INEIGHT

Compliance/Completions Roles & Permissions

Setup Guide

COMPLIANCE

COMPLETIONS

Changelog

This changelog contains only significant or other notable changes to the document revision. Editorial or minor changes that do not affect the context of the document are not included in the changelog.

Rev	Date	Description
1.0	13-June-2025	Initial Release

Contents

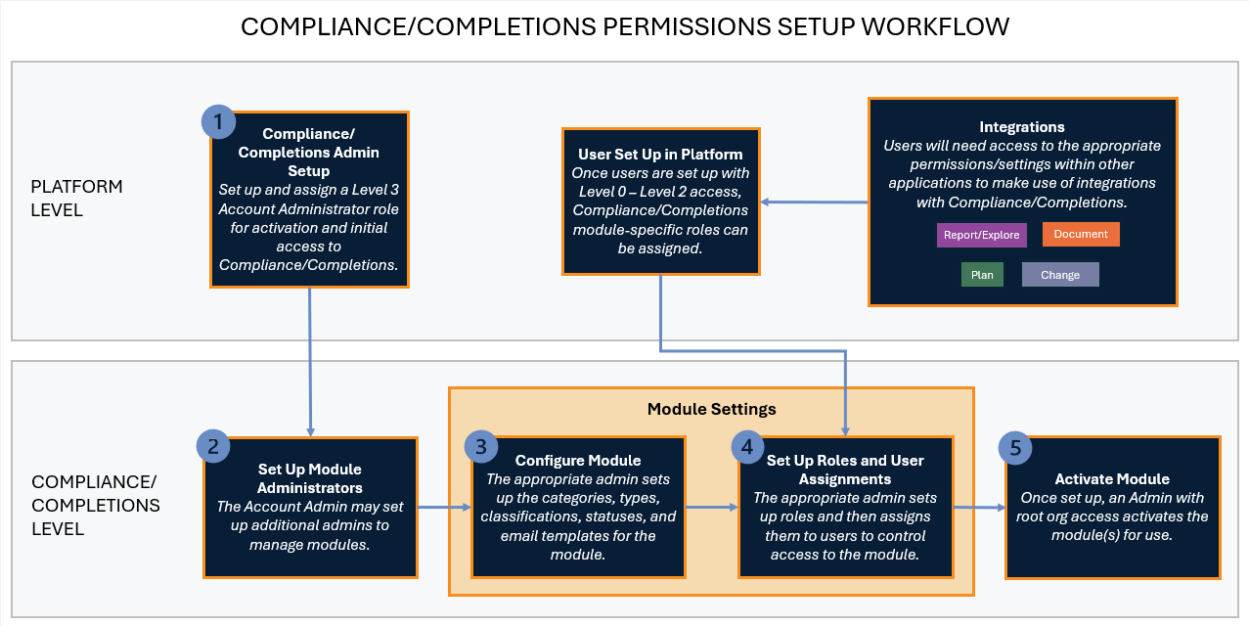
Overview

This guide walks through how to set up the roles and permissions required to use the Compliance and Completions applications. It begins with instruction for setting up roles and permissions at the InEight Platform level for initial administrative access, followed by how to configure roles and permissions within Compliance/Completions for module-level access for admins and end users. This document also includes guidance for setting up access to reporting and Compliance/Completions integrations with other applications.

NOTE:	This document contains multiple links to additional learning content. For all Knowledge Library content that takes you to InEight Compliance, the same information applies to InEight Completions, and you will find the same learning content available in the Completions section of the Knowledge Library.

Compliance/Completions Permissions Setup Workflow

The following diagram walks through the high-level workflow for setting up access to Compliance and Completions for administrators and end users.



A Unique Process

Note that the process for setting up access to Compliance/Completions is different from other InEight U applications. For many of the other applications within the InEight suite, permissions are configured under the roles defined at the InEight Platform level. For example, to set up the access for InEight

Control, a role would be created under Roles and permissions in InEight Platform and the appropriate permissions would be selected under the Control section for that role.

For Compliance and Completions, note that a Level 3 Administrator must be set up at the Platform level for initial access to the Compliance/Completions applications (see step 1 of the above diagram). Once Compliance/Completions is accessible to the admin, all other users can be granted roles and permissions within the Compliance and Completions applications themselves (steps 2 through 5 in the diagram). Note that these users must first have user accounts (with Level 0 –Level 2 access) within InEight Platform.

Basic Steps of the Process

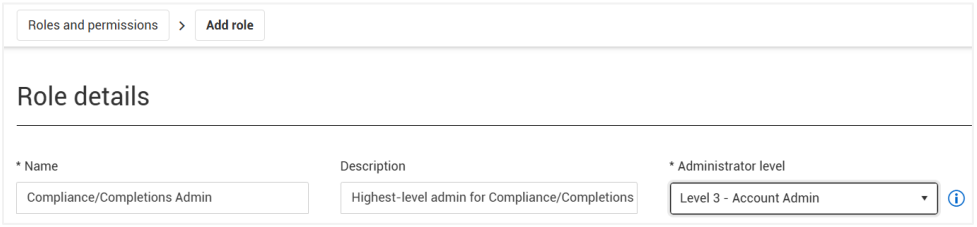
The remainder of this document walks through each step of the process for setting up Compliance/Completions access in greater detail, including links to additional resources as needed, to ensure you get your organization set up effectively.

Administrator Role Setup in InEight Platform

To activate the Compliance/Completion applications and give initial access, an administrator role must be created within InEight Platform and assigned to a user. That user will have full access to Compliance/Completions and can then set up other roles within those applications as needed.

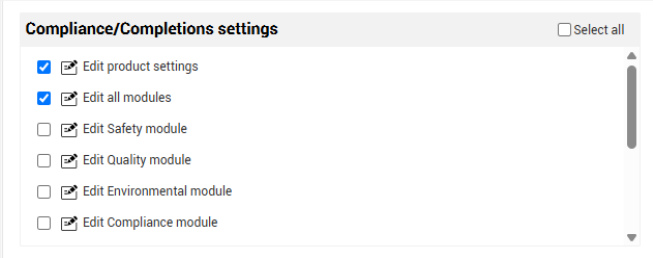
Within InEight Platform, go to **Suite administration > Roles and permissions** and add or edit a role.

- Ensure that the role has Level 3 access.



Compliance/Completions Settings

- Under **Organization and project > Compliance/Completions** settings:



  - Select Edit product settings to give the administrator access to Compliance/Completions product settings at the org and project levels.

- Select Edit all Modules to give initial administrative access to all modules within Compliance/Completions.
- NOTE: There are several permissions listed under the Organization and project > Compliance/Completions settings that might not apply to your organization, such as:
  - Edit punchlist module

    Edit custom module
  - Edit Document module
  - Edit Contract module
  - Edit Change module
  - Edit Plan & Progress module

  These will only have functionality if the corresponding integrations/functionality have been configured. See the *Compliance/Completions Integration with Other Applications* section of this document for details on how to set up integrations between Compliance/Completions and other applications. Otherwise, you can disregard the settings that don't apply by leaving them unchecked.

Other Settings to Consider for the Administrator Role

When setting up the Platform-level administrator role, there are other settings to consider in addition to the Compliance/Completions settings, based on the needs of your administrator within your organization.

Suite Administration

Under the Suite administration section of the role's permissions, you might want to grant the following permissions:

Permission	Considerations
User management > View Users	Granting permission to view users can be helpful for troubleshooting purposes. If a user is not showing up in Compliance/Completions, this would allow the Compliance/Completions administrator to look at the Platform level to confirm if the user is set up in the system.
User management > Assign/unassign roles to users (Level 2 and 3 users only)	The Compliance/Completions administrator does NOT need this permission to administrate roles and permissions within Compliance/Completions. Depending on your organization, you might have a different system-level administrator in charge of adding users and assigning their roles at the Platform level.
Roles and permissions > View roles and permissions	Along with viewing users, this permission can help the Compliance/Completions administrator confirm a user is set up with the appropriate role to use Compliance/Completions as needed.

Permission	Considerations
Application integrations > View InEight Document	This permission allows you to view InEight Document under Application integrations so that integration between InEight Document and other applications, including Compliance/Completions, can be configured. Whether that access is granted to your Compliance/Completions administrator or another administrator at a higher level is a governance question for your organization to consider.

Organization and Project

Under the Organization and project section, the following permissions should be considered:

Permission	Considerations
Projects > View new projects	Projects might reside in the *New* status for a period prior to becoming *Active*. This permission gives the Compliance/Completions administrator access to configure and publish to projects still in the *New* status before they go live.
Projects > View closed projects	There might be a need to look up information from past projects. This would give that ability to the administrator.
Under Projects, all Project structure and Project values permissions	These permissions are required for using the project structure headers within Compliance/Completions.
Documents > View documents	This permission is required to view PDF attachments, including the PDF signatures and doc links within the attachments and is therefore recommended.
Documents > Download documents	Along with the View documents permission, this permission is recommended so that PDF documents can be downloaded as needed.

Master Data Libraries

Under the Master Data Libraries section, consider the following permissions:

Permission	Considerations
Operational employees, owned equipment, rented equipment > View permissions	This permission might be helpful to look within the master data library to confirm if an operational resource that isn't available in Compliance/Completions actually exists in the InEight Platform. This permission is also required to assign operational resources to a project. You might want to grant the Compliance/Completions administrator access to assign an operational resource so they can quickly add them to forms, or you might want that to be controlled by a different role in your organization.
Vendors > View vendors	This permission can help the administrator confirm if a vendor has been set up in InEight Platform. It is also needed for assigning vendors to a project. Whether or not your Compliance/Completions administrator needs to assign vendors to a project depends on how governance of the software is set up in your organization.

Document

Under the Document section, if your administrator will be using InEight Document, this permission grants them access to open the Document application from within InEight Platform, giving easy access to navigate between applications.

Report

Under the Report > Reports section, the administrator should be given access to View reports, along with all the permissions beneath it. This allows the administrator to access the Report application and have full access to view and run reports, configure personalized views, and set up and view subscriptions.

The View integration reports permission should also be selected. This gives access to print reports from within Compliance/Completions, on the Events and Tasks pages.

Explore

Because Compliance/Completions reports are built through APIs, the administrator should have access to the following within the Explore section:

- View Compliance APIs/View Completions web APIs

  This provides access to all Compliance/Completions reporting API data. This access would be for the person in your organization tasked with building out your Compliance/Completions-related corporate reports and dashboards. They would use these APIs to feed data into their reporting tool (e.g., Power BI).

- View API generator, along with its child permissions

  With access to the API generator permissions, the administrator can create an API with a specific data set, and it will generate a link that they can use wherever needed (e.g., Excel, Power BI). This can be an efficient way to build out reports, when time and resources are limited.

NOTE:	Users granted access to the API generator will only see Compliance/Completions data they have been given access to. For example, if they are not granted access to a form in Compliance, they will not have access to that form's data within the API generator.

Role Assignment to User

Once created, the role can then be assigned to the appropriate user to act as the highest-level administrator of Compliance/Completions.

End User Role Setup in InEight Platform

All users given a role within InEight Platform will automatically have access to launch the Compliance/Completions applications but will not have access at that point to perform any functions

within those applications. Their access to do things in the applications will be granted by an administrator within the Compliance/Completions applications at the module level.

When setting up users in InEight Platform, however, there are a few Platform-level permissions to consider.

Permission	Considerations
Organization and project > Projects > View closed projects	Consider if there any roles that might need access to closed projects. For example, a site supervisor who worked on a project now closed but wants to go back to review some trending.
Organization and project > Documents > View documents	This permission is required to view PDF attachments, including the PDF signatures and doc links within the attachments and is therefore recommended.
Document > Document > View InEight Document	Gives access to launch InEight Document from within InEight Platform. This can be useful for users that use both Compliance/Completions and Document.
Report > Reports > View integration reports	Needed to access the Print option on the Events/Tasks pages.

Module Roles & Permissions Setup

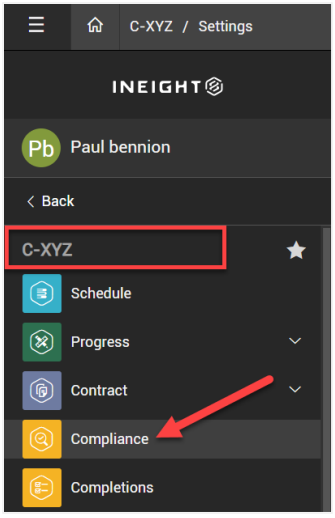
With a Level 3 administrator role set up at the InEight Platform level, that administrator can then access Compliance and Completions to set up roles and permissions at the module level.

Module-Level Administrators

The number of administrators you have for Compliance and Completions will depend on the size and needs of your organization. Smaller companies might find that a single Level 3 administrator is sufficient for managing all Compliance/Completions modules, and there is no need to create additional module-level administrator roles. For other companies, having distinct administrators for each module makes sense, allowing each manager to only have access to the work that they manage. For example, perhaps your organization has different managers for safety and quality work, so you create administrator roles for both the Safety and Quality modules and then give each manager only access to their respective modules.

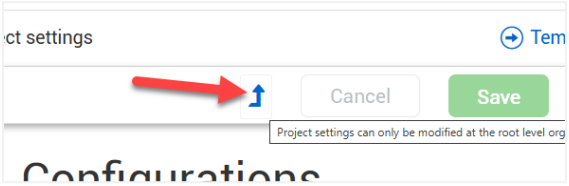
Accessing Compliance/Completions at Organization vs. Project Level

The Compliance and Completions applications can be opened from within InEight Platform at either the organization or project level. The below image shows opening the Compliance application from the organization level.



Because initial setup of the Compliance/Completions modules (setting up categories, types, classifications, etc.) requires organization-level access, it is recommended that the administrator opens Compliance/Completions from the root organization level.

If you find yourself within Module Settings at a project level and need to configure settings at the organization level, an arrow icon gives you easy access to go to the organization level settings.

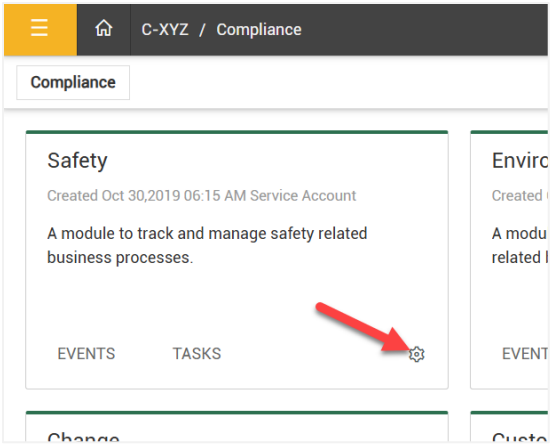


For additional information about organization level and project level settings, consult the following topics:

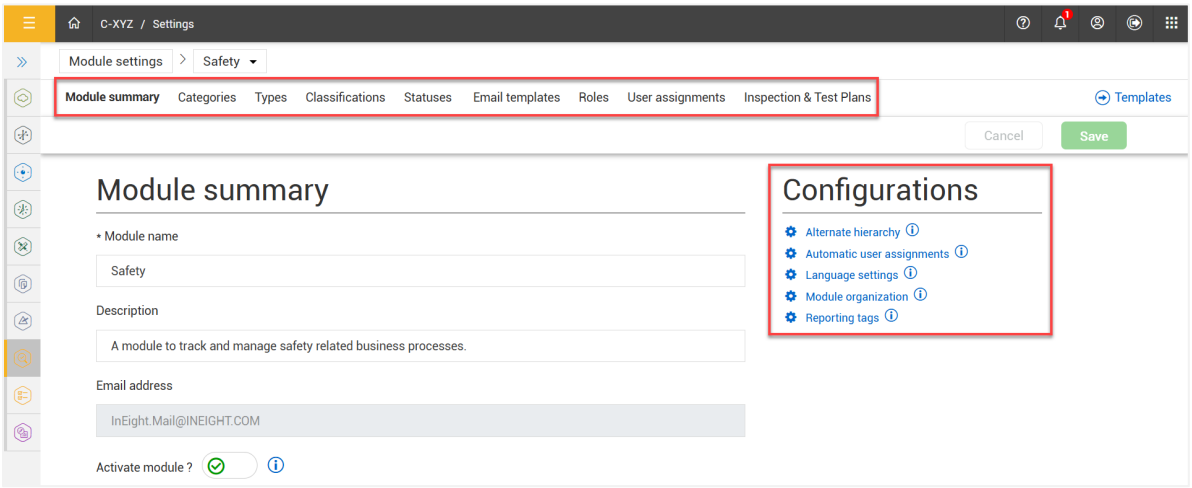
- Organization level settings
- Project level settings

Initial Module Access

For the Level 3 administrator to set up initial access, they need to open Compliance or Completions from the organization level and select the Settings icon on a module's tile.



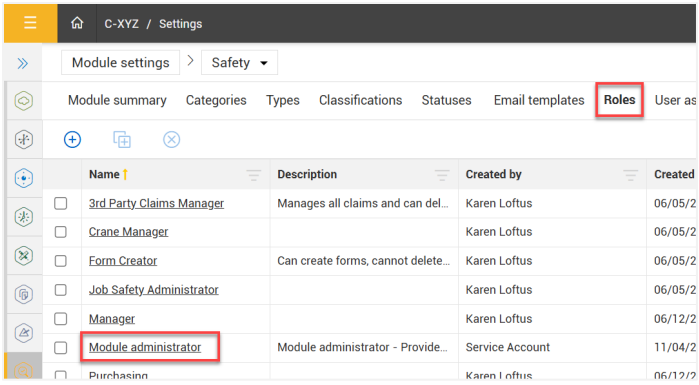
This opens the Module summary page of that specific module at the root organization level. Settings are organized into tabs (Categories, Types, etc.) across the top, and there are additional Configuration settings on the right.



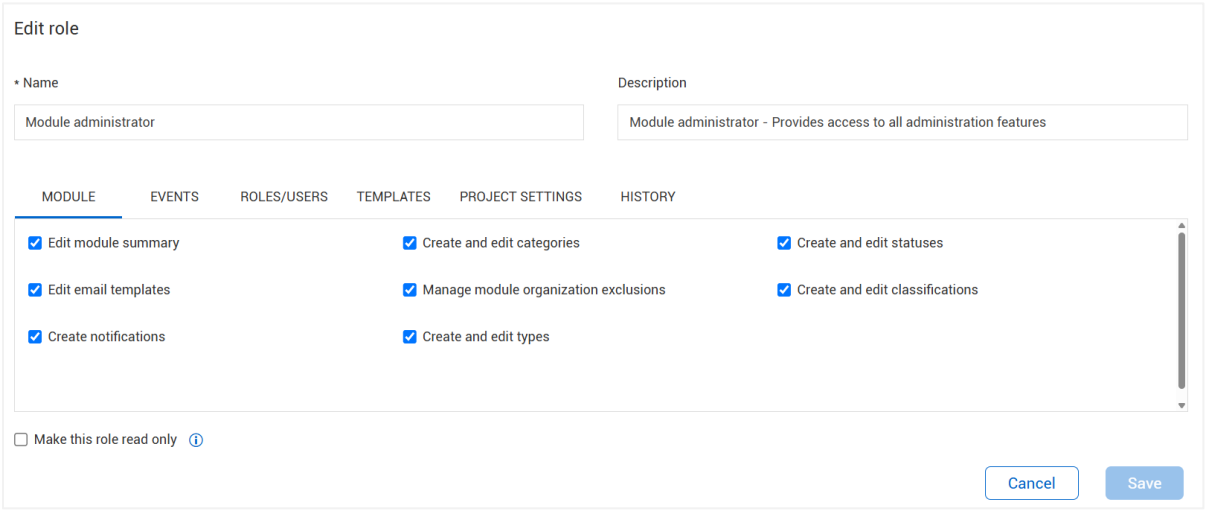
Additional information on the configuration of these settings is covered in the *Module Settings Configuration in the Software* section below.

Module Administrator Role Setup

To set up a role for a module administrator, select the Roles tab from within the Module settings. Note that a Module administrator role already exists by default.



If you open the Module administrator role (by clicking on the role name), the Edit role window opens, where you can view the permissions selected for the role, organized into tabs (Module, Events, Roles/Users, etc.).



Depending on the needs of your organization, you can use this role as is, edit the permissions on this role (by selecting/unselecting access), or you can create a new custom administrator role and select the permissions for the role manually.

Typically, the Module Administrator will have access to most, if not all, permissions for the module. The matrix below shows suggested permissions to allow for a Module Administrator by default, but you might need to include/exclude some permissions based on your company needs (see the considerations below).

	Module Administrator
Module	
Edit Module summary	X
Edit email templates	X
Create notifications	X
Create and edit categories	X

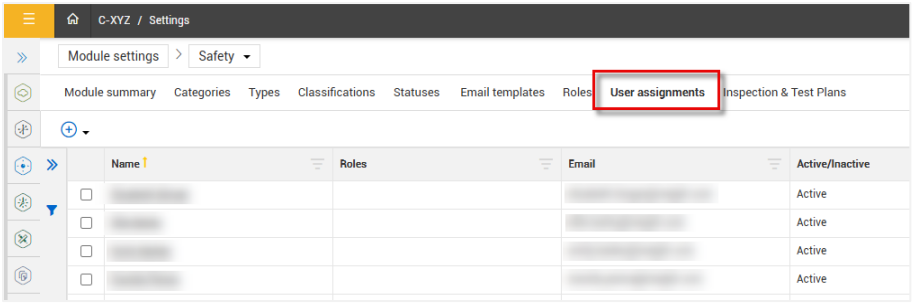
Manage module organization exclusions	X
Create and edit types	X
Create and edit statuses	X
Create and edit classifications	
Events	
Edit completed events/tasks	X
Edit event/task properties	X
Edit event/task proj/org	X
Edit event/task category	X
Edit event/due date	X
Edit event/task status	X
Edit event/task Reporter/Responsible party	X
Edit event/task title	X
Only provide access to own forms/tasks on the event/task list	
Allow access to event/task history	
Roles/Users	
Create and edit roles	X
Create and edit user assignments	X
Restrict the ability to assign users to the following roles:	
Restrict the ability to assign users to only the following reporting tags:	
Templates	
Create and Edit templates	X
Project Settings	
Enable/Disable Project Structure	X
Edit header template	X
Manage Automapping	X
Setup Automapping criteria	X
Perform Automapping	X
Manage Project Inspection and Test Plans	X
Create and edit Inspection and Test Plans	X
Edit header template	X
Manage Project User Groups	X

Create and edit User groups	X

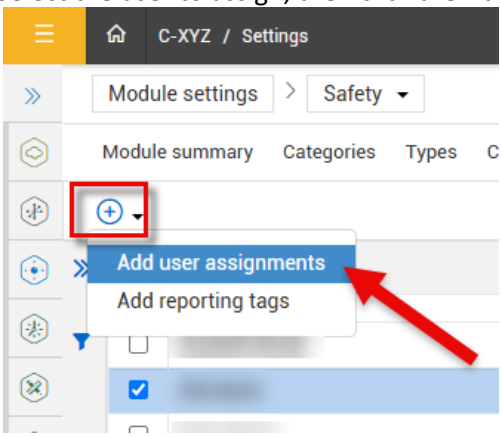
Module Administrator User Assignment

Once the module administrator role is defined to meet your needs, you can assign it to the appropriate user in your organization.

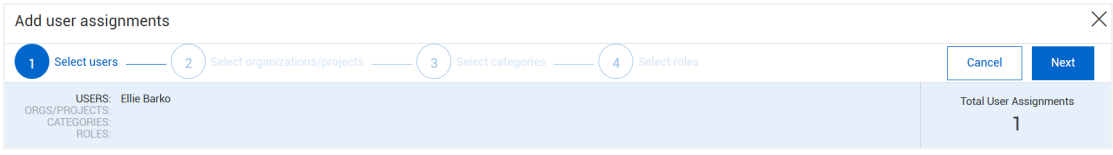
- To assign a user, go to the **User assignments** tab within the Module settings.



  - The list of users that is displayed here comes from all employees within your organization that have been added as users in InEight Platform and given either a Level 0, 1, or 2 roles at the Platform level.
    - The user you select does not need Level 3 access to be assigned the Module administrator role.
- Select the user to assign, then click the **Add** icon and select **Add user assignments**.



- This opens the Add user assignments wizard that walks you through the steps of assigning the user to the appropriate organizations/projects, categories, and roles (in this case, the Module administrator role).

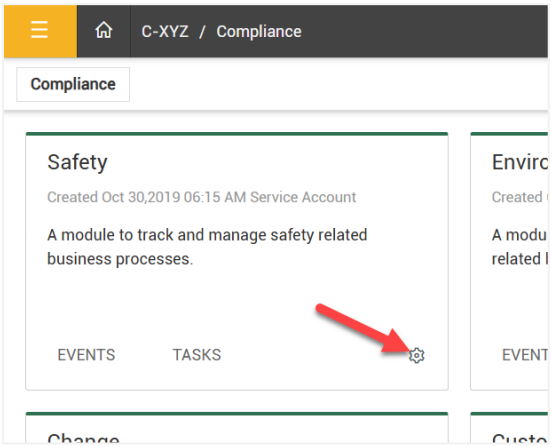


Once assigned the Module administrator role, that user can manage the module based on the access you specified.

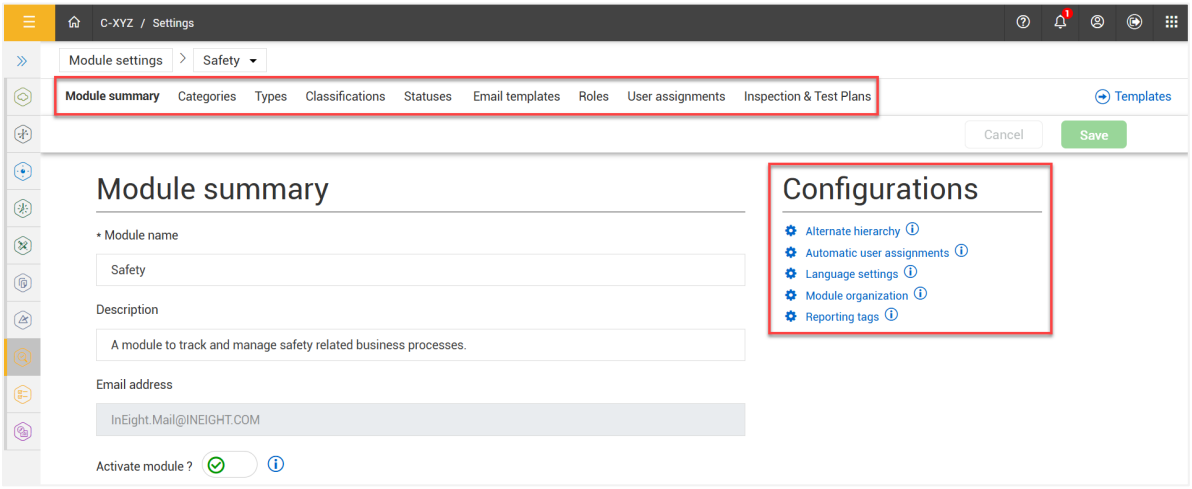
Module Settings Configuration

Once administrators are set up, the appropriate administrator (either the Level 3 Account Administrator, or the Module administrator, depending on your organization) can set up the settings for that module.

To set up module settings, open Compliance or Completions from the organization level and select the Settings icon on one of the module tiles.



This opens the Module summary page of the module settings where you can configure settings from the tabs at the top of the window (Categories, Types, Classifications, etc.) and the Configurations on the right.

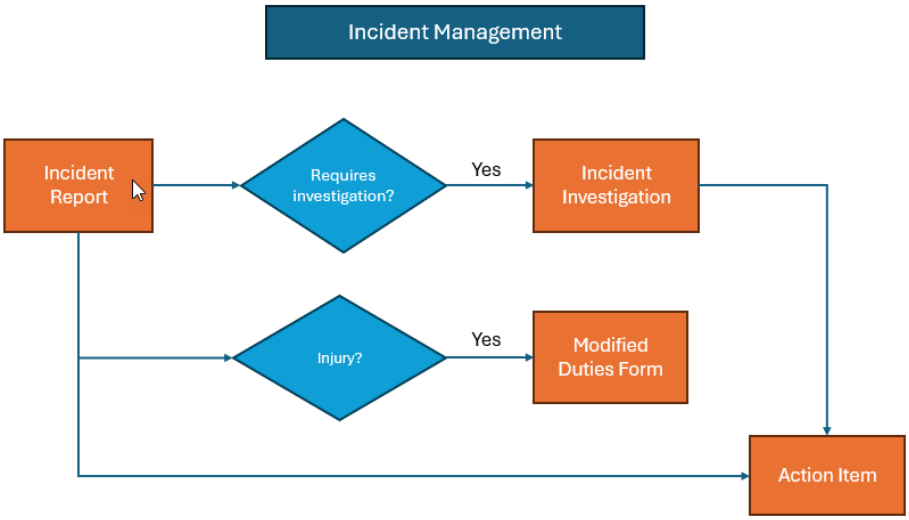


While the configuration of these settings is reasonably straightforward in the software, the planning behind what settings to configure, based on your company's business processes, can be complex. Thinking through the business processes for each module can help you determine the forms/tasks, categories, types, classifications, roles, and user assignments to set up for each module.

For example, when planning the setup of the Safety module, your project team will need to think through what business processes the Safety module will support.

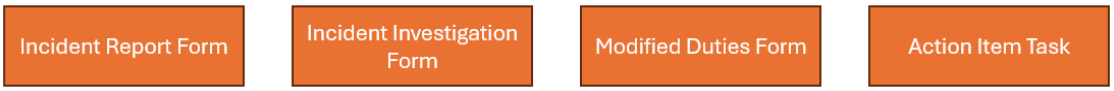
Module Settings Configuration Example

Let's walk through an example of module setup planning for the Safety module, using the example of an Incident Management business process. For Incident Management, let's assume your organization would follow this workflow:



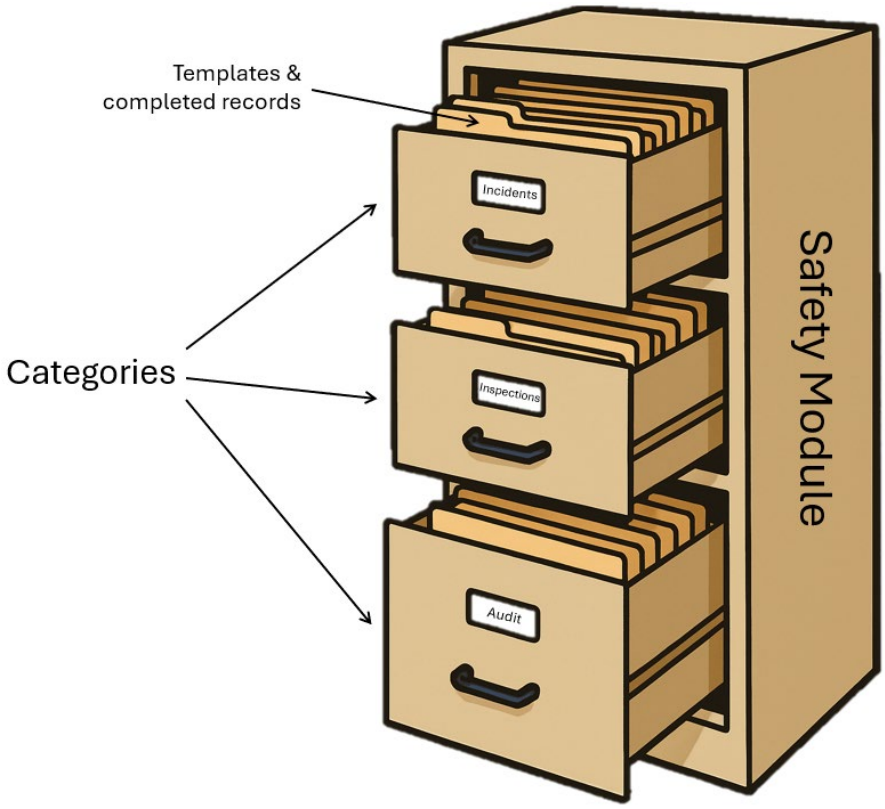
- The process would begin with an initial incident report.
- Depending on the nature of the incident/injury, it might include an incident investigation which could involve different people/groups from across the organization.
- If there is an injury, a modified duties form might be required to document the duties an employee is able to perform while injured.
- Action items might be created/assigned to any individual in the system from either the initial incident report or during the investigation.

Based on this workflow, your company would need the following forms/tasks:



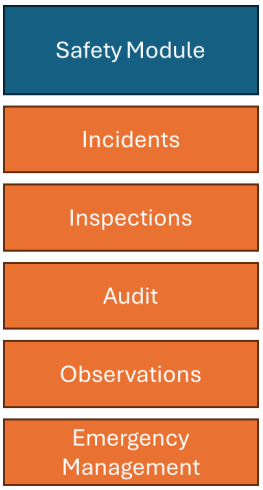
Categories

Categories provide a way to organize your module into smaller areas. If you think of a module as a filing cabinet, the categories would be the different drawers in the filing cabinet. As templates are built, they must be assigned a category. This would be the equivalent of filing the templates into the appropriate drawers of the filing cabinet. As templates are then filled out as forms and tasks in the field, the completed records would also be filed under the same categories assigned to the original templates.

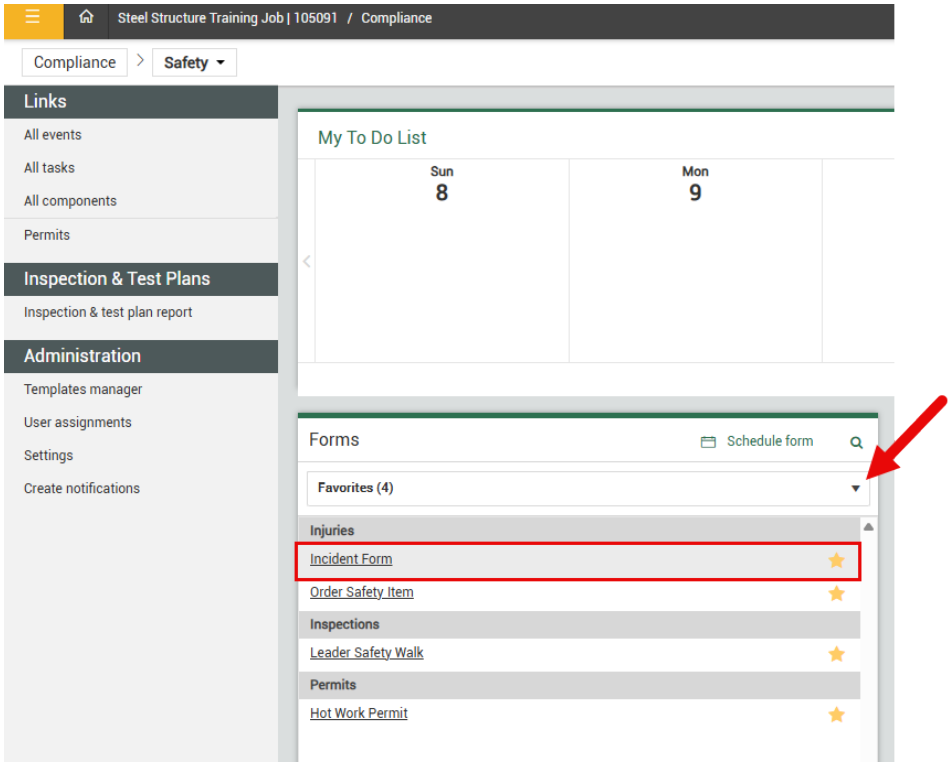


You can also control user access to categories. Thinking of the module as the entire filing cabinet full of blank templates and completed records, when assigning users, you can decide what drawers of the cabinet (categories) they should have access to.

Thinking through the example of the Incident Management business process, let's assume you create an Incidents category for all incident-related forms and tasks, and you make it available to all who would need access to that category. In addition, you create several other categories to organize and manage access to forms for other business processes that fall under the Safety module. For example, users needing access to the Incidents category may or may not need access to the Inspections, Observations, Emergency Management, or Audit categories.



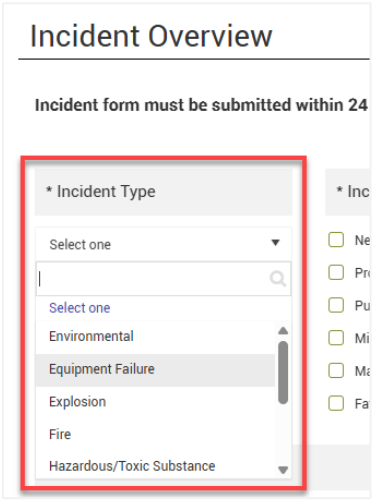
Within Compliance/Completions, as a user, you will only be able to access the forms and tasks under the categories assigned to you. On the module's home page, you will select the category you need to access from a drop-down list.



For more information on the setup and use of categories, see the Categories topic in the Knowledge Library.

Types

Types can be used to classify your forms or tasks for reporting and filtering. You can add a Task drop-down to your form so a type must be selected when filling out the form as shown in the example below.

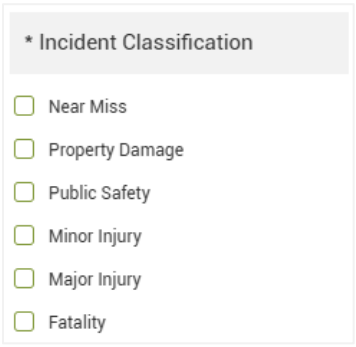


You can only use one type per template.

Types are also one of the criteria you can use to filter the list of templates to use for automapping to particular nodes of your project structure or components in your inspection and test plans. For example, you may have a set of mechanical-related forms that need to be associated with the subsystem node of your project structure, so you filter to the Mechanical type and auto-map that subset of templates to the Subsystem level of your project structure. For more information see the Automapping topic.

Classifications

Classifications are also used to label your forms and tasks for filtering and reporting.



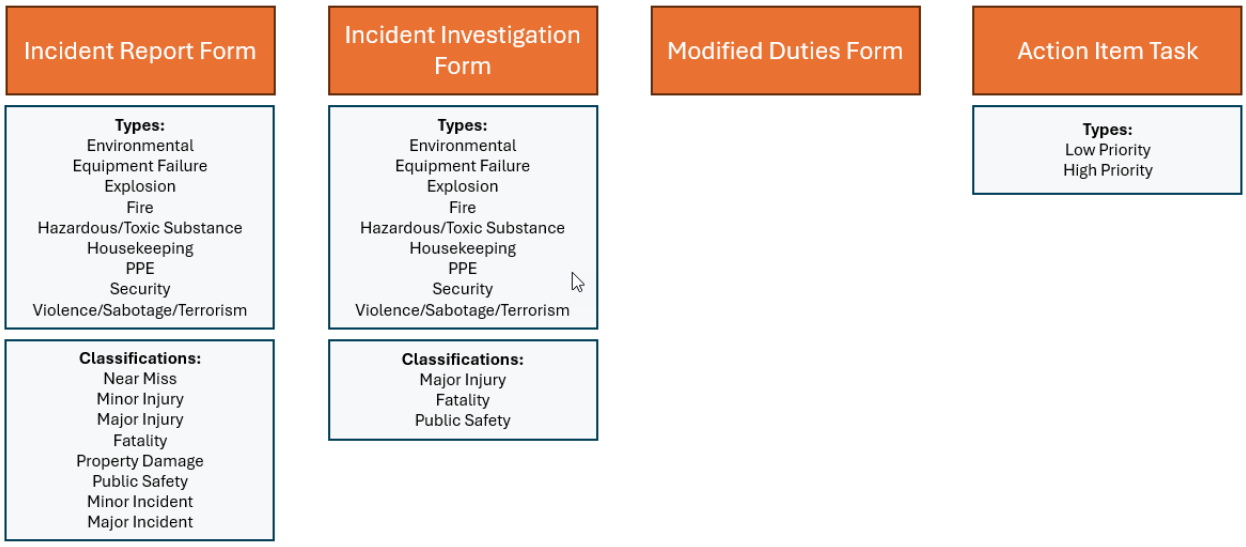
Classifications contain additional functionality where you can apply logic to the classification so that sections appear only if that classification is selected. For example, you might only want the Fatality section to appear if someone checked the Fatality classification.

You can use multiple classifications on a single template, while you can only use one type per template. For example, I may have a classification on a template to indicate Incident Classification (e.g., near miss, property damage, injury, fatality), and have a separate classification on the same template to indicate Incident Level (major incident, minor incident).

For more information on the setup and use of types and classifications, see the topics below:

- Types
- Module Settings > Classifications
- Template Management > Classifications

For our example, we've chosen the following types and classifications for our templates (forms and tasks).



Roles

Within each module, you can set up roles to control what users can do within the module, including how they work with templates, records, and administrative tasks.

NOTE:	As a best practice, you should develop as few roles as possible. You can use organization/project level and categories to limit access to forms and tasks, and roles to focus on what the user can do with the forms/tasks they have access to. For example, you may have a Safety Manager and an Environmental Manager. Both need to participate in workflows and manage forms and records within their respective domains. Both can be assigned the Process Owner role, but the Safety manager will only have access to forms/tasks in the Safety category and the Environmental Manager will only have access to forms/tasks in the Environmental category.

Templates

When it comes to templates, you can use roles to:

- Assign users workflow responsibility (e.g., the Supervisor role has responsibility for step #2 on the Modified Duties form).
- Identify a set of recipients for an email notification (e.g., the VP role receives an email for “high priority” actions).
- Manage access to information on a form (e.g., the Process Owner role is the only role with access to the police report and Investigation section of the Incident Report).

Records

Roles are also used to determine whether a given user can manage existing records. You can individually choose what properties a role should have access to under the Events tab in the role settings. User

groups are also something that some of your roles might need to create. This can be found under the Project Settings tab.

For example:

- The Supervisor role can edit the following event/task properties: project/org, due date, responsible party, title.
- The Process Owner role has access to the history for the Safety and Environmental categories, can edit completed events and all event properties, and can create user groups.

Administrative

Finally, roles are used to identify module administrators. You can choose from various administrative settings under the Module, Roles/Users, Templates, and Project Settings tabs to grant the permissions that an administrative user might require.

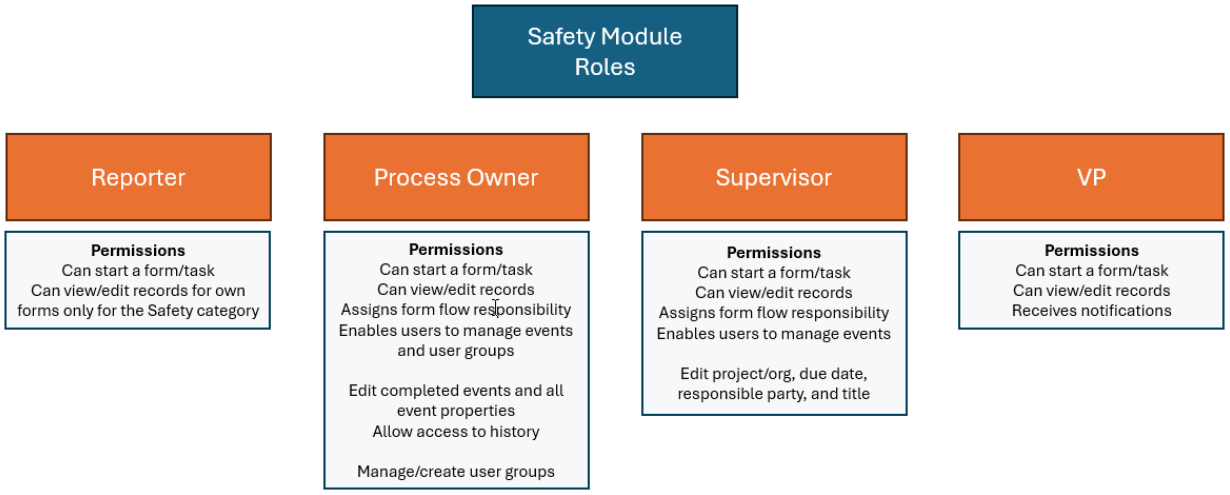
"Own Forms Only" Permission

An important permission to consider roles is the 'Only provide access to own forms/tasks on the even/task list' permission. This can be set for one or more categories in a role. Enabling this setting ensures that users assigned to that role will only have access to see their own forms/tasks on the Event/Task list for the categories specified.

For example, for incident reports, your Foremen might need a Reporter role that allows them to create and review their own incidents, but not review the incidents created by others, while the Safety Manager might need access to view all incidents.

NOTE:	Be aware that the "own forms only" setting applies even if that role is assigned to a step in a form flow that requires access to other forms. For example, a team lead assigned the Review step in a form flow is not able to see incidents coming from other team members because their role has the 'Only provide access to own forms/tasks on the event/task list' permission selected.

For our example, we've come up with the following roles for the Safety module:

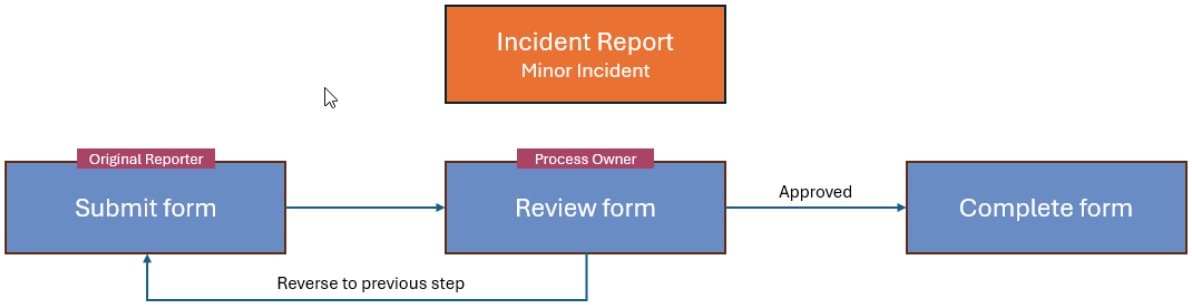


For details on the permissions available within Compliance/Completions and how to set up module-level roles and permissions in the system, review the following Knowledge Library topics:

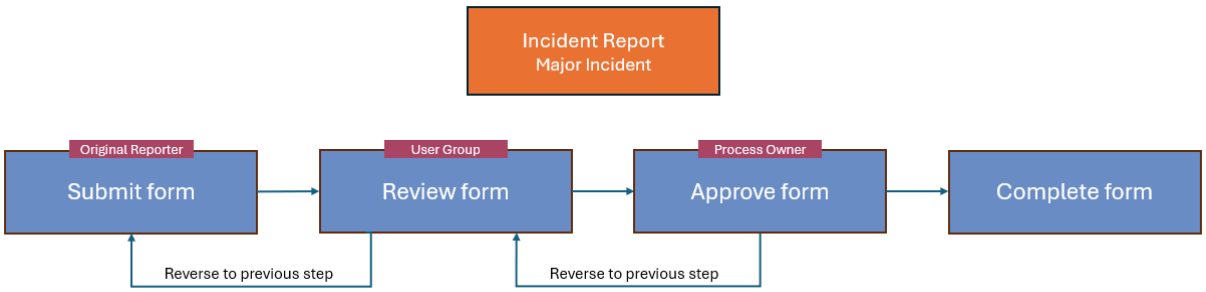
- Roles
- Module permissions
- Events permissions
- Roles and users permissions
- Templates permissions
- Project settings permissions

Form Workflows

Next to consider is if any of the forms require a workflow and what roles are required for each step. For example, for a minor incident, the workflow for the Incident Report may be:



A major incident, however, might require an additional review step.



In Compliance/Completions, you can set up the workflows for your forms using the Form Flows functionality. For more information, consult the Form Flows section of the Knowledge Library.

User Groups

User groups are used to grant a group of people access to a specific record above and beyond what their role typically allows. Groups can be granted responsibility for a specific workflow step or can be applied manually to a single record.

Assigning a user group can be helpful when someone needs temporary or one-time access to edit, review, or approve a record.

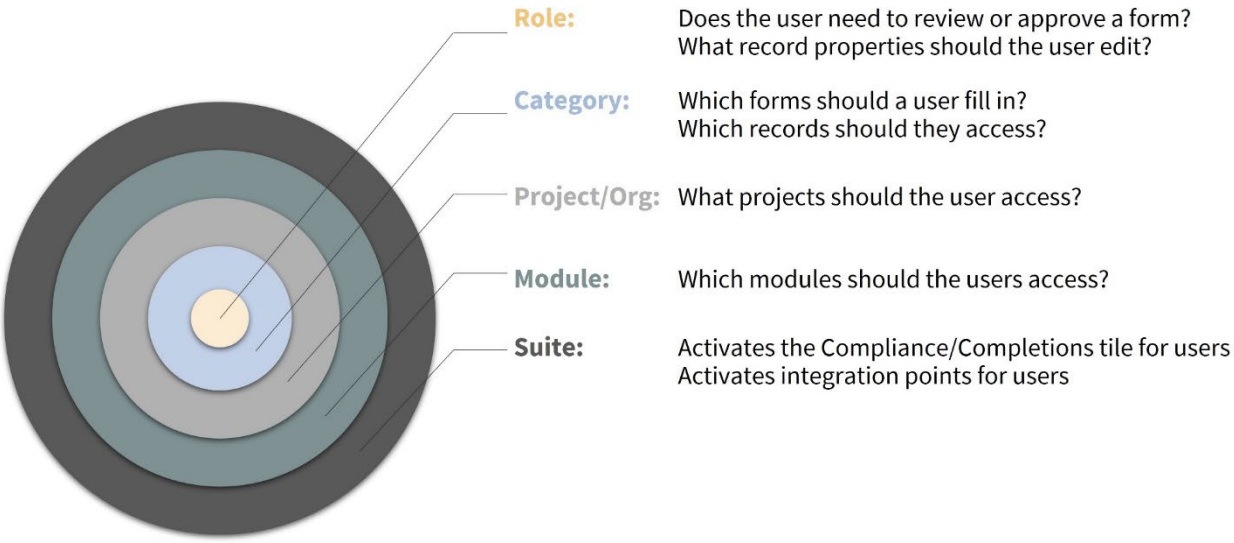
For example, in the Incident Report – Major Incident workflow shown above, a user group assignment is used during the Review phase of the process because the participants will depend on the type and severity of a given incident. If the incident is a fatality, a Fatality Incident group could be assigned to the review step that includes the appropriate members, such as the HSE Lead, HR Manager, Legal Counsel, and a VP. This gives you the flexibility to choose assignees tailored to specific circumstances.

For more information, see the User Groups topic in the Knowledge Library.

User Assignments

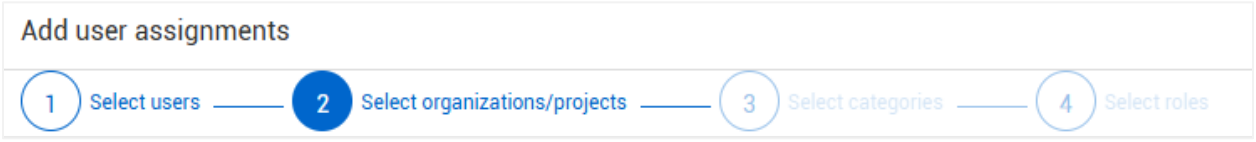
With categories and roles in place, you can start assigning access to the users in your organization. The below diagram illustrates the levels of access for a user, beginning broadly with the user access given at the Suite (Platform) level, and then narrowing down to the specific needs at the Role level.

Note that categories are used to control what access users have to different forms based on the business processes they are involved in, while roles are used to control what a user can do with the forms they've been given access to.



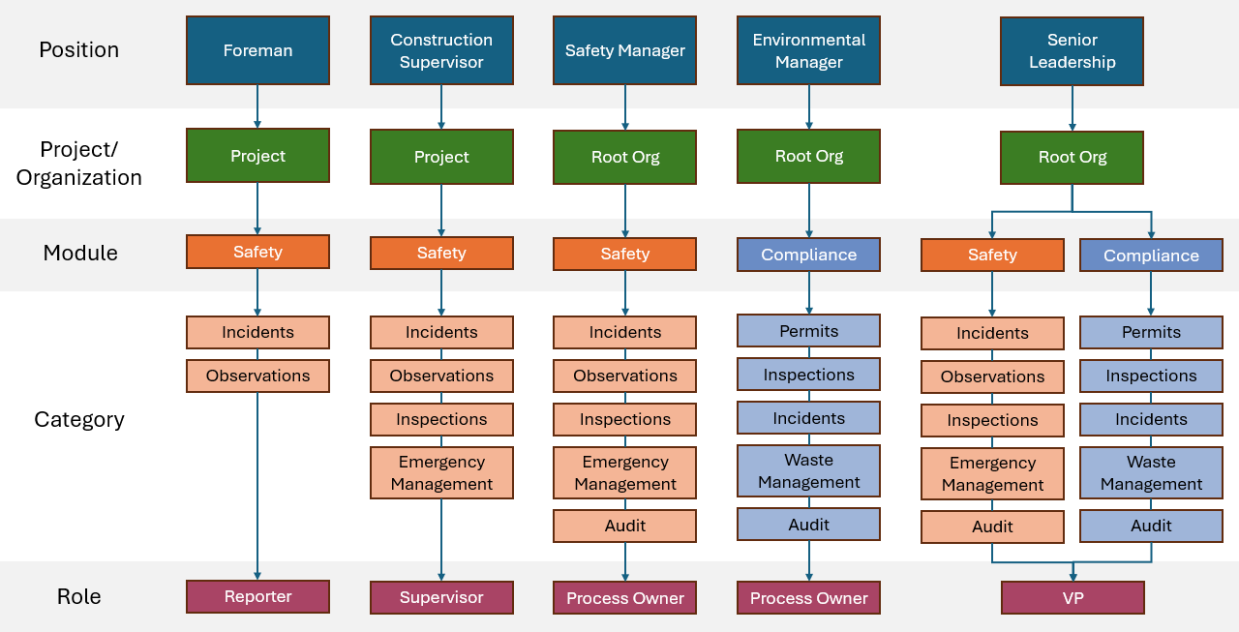
In Compliance/Completions, once you open a module and go to its organization-level settings, when you add a user assignment, the system helps you define access from the organization/project level down to the role level through four steps:

- Select users
- Select the organizations/projects
- Select categories
- Select roles



For our example, as we consider user assignments, let's assume these are some of the positions of users within your organization:

The visual below walks through what assignments we might make for each of these positions at the project/org, module, category, and role levels.



- The foreman only has access to the project he is working on. Within that project, he can only access the Safety module. Within that module, he can only see templates and records for the Incidents and Observations categories. Within those categories, he can only perform actions allowed by the Reporter role.
- The Safety Manager has access to the entire organization (root) and to all the categories within the Safety module. She also has all the permissions related to the Process Owner role.
- The Environmental Manager has access to the entire organization but only has access to the Compliance module (not Safety).
- Senior leadership has access to the entire organization, both modules (Safety and Compliance), and all categories within those modules, but they only have the permissions available for the VP role.

Summary

As walking through this example illustrates, there is a lot to consider when configuring module settings in Compliance/Completions. Because of this, planning typically takes place as part of your organization's software implementation process, working with an InEight consultant who can help guide you through these considerations.

For additional information on the setup of module settings, click on the following topics and/or videos:

- Accessing Module Settings video
- Organization & Module Settings video
- Statuses topic
- Email templates topic

Configurations

Under the Configurations section on the right side of the Module summary page, there are several links to perform additional configuration tasks for the module.

For details on how to use the Configurations links and their purpose, select from the following:

- Configurations
- Language settings
- Module organization
- Reporting tags

Automatic User Assignments

The automatic user assignments configuration setting lets you automatically assign a Compliance/Completions role and categories to all users.

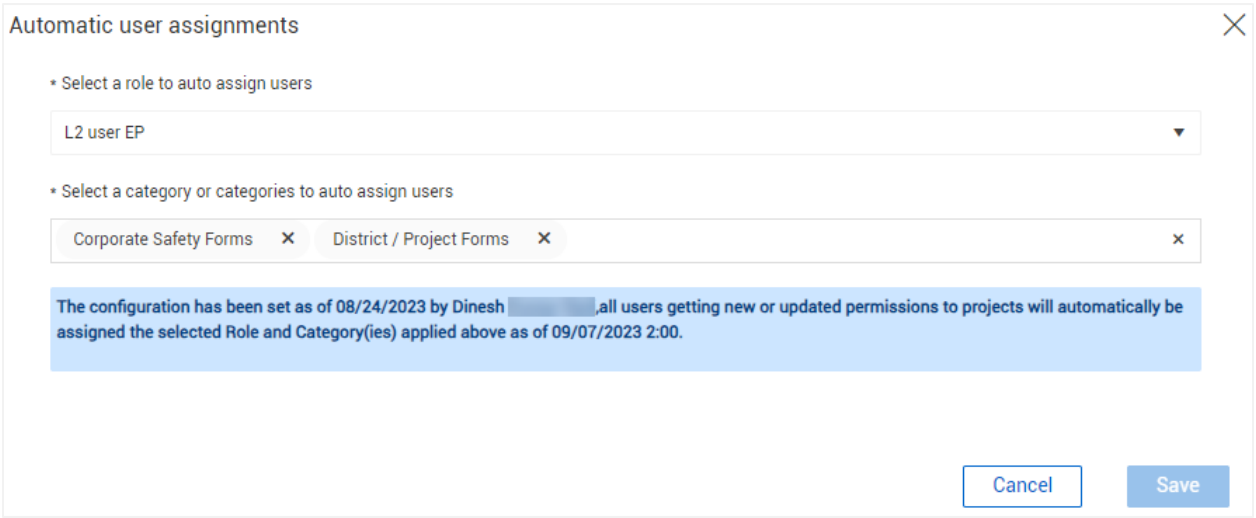
Considerations

- User assignments are not retroactive – they are always forward-looking.
- This function works for users that are directly assigned at the project level. Users assigned at an organization level will not be automatically assigned, even if they inherit access to projects within the organization they are assigned.

Use Case

This feature is especially helpful when planning a new project when you have a high quantity of end users to make assignments for. Typically, you would first make user assignments to managerial and reviewer-type positions that need higher level organizational access and higher-level roles.

You can then configure an automatic user assignment to assign a lower-level role and the appropriate categories to all the remaining end users.



For additional information, see the Automatic User Assignments topic in the Knowledge Library.

Additional Platform-Level Administrators (Optional)

As discussed above, your organization might need additional administrators to manage individual modules. For example, you might have a manager over Quality that would just have access to the Quality module within InEight Completions. In addition, you might want these managers to have additional permissions at the Platform level.

If this is the case, you can create a role for that manager at the Platform level, under Organization and project > Compliance/Completions settings, where you can select the modules they should have access to (for example, Edit Safety module, Edit Quality module).

These administrators would also need Level 3 access.

NOTE:	If module titles are changed within Compliance/Completions Project settings, these changes will display under the Compliance/Completions settings at the Platform level.

Considerations

Users assigned a platform-level role with Level 3 access might have permissions that override those established at the Compliance/Completions level. Additionally, the Level 3 role might possess further administrative capabilities within the suite itself. If you need to restrict access for privacy reasons or prefer to limit administrative privileges, consider creating a module administrator role within Compliance/Completions as described in the *Module-Level Administrators* section above. This role can grant the necessary access for the module they oversee while reducing the risk associated with Level 3 access.

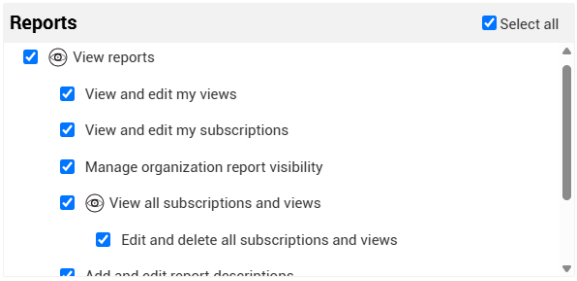
Compliance/Completions Integration with Other Applications

The Compliance and Completions applications include several features to integrate with other InEight applications. To utilize these integrations, the proper settings and permissions must be configured. This section walks through how to configure each of those integration points.

Reporting

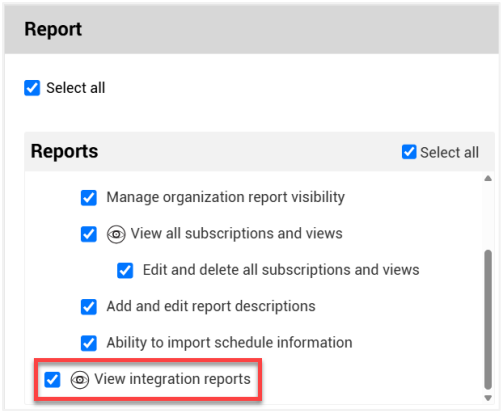
Report

The Compliance/Completions administrator will likely need access to the Report application for running Compliance/Completions-related reports. This is granted in InEight Platform, under Suite administration > Roles and Permissions, under the Report accordion menu, by selecting **View reports**, along with the child permissions beneath it.



For end users, it is recommended that you be selective in giving this level of access because it gives access to all reports, including reports that might contain sensitive information. For example, you might not want to give a field user doing safety observations access to the Reports application where they could also access budget-related reports.

All users should be granted access to print event/task reports within Compliance/Completions. To allow this, select **View integration reports**.

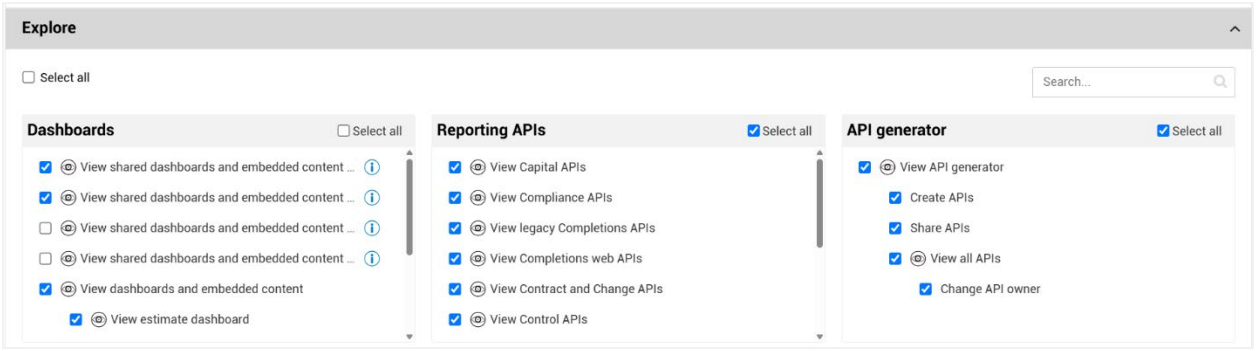


Explore

If you have Compliance/Completions users that need access to Explore dashboards and/or APIs, they will need access granted via the permissions under the Explore accordion menu as part of their role in InEight Platform.

When providing access to Compliance/Completions APIs, care should be taken to consider limiting access to sensitive information. The Compliance/Completions applications include configurations to control access to privacy-regulated information. Users that are not cleared to access that information should not be given access to the Reporting APIs.

NOTE:	Users granted access to the API generator will only see Compliance/Completions data they have been given access to. For example, if they are not granted access to a form in Compliance, they will not have access to that form's data within the API generator.



Master Data

Some of the values in Compliance/Completions are part of the master data set up for your company in InEight Platform, such as project structure values, vendors, and operational resources (employees and equipment used in the field).

Project Structure Values

Your organization might want to define a project structure to organize your data across applications. For example, your project might be organized into areas. Within Compliance/Completions, you can add Project Structure headers to your form templates to organize forms by the areas of your project.

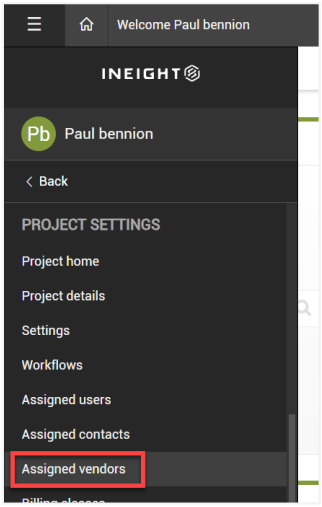
- To use project structure and project values, the administrator must have access to the Project structure and Project values permissions under the Organization and Project > Projects section of their role's permissions.
- To integrate Compliance/Completions with project structure values, a Project Structure must first be set up by an administrator for the project.
    - For details on setting up the Project Structure and values for a project, review the following:
        - Project Value Types topic
        - Project Structure video
        - Defining Project Values video
- Once the Project Structure is set up for the project, within Compliance/Completions a user with access to the module's Project settings must turn on the Project Structure and Automapping toggles.
- For additional information, see:
    - Headers section of the Knowledge Library
    - Master Data Libraries eLearning course (see the Compliance/Completions lesson)

Vendors

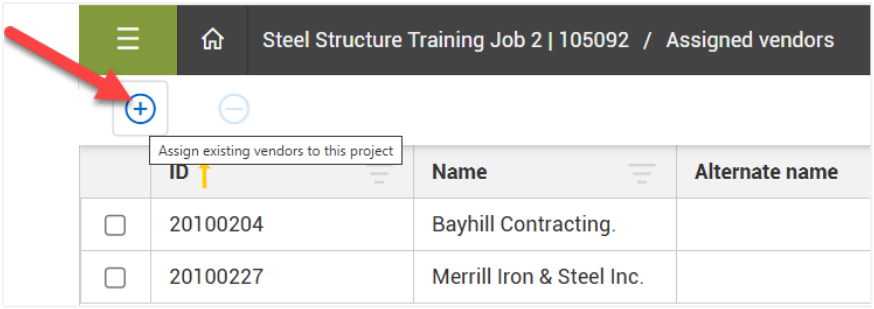
Within Compliance/Completions, there might be the need to indicate the vendor on an event or task. For example, your company might need to indicate the vendor on their receiving forms when materials are dropped off on site.

Vendors are defined in InEight Platform under Master data libraries > Vendors by a system administrator that has access to Master Data Libraries.

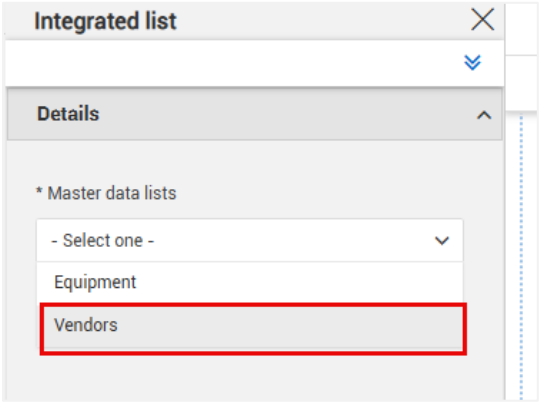
Once set up for your company by the appropriate administrator, they must be assigned for use on a project by someone with the permissions to do so. This is done by selecting Assigned vendors from the project's Project Settings.



This opens the Assigned vendors register where vendors that already exist in the Master Data Library can be assigned to the project.



Once assigned, the vendors will be available to use within Compliance/Completions. The assigned vendors show up as drop-down list options when using the Integrated List question type.



Operational Resources

Operational resources are the employees and equipment used to do the work in the field. In Compliance/Completions, they are used on events and tasks. For example, when filling out a safety form, the person filling it out will need to select the employee who was injured or the equipment that was damaged.

Operational resources are defined in InEight Platform under Master data libraries > Operational resources. Once set up in the Master Data Library, they can be used by other applications, such as InEight Progress and Compliance/Completions. The setting up of these resources is done by a system administrator with access to Master Data Libraries.

Once set up for your company, they must be assigned for use on a project by someone with permissions to do so. This is done by selecting **Assigned operational resources** from the project's Project Settings. This opens the Assigned operational resources register where employees and equipment can be assigned to the project.

Once assigned, they can be used within Compliance/Completions as drop-down list options for the following question types:

Question Type	Operational Resource Type
Integrated List	Equipment
People Picker	Employees (if the Resources option is selected)

NOTE: For the People Picker option, the drop-down list includes software *users*, but to include field-level Operational Resource *employees*, the Resources option needs to be selected.

InEight Document Integration

If your company uses both InEight Compliance/Completions and InEight Document, there are several integration points where information can be shared between applications. This section covers each of those integration points and how to configure permissions and settings so these integrations can be utilized.

Document Server Setup

The appropriate Document server must be added under InEight Platform Suite Administration > Application integrations and mapped to the appropriate Platform projects. See the InEight Document-Platform Application Integrations Guide for more information.

Forms integration

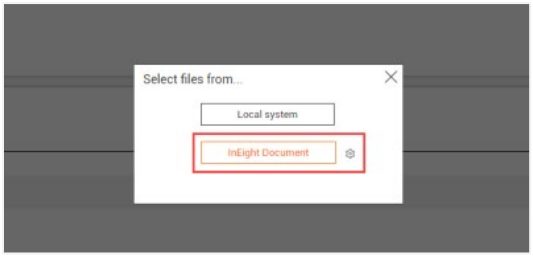
An integration can be set up to transfer and upload the PDF version of Compliance/Completions forms to InEight Document. To use this integration, the following settings must be configured:

- Document APIs must be activated for required projects.
- Within InEight Document:
  - A service account must be set up with the following permissions:
    - Access to upload rules to document register
    - Full access to document module
  - A non-production project must exist to upload the middleware to.
- For more information, see the InEight Document-Compliance-Completions Integration Guide.

Attachments on Compliance/Completions Templates

Attachments within Compliance/Completions can be supporting documents from InEight Document if Document Integration is already set up.

The user pulling in an attachment from Document must be a user within the InEight Document application.



InEight Change Integration

This integration allows users of InEight Change to complete Compliance/Completions tasks related to change order issues from within InEight Change.

To set up this integration, users must have permissions to access InEight Change.

To learn more about how to set up this integration, review the following:

- Template Integration topic
- Admin: Setup Issue in Compliance for Change video
- Compliance to Change Setup Guide

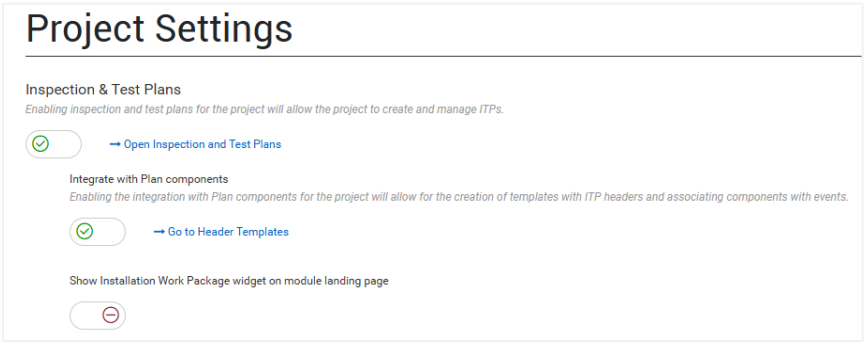
InEight Plan Integration

Within Compliance/Completions, you can activate the Inspection and Test Plans feature for gathering ITP information, including the option to associate InEight Plan components with these ITP events.

To use this integration, the following settings need to be configured:

- Under Project Settings > Plan, select the **Enable Inspection and Test Plan** mapping option.
- In Compliance/Completions, within the project's module settings > Project Settings tab, the following toggles need to be enabled:
  - Inspection & Test Plans

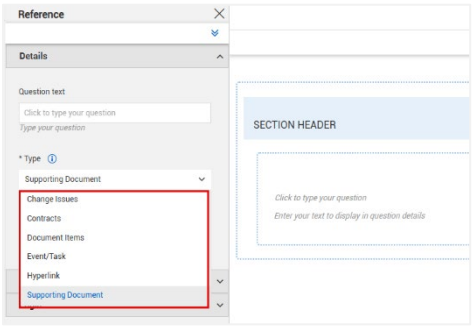
- Integrate with Plan components



- For additional details on how to set up ITPs, including the integration with InEight Plan components, consult the following:
  - Inspection and Test Plans section of the Knowledge Library
  - Completions FAQ (see first question about setting up ITPs)
  - Template Management eLearning course (ITP & Project Structure Overview lesson)

Reference Questions

When building forms, one question type you can add is a Reference question. Among other options, the reference question includes drop-down options to select Change issues, Contracts, or Document items.



To select one of these options, you must already have access to the corresponding application. For example, to reference an issue from InEight Change, you would need access to the InEight Change application to select that option as a reference.

Summary

The InEight Compliance and Completions applications are unique in their approach to user access. Rather than managing all Compliance and Completions settings at the InEight Platform level, only full administrative access is granted at the Platform level, with the more granular access to features and individual settings granted at the Compliance/Completions modular level. In addition, there are specific configurations needed to integrate Compliance/Completions with other InEight applications. This guide has gathered all these considerations into a single document, so you can successfully set up the

appropriate access to the Compliance and Completions applications, while ensuring access to confidential data is controlled.