ITRMBond - Continuous Controls Testing

Baseline Configuration Guide

Rsam Version: 10 | Document Version: 01.00.04

August 2020

www.wegalvanize.com

Contents

About Rsam Baseline Configuration Guides

Rsam Baseline Configuration Guides provide you the information needed to understand the pre-defined configurations for each module. These guides should be referenced to gain a better understanding of how the module is configured and can be used out-of-the-box.

Baseline Configuration Overview

This document describes the baseline configuration and structure for the Rsam Continuous Controls Testing (CCT) module. The baseline configuration allows organizations to automate ongoing control monitoring activities mandated by regulatory requirements and standards such as NIST, FISMA, FEDRamp, SOX, PCI, COSO, ISO, NERC, CMS, OCC, and others. Rsam CCT provides a global repository of controls and control tests while allowing multiple control testing teams to manage their own unique control test plans, from scoping and documentation to execution and certification. With automatic reminder and escalation notifications, you'll never miss another deadline, and with the powerful searching and reporting capabilities of Rsam, you'll be able to generate mission critical certification and attestation reports with the click of a button.

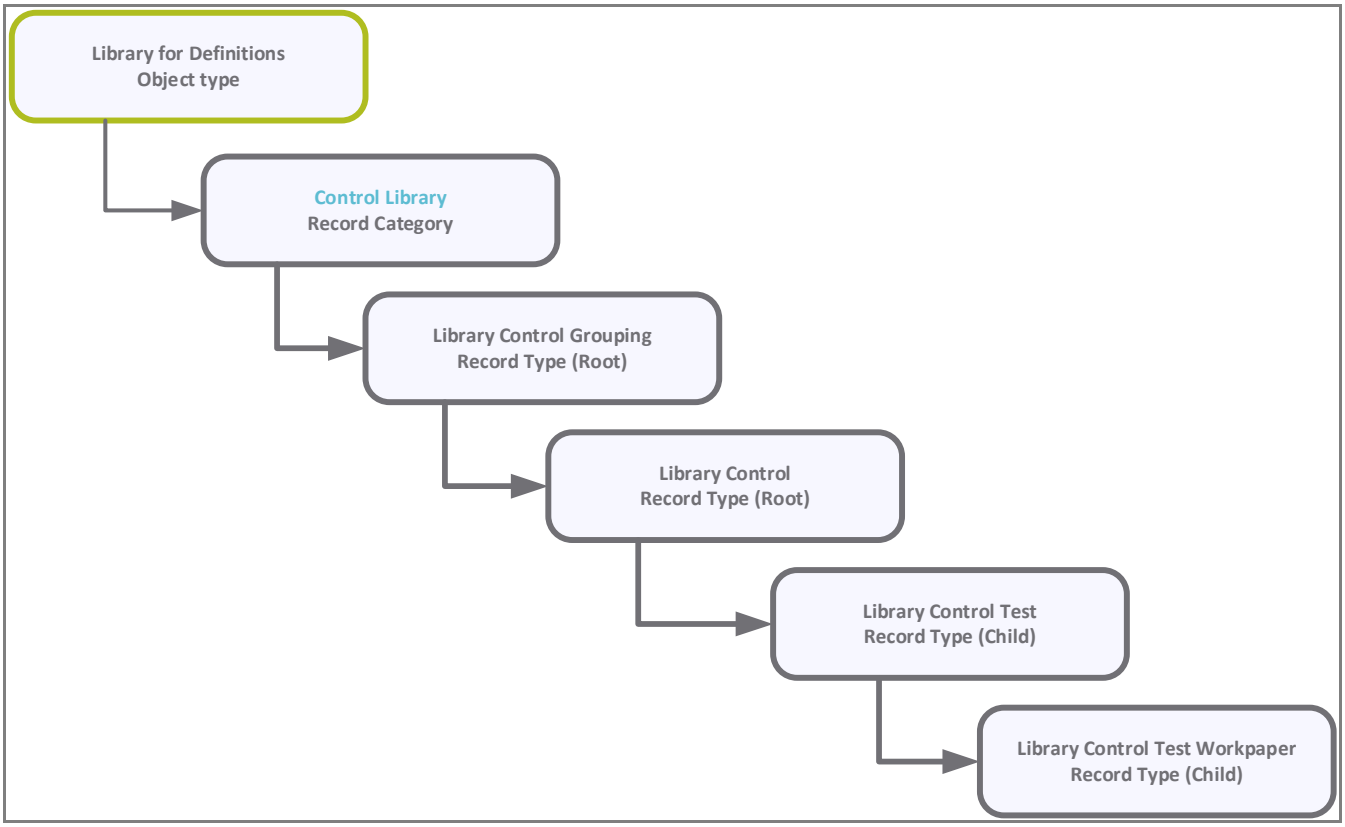
The following is a list of elements that we have configured in the Continuous Controls Testing module:

- Structure
- Home Page Tabs
- Control Testing Workflows

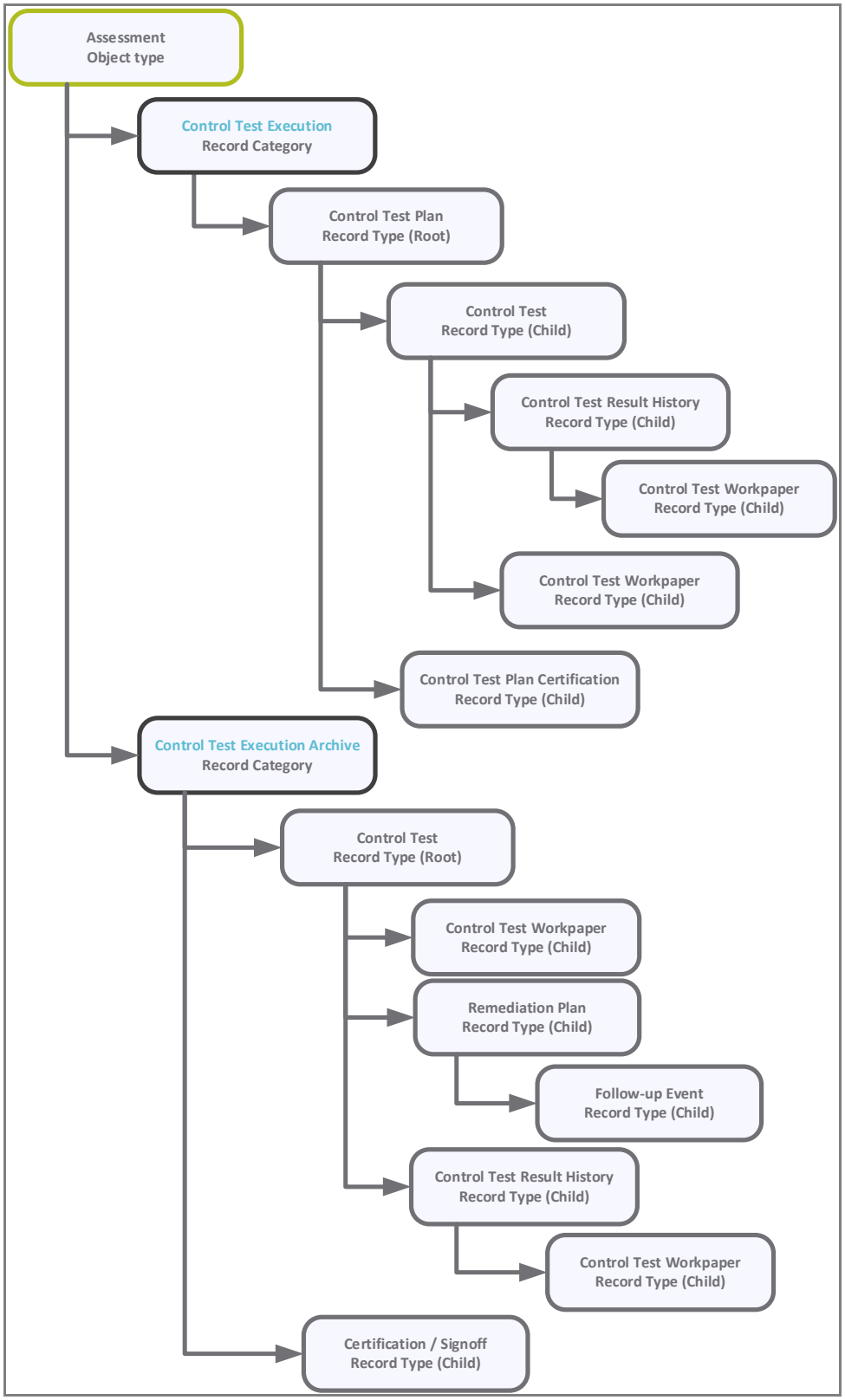
The information on the preceding elements will provide a baseline understanding before you leverage the *Continuous Control Testing Step-by-Step Tutorial* or begin to tailor the module to meet your unique requirements.

Continuous Controls Testing Structure

Continuous Controls Testing module is comprised of two distinct record structures. The first record structure defines the *library* side of the CCT module, which is essentially a content library that defines the control and control test definitions that will be used to generate executable control test plans. The library side of the record structure is situated on the **Library for Definitions** object in Rsam.



The second record structure defines the execution side of the CCT module. This record structure provides the *work space*, where an asset-level control test plan can be defined, and where the asset-level control test results will be submitted and evaluated on a continuous basis. The *execution* side of the record structure can be associated with any Rsam standard object type (Vendors, Applications, Servers, and so on). In the out-of-the-box configuration, the record structure has been associated with the **IT Application** object type.


Assessment
Object type
Control Test Execution
Record Category
Control Test Plan
Record Type (Root)
Control Test
Record Type (Child)
Control Test Result History
Record Type (Child)
Control Test Workpaper
Record Type (Child)
Control Test Workpaper
Record Type (Child)
Control Test Plan Certification
Record Type (Child)
Control Test Execution Archive
Record Category
Control Test
Record Type (Root)
Control Test Workpaper
Record Type (Child)
Remediation Plan
Record Type (Child)
Follow-up Event
Record Type (Child)
Control Test Result History
Record Type (Child)
Control Test Workpaper
Record Type (Child)
Certification / Signoff
Record Type (Child)

Object Types

The following table lists the object types pre-configured in this module.

Object Type	Usage
Library for Definitions	Utilizes the standard Library for Definitions object for managing a library of controls and control tests.
Rsam assessment objects	Test plans can be executed against any Rsam assessment object type (for example, IT Applications, Vendors, and so on).

Record Categories

The following table lists the record categories pre-configured in this module.

Record Category Type	Usage
CON: Control Library	A category type that includes the Library Control Grouping record type and its child record types: Library Control, Library Control Test, and Control Test Workpaper.
CON: Control Test Execution	A category type that includes the Control Test Plan record type and its child record types: Control Test Plan Certification, Control Test, Control Test Result History, and Control Test Workpaper.
CON: Control Test Execution Archive	A category type that includes the Control Test Plan record type and its child record types: Control Test Plan Certification, Control Test, Remediation Plan (POAM), Follow-up Event, Control Test Result History, and Control Test Workpaper.

Record Types

The following table lists the record types pre-configured in this module.

Record Type	Usage
CON: Library Control Grouping	Tracks distinct groups of library controls (and control tests) within the Library for Definitions object.
CON: Library Control	Defines a control at the library level. The control may or may not have associated library control tests.
CON: Library Control Test	Defines a control test for use in control test execution.
CON: Control Test Workpaper	Tracks individual workpapers associated with a given test.
CON: Control Test Plan	A collection of control tests defined on a specific assessment object in Rsam. One assessment object may have multiple test plans, where each is being managed by a different group (for example, a single vendor might have contract controls in one plan and IT security controls in another).

Record Type	Usage
CON: Control Test	A specific test to be executed within a control test plan. This record type is at the center of the control test execution workflow.
CON: Control Test Result History	A read-only record capturing the results of a point-in-time control test result submission.
CON: Control Test Plan Certification	Control test plan certification records are generated for a control test plan on a periodic basis in order to provide a container of recent control test submissions that can be certified as part of an attestation process.

Home Page Tabs

The Baseline Configuration for Continuous Controls Testing contains several Home Page Tabs. These tabs can be configured for various roles and then can be assigned to your users to complete their tasks. All home pages can be accessed from the **ITRMBond** grouping tab on the left navigation pane.

The following table lists the Home Page Tabs available for Continuous Controls Testing.

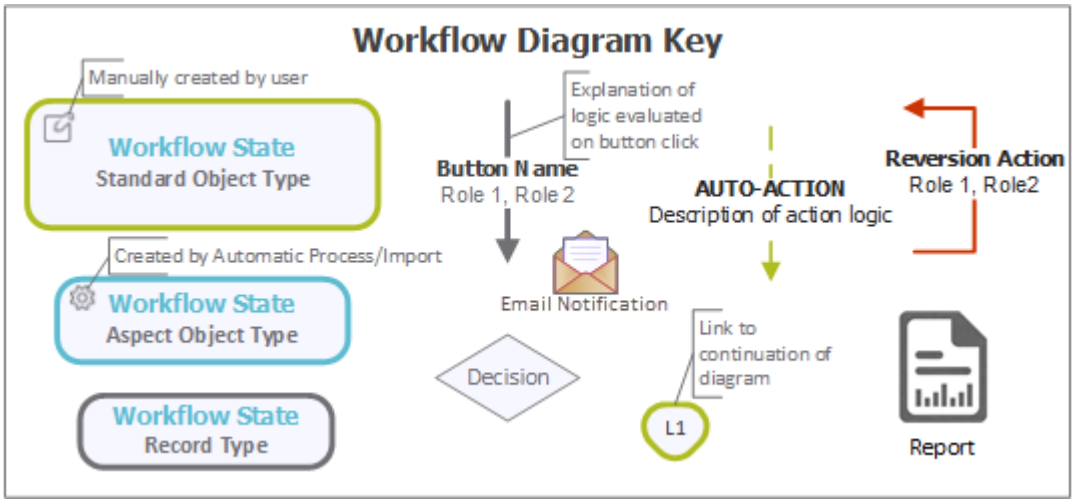
Home Page Tab	Description
ITB: Activities	Provides access to all the task-based activity center tiles for the Continuous Controls Testing module. Users can navigate to tasks from the relevant tiles.
ITB: Dashboards	Provides access to all the activity center tiles containing chart widgets for the Continuous Controls Testing module.
ITB: Shortcuts	Provides quick access to the links to various record categories for the Continuous Controls Testing module.
ITB: Assessment Navigator	Provides quick access to assessment objects and all related records. Typically, this is tab is helpful for power users that need to view all the object information (questionnaires, findings, and more).
CON: Library Controls Navigator	A navigator providing various list views into library control records.
CON: Control Test Plans Navigator	A navigator providing various list views into control test plan records.

Controls Testing Workflows

This section covers details on the following baseline workflows in the Continuous Controls Testing module:

- Library Control
- Control Test Plan
- Control Test
- Control Test Plan Certification

Before proceeding to the specific workflows, it is recommended that you familiarize yourself with the following Rsam workflow diagram key.

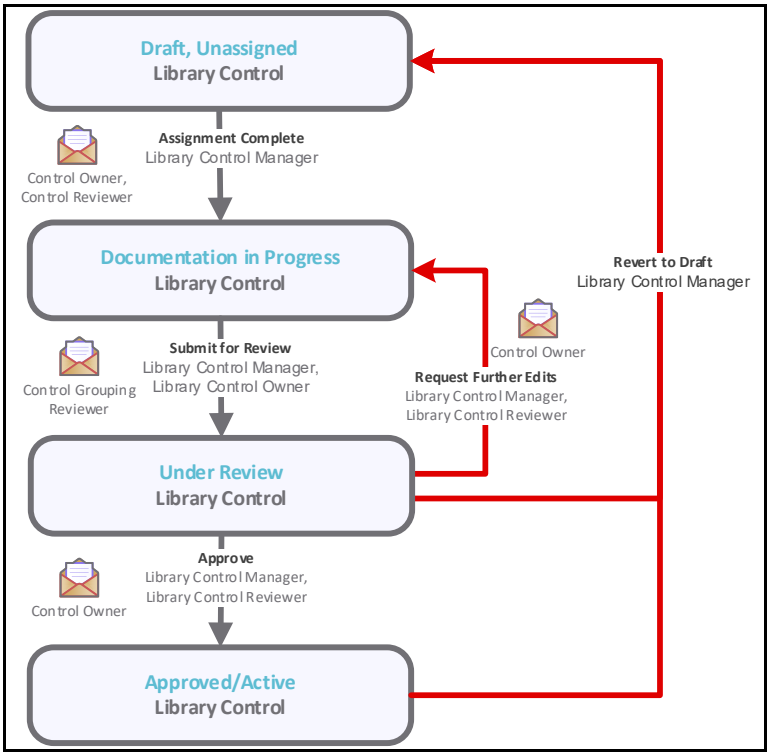


Library Control Workflow

This section covers the workflow diagram, states, and buttons for the baseline Library Control workflow in the Continuous Controls Testing module.

Workflow Diagram

Following image shows the baseline Library Control workflow.



Workflow States

The following table lists the states associated with the baseline Library Control workflow.

State	Description
CON: LIBRARY CONTROL: Draft, Unassigned	The initial state for a new library control.
CON: LIBRARY CONTROL: Documentation in Progress	A library control enters this state from the **Draft**, **Unassigned** state. In this state, the *Library Control Owner* user documents the control and its associated tests.
CON: LIBRARY CONTROL: Under Review	A library control enters this state from the **Documentation in Progress** state. In this state, the *Library Control Reviewer* user reviews the documentation submitted by the Library Control Owner.
CON: LIBRARY CONTROL: Approved/Active	A library control enters this state from the **Under Review** state. Only controls in this state will be available for selection in control test execution workflows.

Workflow Buttons

The following table lists the buttons that are available in the various states of the baseline Library Control workflow.

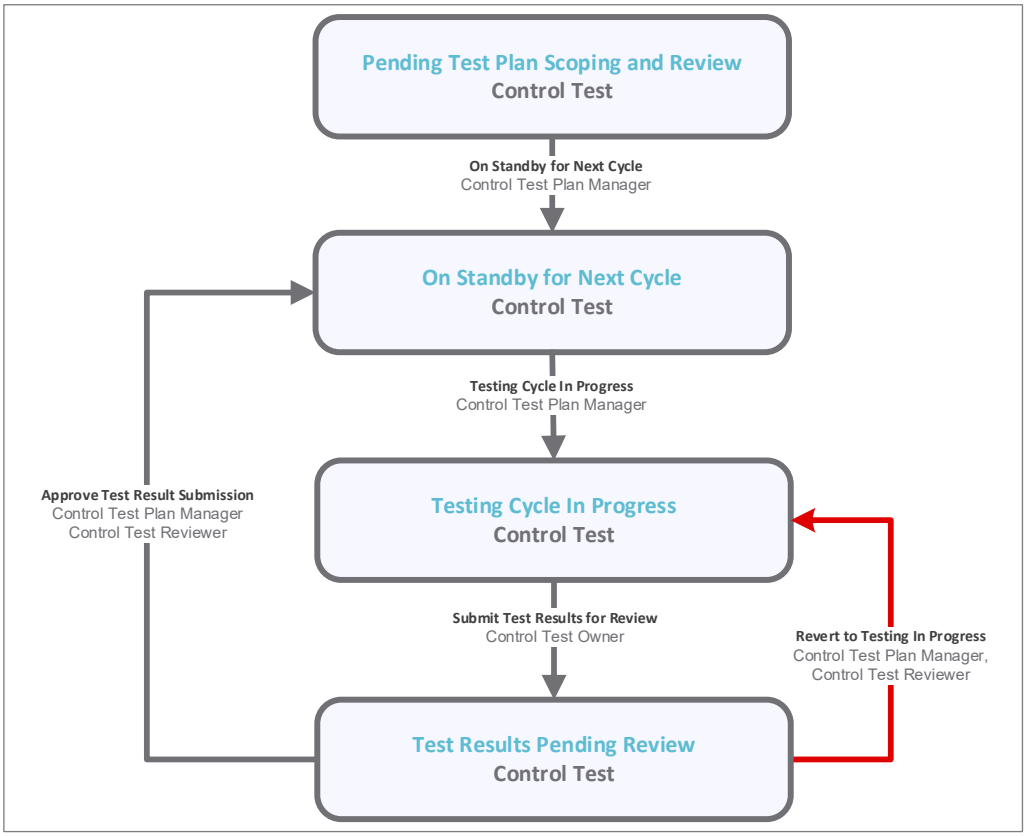
Button	Available to	Notification	Description
CON: LIBRARY CONTROL: Assignment Complete	CON: Library Control Manager	Yes	Available in the **Draft**, **Unassigned** state to move the library control record workflow to the **Documentation in Progress** state. Indicates that assignment is complete and library control is ready for documentation by *owner*.
CON: LIBRARY CONTROL: Revert to Unassigned (Manager)	CON: Library Control Manager	No	Available in the **Documentation in Progress** state to move the library control record workflow back to the **Draft**, **Unassigned** state.
CON: LIBRARY CONTROL: Submit for Review	CON: Library Control Manager CON: Library Control Owner	Yes	Available in the **Documentation in Progress** state to move the library control record workflow to the **Under Review** state. In this state, the *Library Control Owner* user submits the documentation for the library control (and its tests) to the *Library Control Reviewer* user
CON: LIBRARY CONTROL: Approve	CON: Library Control Manager CON: Library Control Reviewer	Yes	Available in the **Under Review** state to move the library control record workflow to the **Approved/Active** state. In this state, the *Library Control Reviewer* user approves the documentation submitted for the library control.
CON: LIBRARY CONTROL: Request Further Edits	CON: Library Control Manager, CON: Library Control Reviewer	Yes	Available in the **Under Review** state to move the library control record workflow to the **Documentation in Progress** state. In this state, the *Library Control Reviewer* user rejects the documentation for the library control.
CON: LIBRARY CONTROL: Revert to Draft (Manager)	CON: Library Control Manager	No	Available in the **Under Review** and **Approved/Active** states to move the library control record workflow to the **Documentation in Progress** state.

Control Test Workflow

This section covers the workflow diagram, states, and buttons for the baseline Control Test workflow in the Continuous Controls Testing module.

Workflow Diagram

Following is the baseline Control Test workflow.



Workflow States

The following table lists the states associated with the baseline Control Test workflow.

Task Workflow State	Description
CON: CONTROL TEST: Pending Test Plan Scoping and Review	The initial state for new control test records when they are added to a control test plan (prior to the plan's final approval and activation).
CON: CONTROL TEST: On Standby for Next Cycle	A control test enters this state from the **Pending Test Plan Scoping and Review** state when the parent test plan is activated. However, not all control tests will necessarily start on the day their parent plan is activated. Individual control tests will become active once their specific **Next Cycle Start Date**

Task Workflow State	Description
	arrives.
CON: CONTROL TEST: Testing Cycle In Progress	A control test enters this state from the **Active**, **Pending Next Text Cycle** state. A control test in this state indicates that testing is in progress by the *Control Test Owner* user.
CON: CONTROL TEST: Test Results Pending Review	A control test enters this state from the **Testing Cycle In Progress** state. In this state, the *Control Test Reviewer* user reviews the testing results submitted by the *Control Test Owner* user in the prior state.

Workflow Buttons

The following table lists the buttons that are available in the various states of the baseline Control Test workflow.

Button	Available to	Notification	Description
CON: CONTROL TEST: On Standby for Next Test Cycle (Manager)	CON: Control Test Plan Manager	No	Available in the **Pending Test Plan Scoping and Review** state to move the control test workflow to the **On Standby for Next Cycle** state.
CON: CONTROL TEST: Testing Cycle in Progress (Manager)	CON: Control Test Plan Manager	Yes	Available in the **On Standby for Next Cycle** state to move the control test workflow to the **Testing Cycle in Progress** state. This button allows the *Control Test Plan Manager* user to force the test into active testing status without waiting for the Next Cycle Start Date to arrive.
CON: CONTROL TEST: Submit Test Results for Review	CON: Control Test Plan Manager CON: Control Test Owner	Yes	Available in the **Testing Cycle In Progress** state. Using this button, the *Control Test Owner* user submits test results to the *Control Test Reviewer* user.
CON: CONTROL TEST: Approve Test Result Submission	CON: Control Test Plan Manager CON: Control Test Reviewer	Yes	Available in the **Test Results Pending Review** state. Using this button, the *Control Test Reviewer* user approves the results submitted by the *Control Test Owner* user.
CON: CONTROL TEST: Revert to Testing in Progress	CON: Control Test Plan Manager CON: Control Test Reviewer	Yes	Available in the **Test Results Pending Review** state to move the control test workflow back to **Testing Cycle In Progress** state. Using this button, *Control Test Reviewer* user rejects results submitted by the *Control Test Owner* user.
CON: CONTROL TEST: Revert to On Standby for Next	CON: Control Test Plan Manager	No	Available in the **Testing Cycle In Progress** state to move the control test workflow to the **On Standby for Next Text Cycle** state.

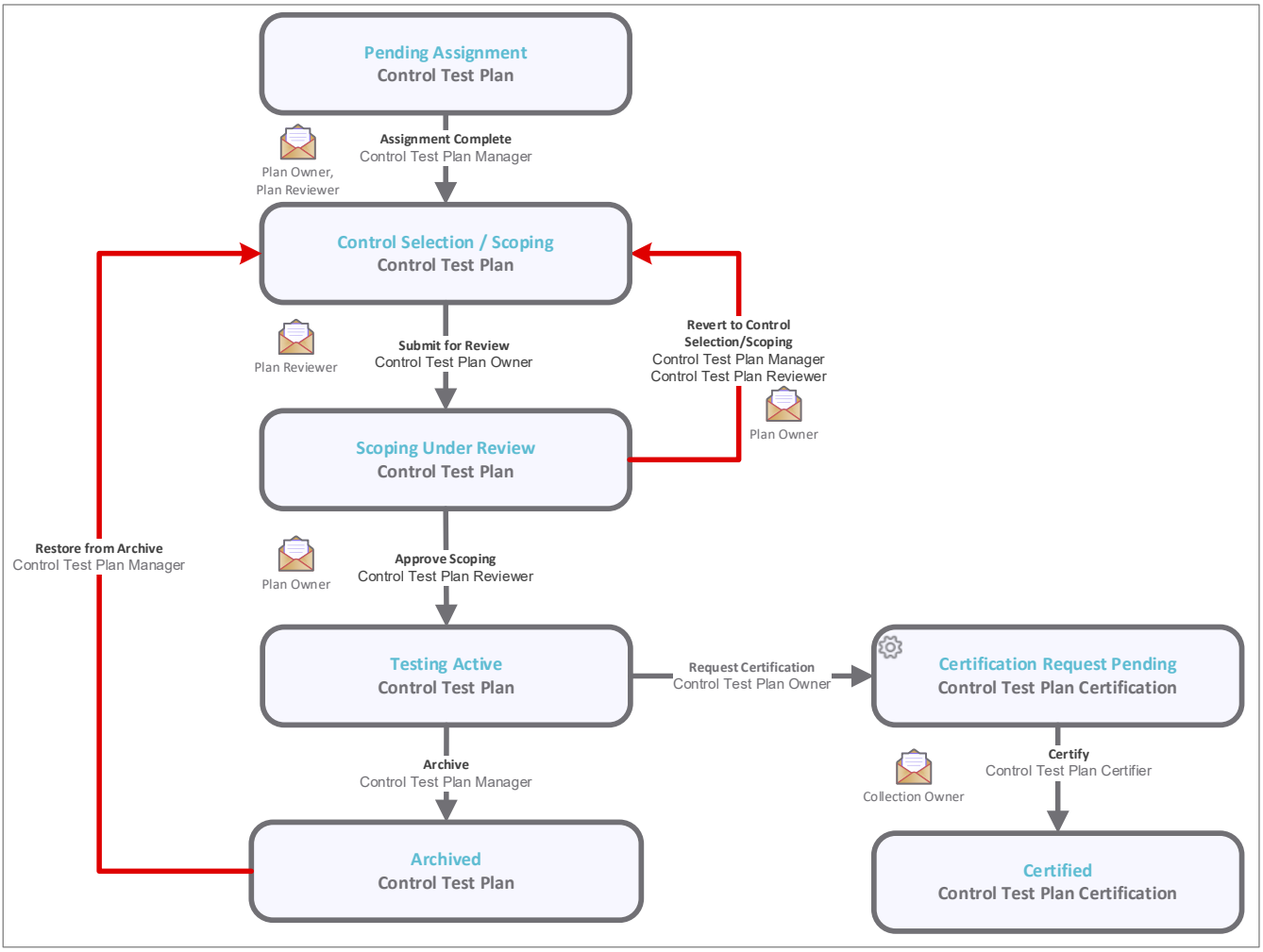
Button	Available to	Notification	Description
Test Cycle (Manager)			
CON: CONTROL TEST: Revert to Pending Collection Scoping and Review (Manager)	CON: Control Test Plan Manager	No	Using this button, the *Control Test Plan Manager* user moves the control test workflow back to the **Pending Test Plan Scoping and Review** state.

Control Test Plan Workflow

This section covers the workflow diagram, states, and buttons for the baseline Control Test Plan workflow in the Continuous Controls Testing module.

Workflow Diagram

Following is the baseline Control Test Plan workflow.



Workflow States

The following table lists the states associated with the baseline Control Test Plan workflow.

Workflow State	Description
CON: CONTROL TEST PLAN: Pending Assignment	The initial state for a new control test plan.
CON: CONTROL TEST PLAN: Control Selection / Scoping	A control test plan enters this state from the **Pending Assignment** state after an owner has been assigned. In this state, the *Control Test Plan Owner* user selects the controls and tests to be included in the test plan.
CON: CONTROL TEST PLAN: Scoping Under Review	A control test plan enters this state from the **Scoping Under Review** state. In this state, the *Control Test Plan Reviewer* user reviews the plan scoping submitted by the *Control Test Plan Owner* user.
CON: CONTROL TEST PLAN: Testing Active	A control test plan enters this state from the **Scoping Under Review** state. This is the state in which test execution activities ensue. Individual control tests have their own execution workflow states within the test plan.
CON: CONTROL TEST PLAN: Archived	A state for maintaining an audit history of archived test plans once they are no longer active.

Workflow Buttons

The following table lists the buttons that are available in the various states of the baseline Control Test Plan workflow.

Button	Available to	Notification	Description
CON: CONTROL TEST PLAN: Assignment Complete	CON: Control Test Plan Manager	Yes	Available in the **Pending Assignment** state to indicate that the assignment is complete and move the control test plan workflow to the **Control Selection / Scoping** state.
CON: CONTROL TEST PLAN: Submit for Review	CON: Control Test Plan Manager CON: Control Test Plan Owner	Yes	Available in the **Control Selection / Scoping** state to move the control test plan workflow to the **Scoping Under Review** state.
CON: CONTROL TEST PLAN: Generate Tests from Library Control Selections	CON: Control Test Plan Manager CON: Control Test Plan Owner	No	Available in the **Control Selection / Scoping** state to create control tests for the current control test plan based on the selected library controls (and their child library control tests).
CON: CONTROL TEST PLAN:	CON: Control Test Plan	Yes	Available in the **Scope Under Review** state to move the control test plan workflow to the

Button	Available to	Notification	Description
Approve Scoping	Manager CON: Control Test Plan Reviewer		**Testing Active** state. Using this button, the *Control Test Plan Reviewer* user approves and activates the test plan.
CON: CONTROL TEST PLAN: Revert to Control Selection / Scoping	CON: Control Test Plan Manager CON: Control Test Plan Reviewer	Yes	Available in the **Scoping Under Review** state to reject the test plan submission and move the control test plan workflow back to the **Control Selection / Scoping** state.
CON: CONTROL TEST PLAN: Revert to Control Selection / Scoping (Manager)	CON: Control Test Plan Manager	No	Available in the **Scoping Under Review** and **Testing Active** states. Using the button, the *Control Test Plan Manager* user moves the control test plan workflow back to the **Control Selection / Scoping** state.
CON: CONTROL TEST PLAN: Request Certification	CON: Control Test Plan Manager CON: Control Test Plan Owner	Yes	Available in the **Testing Active** state. Using this button, the *Control Test Plan Owner* user creates a control test plan certification record, which is auto-populated with references to the most recent control test history for each of the plan's control tests.
CON: CONTROL TEST PLAN: Archive	CON: Library Control Manager	No	Available in the **Testing Active** state. Using this button, the *Control Test Plan Owner* user archives a copy of the control test plan.
CON: CONTROL TEST PLAN: Restore from Archive	CON: Library Control Manager	No	Available in the **Archived** state. Using this button, the *Control Test Plan Manager* user restores the control test plan from the **Archived** state.

Control Test Plan Certification Workflow

This section covers the workflow diagram, states, and buttons for the baseline Control Test Plan Certification workflow in the Continuous Controls Testing module.

Workflow Diagram

Refer the **Control Test Plan** workflow diagram.

Workflow States

The following table lists the states associated with the baseline Control Test Plan Certification workflow.

Workflow State	Description
CON: CONTROL TEST PLAN CERTIFICATION: Certification Request Pending	The initial workflow state for a new control test plan certification record.
CON: CONTROL TEST PLAN CERTIFICATION: Certified	A control test plan certification record enters this state from the Certification Request Pending state when a control test plan certification has been certified by the *Control Test Plan Certifier* user.

Workflow Buttons

The following table lists the buttons that are available in the various states of the baseline Control Test Plan Certification workflow.

Button	Available to	Notification	Description
CON: CONTROL TEST PLAN CERTIFICATION: Certify	CON: Control Test Plan Certifier	Yes	Available in the **Certification Request Pending** state. Using this button, the *Control Test Plan Certifier* user certifies/attests the collection of control tests submitted for the current period.
CON: CONTROL TEST PLAN CERTIFICATION: Initialize New Certification	System	Yes	Rsam uses this button to initialize newly created control test plan certification records (populating links to relevant control test histories, sending email notifications, etc.).

Workflow Roles

The following table lists the workflow roles that perform tasks associated with the states in the baseline Control Testing workflows.

User ID	Role	Description
r_library_control_manager	**CON: Library Control Manager**	Manages the global library of controls across all library groupings.
r_library_control_owner	**CON: Library Control Owner**	Owns the documentation of a specific library control and its tests.

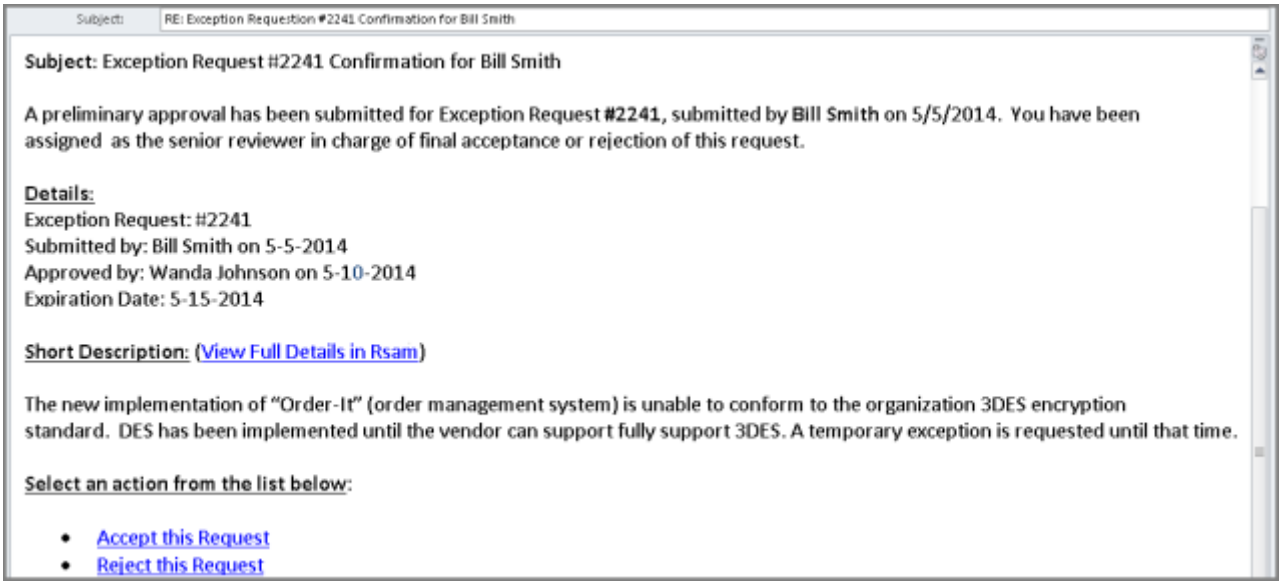
User ID	Role	Description
r_library_control_reviewer	**CON: Library Control Reviewer**	Reviews the documentation of a specific library control and its tests.
r_control_test_plan_manager	**CON: Control Test Plan Manager**	Manages control test execution activities for a given assessment object across all test plans / test groups.
r_control_test_plan_owner	**CON: Control Test Plan Owner**	Owns a specific test plan on an assessment object.
r_control_test_plan_reviewer	**CON: Control Test Plan Reviewer**	Reviews a specific test plan on an assessment object.
r_control_test_owner	**CON: Control Test Owner**	Owns a specific control test within a test specific plan on an assessment object.
r_control_test_reviewer	**CON: Control Test Reviewer**	Reviews a specific control test within a test specific plan on an assessment object.
r_control_test_plan_certifier	**CON: Control Test Plan Certifier**	Certifies test pans on a periodic basis by signing off on the tests submitted and approved for that period.
r_active_library_control_viewer	**CON: Active Library Control Viewers** (for Execution-side users)	Provides read-only access to active library controls for those test execution users that need to see them.

In addition to the preceding roles, the Rsam installation package includes an administrative role, **U: Object Administrator**, as well as a sample user for that role, **r_admin**. This user has access to all record types, object types, workflow states, and workflow buttons across all Rsam baseline modules. Rsam Administrators should take necessary precautions to restrict standard users from accessing Rsam with this administrative role. If additional administrative roles are required, you can create it from **Manage > Users/Groups**.

Appendix 1: Offline Decision Making

Rsam email notifications are configurable including what notification should be sent, what users or roles will receive the notifications, and the content in the notifications.

Offline Decision Making is a powerful and popular feature of Rsam. It provides the Rsam platform directly to the users to perform workflow actions without connecting to the Rsam module. The following image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Offline Decision Making actions.

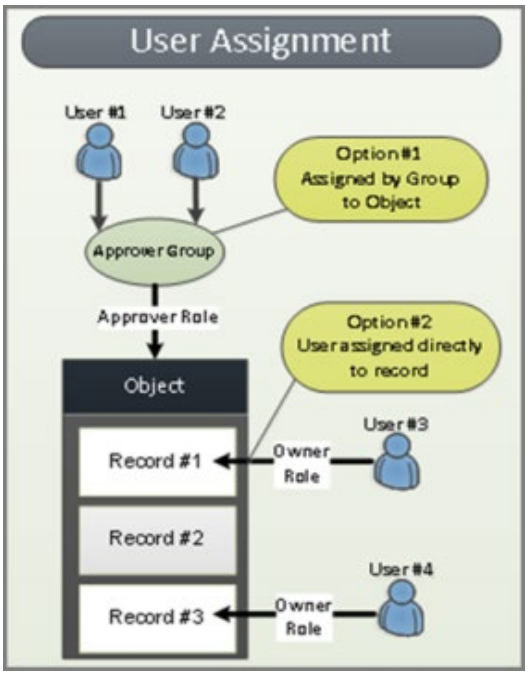


Appendix 2: User Assignment Options

Rsam allows organizations to customize configurations and workflows to their specific business practices. There are many methods by which users can be assigned roles (such as, who is responsible for reviewing and approving exceptions). The following are the most common assignment methods:

- Individual users are assigned to a group. The group is then assigned to the object under which the records are saved. When assigned to the object, the group is also given a specific role. This accomplishes the following:
    - All users in that group inherit the role assigned to the group in the context of the object and all the records under that object.
    - All users in that group have the functionality allocated to that role in the context of the object and all of the records under that object.
- Individual users are assigned a specific role directly in a record. This provides the same result as above – granting the user the functionality with the allocated role. However, it is only in the context of that specific record. No other permissions are granted to the parent object or any other record under that object.

The method for implementing the assignment can also be customizable. The assignment can be manually made through an attribute, assigned when the records are created or imported, or automatically made at different points in the workflow.



Appendix 3: Rsam Documentation

Continuous Controls Testing Tutorial

For a detailed walk-through of the Continuous Controls Testing user experience, refer the *Continuous Controls Testing Step-by-Step Tutorial*. You should have received the *Continuous Controls Testing Step-by-Step Tutorial* along with the Continuous Controls Testing instance. If not, contact your Rsam Customer Representative to obtain an electronic copy of the *Continuous Controls Testing Step-by-Step Tutorial*.

Online Help

This document provides an overview of the Continuous Controls Testing configuration. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Provide the **User ID** as ***r_admin*** and provide the **Password**.

2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

   The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.