Waiver Management

Documenting Exceptions and Exclusions

05-15-2025

Cyturus Technologies, Inc.

Introduction

In real-world governance, risk, and compliance (GRC) programs, not every control, policy, or requirement can be fully implemented at all times. Business conditions shift, resource constraints emerge, technical limitations arise, and at times, certain risks must be knowingly accepted for a defined period. When these situations occur, it becomes critical to document, track, and manage these exceptions in a formal, auditable, and transparent manner.

To support this business need, Cyturus introduces an integrated Waiver Management function within the CRT platform. This functionality allows organizations to record and manage any temporary deferment, exception, or documented deviation related to:

- Cybersecurity Practices
- Compliance Controls
- Internal Policies
- Third-Party Risks
- Regulatory or Framework Requirements

Rather than relying on informal approvals or undocumented workarounds, the CRT Waiver function empowers organizations to implement a structured, risk-informed, and time-bound waiver process that reinforces accountability and enables executive oversight.

What is a Waiver?

A waiver is a formal declaration that a known deviation from a defined expectation (practice, control, policy, or requirement) is being accepted for a limited period of time. Waivers are not blanket exemptions—they are specific temporary exceptions that require:

- A stated justification
- A clearly defined duration
- An approval based on risk and/or length
- Periodic review and reassessment

This approach ensures that a potential risk is visible, acknowledged, governed, and monitored.

Why Use the Waiver Functionality?

At first glance, Waivers appear to offer little value beyond bureaucratic documentation, however, Organizations utilize waivers to:

- Document when a control or policy cannot yet be implemented
- Accept known risks under specific, pre-approved conditions
- Provide stakeholders with visibility into compliance gaps
- Ensure that exceptions are tied to remediation plans or reassessment checkpoints
- Waivers also serve as a governance safeguard, ensuring that temporary gaps do not become permanent blind spots.

How Waivers Work in the CRT

The CRT Waiver Management function provides:

- Time-bound waiver options ranging from 7 to 365 days
- Customizable approval workflows based on waiver length and risk level
- Justification requirements scaled to the potential risk created by the waiver
- Pre-expiration review checkpoints to confirm closure, renewal, or escalation

For example, a 7-day waiver may only require Manager-level approval, while a 180-day waiver may escalate to a Director, VP, or Executive approver. Additionally, in modules like the Risk Register or Third-Party Risk Management (TPRM), the assigned Risk Rating can dynamically alter the required approver tier, ensuring that high-risk exceptions receive the scrutiny they require.

Waivers and Scoring

While waivers are not currently tied to scoring within the CRT's Cyber Maturity Index (CMI®), they play a critical role in contextualizing assessment results and maintaining audit integrity. Waivers help clarify when an item is not implemented due to active risk acceptance—not oversight—supporting honest, actionable reporting and effective remediation planning.

Prerequisites

The Waiver functionality is not a stand-alone module requiring additional licensing, contract update, or Instance Admin configurations. The CRT has certain defaults configured, but requires specific configurations covered in this Guide.

Waiver Management in the CRT

When we decided to build in a comprehensive Waiver Management solution, we interviewed clients, organizations, and even some prospects. We performed research on current waiver processes, and designed a solution that best met the requirements and also included some specific use case configurations.

Waiver Management is not a separate CRT module, but it does require specific entitlements. It is integrated into all CRT Modules and configured centrally at the Instance level in Attribute Management which establishes the Waiver Management functionality across all Clients within that Instance. In a future update we want to extend the Waiver Approval configuration to the Organization level.

Waiver Configuration

When configuring Waiver Management, the first step is setting up the Waiver Approver Types. The CRT comes with the following default Waiver Approver Types. These can be adjusted by an Instance Admin, but are sufficiently preconfigured for most organizations.

List Type

Waiver Approver ▼	+ Add

Sort No ∧	Waiver Approver Name	Description	Color	Status	Actions
1 ⇕	Manager		■	Active	✏ ✕ 🗑
2 ⇕	Sr. Manager		■	Active	✏ ✕ 🗑
3 ⇕	Director		■	Active	✏ ✕ 🗑
4 ⇕	Vice President		■	Active	✏ ✕ 🗑
5 ⇕	Executive Sponsor		■	Active	✏ ✕ 🗑
6 ⇕	Board		■	Active	✏ ✕ 🗑

10 ▼   Showing 1 to 6 of 6 records   ‹ **1** ›

Step two (2) in setting up the configuration requires establishing the Approval Process for each Waiver duration. There are 8 default durations setup in the CRT Waiver Management.

List Type

Waiver Duration ▼	+ Add

Sort No ∧	Waiver Duration Name	Description	Color	Status	Configure
1 ⇕	7 days		■	Active	⚙
2 ⇕	14 days		■	Active	⚙
3 ⇕	30 days		■	Active	⚙
4 ⇕	60 days		■	Active	⚙
5 ⇕	90 days		■	Active	⚙
6 ⇕	120 days		■	Active	⚙
7 ⇕	180 days		■	Active	⚙
8 ⇕	365 days		■	Active	⚙

10 ▼   Showing 1 to 8 of 8 records   ‹ **1** ›

Step three (3) is the first place that a default configuration is not included. Each of the defined durations require an approval configuration to define the approver flow.

Approver	Functional Role	Action
Manager	Waiver Approver	✏ 🗑
Sr. Manager	Waiver Approver	✏ 🗑
Director	Waiver Approver	✏ 🗑
Vice President	Waiver Approver	✏ 🗑

First select Attribute Management from the Administration Menu.
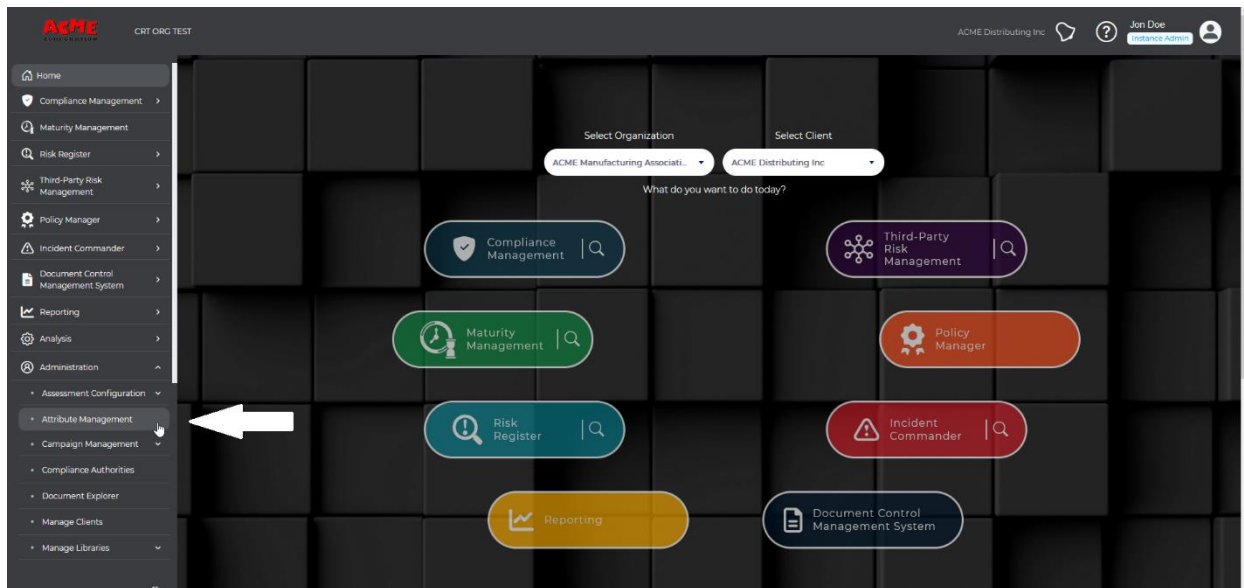
Once you have selected Attributre Management, you will select Manage Lists and then Waiver Duration from the drop-down. Please note Lists are displayed alphabetically so Waiver is near the bottom.
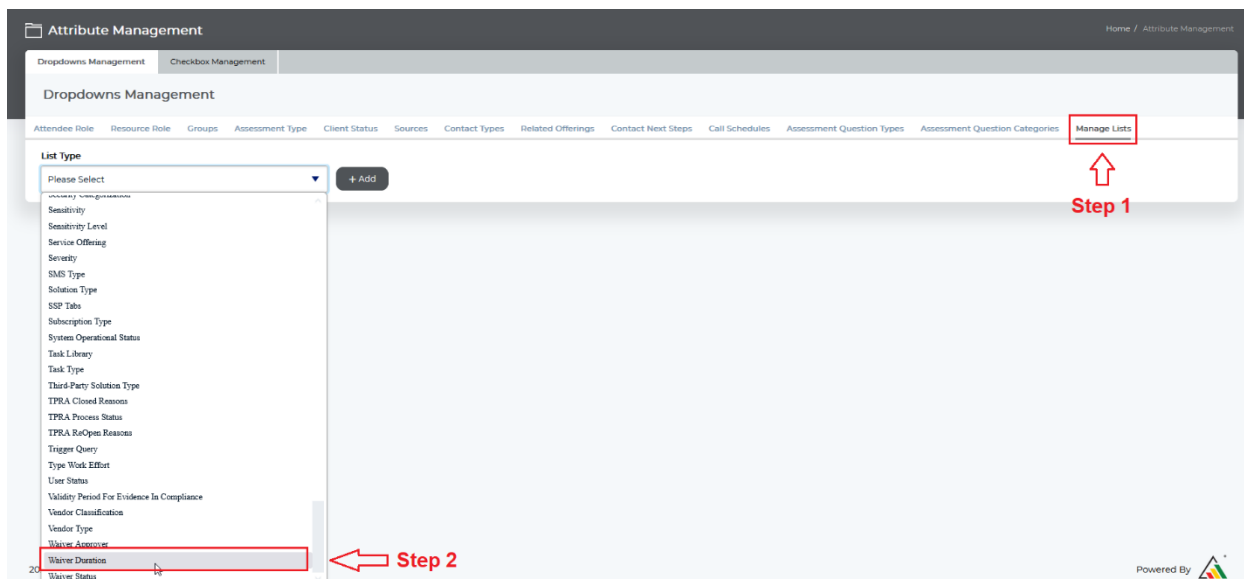
The available Waiver Durations are now displayed.

Click the Configure action button to setup the workflow for the selected Waiver duration. In this example I am selecting a duration of 7 Days.

The Waiver Configuration form allows you to configure the required 7 day Waiver approval process for any CRT Module. This is useful when a different series of approvers are required for TPRM or a Policy Waiver vs the required approval for an internal Compliance Waiver.

As you can see in the screen shot below, a 7 Day Waiver duration is only available in two modules, Compliance and Risk.

To enable the 7 Day Waiver in any additional module, one must only click the checkbox and then select the Link Approvers for that module to configure the Approvers required to approve a 7 day Waiver for the Module.
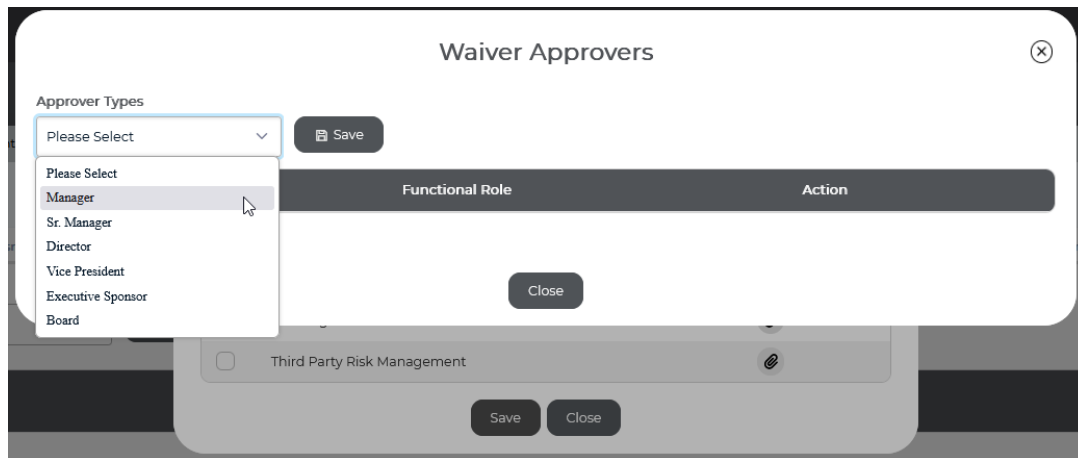
It is now time to configure the approver for a 7 day Waiver in the DCMS module.

Select an Approver Role from the Approver Type dropdown and click save.

You will now notice that a Manager is now required to approve a 7 day Waiver in the DCMS Module.

Adding a second Approver is just as simple. Select the Approver Role and click Save once again.

Now a Manager and Sr Manager are required to Approve a 7 day Waiver for the DCMS module. This process is repeated for each duration within each applicable module in the initial configuration. Once completed, the CRT will require only those necessary Approvers based on the duration of the requested Waiver.

Assigning Approver Roles to User Entitlements

In a slight deviation from the customary zero trust 3D-RBAC method of assigning Entitlements to Users, when assigning Waiver Entitlements, if a User that is granted the entitlement of Waiver Approver, the Approver Role must be selected during the assignment process. This is a multi-select drop-down enabling a single user to be various approver types based on the Waiver Duration configuration previously configured.
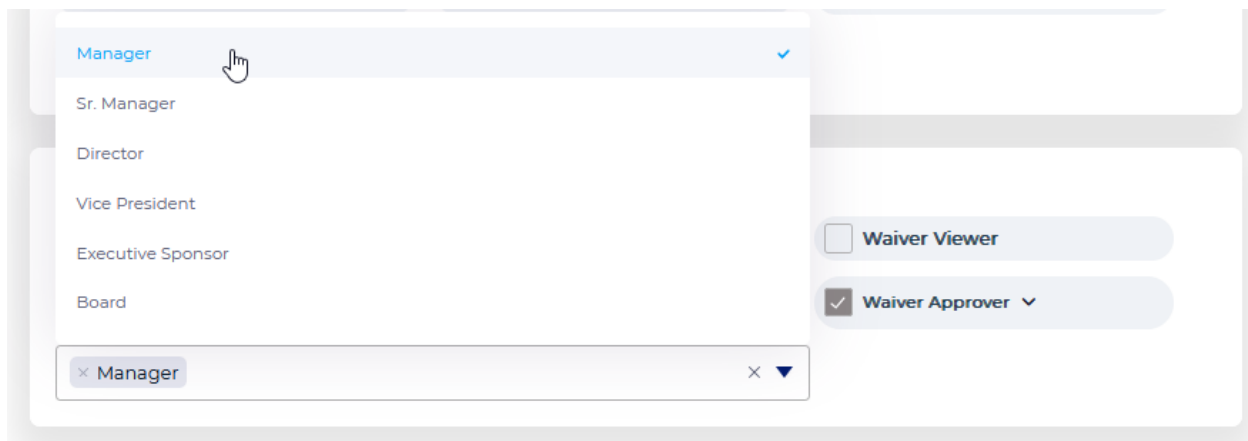
The importance of assigning an Approver Type to a User account will be explained in detail when Requesting a new Waiver. This provides the opportunity for the Waiver Requestor to define the specific Approvers (Users) configured in the Approval path for their requested Waiver.

Accessing Waiver Management
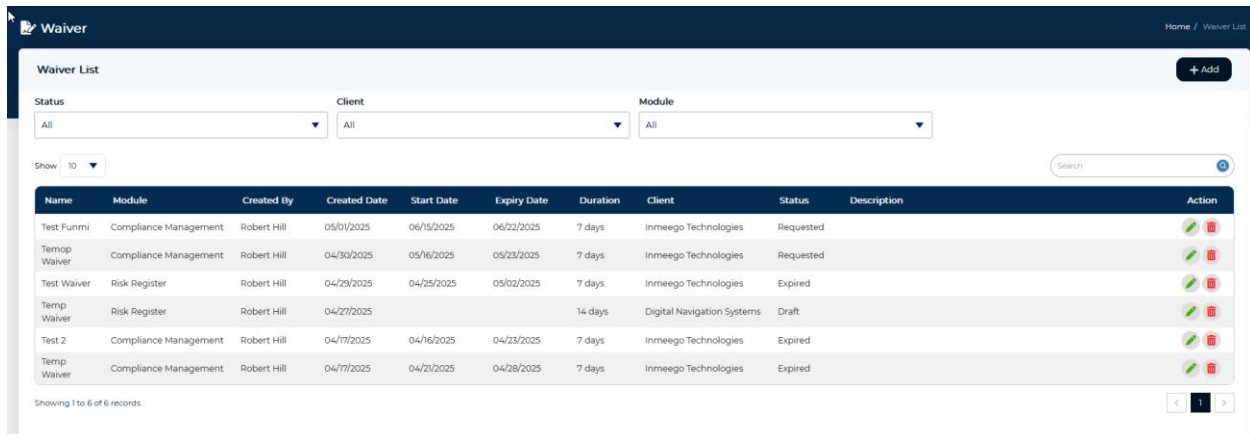
Consistency is a driving element when we are developing new functionality within the CRT. Designing and building the Waver Management functionality was no different. You will see the unique Waiver icon within each module of the CRT.

This icon not only launches Waiver Management for this specific element within the CRT, it also shows the number of active Waivers attached to that element. This could be a Policy, a Risk, or even a single Compliance requirement. To access all Waivers to which a user has access (Author, Manager, Approver) one can utilize the left hand menu and select Waiver Management.
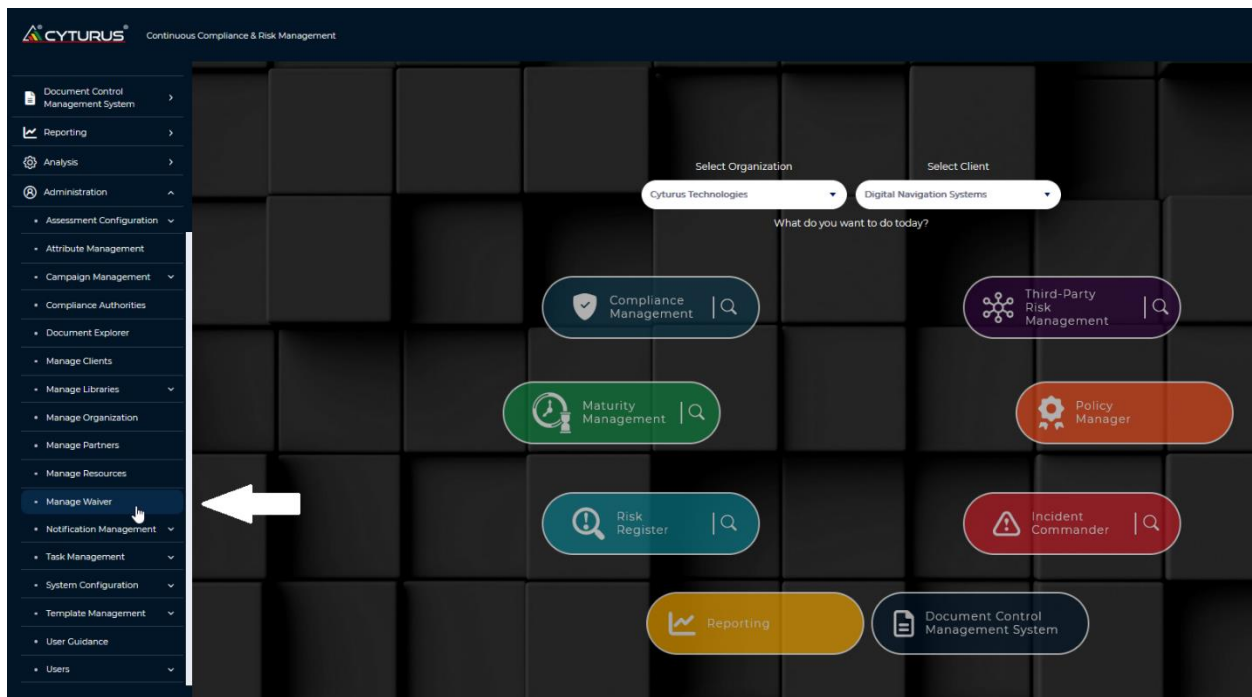
The Waiver Management form displays a listing of all Waivers to which the current User has access.

Requesting a New Waiver

When one needs to generate a new Waiver for approval, one can chose the specific element and click on the Waiver icon or select Waiver Management from the Admin menu.

When clicking on the Waiver icon, if there are existing Waivers attached to the selected element, then a Waiver List form displaying the existing Waivers will be displayed so the user can select the applicable Waiver or simply click on the [+ Add] button to initiate a new Waiver.

If, when selecting the Waiver icon, there is no previous Waiver attached, the CRT will prompt the user with the following notice:
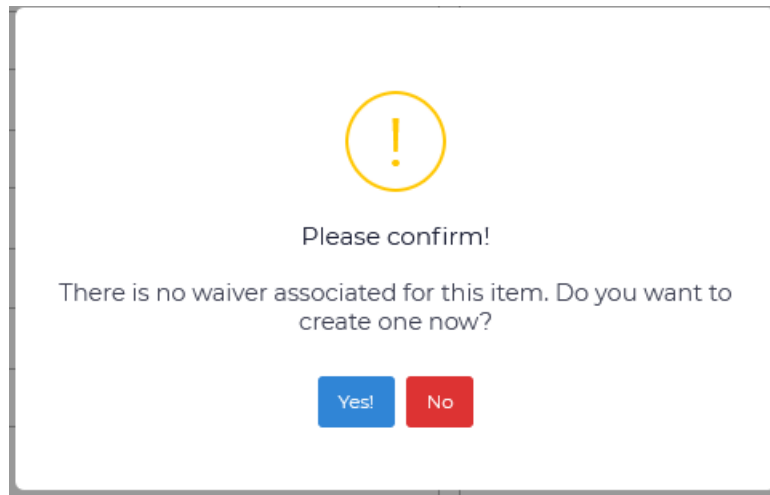
Selecting [No] will return the user to the previous screen, or by selecting [Yes], the CRT will initiate the creation of a new Waiver.

Select the Duration previously configured in the Attribute Management. If a Waiver Duration setting for the selected module has not been configured, it will not display in the dropdown.

Add a descriptive name for the Waiver as well as the anticipated Start Date. The Expiration Date will calculate based on the selected Duration and Start Date

You will notice once the Duration has been selected, the necessary Approver Types are populated. Once you have completed filling in the basic Waive details, Click [Create and Continue] to initiate the process of creating a new Waiver.

The next Waiver form is where the user can provide the necessary details including the full Description, Justification, and then specific Business Justification, in an impact is predicted as well as the Technical Justification if applicable.

At the top of the form, you will notice two tabs. The first is for the Waiver Details and the second is for configuring the Approver workflow. Select on the Approvers tab.

Once on the Approvers tab, you can see the listing of required Approvers based on the selected Duration. Using the dropdown for each approver, select the Approver to which you previously assigned the Waiver Approver entitlement and the Approver Type assigned to that User.

Once the details for the Waiver have been entered and the Approval chain has been configured, the user can select the [Submit] button. Until it is ready to be Submitted, the Waiver request remains in a draft state. The Approval process has not yet begun, and now notifications have been sent.

Once the Waiver has been Submitted and the Submitted note entered, the Waiver is then locked pending Approval from the identified Approvers. A user with Waiver Manager

entitlements can edit certain details or delete a Waiver once it has been submitted for approval.

Once approved, the Waiver will change status to *Issued* at the Start Date and then will change again to *Expired* once the Expiration Date is reached.

Support Options

If you have any questions or issues configuring this new functionality, please contact Cyturus Support for assistance.