determine the operational status of controls, completeness and accuracy of documentation; and delivers work papers and evidence that is often leveraged by the external auditor.
- Issue Manager. A user in this role is responsible for managing issues, and in that capacity creates and maintains issues and remediation plans.
- Incident Result Manager. A user in this role is responsible for managing incident results, assigning them to appropriate individuals for review and remediation.
- Incident Result Investigator. A user in this role is responsible for researching incident results, determining the remediation actions required and ultimately proposing or acting on those actions to accept or close the incident.

- Perspective Manager. A user in this role has access to Perspective Management and is responsible to manage perspectives across EGRCM objects and modules. The user maintains hierarchies and perspectives within the hierarchies.
- Assessment Manager. A user in this role has access to Assessment Management to create and manage assessment plans and all assessments. This user also has the authority to initiate and close active assessments.
- Survey Manager. A user in this role has access to Survey Management to create and manage survey templates and surveys. This user also has the authority to initiate and close surveys.
- System Administrator. A user in this role has the responsibility to define and maintain the setup and configuration data for the EGRCM instance.
- External Auditor. A user in this role is someone outside the organization who performs audit testing and views control information.

Start your security model off small, and then as you see how the users will interact with tasks pertaining to your business objectives, you can continue to refine security access. It is easier to add granularity in the security model than it is to remove excess granularity.

Constructing Duty Roles

The duty role defines what a user can do within the application. A set of duty roles is provided. Each role is defined as logical groupings of a task a user performs within the various areas of the application. For EGRCM these areas include Process, Risk, Control, Issues and Remediation, and Assessment. For CCM the main areas include Models, Continuous Controls, and Incident Results. Common to both are Perspectives, Reporting, and System Administration. Each duty roles includes the set of privileges needed to perform a certain aspect of work for a specific object, such as creating controls, managing controls, viewing controls, reviewing control changes, approving control changes, and other activities specific to an object.

Seeded duty roles are available; you are strongly recommended to use them. However, you may find that delivered duty roles do not align with how your organization segregates work responsibilities, or have functionality you do not wish to use.

- Review the delivered duty roles. You cannot change the seeded duty roles. If you need to make changes, create a new duty role by copying a delivered one. Then remove functionality from, or add it to, the copy.

  For example, the Review Control Assessment seeded duty role includes the privilege to add attachments to completed controls during review. This may be something your organization does not allow the Control Assessment Reviewer to do. To remove this privilege, make a copy of the Review Control Assessment duty role, give it a new name, and remove this privilege from the new duty role.

- Construct duty roles in a way that aligns the tasks a user performs in a job. A user may perform multiple tasks that cross into different areas of the application. It is best to keep these tasks grouped into separate duty roles and then combine them in the job duty role.

  For example, the Control Manager needs the ability to administer controls and issues. It is better to have two duty roles, one for Control Administration and the

other for Issue Administration, than to have one duty role that combines the two sets of tasks together.

Keep this in mind as you define new duty roles, since this will provide you with the most reusability of duty roles. The delivered duty roles were created following this practice.

Constructing Data Roles

The data role defines which set of data the user has access to within the application. The system matches on the criteria for all the data roles within each user's job roles to determine the set of data to which the user has access. As covered in "Security Components" (page 2-1), two types of data role are delivered: primary data roles that include module, state, and state action, and composite data roles that reference a set of primary data roles to form the basic data access needed for a job role.

- Each primary data role is intended to be referenced by many composite data roles, depending on what actions are needed. You should not need to create primary data roles with module, state, and state action, but simply reference the delivered primary data roles.
- The application is delivered with primary data roles for all EGRCM standard objects within the module template, but without the Module filter. For a custom module, include the Module filter in the custom data roles. Refer to "Security for a New EGRCM Module" (page 2-23). For CCM, the application is delivered with primary data roles for models, continuous controls, incident results, access requests, entitlements, and global and path conditions.
- A seeded composite data role exists for each seeded job duty role. Composite data roles have the same name as the job duty role, with the suffix *Data Role*. Each composite data role contains references to all the primary data roles that supply access to data required for the job.
- Data roles are extremely powerful in that, by their very construct, they define the degree of security to be implemented for all the duty roles (privileges) they are coupled with in the job role definition.

Data Roles and Perspectives

As delivered, the Continuous Control Monitoring module is seeded with the following perspectives:

Perspective	Associated Objects
Business Object	Entitlements, Models, Controls, Global Conditions
Datasource	Entitlements, Models, Controls, Results, Global and Path Conditions
CCM Type	Models, Controls, Results
CCM Participant Groups (upgrade only)	Models, Controls, Results

As delivered, the Financial Governance module does not have perspectives (other than the seeded Activity Type perspective). This means that until you introduce perspectives into the module, access is determined only by whether a user has been granted the functional privilege and has access to the module.

In either case, you are likely to add perspectives as you implement security:

- As you plan perspectives for your module, keep in mind that they are the means for segregating the data sets to which users have access. If you want only certain users to have access to a subset of operational data, define perspectives and include perspective filters in the composite data roles.
- First you must define the perspective. The values within the perspective are what will be associated to the application data. These same values are included within the data role. Their perspective must be defined with all its values before you can build the perspective data roles. Through the use of a perspective data role and associating perspective values to the operational data, you indicate the data to which each user has access. See the "Perspective Management" chapter of the *GRC User Guide*.
- Perspectives are hierarchical. Within a data role, you can grant access to all data descending from a level of the hierarchy, by selecting that level within the hierarchy and selecting an Includes Children option. This can reduce maintenance of the data role, since a filter defined this way does not have to change when new subordinate values are entered in the hierarchy.

  For example, an Organization perspective may be defined so that the root (highest-level) node is ABC Corp. Its immediate children include Division1, Division2, and Division3. Each of these has child nodes; those of Division2, for instance, are Department1 and Department2, and Region1 and Region2 (and each of the Region nodes has child nodes).

  You can define roles that provide access to data at any level of the hierarchy, or to specific values:

  – For all data within the hierarchy, select ABC Corp and specify Includes Children.

  – For all data for a specific value and its subordinates (hierarchical branch), select a parent value and specify Includes Children. If, in this example, your parent value is Division2, the role would grant access to data associated with Division2, Department1, Department2, Region1 and Region2 and all the values contained within the subfolders Region1 and Region2

  – For data only within a specific value, select that value, but do not specify Includes Children. If you select a value that does have children, you are granting access only to the data associated with the value, and not to its children.

    For example, if you select Division2 but do not specify Includes Children, then the role does not have access to data for Region1, Region 2, Department1, or Department2.
- To introduce data-level security, create a custom perspective data role with the appropriate perspective filters, and then reference the appropriate composite data role. If you use this technique, the system interjects the perspective filter into each primary data role included in the composite.

Consider the perspective hierarchy described on page 2-13. Each of the three divisions has its own Control Manager, and each manager is to have access only to controls within his division.

To accomplish this, define three custom perspective data roles, one for each of the three divisions:

– In each role, create a filter that sets the Organization perspective equal to one of the Division values — Division1 for a role called Control Manager Division 1 Data Role, Division2 for a role called Control Manager Division 2 Data Role, and Division3 for a role called Control Manager Division 3 Data Role.

– In all three roles, create a filter that sets the Data Role attribute equal to Control Manager Data Role. This provides access to data defined by the seeded Control Manager composite data role.

It's strongly recommended that the custom perspective data role reference a seeded composite data role. The custom perspective data role will automatically include any changes introduced to the seeded content in subsequent patches or releases.

- If a role includes more than one perspective value, it may treat those values with AND or OR logic, depending on how the role is configured. When values are combined in one filter, OR logic applies. For example, if a role contains one perspective filter that sets Organization equal to "Division1;Division2" the role grants access to all controls associated with either Division1 or Division2 (or both).

  When values are specified in distinct filters, however, AND logic applies. If, for example, a role contains two perspective filters, one sets Organization equal to "Division1" and the other sets Organization equal to "Division2," then the role grants access only to controls that have both Division1 and Division2 as the value for the Organization perspective.

- When a job role includes several data roles based on perspectives, those perspectives are joined by OR logic. This is desirable when a user requires access to objects associated with any of multiple perspective values — for example, controls for which the value of a perspective called Manufacturing Region is North America or controls for which the value of a perspective called Sales Region is North America. (This returns a broader set of data than a single data role specifying data that meets both conditions.) So to expand the breadth of a job role, include multiple perspective data roles within it.

- During the initial phases of an implementation, it's recommended that you start with broader security access and over time, as you understand how the various security components of the application function, add granularity where necessary.

Configuring Access to Datasources and Business Objects

In most cases, a "datasource" is a business application subject to CCM models and controls, although a datasource called GRC represents the GRC instance itself. A "business object" is a set of conceptually related data points. Each has its own perspective hierarchy, which is updated automatically as new datasources are configured or business objects are added.

Each datasource is represented by a value in a perspective hierarchy, and each business object is represented by a value in a second perspective hierarchy. (These are system perspectives. They are updated in the background when new datasources are configured or business objects are added. Users have no access to these hierarchies in Perspective Management.)

Composite data roles may include filters that select perspective values representing datasources and business objects to which users will be granted access.

- When a composite data role references primary data roles that specify states that can apply to continuous controls, models, entitlements, or global conditions, the composite role must include a datasource filter and a business object filter. (If a role's business-object filter selects the perspective value for either of two objects — User or Access Entitlement — the datasource filter must select the perspective value for the GRC datasource.)
- When a composite data role references primary data roles that specify states that can apply to incidents, access requests, or path conditions, the composite role must include a datasource filter, but should not include a business object filter.

Seeded data roles are configured so that when a filter selects datasources or business objects, it names the root node of its perspective hierarchy and uses the Includes Children condition. As a result, seeded data roles grant access to all datasources and all business objects.

However, pages in which models, continuous controls, incident results, global conditions, and entitlements are managed, created, or edited can be secured by datasource or business object, and so you may want to create data roles that grant access to specific datasources or specific business objects. As you do, be aware that a given data role must contain no more than one filter for datasource and one filter for business object. Each of these filters can name more than one datasource or business object. This implements required OR logic — data may come from any one of the named datasources or business objects (rather than being required to come from all of them at once).

State Action

The state of an object identifies where it is within its life cycle. As activities are performed on an object, its state changes. Activities include updating values and submitting the change for review and approval, rejecting or approving the change, marking the remediation of an issue complete, closing an issue, and so forth.

The actions that can be performed against an object are determined by its state. Not all actions or activities are appropriate when an object is in a given state. This is controlled through the inclusion of the state within the primary data role. Duty roles identify specific sets of functional access and actions (privileges) a job role is granted. The state within the primary data role identifies which state the object must be in for this functional access and set of actions to be available.

The following tables list states appropriate to EGRCM objects and CCM objects, and actions appropriate to each state. Refer to these tables as you define custom primary data roles.

Make a note of the set of states that are appropriate for an action. When defining new primary data roles, you must include the correct state action for the appropriate

entity so that this functionality is available only when the object is in the state identified by the data role.

Note: The application is seeded with a complete set of primary data roles for all objects, so it is highly unlikely that you will have to create a primary data role or a composite data role.

EGRCM Objects

Risk and Risk Objects A–J, Event, Consequence, Control and Control Objects A–J, Process, Base Object A–F, Perspective, Assessment Template, Assessment Plan, and Survey Template

State	Description
New	Created and saved
In Edit	Changes made and saved, but not submitted
In Review	Submitted and awaiting review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the approver has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved

Assessment Result

State	Description
New	New assessment available for assessor to complete
In Edit	Changes made and saved, but not submitted
In Review	Completed assessment is submitted and awaits review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the approver has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved
Canceled	Assessment Manager has canceled the assessment

Risk Analysis and Risk Evaluation

State	Description
In Edit	Active analysis or evaluation available to be completed
Complete	Analysis or evaluation results are completed

Issue

State	Description
New	Created and saved
Reported	Submitted for validation

In Edit	Changes made and saved, but not yet submitted
In Review	Submitted change is available for review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the reviewer has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved
Closed in Review	Issue is closed and is in review
Closed Approve	Review is completed for a closed issue, which awaits approval
Closed Additional Information in Review	A closed issue is in review, and the reviewer has asked for more information
Closed Additional Information in Approval	A closed issue awaits approval, and the approver has asked for more information

Remediation Plan

State	Description
New	Created and saved
In Edit	Changes made and saved, but not yet submitted
In Review	Submitted change is available for review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the reviewer has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved
Completed Review	Remediation is completed and is in review
Completed Approve	Review completed for a completed remediation, which awaits approval
Completed Additional Information in Review	A completed remediation is in review, and the reviewer has asked for more information
Completed Additional Information in Approval	A completed remediation awaits approval, and the approver has asked for more information

Assessment

State	Description
New	Created and saved
Active	Active assessment
Closed	Closed

Survey

State	Description
New	Created and saved
Open	Open and available for responders
Closed	Closed

CCM Objects

Incident Results

State	Description
In Investigation	Incident generated and awaiting investigation
Approved	Incident status updated and incident submitted
Closed	Incident closed by system

Continuous Control

State	Description
Approved	Continuous control created or edited
Invalid	After an upgrade, control validation fails

Model

State	Description
Approved	Model created or edited
Invalid	After an upgrade, model validation fails

Constructing Job Duty Roles

The job duty role is a type of job role that includes references only to duty roles. Isolating the functionality access from the data access provides reusability of the job duty role and makes it easier to construct new data access specific to job roles for the user community.

For example, the Control Manager Job Duty Role contains the following duty roles: Create New Control, Control Management, Create Issue for Control within Control Management, Create Issue for Control Assessments, Control Viewing, Control Assessment Result Viewing, and Control Reporting.

Instead of having to include these seven duty roles in each job role you create for specific data access, you reference only the job duty role, which has already formed the grouping.

The application is seeded with sets of job duty roles for the seeded job roles that are appropriate for the Financial Governance module, as well as for the Continuous Control Monitoring module. Each job duty role contains all the functional access needed for the job and defines "what can the user do" within the application.

- The UI allows you to construct job roles that include duty roles and data roles, but it is strongly recommended that you construct job duty roles to form groupings of duty roles. In this way you can reference the job duty role in job roles when you combine the functional and data access together. Each job duty role can be used in multiple job roles. This technique also makes it easier for you to make changes to the functional access, since changing a single job duty role applies the change to all users who perform a job against differing sets of data.
- Review the delivered job duty roles. Even if you did not create custom duty roles, you may find that the job duty role contains functionality that does not align with your compliance process. You cannot change seeded job duty roles

directly. Create a new job duty role by making a copy of a delivered role and then removing duty roles from, or adding them to, the copy.

Constructing Job Roles

The job role brings both the functional access and the data access together to form precisely "what the user can do" to "which set of data." The application comes with seeded job roles appropriate for the Financial Governance module, as well as the Continuous Control Monitoring module.

These seeded job roles are available for you to use to build out custom job roles you define to introduce data-level security. Each job role has a reference to the appropriate job duty role and the appropriate data role.

- Create a job role for each set of functional access and unique set of data access required for all the operational data secured by perspectives.

  Earlier, the "Constructing Data Roles" section presented a sample Organization perspective (page 2-13) that established three divisions. The section discussed creating three custom perspective data roles (page 2-14), each of which granted access to control-management data for one of the divisions.

  Using those data roles, you can create job roles, one for each division. All three job roles would cite the Control Manager Job Duty Role, which encompasses all the functionality a user requires to serve as a Control Manager. Each of the three job roles would also cite one of the custom perspective data roles configured to provide access to the data for each division: Control Manager Division 1 Data Role, Control Manager Division 2 Data Role, and Control Manager Division 3 Data Role.

  Note: It's recommended that you include the perspective value within the job role name so that you can easily identify the data that a given job role uses, and to make it easier to locate job roles when assigning them to users.

- A job role can reference other job roles. This type of job role can contain only other job roles, and acts as a way to group a set of job roles needed for a specific user type.

  For example, you can create a job role named Basic Financial Governance Access Job Role; it might contain two other job roles called GRC User Job Role and Financial Governance Job Role. Then you could grant only the Basic Financial Governance Access Job Role, rather than the two separate roles, to any user who would qualify to have both those roles.

Perspective Matching Based on the Data Roles within the Job Role

When an object contains perspectives, a user's data roles must have at least one of the object's perspective values in order for the user to have access to the object.

When a job role contains data roles with perspectives, the system compares all the perspective values within the data role against those in the object.

The data role drives which perspectives to match on for the user:

- For the user to have access to the data, at least one value for each perspective filter within the data role must match a perspective value associated with the object.

For example, assume both the Financial Governance and IT Governance modules identify an Accounts Payable process, with Organization perspective values of Division1 and Division2. User1 has a data role that permits viewing of processes for the Financial Governance module for Division1. User1 can view the Accounts Payable process, since Financial Governance and Division1 match values for Module and Organization.

- If the data does not have a value for a perspective within the data role, then it cannot be matched on.

  For example, User1 has a job role that includes a data role that allows users to view the Process object. The data role for this job role contains these criteria: Module = Financial Governance, Organization = Division1, and Major Process = Procure to Pay.

  The Accounts Payable process is related to the Organization value of Division1, but Major Process is not completed.

  User1 does not have access to Accounts Payable, since the data role for this job role contains both the Organization and Major Process perspectives. The criteria for Major Process cannot be matched since no value is specified on the object.

Manage Users

The basic security principle is that a user does not have access to application functionality unless it is specifically granted to the user.

- All users must have basic access to EGRCM that is provided by the seeded GRC User Job Role. This job role includes only the basic privilege to log into the application and see the Welcome dashboard. Beyond this, each user's security profile must be updated to grant privileges to perform other activities, and to define precisely the application data to which the user has access.

  Note: The user has access to the operational data that is not secured by a perspective based solely on functional access. Some operational data is not secured by perspectives, such as survey management objects and assessment management objects, and access to this data is based on the functional access. Likewise, if an object that does support perspectives is defined without any perspectives, any user that has functional access and data roles that specify this object will have access to it.

  For example, the Order to Cash process is defined without any perspectives associated to it. All users who have a data role to view the process object in the Approved state regardless of any of the perspective filters contained in their data roles will be able to view the Order to Cash process.

- To have the Financial Governance module displayed within the Navigator, the user must have the Financial Governance Module Job Role.
- To have the Continuous Control Monitoring module displayed within the Navigator, the user must have one of the Continuous Control Monitoring Job Roles, such as Continuous Control Manager Job Role or Continuous Control Viewer Job Role.
- Select all other appropriate job roles for each user.

- Each user must have a unique email address. Users cannot share an email address.
- A user assigned multiple job roles has access that is the combination of all those job roles.

  For example, if the user has the job roles for performing control maintenance and issue maintenance for the Financial Governance module, then within the Navigator for Financial Governance, both the Control Management and Issue Management entries are available.

Define a User with Access to All Operational Data

It's recommended that you define at least one "Super User" — a user who can view all operational data. To do this, create data roles for perspectives associated to the objects. Include a filter with the Includes Children condition, and select the root value. Include this data role with the viewing job duty role for the object.

For example, assume the Financial Governance module is configured to have Process, Risk, and Control objects; an Organization perspective is associated with all three objects; a Major Process perspective is associated with the Process object, and a Risk Category perspective is associated with the Risk object.

Because the Organization perspective is associated with all three objects in this module, this perspective can be used to define the data roles.

1. Create three custom perspective data roles: All Processes Viewer Data Role, All Risks Viewer Data Role, and All Controls Viewer Data role:
   - All three roles contain a filter that sets the Organization perspective equal to Organization (its root value), and specifies the Includes Children condition.
   - Each contains a filter that sets the data role equal to the seeded viewer role for its object: Process Viewer Data Role, Risk Viewer Data Role, and Control Viewer Data Role, respectively.
2. Define three custom job roles: All Processes Viewer Job Role, All Risks Viewer Job Role, and All Controls Viewer Job Role:
   - All Processes Viewer Job Role includes the All Processes Viewer Data Role created in step 1 and the seeded Process Viewer Job Duty Role.
   - All Risks Viewer Job Role includes the All Risks Viewer Data Role created in step 1 and the seeded Risk Viewer Job Duty Role.
   - All Controls Viewer Job Role includes the All Controls Viewer Data Role created in step 1 and the seeded Control Viewer Job Duty Role.
3. Assign the new custom job roles to a user.

Use Case: Access to Results within Incident Result Management

Specific to CCM, access to incident data is driven by the perspective values assigned to the incident. A user who creates a control selects perspective values in a panel of the control-creation page labeled "Result Management Perspective Assignment." Initially, these values are assigned to incidents generated by the control.

Consider these points while defining job roles for Incident Result Management:

- To be granted access to Incident Result Management, a user must have a job role that cites a job duty role with at least one of these privileges: Manage Incident Result, Edit Incident Result, View Incident Result.
- Within Incident Result Management, access to an incident is granted by a data role specifying perspective values that match those assigned to the incident.

  (The role would contain a filter specifying another data role, which would contain filters for module, state, state action, and CCM Type values appropriate for incident review. In the new role, one or more additional filters would select perspective values assigned to the incident.)

For example assume an access control, called Create Suppliers & Create Payments for Division1, has an incident raised against it. The control's creator selected Division1, from an Organization perspective, as its Result Management Perspective Assignment.

Also assume that an Incident Result Investigator Job Role has:

- An Incident Result Investigator Job Duty Role, which has a Manage Incident Result duty role, which has the incident-review privileges: Manage Incident Result, Edit Incident Result, and View Incident Result.
- An Access Incident Result Investigator Data Role, which has the Investigate Access Incident Result Primary Data Role, which has values appropriate for access issue investigation: it filters for the In Investigation state, the Edit state action, the CCM module, and the Access CCM Type value.

For a user to have access to the incident generated by the Create Suppliers & Create Payments for Division1 control:

- Create a new data role called, say, Division1 Data Role. In it, create two filters, one to select the Access Incident Result Investigator Data Role, and the other to select the Division1 value from the Organization perspective.
- Create a new job role: Copy the Incident Result Investigator Job Role, remove the Access Incident Result Investigator Data Role from it, and replace that role with the Division1 Data Role.
- Assign the new job role to the user. The system then not only grants the user access to the incident, but also generates a worklist for the user to investigate the incident.

Use Case: Access to Issues within Issue Management

Specific to EGRCM, access to issue data is driven by the object the issue is raised against. Therefore issue security access combines issue privileges and data access to objects within a module. Consider these points while defining users' job roles for Issue Management:

- To be granted access to Issue Management, a user have a job role that cites a job duty role with at least one of these privileges: View Issues, Create Issue, Edit Issue, Validate Issue, Close Issue, Review Issue Changes, Approve Issue Changes.

- Within Issue Management, a user has access to an issue if he has access to the object against which the issue is raised. That means the user's other job roles determine the issues to which the user has access.

  For example, a control called Segregation of Duties for Division1 within the Financial Governance module has an issue raised against it.

  – User1 has an Issue Manager Job Role that includes a job duty role containing the View Issues and Validate Issue privileges and data roles to edit issues when in the Reported, Approved, In Edit, and Rejected states for the Financial Governance Module.

  – User1 also has a Control Manager Job Role that includes a job duty role containing privileges to create, edit, and view the control object and a data role to view the control object for the Financial Governance module when the state is equal to Approved.

  – Upon navigating to Issue Management within the Financial Governance module, User1 sees the issue raised against the Segregation of Duties control because of the privileges and data access granted by the Control Manager Job Role and the Issue Manager Job Role.

  – The system also generates a worklist entry for User1 to validate the submitted issue for the Segregation of Duties control, because User1 is granted the Edit Issue data role when the state of the issue is Reported within the Issue Manager Job Role.

Security for a New EGRCM Module

If you configure a new module for EGRCM, you must define new security roles for the objects configured within the new module. (This does not apply to the Financial Governance or CCM module.)

First, review the module definition and identify all the template objects being used. For example, an IT Governance module may include:

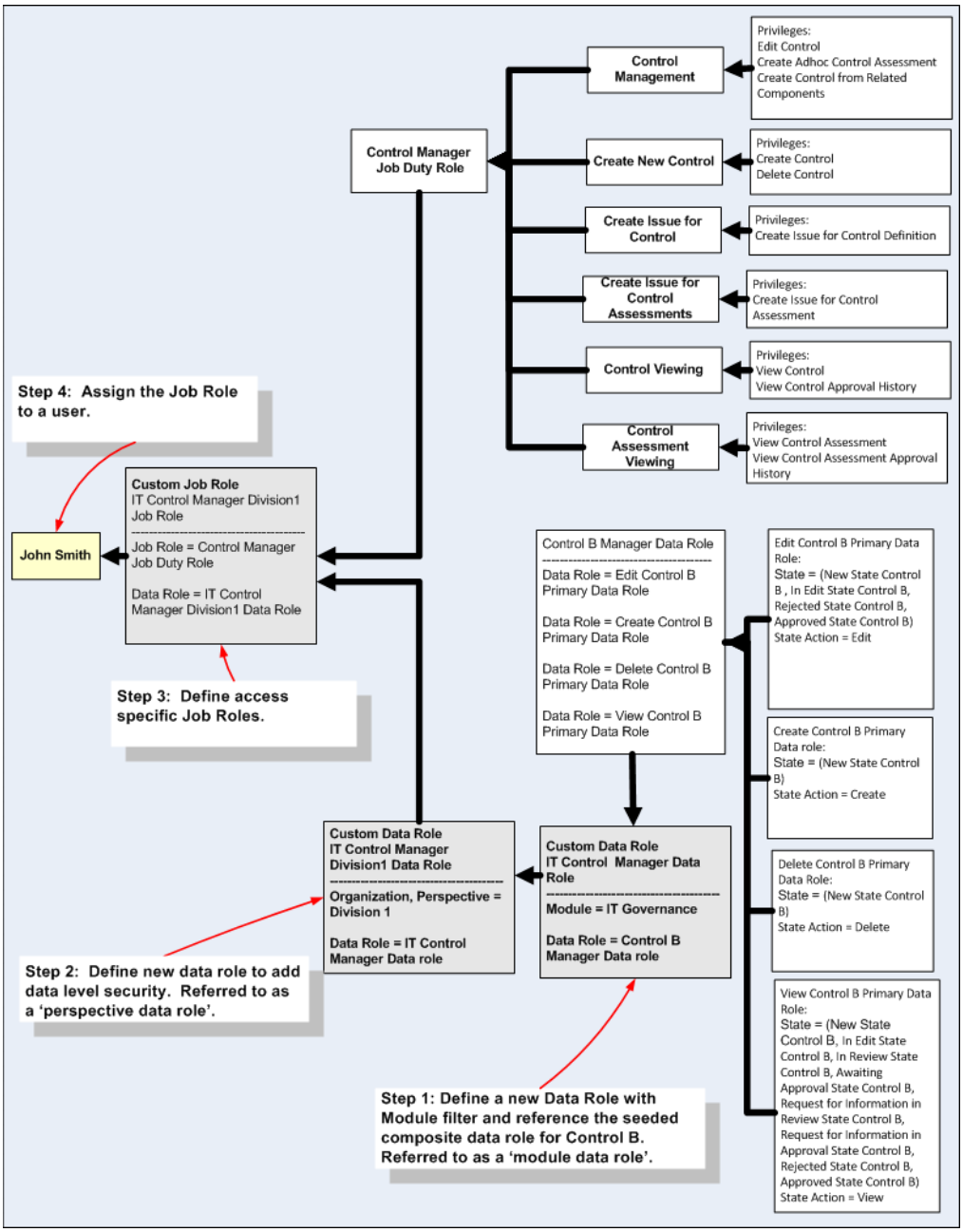
Object	Relabel	Module Specific
Base Object A	IT Policy	×
Base Object B	IT Project	×
Base Object D	IT Process	×
Risk Object B	IT Risk	×
Control Object B	IT Control	×
Control Object H	Sub Control	×
Base Object F	Control Objective	×
Event	Event	
Consequence	Consequence	
Issue Object A	Issue	×
Remediation Plan	Remediation Plan	

Next, identify the types of job roles you need for this new module and the type of functional access each job role needs. You can use the seeded duty and job duty roles for the functional access if these meet your business requirements. If not, see "Constructing Duty Roles" and "Constructing Job Duty Roles" (pages 2-11 and 2-18).

Then complete the following steps:

1. Define a data role for each seeded composite data role for the standard objects in the new module and include the module filter. This is also referred to as the "module data role." See "Define Data Roles for the New Module" (page 2-25).
2. Define perspective data roles for data-level security as needed. See "Define Perspective Data Roles for Data Level Security" (page 2-26).
3. Define new job roles. See "Define New Job Roles" (page 2-26).
4. Assign the new job roles to users.

The following diagram illustrates the steps to define the IT Control Manager Division 1 Job Role for the IT Governance module. Shaded boxes represent roles that are needed for the custom module; unshaded boxes are seeded roles.



Define Data Roles for the New Module

The application is delivered with a complete set of primary and composite data roles for all the objects within the module template.

The application is seeded with primary data roles for standard objects in the module template. For each, the object name is contained within the role name, and each references the specific state for the standard object the primary data role serves. The roles do not contain the module filter. For example:

Name: Edit Control Object B Primary Data Role

Description: Data access criteria to edit Control Object B data

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
States	Data Attributes	State	Equals	New State Control Object B, In Edit State Control Object B, Rejected State Control Object B, Approved State Control Object B	Include
Action	Data Attributes	Action	Equals	Edit	Include

The seeded composite data roles for the standard objects are defined similarly to those that support the seeded job roles for Financial Governance. These composites form groupings of data access against each of the standard objects. For example:

Name: Control Object B Manager Data Role

Description: Composite data role for access to edit Control Object B data

Filter Name	Object	Attribute	Condition	Data Role	Include/Exclude
Edit	Data Attributes	Data Role	Equals	Edit Control Object B Primary Data Role	Include
View	Data Attributes	Data Role	Equals	View Control Object B Primary Data Role	Include
View Assessment	Data Attributes	Data Role	Equals	View Control Object B Operational Assessment Results Primary Data Role	Include
View Design Review	Data Attributes	Data Role	Equals	View Control Object B Design Review Assessment Results Primary Data Role	Include
View Audit Test	Data Attributes	Data Role	Equals	View Control Object B Audit Test Assessment Results Primary Data Role	Include
View Certification	Data Attributes	Data Role	Equals	View Control Object B Certification Assessment Results Primary Data Role	Include
Create	Data Attributes	Data Role	Equals	Create Control Object B Primary Data Role	Include
Delete	Data Attributes	Data Role	Equals	Delete Control Object B Primary Data Role	Include

Because primary data roles for standard objects do not include module, you must define custom "module data roles." Each of these associates the new module with the seeded composite data role for one of the objects selected for the new module.

For example, the sample IT Governance module uses Control Object B for its control object. You might create this role:

Name: IT Control Manager Data Role

Description: Maintain IT Control data access

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
Module	Data Attributes	Module	Equals	IT Governance	Include
Data Role	Data Attributes	Data Role	Equals	Control Object B Manager Data Role	Include

Define Perspective Data Roles for Data-Level Security

To introduce data-level security for the new module, follow a process very similar to the one used for the Financial Governance module. Create custom data roles, each of which contains at least one filter that specifies at least one perspective value to be applied to an object, and another filter which in this case references the module data role for that object (as created in "Define Data Roles for the New Module," above).

For example, suppose (once again) the Organization perspective includes values that divide a company into divisions, and one of these values is Division1. In the IT Governance module, you want to provide a Control Manager with access only to controls in Division1. Create a role (called, for instance, IT Control Manager Division 1 Data Role) that includes two filters:

- A filter called Division1 sets the Organization perspective equal to Division1.
- A filter called Control Manager sets the data role equal to the IT Control Manager Data Role created (above) to apply control-management data access to the IT Governance module.

The system joins the perspective-filter criterion with all the filter criteria introduced in the module data role, as well as within each of the primary data roles contained in the seeded Control Object B Manager Data Role.

The system uses AND logic to join the perspective filter with other data role criteria, and so grants access to controls for which all of the following are true:

- The perspective value associated to a control must equal Division1 (the condition of the Division1 filter).
- The control must exist in the IT Governance module (a condition of the IT Control Manager Data Role).
- The control must be of the object type Control Object B and must be in one of the following state/action combinations (a condition of the IT Control Manager Data Role, because each combination is defined in one of the primary data roles that belong to the Control Object B Manager Data Role, which in turn is a component of the IT Control Manager Data Role).
  - Control State equals any of New State Control, In Edit Stat Control, Rejected State Control, or Approved State Control AND Action equals Edit.
  - Control State equals New State Control AND Action equals Delete.
  - Control State equals any of New State Control, In Edit State Control, In Review State Control, Awaiting Approval State Control, Request for Information in Review State Control, Request for Information in Approval State Control, Rejected State Control, or Approved State Control, AND Action equals View.

Define New Job Roles

Create new job roles for the new module as described in "Constructing Job Roles" (page 2-19). The only difference is that these job roles reference the new job duty role and data roles created for the new module.

Create Job Roles for Issue and Remediation Plan for a Custom Module

Job roles for issue and remediation plans for a custom module are handled slightly differently than for other standard objects.

Access to issues is based on the user having the appropriate functional access to the Issue object and having data access to the Issue object and data access to the object the issue is against.

There is only one Remediation Plan object, and it is not module-specific. Access to Remediation Plan is based on having the appropriate functional access to the Remediation Plan object and having data access to the Remediation object.

When defining a new Issue Job Role for the custom module, it is necessary to add in the module filter as described in "Define Data Roles for the New Module" (page 2-25). However, you will never build a perspective data role for the Issue object; issues do not have perspectives.

For example, an IT Issue Manager Data Role might contain two filters:

- A filter called Module sets the module equal to IT Governance.
- A filter called Data Role sets the role equal to the seeded Issue Object A Manager Data Role.

The issues to which a user actually has access are based on the object against which the issues are logged. A user has access only to issues within Issue Management for objects the user can access in other work areas. So a user who is an Issue Manager is able to edit and maintain issues only for objects to which the user has access. Therefore to define new issue job roles for a custom module:

- Define the module data role to grant access to the Issue object in the new module.
- Define the module-specific job role that references the new module data role.
- For access to remediation plans, use the seeded job roles. There is only one Remediation Plan object, which spans all modules. Users with access to Remediation Plan data have access to all remediation plans within the application.

Security for Event and Consequence

Like Remediation Plan, there is only one object for each of Event and Consequence. This means there is no need for custom security roles to grant a user access to these objects; the seeded roles can be used.

Event and Consequence are also not module-specific. Regardless of the module from which a user navigates into Risk Management, the user sees all instances.

These components do not have perspectives, so there is no data-level security for them.

A

Appendix

This appendix provides additional information about GRC security.

Troubleshooting

If a user should have access to data but cannot see it, the problem is probably an incorrect data role.

- Review the perspective filter that is included in the user's data role. Does it reference the correct perspective hierarchy and value? Is the condition correct?
- Is the correct composite data role referenced for the user's job role?

Impact of Changing a Perspective Used in Data Roles

Over time it may be necessary to make changes to perspectives used for data-level security. It is important to understand if a change will impact security, and how.

Change	Impact
Changing the name, description, or status of a value within the perspective hierarchy	No
Moving a value to a new position within the hierarchy so that it retains its original parent value	No
Moving a value to a new position in the hierarchy so that it changes its parent value	Yes For users with a data role in which a perspective filter is set to equal this value, there is no impact. If a data role includes a perspective filter that refers to the original parent and uses the Includes Children condition, users assigned the role no longer have access to objects associated to the value that was moved. If a data role includes a perspective filter that refers to the new parent and uses the Includes Children condition, users assigned the role now have access to objects associated to the value that was moved.

Change	Impact
Removing a value from the hierarchy	Yes Any object associated with the perspective value that was removed will no longer be accessible. The Unassigned Perspective Values security report will report these objects. When you find it necessary to remove a value from a perspective hierarchy, first change all objects that are associated with that value to a new perspective value and update users' data roles accordingly. If that new value does not already exist within the perspective hierarchy: • Update the perspective hierarchy with the new value. • Update objects associated with the value to be removed to the new perspective value. • If necessary, update the data roles that referenced the value to be removed to the new value or a parent value with Includes Children. • Update the perspective hierarchy to remove the perspective value.
Changing the status of the perspective hierarchy to Inactive	Yes Any object associated with the perspective hierarchy is no longer accessible. This change requires multiple steps. If this perspective hierarchy is to be replaced by a newly created one: • Define the new hierarchy first. • Define new data roles for this hierarchy or update existing data roles. If existing data roles are updated, users whose job roles reference the changed data roles will have new access. If a new perspective hierarchy is not needed, but an existing perspective hierarchy will be used: • If necessary, update the existing perspective hierarchy with values. • If necessary, define new data roles for the new values or update existing data roles for the new values. In either case: • Optionally, assign the new data roles to the appropriate users by either creating new job roles or including the new data roles in existing job roles. • Change the objects associated to values in the perspective hierarchy to be retired to the new perspective hierarchy. • Update the perspective hierarchy status to Inactive. • Optionally, update the status to Inactive for the data roles for the inactive perspective hierarchy. • Optionally, remove inactive data roles from the job roles.