



User Types and Entitlements

Understanding 3D RBAC and Primary Security Roles

Version: 1.5
February 2025

Contents

User Types and Associated Entitlements	3
Defining 3D RBAC	3
Primary Security Roles	4
Data Manager vs Non-Data Manager Entitlements.....	4
Module Entitlements	5
1. Compliance	6
2. Maturity	9
3. Risk Register	11
4. Incident Commander	12
5. Policy Manager.....	14
6. DCMS.....	15
7. Waiver Management	17
8. Specialty Entitlements	19
Access Profiles (Future Update).....	20

User Types and Associated Entitlements

This guide provides an overview of the entitlements that can be assigned to a User within our CRT compliance & maturity control center. In this document, the term *Access Profile* refers to the unique combination of entitlements assigned to a user, tailored to their specific job responsibilities and aligned with the principles of 3D RBAC. The term *Access Profile* replaces the legacy term *Role* to better reflect the flexibility and granularity of our approach. By understanding these entitlements and their functionalities, you can effectively assign the appropriate authorizations to your team members, ensuring operational efficiency, consistency, and security within your compliance processes.

In traditional systems, a *Role* was synonymous with predefined application functions or user groups. Under our 3D RBAC framework, entitlements are far more granular, enabling the creation of custom Access Profiles for individual users based on their unique roles and organizational requirements. This approach enhances operational precision and strengthens overall security.

Defining 3D RBAC

Cyturus was a pioneer in developing and deploying 3D RBAC (Three-Dimensional Role-Based Access Control). 3D RBAC is an advanced access control model that expands upon traditional Role-Based Access Control (RBAC) by introducing additional layers of granularity and flexibility. It allows for more precise and dynamic assignment of user permissions, aligning access with specific job responsibilities, operational needs, and security requirements. The "3D" in 3D RBAC refers to the three dimensions that shape access control decisions:

1. **Primary Security Role (Who):**

This dimension represents the user's functional role or job responsibilities within the organization, such as "Client Admin," "Manager," "User," or "Guest." A Primary Security Role (PSR) defines the baseline entitlements available to a user to perform their duties.

2. **Entitlements (What):**

This dimension specifies the individual permissions or actions a user is authorized to perform, such as "Compliance Manager," "Compliance Viewer," or "Evidence Auditor." Entitlements provide granular control over access and functionality within our platform.

3. **Context (Where/When/Why):**

This third dimension accounts for contextual factors that influence access, such as a specific Client, Engagement, location, time of access, or specific scenarios. For example, a user might only have certain entitlements during business hours, for a specific client, within a particular entitlement.

Benefits of 3D RBAC:

- **Granularity:** Provides fine-tuned control over access, enabling specific entitlements tailored to unique operational needs of a specific user.
- **Flexibility:** Adapts to dynamic organizational structures and evolving job requirements.
- **Security:** Reduces over-permissioning and minimizes the risk of unauthorized access by aligning entitlements with both roles and context.
- **Auditability:** Enhances the ability to track and report on access decisions by incorporating multiple dimensions.

By incorporating these three dimensions into our CRT platform design initially, our 3D RBAC provides our clients with a robust framework for managing access securely and efficiently while adapting to the complexities of modern, dynamic environments.

Primary Security Roles

Primary Security Roles (PSR) in Cyturus' 3D RBAC Framework

Cyturus provides two User Type options that determine which Primary Security Roles (PSRs)—the "Who" dimension in 3D RBAC—are available based on the selected User Type. The User Type acts as the foundational filter, limiting the available PSRs and subsequently controlling what entitlements can be assigned. The two User Types are **Instance** and **Client**. Below, we outline the available PSRs for each User Type and the purpose behind their selection.

User Type 1: 'Instance'

This User Type applies to individuals affiliated with a Consulting Organization or MSSP. Their role revolves around managing multiple clients, configurations, and internal processes for their clients.

Available Instance PSRs:

1. **Admin** – Full access to all instance configurations and data.
2. **Client Admin** – Data Manager role that Manages specific client accounts, licenses, users, and configurations.
3. **Instance Manager** – Manages consulting organization data across clients.
4. **Instance Consultant** – Performs data management tasks but cannot hold "Owner" level entitlements. Designed for non-FTE consultants.
5. **Instance User** – Handles tasks and operational duties without direct data management or ownership roles.

User Type 2: 'Client'

This User Type is designated for individuals affiliated with an external client or business entity. Their access is limited to data relevant to their specific organization.

Available PSRs:

1. **Client Manager** – A data management role with permissions to manage their client details, users, and entitlements, including "Owner" roles.
2. **Client Consultant** – A data management role limited to "Manager" permissions; cannot hold "Owner" entitlements.
3. **Client User** – A contributor role for client-specific data access, allowing "Owner" but not "Manager" permissions.

Shared PSRs (Available for Both User Types):

1. **Guest** – Provides limited, view-only access to data.
2. **Auditor** – Restricted access for auditing purposes, applicable to either consulting or client-specific data.

By structuring PSRs in this way, Cyturus ensures that access control remains flexible, granular, and aligned with each user's role and responsibilities, while maintaining security and compliance.

Data Manager vs Non-Data Manager Entitlements

The primary difference between a **Data Manager** (paid license) and a **non-Data Manager** (non-paid license) lies in the level of access, functionality, and responsibilities granted by each entitlement. The primary differences are tied to the level of functionality and management of the data elements within the CRT.

1. Data Manager (Paid Licenses)

A Data Manager is a licensed user who typically has permissions and responsibilities related to managing and controlling data within the platform and uses the CRT in their everyday work activities.

Key Characteristics:

- **Enhanced Access:** Full access to create, modify, and delete data, such as adding records, editing sensitive information, and configuring data structures.
- **Administrative Capabilities:** Ability to manage user roles, permissions, workflows, and overall system configurations.
- **Data Ownership:** Responsible for maintaining data accuracy, integrity, and compliance with organizational policies or regulatory requirements.
- **Analytics and Reporting:** Access to advanced analytics, reporting tools, and dashboards to monitor data usage and performance.

2. Non-Data Manager (Non-Paid License)

A Non-Data Manager (NDM User) is a limited-access user who interacts with the platform at a basic level, often with restricted access and permissions. These users have limited interaction with the CRT and are typically users with a defined tasks or responsibility over a single data element.

Key Characteristics:

- **Limited Access:** Can view or consume data but has limited ability to modify or manage it. An example would be a Data Manager assigns a one-time remediation task to a NDM User to complete. That NDM User is not responsible for the overall management of all the associated remediation tasks for a compliance finding.
- **Non-Administrative Role:** Restricted from performing administrative tasks such as changing settings, managing users, or configuring data workflows.
- **View-Only or Contributor Role:** May only be allowed to perform specific tasks like submitting requests, providing input, or viewing reports, depending on assigned entitlements within a specific module.
- **Cost-Free Usage:** Designed for users who do not require advanced access, reducing licensing costs for organizations while still enabling collaboration across the organization and stakeholders.

3. Summary of Key Differences

Feature	Data Manager (Paid License)	Non-Data Manager (Non-Paid License)
Access Level	Access to add, manage, and edit data as well as assign tasks and manage updates	Limited to viewing or specific basic add data actions – ie update tasks, add risks, upload evidence
Administrative Rights	Yes – configure settings, manage users, and update data elements	No – access to administrative tasks
Responsibility	Oversees data accuracy, compliance maturity, and CRT use	Basic user with limited ability to add specific data elements – tasks, evidence, risks, details

Module Entitlements

Within the CRT, authorizations are managed through individual entitlements. The availability of these entitlements is determined by the assignment of a Primary Security Role (PSR), defined as the first dimension of 3D RBAC. Using

the PSR to govern available entitlements ensures consistency when configuring user access. For example, if a user is assigned a PSR of "User," they would not have access to Manager-level entitlements; instead, they would be limited to Contributor or Viewer-level entitlements, as the PSR of "User" does not permit Manager-level access.

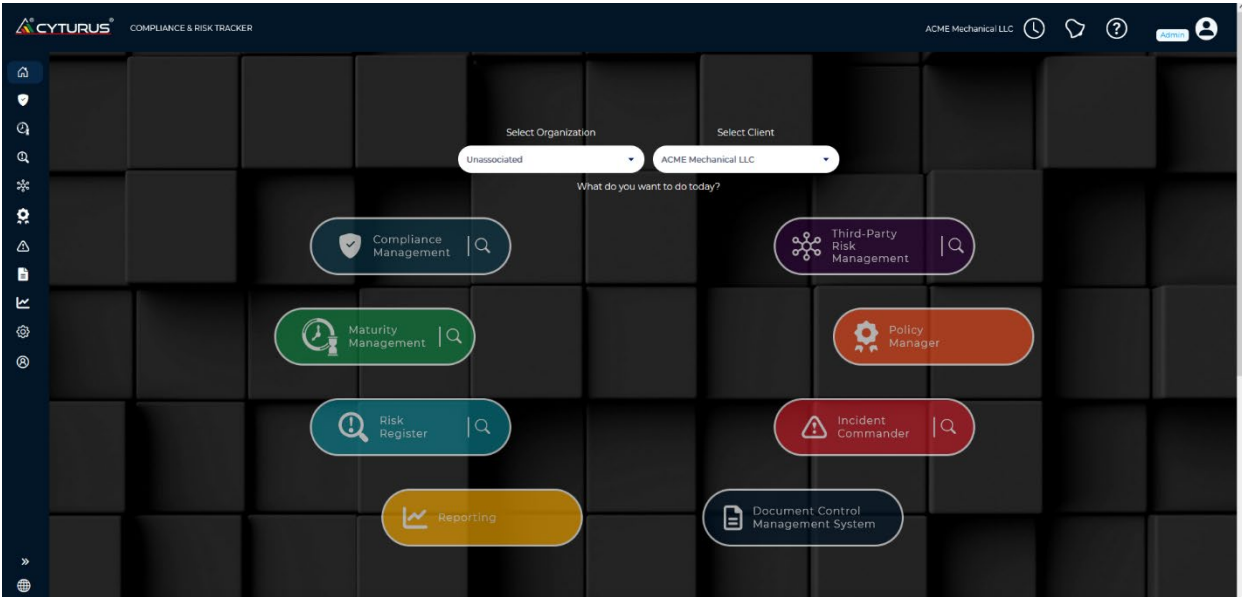


Figure 1.1 – CRT General Dashboard showing available modules

1. Compliance

The Compliance module entitlements include authorizations specific to the Compliance Module including Audit functions, Project Manager, and SSP Manager. These entitlements are specific to each Client Engagement.

Figure 1.1 – Compliance Management Entitlements

Compliance Manager

- **Entitlement Definition:** The Compliance Manager is responsible for managing the overall compliance framework, including performing interviews, compliance reviews over time, and generating reports.

- **Capabilities:** Users with this entitlement can configure compliance requirements, align controls across different standards, generate compliance reports, and oversee contributor activities. They also hold authority over updates to the compliance framework.
- **Why Select This Entitlement:** Choose this role if the user is responsible for establishing compliance standards and ensuring alignment with relevant frameworks.
- **Example Use Case:** Managing compliance status with internal and external stakeholders as well as auditors.
- **PSR Selection:** Manager, Consultant, Client Admin

Compliance Contributor

- **Entitlement Definition:** A Compliance Contributor provides information, documentation, and support needed to fulfill compliance requirements.
- **Capabilities:** They can upload evidence, respond to information requests, and contribute insights on control effectiveness.
- **Why Select This Entitlement:** Assign this role to subject matter experts or team members who need to provide specific compliance evidence or information but are not using the CRT as a primary part of their job responsibilities.
- **Example Use Case:** An IT staff member contributes firewall configuration data to demonstrate compliance with network security controls.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Compliance Viewer

- **Entitlement Definition:** The Compliance Viewer is able to access and view compliance activities, reports, and progress without editing rights.
- **Capabilities:** They can view compliance statuses, evidence, and reports to stay informed of the organization's compliance standing.
- **Why Select This Entitlement:** Ideal for executives or stakeholders who need visibility into compliance without the inherent liability associated with performing and updating day-to-day tasks.
- **Example Use Case:** A CISO wants to track the progress of compliance activities and monitor readiness for upcoming audits.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Compliance Owner

- **Entitlement Definition:** The Compliance Owner holds ultimate responsibility for compliance success, ensuring that all activities are completed and standards are met.
- **Capabilities:** They oversee all compliance aspects, approve frameworks and activities, and make critical compliance decisions.
- **Why Select This Entitlement:** Best for senior leaders accountable for ensuring compliance is achieved and maintained.
- **Example Use Case:** The head of compliance signs off on final compliance reports before they are submitted to an external auditor.
- **PSR Selection:** Manager, Consultant, Client Admin

Evidence Manager

- **Entitlement Definition:** The Evidence Manager is responsible for collecting, organizing, and maintaining compliance evidence needed for audits.

- **Capabilities:** They can request, gather, and store evidence from contributors, update documentation, and manage the status of evidence requests. They also ensure that collected evidence meets the compliance requirements.
- **Why Select This Entitlement:** Assign this role to users who need to collect and verify evidence for compliance audits and coordinate with contributors.
- **Example Use Case:** Gathering IT system configuration evidence from various teams for a scheduled audit and ensuring all necessary documentation is readily accessible.
- **PSR Selection:** Manager, Consultant, Client Admin

Evidence Viewer

- **Entitlement Definition:** The Evidence Viewer can view collected evidence but cannot modify or request it.
- **Capabilities:** They have read-only access to evidence related to the specific engagement to which they have been entitled. All access, including viewing of evidence, is logged.
- **Why Select This Entitlement:** Useful for auditors or stakeholders who need to review evidence without altering it.
- **Example Use Case:** An internal auditor reviews collected evidence prior to an official external audit.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Auditor

- **Entitlement Definition:** The Auditor is responsible for evaluating compliance and ensuring all activities meet regulatory standards.
- **Capabilities:** They can view and assess compliance controls, audit the notes and status provided, and make recommendations.
- **Why Select This Entitlement:** Assign to users who need to perform internal or external audits of compliance activities.
- **Example Use Case:** A third-party auditor evaluates the organization's adherence to CMMC standards and provides feedback on areas of improvement.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Evidence Auditor

- **Entitlement Definition:** The Evidence Auditor focuses specifically on reviewing the evidence to ensure its accuracy, validity, and compliance.
- **Capabilities:** They can view submitted evidence, provide validation, and mark as Met or Not Met.
- **Why Select This Entitlement:** Ideal for Auditors who need to validate the completeness and correctness of the gathered compliance evidence.
- **Example Use Case:** A audit team member reviews all collected evidence to confirm it meets regulatory requirements as part of an audit.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Project Manager

- **Entitlement Definition:** The Project Manager oversees the planning, execution, and delivery of compliance and maturity projects.
- **Capabilities:** They can create projects, assign roles to team members, manage timelines, and monitor project status. They can also have access to view and contribute to compliance evidence and ensure that key milestones are met if those entitlements are provided.

- **Why Select This Entitlement:** If you need someone to coordinate across different compliance teams and ensure that activities are on track, this role is essential.
- **Example Use Case:** A compliance initiative to align the organization with CMMC standards needs coordination between different departments—the Project Manager sets timelines and tracks progress across various contributors.
- **PSR Selection:** Manager, Consultant, Client Admin

SSP Manager

- **Entitlement Definition:** The SSP Manager entitlement controls SSP access.
- **Capabilities:** They can create projects, assign roles to team members, manage timelines, and monitor project status. They can also have access to view and contribute to compliance evidence and ensure that key milestones are met if those entitlements are provided.
- **Why Select This Entitlement:** If you need someone to coordinate across different compliance teams and ensure that activities are on track, this role is essential. SSP Managers might also need visibility into POA&M activities to update compliance documentation accordingly. See [POA&M Manager](#)
- **Example Use Case:** A compliance initiative to align the organization with CMMC standards needs coordination between different departments—the Project Manager sets timelines and tracks progress across various contributors.
- **PSR Selection:** Manager, Consultant, Client Admin

2. Maturity

The Maturity module entitlements include authorizations specific to managing the deficiencies and associated remediation activities including POA&M management and reporting.

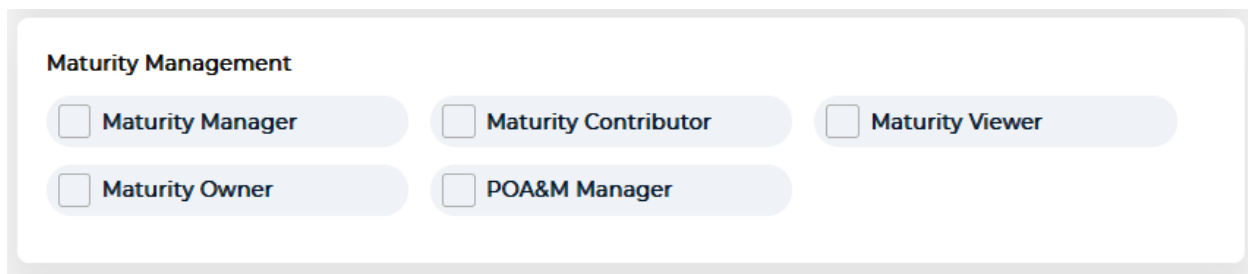


Figure 2.1 – Maturity Management Entitlements

Maturity Manager

- **Entitlement Definition:** The Maturity Manager entitlement is responsible for managing the improvements in maturity over time, including identifying deficiencies, creating Horizons and Workteams, defining and assigning tasks, and generating status reports.
- **Capabilities:** Users with this entitlement can configure maturity elements, align controls across different standards, generate remediation reports, and oversee contributor activities. They also hold authority over updates to the compliance efforts.
- **Why Select This Entitlement:** Choose this role if the user is responsible for establishing remediation activities and ensuring alignment with relevant resources performing the work efforts.
- **Example Use Case:** Reporting remediation status with internal and external stakeholders as well as auditors.
- **PSR Selection:** Manager, Consultant, Client Admin

Maturity Contributor

- **Entitlement Definition:** A Maturity Contributor provides information, documentation, and support needed to fulfill remediation activities.
- **Capabilities:** They can upload updated evidence, respond to remediation requests, and contribute insights on control implementations and effectiveness.
- **Why Select This Entitlement:** Assign this role to subject matter experts or team members who need to provide specific remediation evidence or information but are not using the CRT as a primary part of their job responsibilities.
- **Example Use Case:** An IT staff member updates a firewall configuration to align network security controls with compliance requirements
- **PSR Selection:** Manager, Consultant, Client Admin, User

Maturity Viewer

- **Entitlement Definition:** The Maturity Viewer is able to access and view remediation activities, reports, and progress without edit entitlements.
- **Capabilities:** They can view maturity status, tasks, and reports to stay informed of the organization's remediation efforts.
- **Why Select This Entitlement:** Ideal for executives or stakeholders who need visibility into remediation activities without the inherent liability associated with performing and updating day-to-day tasks.
- **Example Use Case:** A CISO wants to track the progress of compliance remediation activities and monitor readiness for upcoming audits.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Maturity Owner

- **Entitlement Definition:** The Maturity Owner holds ultimate responsibility for compliance remediation activities, ensuring that all deficiencies and deviations are documented, completed, and standards are met.
- **Capabilities:** They oversee all remediation aspects, approve tasks and activities, and make critical remediation decisions.
- **Why Select This Entitlement:** Best for senior leaders accountable for ensuring compliance is achieved and maintained.
- **Example Use Case:** The head of compliance signs off on final remediation efforts before they are submitted to an external auditor.
- **PSR Selection:** Manager, Consultant, Client Admin

POA&M Manager

- **Entitlement Definition:** The Plan of Action and Milestone (POA&M) Manager entitlement controls and reports on POA&M status.
- **Capabilities:** They can create projects, assign roles to team members, manage timelines, and monitor project status. They can also have access to view and contribute to compliance evidence and ensure that key milestones are met.
- **Why Select This Entitlement:** If you need someone to coordinate remediation activities with a framework designated POA&M guidelines across different compliance teams and ensure that activities are on track and provide the required reporting, this role is essential. POA&M Managers may need access to SSP data to align remediation efforts with compliance gaps. See [SSP Manager](#)

- **Example Use Case:** A compliance initiative to align the organization with CMMC standards needs coordination between different departments—the POA&M Manager sets tasks, timelines and tracks progress across the various contributors.
- **PSR Selection:** Manager, Consultant, Client Admin

3. Risk Register

The Risk Register module entitlements include authorizations specific to managing risks, remediation, and contingency planning.

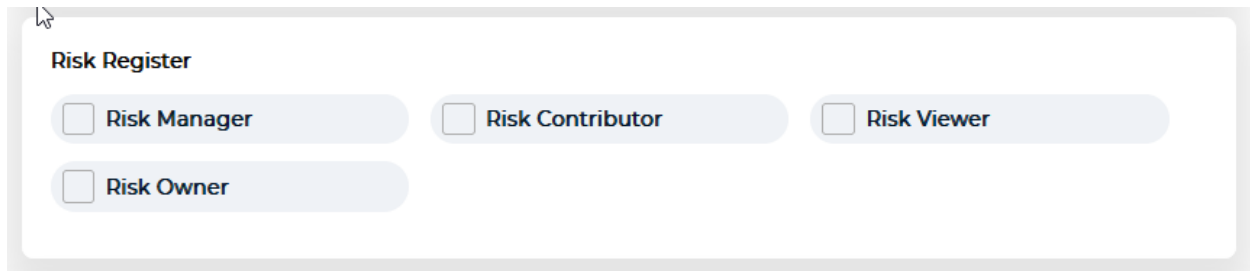


Figure 3.1 – Risk Register Entitlements

Risk Manager

- **Entitlement Definition:** The Risk Manager entitlement is responsible for configuring the Risk Register .
- **Capabilities:** Users with this entitlement can configure the Risk Register elements, align Risk Groups and Spotlights, and generate Risk reports, and oversee contributor activities. They also hold authority over updates to risk reduction efforts.
- **Why Select This Entitlement:** Choose this role if the user is responsible for establishing risk activities and ensuring alignment with relevant resources performing the work efforts.
- **Example Use Case:** Reporting on Risk status with internal and external stakeholders as well as auditors.
- **PSR Selection:** Manager, Consultant, Client Admin

Risk Contributor

- **Entitlement Definition:** A Risk Contributor provides information, documentation, and support needed to document and track risk related activities.
- **Capabilities:** They can upload updated evidence, respond to new reported risk, and contribute insights on mitigation and contingency implementations and effectiveness.
- **Why Select This Entitlement:** Assign this role to subject matter experts or team members who need to provide specific risk related evidence or risk information but are not using the CRT as a primary part of their job responsibilities.
- **Example Use Case:** An IT staff member updates a firewall configuration to align network security controls with compliance requirements and needs to update the associated risk on the Risk Register.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Risk Viewer

- **Entitlement Definition:** The Risk Viewer is able to access and view Risks, reports, and mitigation progress.
- **Capabilities:** They can view Risks on the Register and reports to stay informed.
- **Why Select This Entitlement:** Ideal for executives or stakeholders who need visibility into risk related activities without the inherent liability associated with updating details on specific risks.

- **Example Use Case:** A CISO wants to track the progress of risk mitigation activities and monitor contingency planning
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Risk Owner

- **Entitlement Definition:** The Risk Owner holds ultimate responsibility for managing a specific Risk
- **Capabilities:** They own all aspects of the Risk for which they are designated as Owner
- **Why Select This Entitlement:** Enables the User to be included in the Risk Owner drop down list
- **Example Use Case:** The head of a department is assigned as a specific Risk Owner relative to their department. They sign off on final mitigation efforts before they are submitted to a Risk Assessor.
- **PSR Selection:** Manager, Consultant, Client Admin

4. Incident Commander

The Incident Commander module

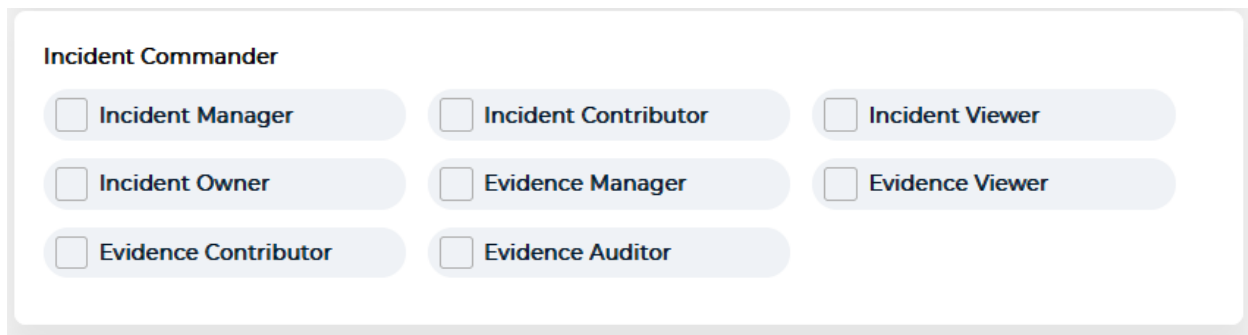


Figure 4.1 – Incident Commander Entitlements

Incident Manager

- **Entitlement Definition:** The Incident Manager entitlement is responsible for configuring and managing the Incident Commander module.
- **Capabilities:** Users with this entitlement can configure the Incident Commander elements, add new Incidents and generate Incident reports while overseeing contributor activities. They also hold authority over updates to Incident risk reduction efforts.
- **Why Select This Entitlement:** Choose this role if the user is responsible for initiating Incident activities and ensuring alignment with relevant resources performing the response and remediation work efforts.
- **Example Use Case:** Reporting on Incident status with internal and external stakeholders.
- **PSR Selection:** Manager, Consultant, Client Admin

Incident Contributor

- **Entitlement Definition:** An Incident Contributor provides information, documentation, and support needed to document and track Incident related activities.
- **Capabilities:** They can upload updated evidence, respond to new reported Incidents, and contribute insights on response and remediation effectiveness.
- **Why Select This Entitlement:** Assign this role to subject matter experts or team members who need to provide specific Incident related details but do not use the CRT as a primary part of their job responsibilities.
- **Example Use Case:** An IT staff member uploads AD Device listing to provide details related to an Incident.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Incident Viewer

- **Entitlement Definition:** The Incident Viewer is able to view Incidents and generate reports
- **Capabilities:** They can view Incident details and reports to stay informed.
- **Why Select This Entitlement:** Ideal for executives or stakeholders who need visibility into Incident related activities without the inherent liability associated with updating details on specific Incidents.
- **Example Use Case:** A CISO wants to track the progress of Incident response activities and monitor recovery progress
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Incident Owner

- **Entitlement Definition:** The Incident Owner holds ultimate responsibility for managing a specific Incident
- **Capabilities:** They own all aspects of the Incident for which they are designated as Owner
- **Why Select This Entitlement:** Enables the User to be included in the Incident Owner drop down list
- **Example Use Case:** A Information Security Sr Analyst is assigned as a specific Incident Owner relative to their expertise. They sign off on all recovery and remediation efforts before they are submitted for Executive approval.
- **PSR Selection:** Manager, Consultant, Client Admin

Evidence Manager

- **Entitlement Definition:** The Evidence Manager entitlement provides permissions for managing Evidence associated with evidence associated with an Incident.
- **Capabilities:** Users with this entitlement can add new evidence to Incidents, edit existing Incident evidence, and generate Incident evidence reports while overseeing Evidence Contributor activities.
- **Why Select This Entitlement:** Choose this role if the user is responsible for managing Incident Evidence and ensuring relevant resources are adding the appropriate evidence during an Incident.
- **Example Use Case:** Examining and confirming evidence validity associated with an Incident.
- **PSR Selection:** Manager, Consultant, Client Admin

Evidence Contributor

- **Entitlement Definition:** The Evidence Contributor entitlement provides permission to add Incident evidence
- **Capabilities:** Users with this entitlement can add new evidence to Incidents and generate evidence reports.
- **Why Select This Entitlement:** Choose this role if the user is responsible for adding evidence to an Incident
- **Example Use Case:** Examining and confirming evidence validity associated with an Incident.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Evidence Viewer

- **Entitlement Definition:** The Evidence Viewer entitlement provides visibility to Incident evidence
- **Capabilities:** Users with this entitlement can view Incident evidence
- **Why Select This Entitlement:** Choose this role if the user has a need to view Incident evidence
- **Example Use Case:** Examining evidence associated with an Incident.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Evidence Auditor

- **Entitlement Definition:** The Evidence Auditor entitlement provides visibility to Incident evidence but as part of a specific set of Auditor Entitlements
- **Capabilities:** Auditors with this entitlement can view Incident evidence
- **Why Select This Entitlement:** Choose this role if an Auditor has a need to view Incident evidence
- **Example Use Case:** An auditor examining evidence associated with an Incident.
- **PSR Selection:** Auditor

5. Policy Manager

The Policy Management module provides...

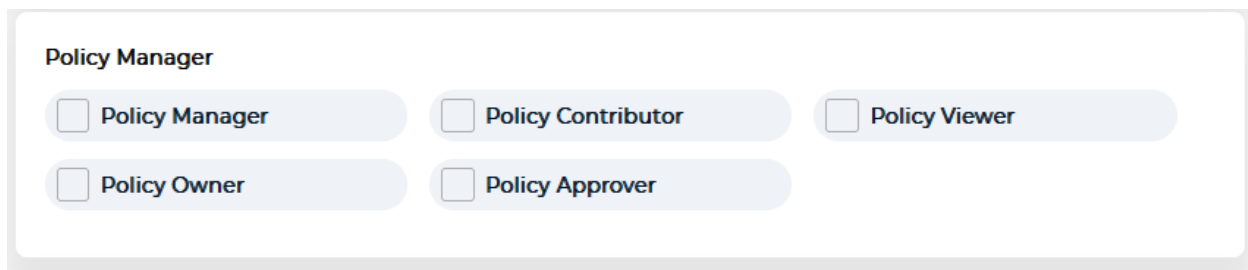


Figure 5.1 – Policy Manager Entitlements

Policy Manager

- **Entitlement Definition:** The Policy Manager entitlement is responsible for configuring and managing the Policy Manager Module.
- **Capabilities:** Users with this entitlement can configure the Policy Manager elements, add new Policies and export Policy reports while overseeing Contributor activities. They also hold authority over updates to Policies and the review process.
- **Why Select This Entitlement:** Choose this role if the user is responsible for initiating Policy activities and ensuring alignment with relevant department resources authoring and approving Policy work efforts.
- **Example Use Case:** Reporting on Policy status with internal and external stakeholders.
- **PSR Selection:** Manager, Consultant, Client Admin

Policy Contributor

- **Entitlement Definition:** A Policy Contributor provides detailed Policy information, uploads draft documentation, and provides the support needed to document and track Policies and Policy development activities.
- **Capabilities:** They can upload updated Policy verbiage, respond to new Policy requests, and contribute insights on Policy effectiveness.
- **Why Select This Entitlement:** Assign this role to subject matter experts or team members who need to provide specific Policy related details but do not use the CRT as a primary part of their job responsibilities.
- **Example Use Case:** An IT staff member drafts a technical Policy to provide details related to a regulatory requirement and needs to upload into the Policy Manager as a Draft for review and approval processing.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Policy Viewer

- **Entitlement Definition:** The Policy Viewer is able to view policies and generate reports.
- **Capabilities:** They can view policy details and reports to stay informed.

- **Why Select This Entitlement:** Ideal for executives or stakeholders who need visibility into policies related activities without the inherent liability associated with updating details on specific policies.
- **Example Use Case:** A CISO wants to track the progress of policies activities and monitor progress.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Policy Owner

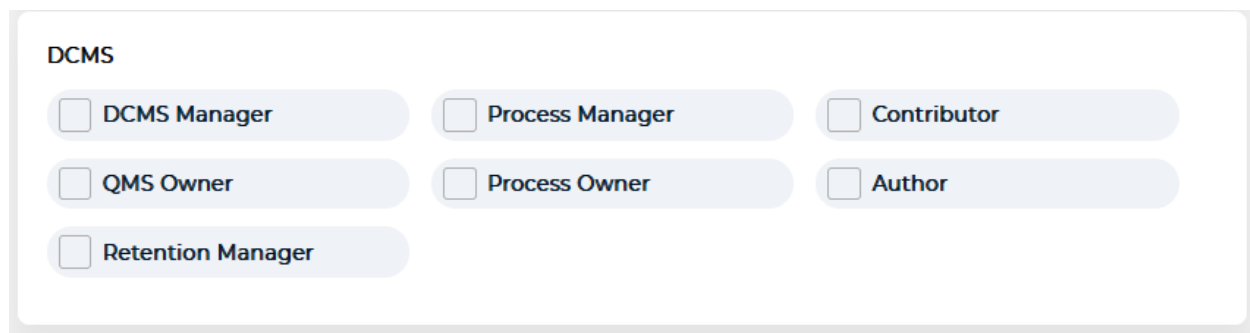
- **Entitlement Definition:** The Policy Owner holds ultimate responsibility for maintaining and managing specific Policies
- **Capabilities:** They own all aspects of the Policy for which they are designated as Owner
- **Why Select This Entitlement:** Enables the User to be included in the Policy Owner drop down list
- **Example Use Case:** A business leader is assigned as a specific Policy Owner relative to their position and expertise within the organization. They sign off on all drafts and revision efforts before they are submitted for Executive approval and distribution.
- **PSR Selection:** Manager, Consultant, Client Admin

Policy Approver

- **Entitlement Definition:** The Policy Approver holds responsibility for approving all updates and changes to a specific Policy
- **Capabilities:** The Policy Approver owns the final approval of the Policy for which they are designated as Owner prior to distribution to the organization
- **Why Select This Entitlement:** Enables the User to be included as a Policy Approver in the drop down list
- **Example Use Case:** An executive is assigned as a Policy Approver relative to their position and expertise within the organization. They sign off on Policies for the Executive approval prior to distribution
- **PSR Selection:** Manager, Consultant, Client Admin

6. DCMS

The Document Control Management System provides



DCMS

<input type="checkbox"/> DCMS Manager	<input type="checkbox"/> Process Manager	<input type="checkbox"/> Contributor
<input type="checkbox"/> QMS Owner	<input type="checkbox"/> Process Owner	<input type="checkbox"/> Author
<input type="checkbox"/> Retention Manager		

Figure 6.1 – DCMS Entitlements

DCMS Manager

- **Entitlement Definition:** The DCMS Manager entitlement is responsible for configuring and managing the DCMS Module.
- **Capabilities:** Users with this entitlement can configure the DCMS elements, add new documents and export necessary reports while overseeing Contributor activities. They also hold authority over updates to managed documents and the review process.

- **Why Select This Entitlement:** Choose this role if the user is responsible for initiating document update activities and ensuring alignment with relevant department resources authoring and approving document work efforts.
- **Example Use Case:** Reporting on document status with internal and external stakeholders.
- **PSR Selection:** Manager, Consultant, Client Admin

Process Manager

- **Entitlement Definition:** The “Process Manager” entitlement ensures that the user appears in the “Process Manager” drop lists as part of the DCMS review and approval process. Users with this entitlement can also view all DCMS list items.
- **Capabilities:** **Ability to approve documents in the approval process when the user is listed as a Process Manager on that document.**
- **Why Select This Entitlement:** When you want a user to be responsible for being part of the approval process of documents.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Contributor

- **Entitlement Definition:** The “Contributor” entitlement ensures that the user appears in the “Contributor” drop lists as part of the DCMS creation, review, and approval process. Users with this entitlement can also view all DCMS list items.
- **Capabilities:** You must be a contributor if you wish to enter change requests for already existing DCMS items.
- **Why Select This Entitlement:**
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

QMS Owner

- **Entitlement Definition:** The “QMS Owner” entitlement ensures that the user appears in the “QMS Owner” drop lists as part of the DCMS review and approval process.
- **Capabilities:** Similar to that of the Process Manager, with the exception of that users with this entitlement may be an approver of this type. **Ability to approve documents in the approval process when the user is listed as a QMS Owner on that document.**
- **Why Select This Entitlement:** When you want a user to be responsible for being part of the approval process of documents.
- **PSR Selection:** Manager, Consultant, Client Admin

Process Owner

- **Entitlement Definition:** The “Process Owner” entitlement ensures that the user appears in the “Process Owner” drop lists as part of the DCMS review and approval process. Users with this entitlement can also view all DCMS list items.
- **Capabilities:** Similar to that of the Process Manager, with the exception of that users with this entitlement may be an approver of this type. **Ability to approve documents in the approval process when the user is listed as a Process Owner on that document.**
- **Why Select This Entitlement:** When you want a user to be responsible for being part of the approval process of documents.
- **PSR Selection:** Manager, Consultant, Client Admin

Author

- **Entitlement Definition:** The author is responsible for creating documents within the system and shows up in the “Author” droplist within the application.
- **Capabilities:** Creating, Saving, and Publishing documents to the DCMS list.
- **Why Select This Entitlement:** If you have a user that you want to have author ability and show up in the “Author” drop list.
- **PSR Selection:** Manager, Consultant, Client Admin

Retention Manager

- **Entitlement Definition:** The Retention Manager entitlement can be given to any individual who would be responsible for the act of deleting a DCMS document.
- **Capabilities:** Deleting of a DCMS document.
- **Why Select This Entitlement:** If you have users that also require the ability to delete their, or other documents within the system.
- **PSR Selection:** Manager, Consultant, Client Admin

7. Waiver Management

The Waiver Management entitlements differ from other module entitlements as Waiver Management is not an independent module, but is an operational function of each module...



Figure 7.1 – Waiver Management Entitlements

Waiver Manger

- **Entitlement Definition:** The Waiver Manager entitlement is responsible for configuring and managing Wavers.
- **Capabilities:** Users with this entitlement can add and manage Wavers originating in any CRT Module and export necessary reports. They also hold authority over updates to Waiver documents and the review process.
- **Why Select This Entitlement:** Choose this role if the user is responsible for initiating Waiver documents, update activities, or ensuring alignment with relevant department resources authoring and approving Waiver documents.
- **Example Use Case:** Reporting on Waiver status with internal and external stakeholders.
- **PSR Selection:** Manager, Consultant, Client Admin

Waiver Contributor

- **Entitlement Definition:** The Contributor entitlement ensures that the user can initiate a new Waiver request or add information as part of the Waiver creation, review, and approval process. Users with this entitlement can also view Wavers.
- **Capabilities:** You must be a contributor if you wish to enter details or attachments to existing DCMS items.

- **Why Select This Entitlement:** Select this entitlement when the user needs access and responsibility for adding and editing their Waivers but not managing others Waivers and details.
- **Example Use Case:** Business unit lead needs to add and manager a Risk Waiver for their product pending a security update.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Waiver Viewer

- **Entitlement Definition:** The Waiver Viewer is able to view most Waivers and generate reports
- **Capabilities:** They can view Waiver details and reports to stay informed.
- **Why Select This Entitlement:** Ideal for executives or stakeholders who need visibility into Waiver related activities without the inherent liability associated with influencing details on specific Waivers in the process.
- **Example Use Case:** A CISO wants to track the progress of a specific vulnerability response activity and monitor progress as well as business justification from the Waiver Owner pending the completion of a delayed remediation action.
- **PSR Selection:** Manager, Consultant, Client Admin, User, Guest

Waiver Owner

- **Entitlement Definition:** The Waiver Owner entitlement ensures that the user appears in the “Waiver Owner” drop lists as part of the Waiver review and approval process. Users with this entitlement can also view all Waivers.
- **Capabilities:** Similar to that of the Waiver Manager, with the exception of that users with this entitlement may be an approver also. Ability to approve Waivers in the approval process when the user is listed as a Process Owner on that Waiver.
- **Why Select This Entitlement:** When you want a user to be responsible for being part of the approval process of Waivers.
- **PSR Selection:** Manager, Consultant, Client Admin

Waiver Auditor

- **Entitlement Definition:** The Waiver Auditor entitlement provides visibility to Waivers and associated details but as part of a specific set of Auditor Entitlements
- **Capabilities:** Auditors with this entitlement can view Waivers and attached details
- **Why Select This Entitlement:** Choose this role if an Auditor has a need to view Waivers
- **Example Use Case:** An auditor examining evidence associated with a decision to provide a Waiver.
- **PSR Selection:** Auditor

Waiver Approver

- **Entitlement Definition:** The Waiver Approver holds responsibility for approving all updates and changes to a specific Waiver
- **Capabilities:** The Waiver Approver owns a step in the approval process for the Waiver to which they are designated as an Approver
- **Why Select This Entitlement:** Enables the User to be included as a Waiver Approver in the drop down list
- **Example Use Case:** An executive is assigned as a Waiver Approver relative to their position and expertise within the organization. They sign off on Waivers as the Executive approver
- **PSR Selection:** Manager, Consultant, Client Admin

8. Specialty Entitlements

There are certain Specialty Entitlements that enable very specific functions or access. These are generally limited to a select sub-set of users in conjunction with other entitlements, but are not required.

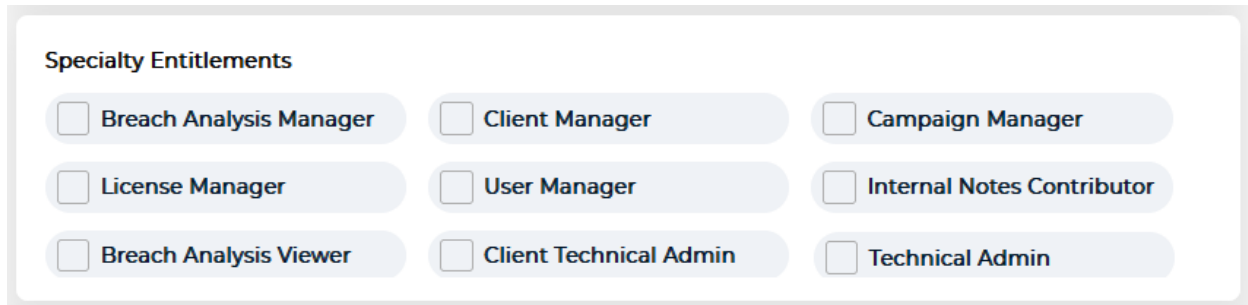


Figure 8.1 – Specialty Entitlements

Data Manager Specialty Entitlements

Client Manager

- **Entitlement Definition:** Provides access to the Client, enabling configuration management
- **Capabilities:** Add, Edit, and Manage Client details
- **Why Select This Entitlement:** When a has responsibility for maintaining details pertinent to a specific Client to update details including contact, technical resources, and physical locations
- **Example Use Case:** The IT Manager resigned at a client, and the new Manager's details need to be updated in the CRT. This entitlement is required to perform this update.
- **PSR Selection:** Manager, Consultant, Client Admin

User Manager

- **Entitlement Definition:** Provides access to Manage User details and entitlements
- **Capabilities:** User Managers can create users, assign entitlements to team members, manage authorizations, and monitor usage. They can also have access to view user logs but are limited to managing Users at or below their assigned PSR level.
- **Why Select This Entitlement:** Provide access to someone coordinating user access across different teams and ensure that users have only the required access.
- **Example Use Case:** A compliance initiative to align the organization with CMMC standards needs coordination between different departments—the User Manager sets appropriate access to the specific engagements. timelines and tracks progress across various contributors.
- **PSR Selection:** Manager, Consultant, Client Admin

Campaign Manager

- **Entitlement Definition:** Provides Add/Edit functionality for configuring and managing Campaigns
- **Capabilities:** The Campaign Manager can create new Campaigns, edit existing Campaigns, and perform analysis on the responses of the Campaign.
- **Why Select This Entitlement:** Provide access to a user needing to add, configure, edit or analyze a Campaign.
- **Example Use Case:** An company needs to send out a quick assessment or questionnaire to current or potential clients asking for details on their use of a product or application that has been identified as vulnerable so they can determine the potential risk.
- **PSR Selection:** Manager, Consultant, Client Admin

Internal Notes Contributor

- **Entitlement Definition:** Entitlement to enable access to the Compliance Module Internal Notes functionality
- **Capabilities:** The CRT allows internal notes to be captured during an Assessment. This entitlement provides the user with visibility to the internal notes tab.
- **Why Select This Entitlement:** Provide access to a user needing to add or edit internal notes.
- **Example Use Case:** An Assessment is being conducted and an Assessor needs to make an internal, non-client facing, note for reference or pose a question to another internal Assessor.
- **PSR Selection:** Manager, Consultant, Client Admin, User

Non Data Manager Specialty Entitlements

- **Technical Admin** – Instance resource entitlement to access logs and to change the System Configuration details for the CRT Application
- **Client Technical Admin** - Client resource entitlement to add/edit technical configuration for a Client (File Repo, SSO, client logo, and other technical configuration settings)
- **License Manager** – Enables the user to manage Client Licensing. Please note that enabling Client access could incur additional costs based on the licenses provided by the License Manager.
- **Sales Manager** – Users with this entitlement are listed in the Sales Manager dropdown and manage sales resources
- **Sales Representative** - Users with this entitlement are listed in the Sales Representative dropdown

Access Profiles (Future Update)

Building the Right Access Profiles for Your Team

Selecting the appropriate entitlements is crucial to streamline compliance processes while maintaining security and accountability. Assign access based on responsibilities within the compliance framework, ensuring that users have the right capabilities to perform their duties effectively. Whether it's managing projects, contributing evidence, or ensuring compliance accuracy, each entitlement and the accumulation into an Access Profile is designed to meet specific needs within your organization.

Summary of Entitlements

Full Access & Management: Compliance Manager, Compliance Owner, Project Manager,

As Needed Access: Compliance Contributor

Evidence Handling: Evidence Manager, Evidence Viewing,

Audit & Review:, Auditor, Evidence Auditor

Example Scenarios for Access Profile

- If your organization is starting a new compliance initiative and you need someone to coordinate all the moving parts, assign the Project Manager entitlement.
- For someone responsible for ensuring internal controls align with evolving regulatory standards, use the Compliance Manager role.
- When gathering documentation for an audit, assign Evidence Manager and Compliance Contributor roles to ensure evidence is collected, validated, and organized effectively.

We hope this guide helps you make informed decisions about assigning roles in the CRT. If you have any questions or need further assistance, please reach out to our support team.