Spring 5-18-2018

User's Manual for Tardigrade Risk Assessment

Alexis M. Shook
University of New Orleans, ashook@uno.edu

Follow this and additional works at: https://scholarworks.uno.edu/td

Part of the Computer Engineering Commons, Rhetoric and Composition Commons, and the Technical and Professional Writing Commons

Recommended Citation
https://scholarworks.uno.edu/td/2492

This Thesis is brought to you for free and open access by the Dissertations and Theses at ScholarWorks@UNO. It has been accepted for inclusion in University of New Orleans Theses and Dissertations by an authorized administrator of ScholarWorks@UNO. The author is solely responsible for ensuring compliance with copyright. For more information, please contact scholarworks@uno.edu.
User's Manual for Tardigrade Risk Assessment

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of the
requirements for the degree of

Master of Arts
in
English

By
Alexis Morganne Shook
B.A. University of New Orleans, 2016
M.A. University of New Orleans, 2018
May 2018
# Table of Contents

1 ABOUT THIS USER'S MANUAL .......................................................................................................................... 1

1.1 INTENDED AUDIENCE ............................................................................................................................. 2

1.2 TYPOGRAPHICAL CONVENTIONS ............................................................................................................. 2

2 GETTING STARTED ......................................................................................................................................... 3

2.1 OVERVIEW OF TARDIGRADE ....................................................................................................................... 3

2.2 ROLES AND RESPONSIBILITIES .................................................................................................................. 4

2.3 HARDWARE REQUIREMENTS ....................................................................................................................... 6

2.4 SOFTWARE REQUIREMENTS ........................................................................................................................ 6

2.5 CYBERSECURITY ASSESSMENT .................................................................................................................. 7

2.6 INTERNAL CONTROL ASSESSMENT ............................................................................................................ 8

2.7 SECURITY REQUIREMENT TRACEABILITY MATRIX ..................................................................................... 9

2.8 ACCESSING TARDIGRADE .......................................................................................................................... 10

2.9 ROLE-BASED ACCESS ............................................................................................................................... 11

3 CYBERSECURITY ........................................................................................................................................ 12

3.1 CONDUCTING CYBERSECURITY ASSESSMENT FOR INHERENT RISK PROFILE ................................. 12

3.1.1 Assigning a Task ...................................................................................................................................... 12

3.1.2 Conducting a Task ................................................................................................................................... 14

3.1.3 Reviewing a Task .................................................................................................................................... 15

3.2 CONDUCTING CYBERSECURITY ASSESSMENT FOR DOMAIN MATURITY ........................................... 17

3.2.1 Assigning a Task ...................................................................................................................................... 17

3.2.2 Conducting a Task ................................................................................................................................... 19

3.2.3 Reviewing a Task .................................................................................................................................... 20

3.3 CYBERSECURITY DASHBOARD REPORTS .............................................................................................. 22

3.3.1 Printing Cybersecurity Dashboard Reports ............................................................................................. 23

3.4 CYBERSECURITY ADMIN PANEL ............................................................................................................. 24
Abstract

This user-guide provides instructions for operating Tardigrade 1.1.3, a cybersecurity software for Nollysoft, LLC. This guide instructs users step-by-step on how to set security controls, risk assessments, and administrative maintenance. Tardigrade 1.1.3 is a Risk Assessment Enterprise that evaluates the risk level of corporations and offers solutions to any security gaps within an organization. Tardigrade 1.1.3 is a role-based software that operates through three modules, Cybersecurity Assessment, Internal Control, and Security Requirement Traceability Matrix.

Keywords Cybersecurity, Technical Writing, Professional Writing, Software, Manual, User-guide
1 About this User’s Manual

This document is intended to give you a comprehensive insight into Tardigrade application. It is meant to get you started with Tardigrade and introduce you to its basic functions. This guide assumes that you have a basic knowledge and experience using web-based applications.

This document is divided into the following chapters:

- Chapter 1, About this User’s Manual, Intended Audience and Typographical Conventions
- Chapter 2, Getting Started with Tardigrade
- Chapter 3, Cybersecurity Assessments
- Chapter 4, Internal Control Assessments
- Chapter 5, Security Requirement Traceability Matrix
- Chapter 6, Reference Tables
- Chapter 7, My Account
- Chapter 8, User Administration
- Chapter 9, Help and All Supporting Documentation
- Appendix A: Glossary: Provides definitions of technical terms that appear in the guide.
- Appendix B: List of figures in the User Manual
1.1 Intended Audience

This document is intended as a complete guide for using Tardigrade. This document allows users to learn how to use Tardigrade and understand its various capabilities through the user interface. This guide assumes that users have some knowledge of the risk assessment process. For more information, visit https://www.nollysoft.com.

1.2 Typographical Conventions

To make information easier to find and important information stand out, we will be using the following conventions:

- User roles appear in **bold** type in definitions and task steps
- Menu items and all user interface items also appear in **bold**.
- Steps are numbered and sub-steps are bulleted.
- Notes are indicated as the following:

| Note: | Notes tell you of important information: either things that will make your life easier or information you want to take special notice of. Notes are added commentary to the main body of text, and contain essential information which should not be overlooked. |
2 Getting Started

2.1 Overview of Tardigrade

Tardigrade is a Software as a Service (SaaS) application that helps you conduct in-depth assessment of the following components in your organization’s cybersecurity framework. Once a company assesses their security risk through the Cybersecurity and Internal Control Assessments, the Security Requirement Traceability Matrix allows the organization to select the security control they see fit. Each component may be purchased as separate assessment and security solutions. Or all three modules can be used to provide the most cybersecurity protection.

<table>
<thead>
<tr>
<th>Module</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Assessment</strong></td>
<td>Tardigrade Cybersecurity Assessment helps organizations identify their risks and determine their cybersecurity preparedness. The assessment solution provides businesses with repeatable and measurable processes to inform senior management of their organization’s cybersecurity preparedness over time.</td>
</tr>
<tr>
<td><strong>Internal Control Assessment</strong></td>
<td>Tardigrade Internal Control solution enables organizations to understand deficiencies in their system of internal control to allow the creation of effective mitigating controls to help achieve business objectives.</td>
</tr>
<tr>
<td><strong>Security Requirement Traceability Matrix</strong></td>
<td>Tardigrade Security Requirement Traceability Matrix solution allows organizations to effectively select security controls from Standards and Regulations for implementation either as a part of a Secure Software Development Lifecycle (SSDLC) or regulatory mandate.</td>
</tr>
</tbody>
</table>
2.2 Roles and Responsibilities

The following image depicts the functional flow and roles and responsibilities of the users using Tardigrade:

![Enterprise Risk Assessment (ERA) Flow](image)

*Figure 1: The roles and functional flow of the Enterprise Risk Assessment*
The various roles and their responsibilities that the users of Tardigrade can have are described below:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task Assigner</strong></td>
<td>• The Task Assigner role assigns tasks to an assessor (the person who conducts assessment).</td>
</tr>
<tr>
<td></td>
<td>• It is not possible to reassign an incomplete task (task that is already assigned but an assessment has not been completed) until the initial task is completed.</td>
</tr>
<tr>
<td></td>
<td>• Different tasks can be assigned to the same assessor.</td>
</tr>
<tr>
<td></td>
<td>• When a task is assigned to an assessor, an email notification is sent to the assessor to inform the person that a task has been assigned and waiting for assessment.</td>
</tr>
<tr>
<td><strong>Task Assessor</strong></td>
<td>• The Task Assessor role allows a person to assess a task that is assigned to that role.</td>
</tr>
<tr>
<td></td>
<td>• An assessor can be assigned multiple tasks at the same time.</td>
</tr>
<tr>
<td></td>
<td>• After an assessor completes an assessment, an email notification is sent to the reviewer (manager) who reviews and verifies the assessment for accuracy and completeness.</td>
</tr>
<tr>
<td><strong>Reviewer</strong></td>
<td>• The Reviewer role allows a person to review an assessment conducted by an assessor.</td>
</tr>
<tr>
<td></td>
<td>• The reviewer verifies and validates the assessment for accuracy and completeness.</td>
</tr>
<tr>
<td></td>
<td>• A reviewer can approve or reject an assessment on a page by page basis. After the review is complete, the outcome of the review is sent to the assessor via an email notification.</td>
</tr>
<tr>
<td></td>
<td>• If an assessment is rejected, the assessor will go and reconduct the assessment for the pages of the assessment that were rejected.</td>
</tr>
</tbody>
</table>
2.3 Hardware Requirements

Tardigrade is deployed as Software as a Service (SaaS). The user does not need any hardware to implement the solution. To access the application, users should follow the recommendation below.

Minimum configuration required:

- Laptop or desktop running Intel Core i5 CPU @2.5GHz processor or higher.
- 4 GB of RAM or higher.
- Strong internet connectivity.

2.4 Software Requirements

You can access Tardigrade on the following operating systems:

- Windows
- Mac
- Linux

The following browsers are supported:

- Firefox version 54.0 or higher
- Google Chrome version 60.0 or higher
- Microsoft Edge version 40.0 or higher
- Internet Explorer version 11.0 or higher
- Safari version 11.0 or higher

Note: Tardigrade is not currently optimized for mobile devices. Though it will work on them but the user experience will be less than expected. Future release of Tardigrade will be optimized to support mobile devices.
2.5 Cybersecurity Assessment

Overview: The Cybersecurity Assessment, which consists of the Inherent Risk Profile and Cybersecurity Maturity, is inspired by the FFIEC Assessment mandate. This offering allows an organization to identify risks, determine cybersecurity maturity preparedness, and create effective risk management strategies.

Cybersecurity Assessment: Inherent Risk is the level of risk posed to an organization by the following:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Cybersecurity Assessment: Domain Maturity provides information about the cybersecurity maturity of an organization based on assessed maturity domain and the corresponding assessment factors.

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cyber Controls
- External Dependency Management
- Cyber Incident Management and Resilience
2.6 Internal Control Assessment

**Overview:** The Internal Risk Assessment consists of the Component Compliance, Deficiency, and Principle Compliance. The Internal Control solution enables organizations to understand deficiencies in their system of internal control to allow creation of an effective mitigating controls to help achieve business objectives. It is based on industry standards and best practices framework (Committee of Sponsoring Organizations of the Treadway Commission or COSO).

The Internal Control Principle is

- **Internal Control Assessment:** Component Compliance reports provide compliance information based on assessed components. The Component Compliance gives a report on the five components of Internal Control which include:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring activities.

- **Internal Control Assessment:** Deficiency reports provide information about the identified deficiency with the organization internal control as assessed.

- **Internal Control Assessment:** Principle Compliance reports provide compliance information based on assessed principles. The assessed principles included:
  - Demonstrates Commitment to Competence
  - Demonstrates Commitment to Integrity and Ethical Values
  - Enforces Accountability
  - Establishes Structure, Authority, and Responsibility
  - Exercises Oversight Responsibility
2.7 Security Requirement Traceability Matrix

Overview: The Security Requirement Traceability Matrix (SRTM) provides ability to select security controls from industry standards and regulations/laws for implementation either as a part of a Secure Software Development Lifecycle (SSDLC) or regulations mandate. Currently, Tardigrade supports the following standards and regulations:

SRTM Standards:
- NIST 800-53 R4
- ISO 27001-2013

SRTM Regulations:
- Sarbanes-Oxley (SOX)
- Monetary Authority of Singapore (MAS)
2.8 Accessing Tardigrade

Tardigrade is offered as a Software as a Service (SaaS) application. To log on to the application interface:

1. Start your browser.

2. In the address field at the top of your browser, enter a functional application URL.

3. Press Enter.
   Tardigrade prompts you to enter Username and Password.

   ![Tardigrade Log on Screen]

   Tardigrade Log on Screen

4. Enter the Username and Password.

5. Click Login.
   The Tardigrade main screen appears.

   ![Tardigrade main screen]

   Tardigrade main screen
2.9 Role-based Access

Since Tardigrade is a role-based application, not all users except the System Administrator have access to all functionalities of the application. For example, a task assigner would not have access to the task conducting page and vice versa.

When you access a feature that you do not have permission to access, a message “You are not authorized to access this resource.” appears.
3 Cybersecurity

Cybersecurity assessment allows you to conduct an assessment to determine the state of preparedness and maturity of each of the major cybersecurity domains of an organization. You can perform Cybersecurity assessment for:

- **Inherent Risk Profile**
- **Domain Maturity**

Additionally, you can create Cybersecurity Dashboard Reports for Inherent Risk Profile and Domain Maturity Assessments.

### 3.1 Conducting Cybersecurity Assessment for Inherent Risk Profile

To perform Cybersecurity Assessment for Inherent Risk Profile, you can do the following:

- **Assign a task**
- **Conduct a task**
- **Review a task**

#### 3.1.1 Assigning a Task

In Tardigrade, to perform Cybersecurity Assessment analysis for Inherent Risk Profile, the first step in the process involves a **task assigner** allocating a task to an **assessor** who performs it.

**Note:** A user whose role is defined as an **Assigner** can assign a task. To know more about roles and responsibilities, refer to Roles and Responsibilities.

To assign a task:

1. From the main menu, go to Assessment » Cybersecurity » Inherent Risk Profile » Inherent Risk Profile Assign Task.
   The Inherent Risk Profile Assessment page appears.

   ![Inherent Risk Profile Assessment page](image)

   **Inherent Risk Profile Assessment page**

2. **Click**
   The Assign Inherent Risk Profile Assessment panel appears.
Assign Inherent Risk Profile Assessment panel

3. From the **Name** drop-down list, select the user to whom you want to assign the assessment task.

4. From the **Component** drop-down list, select one of the following components:
   - Technologies and Connection Types
   - Delivery Channels
   - Online/Mobile Products and Technology Services
   - Organizational Characteristics
   - External Threats

   **Note:** If you select a component that is already assigned for assessment, a message “**Component already in progress!**” appears, indicating that you cannot assign the same component for assessment.

5. Click **Save**.
   A message appears “**Assessment is assigned**”.
3.1.2 Conducting a Task

The second step in conducting Cybersecurity Assessment for Inherent Risk Profile is performing the assigned task.

Note: In Tardigrade, a user whose role is defined as an **Assessor** can conduct a task.
To know more about roles and responsibilities, refer to [Roles and Responsibilities](#).

To conduct a task:

1. From the main menu, go to **Assessment » Cybersecurity » Inherent Risk Profile » Inherent Risk Profile Conduct Task**.
The **Inherent Risk Profile Assessment** page appears with a list of assigned tasks.

2. From the list of tasks, select a task.
The details of the task appear in the **Conduct Internal Assessment** panel.

   Conduct Internal Assessment panel – Conducting a task

3. Enter the data required to complete the task.
   Click **Next** or **Previous** to navigate the pages of the task.

   Conduct Internal Assessment panel – Next and Previous buttons

4. [Optional] Click **Save & Continue** to save your current task.
5. [Optional] Click **Save & Exit** to resume the task later.

6. After entering the data required to complete the task, click **Finish** to complete the task.
   A message appears **“Assessment submitted for review”**. The assessment task is completed and it is sent to the Reviewer.

### 3.1.3 Reviewing a Task

The third and last step in Cybersecurity Assessment for Inherent Risk Profile is to review the task. As a reviewer, you can either approve or reject the cybersecurity assessment.

**Note:** In Tardigrade, a user whose role is defined as a **Reviewer** can review a task. To know more about roles and responsibilities, refer to [Roles and Responsibilities](#).

To review a task:

1. From the main menu, go to **Assessment** » **Cybersecurity** » **Inherent Risk Profile** » **Inherent Risk Profile Review Task**. The **Inherent Risk Profile Assessment** page appears with a list of tasks to review.

2. From the list of tasks, select a task. The details of the task appear in the **Conduct Internal Assessment** panel.

![Conduct Internal Assessment panel – Reviewing a task](image)

3. Review the data. Click **Next** or **Previous** to navigate the pages of the task.

4. Select an **Assessment Response**.

5. [Optional] Enter your comments in **Reviewer Comment** text box.

6. [Optional] Click **Save & Continue** to save your current task.
7. [Optional] Click **Save & Exit** to resume your task later.

8. After reviewing the data required to complete the task, do one of the following:
   
   - Click **Approve**.
     A message appears “**Assessment is approved**” indicating that the assessment is complete.
   
   - Click **Reject**.
     The assessment is sent to the Assessor's list of assigned tasks who must perform the assessment again.
3.2 Conducting Cybersecurity Assessment for Domain Maturity

To perform Cybersecurity Assessment for Domain Maturity, you can do the following:

- Assign a task
- Conduct a task
- Review a task

3.2.1 Assigning a Task

In Tardigrade, to perform Cybersecurity Assessment analysis for Domain Maturity, the first step in the process involves a task assigner allocating a task to an assessor who performs it.

Note: A user whose role is defined as an Assigner can assign a task. To know more about roles and responsibilities, refer to Roles and Responsibilities.

To assign a task:

1. From the main menu, go to Assessment » Cybersecurity » Domain Maturity » Domain Maturity Assign Task. The Domain Maturity Assessment page appears.

   ![Domain Maturity Assessment page]

2. Click  
   The Create Domain Maturity Assessment panel appears.

   ![Create Domain Maturity Assessment panel]
Create Domain Maturity Assessment panel

3. From the Name drop-down list, select the user to whom you want to assign the assessment task.

4. From the Component drop-down list, select one of the following components:
   - Threat Intelligence & Collaboration
   - Cybersecurity Controls
   - External Dependency Management
   - Cyber Incident Management and Resilience

**Note:** If you select a component that is already assigned for assessment, a message “Component already in progress!” appears, indicating that you cannot assign the same component for assessment.

5. Click Save.
   A message appears “Assessment is assigned”.
3.2.2 Conducting a Task

The second step in conducting Cybersecurity Assessment for Domain Maturity is performing the assigned task.

Note: In Tardigrade, a user whose role is defined as an Assessor can conduct a task. To know more about roles and responsibilities, refer to Roles and Responsibilities.

To conduct a task:

1. From the main menu, go to Assessment » Cybersecurity » Domain Maturity » Domain Maturity Conduct Task. The Domain Maturity Assessment page appears with a list of assigned tasks.

2. From the list of tasks, select a task. The details of the task appear in the Conduct Internal Assessment panel.

3. Enter the data required to complete the task. Click Next or Previous to navigate the pages of the task.
4. [Optional] Click **Save & Continue** to save your current task.

5. [Optional] Click **Save & Exit** to resume the task later.

6. After entering the data required to complete the task, click **Finish** to complete the task. A message appears “Assessment submitted for review”.
   The assessment task is completed, and it is sent to the Reviewer.

### 3.2.3 Reviewing a Task

The third and last step in Cybersecurity Assessment for Domain Maturity is to review the task. As a reviewer, you can either approve or reject the cybersecurity assessment.

**Note:** In Tardigrade, a user whose role is defined as a **Reviewer** can review a task. To know more about roles and responsibilities, refer to [Roles and Responsibilities](#).

To review a task:

1. From the main menu, go to **Assessment » Cybersecurity » Domain Maturity » Domain Maturity Review Task**.
   The **Inherent Risk Profile Assessment** page appears with a list of tasks to review.

2. From the list of tasks, select a task.
   The details of the task appear in the **Conduct Internal Assessment** panel.

   ![Conduct Internal Assessment panel](image)

   *Conduct Internal Assessment panel – Reviewing a task*

3. Review the data.
   Click **Next** or **Previous** to navigate the pages of the task.

4. Select an **Assessment Response**.
5. [Optional] Enter your comments in **Reviewer Comment** text box.

6. [Optional] Click **Save & Continue** to save your current task.

7. [Optional] Click **Save & Exit** to resume your task later.

8. After reviewing the data required to complete the task, do one of the following:

   - Click **Approve**.
     A message appears **“Assessment is approved”** indicating that the assessment is complete.

   - Click **Reject**.
     The assessment is sent to the Assessor’s list of assigned tasks who must perform the assessment again.
3.3 Cybersecurity Dashboard Reports

For Cybersecurity Assessment, you can publish reports that can be viewed on the Tardigrade dashboard. You can also print the reports from the dashboard.

To publish a dashboard report:

1. From the main menu, go to Dashboard » Cybersecurity and select a report from the following reports:
   - Inherent Risk Detail Result
   - Inherent Risk Summary Result
   - Maturity Result
   - Chart of Assessment Factor
   - Charts of Component
   - Compliance Result
   - Maturity Target

2. In the dashboard page, use the respective date picker icons to enter the Start Date and the End Date.

3. Click Search. The relevant results are displayed.

![Cybersecurity Dashboard Reports search results page](image-url)
3.3.1 Printing Cybersecurity Dashboard Reports

To print a report:

1. In the Cybersecurity Dashboard Reports search results page, click Proceed to download Report.
   A pop-up window displaying the PDF version of the report.

2. From the pop-up window, print the report or save it on your local system.
3.4 Cybersecurity Admin Panel

The Cybersecurity Admin panel allows you to add, edit and delete the following:

- Inherent Risk Category
- Inherent Risk Question
- Inherent Risk Level
- Assessment Factor
- Maturity Component
- Maturity Domain
- Maturity Declarative Statement

**Note:** You need to be logged on as the System Administrator to access the Cybersecurity Admin Panel.

To access the Cybersecurity Admin panel, in the left Administration panel, navigate to System Maintenance » Application Administration » Cybersecurity.
3.4.1 Inherent Risk Category

Adding an Inherent Risk Category

To add an Inherent Risk Category:

1. Navigate to **System Maintenance** in the left **Administration** panel and navigate to **Application Administration » Cybersecurity » Add/Edit Inherent Risk Category**. The **Add Category** page appears.

```
Add Category page
```

2. To add an Inherent Risk Category, click . The **Add New Category** panel appears.

3. Enter the name of the **Component**.

4. Click **Save**.

Editing an Inherent Risk Category

To edit an Inherent Risk Category:

1. Select the Inherent Risk Category on **Add Category** page.

2. Click . The **Add New Category** panel appears.

3. Modify the name of the **Component**.

4. Click **Save**.
Deleting an Inherent Risk Category

To delete an Inherent Risk Category:

1. Select the Inherent Risk Category on Add Category page.

2. Click 🗑️. 
   A message appears “Do you want to delete the Component?”. 

3. Click Delete.

3.4.2 Inherent Risk Question

Adding an Inherent Risk Question

To add an Inherent Risk Question:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » Cybersecurity » Add/Edit Inherent Risk Question. The Add Question page appears.

2. To add an Inherent Risk Question, click 🗑️.  
   The Add New Question panel appears.

3. From the drop-down list, select a Component.
Select Component—Add Question page

4. Enter the Question.

5. Click Save.

Editing an Inherent Risk Question

To edit an Inherent Risk Question:

1. Select the Inherent Risk Question on Add Question page.

2. Click  
   The Add New Question panel appears.

3. Modify the name of the Component and the Question.

4. Click Save.
Deleting an Inherent Risk Question

To delete an Inherent Risk Category:

1. Select the Inherent Risk Question on Add Category page.

2. Click 
   A message appears “Do you want to delete the Question?”.

3. Click Delete.

3.4.3 Inherent Risk Level

Adding an Inherent Risk Level

To add an Inherent Risk Level:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » Cybersecurity » Add/Edit Inherent Risk Level. The Add Inherent Risk Level page appears.

Add Inherent Risk Level page

2. To add an Inherent Risk Level, click .
   The Add New Risk Level panel appears.

3. From the drop-down list, select a Question.

4. Enter the Description, Risk Level and Risk Value.

5. Click Save.
Editing an Inherent Risk Level

To edit an Inherent Risk Level:

1. Select the Inherent Risk Level on Add Inherent Risk Level page.

2. Click 
   The Add New Risk Level panel appears.

3. Modify the Question, Description, Risk Level and Risk Value.

4. Click Save.

Deleting an Inherent Risk Level

To delete an Inherent Risk Level:

1. Select the Inherent Risk Level on Add Inherent Risk Level page.

2. Click 
   A message appears “Do you want to delete the Risk Value Level?”.

3. Click Delete.
3.4.4 Assessment Factor

Adding an Assessment Factor

To add an Assessment Factor:

1. Navigate to **System Maintenance** in the left **Administration** panel and navigate to **Application Administration » Cybersecurity » Add/Edit Assessment Factor**. The **Add Assessment Factor** page appears.

   ![Add Assessment Factor page](image)

   *Add Assessment Factor page*

2. To add an Assessment Factor, click . The **Add Assessment Factor** panel appears.

3. From the drop-down list, select a **Component**.

4. Enter the **Assessment Factor**.

5. Click **Save**.
**Editing an Assessment Factor**

To edit an Assessment Factor:

1. Select the Assessment Factor on **Add Assessment Factor** page.

2. Click 
   The **Add Assessment Factor** panel appears.

3. Modify the **Component** and the **Assessment Factor**.

4. Click **Save**.

**Deleting an Assessment Factor**

To delete an Assessment Factor:

1. Select the Assessment Factor on **Add Assessment Factor** page.

2. Click 
   A message appears “**Do you want to delete the Assessment Factor?**”.

3. Click **Delete**.
3.4.5 Maturity Component

Adding a Maturity Component

To add a Maturity Component:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » Cybersecurity » Add/Edit Maturity Component. The Add Maturity Component page appears.

![Add Maturity Component page](image)

Add Maturity Component page

2. To add a Maturity Component, click . The Add Maturity Component panel appears.

3. From the drop-down list, select an Assessment Factor.

4. Enter the name of the Component.

5. Click Save.

Editing a Maturity Component

To edit a Maturity Component:

1. Select the Maturity Component on Add Maturity Component page.

2. Click . The Add Maturity Component panel appears.

3. Modify the Assessment Factor and the name of the Component.

4. Click Save.

Deleting a Maturity Component
To delete a Maturity Component:

1. Select the Maturity Component on Add Maturity Component page.

2. Click \( \text{Delete} \). A message appears “Do you want to delete the Component?”.

3. Click Delete.

### 3.4.6 Maturity Domain

**Adding a Maturity Domain**

To add a Maturity Domain:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » Cybersecurity » Add/Edit Maturity Domain. The Maturity Domain page appears.

   ![Maturity Domain page](image)

   *Maturity Domain page*

2. To add a Maturity Domain, click \( \text{Add} \). The Add Maturity Domain panel appears.

3. Enter the Domain Name.

4. Click Save.
Editing a Maturity Domain

To edit a Maturity Domain:

1. Select the Maturity Domain on Maturity Domain page.

2. Click 📝. The Add Maturity Domain panel appears.

3. Modify the Domain Name.

4. Click Save.

Deleting a Maturity Domain

To delete a Maturity Domain:

1. Select the Maturity Domain on Maturity Domain page.

2. Click ⌼. A message appears “Do you want to delete the Domain Name?“.

3. Click Delete.
3.4.7 Maturity Declarative Statement

Adding a Maturity Declarative Statement

To add a Maturity Declarative Statement:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » Cybersecurity » Add/Edit Declarative Statement. The Maturity Declarative Statement page appears.

![Maturity Declarative Statement page]

2. To add a Maturity Declarative Statement, click . The Add Maturity Declarative Statement panel appears.

3. From the drop-down lists, select the Assessment Factor and Risk Level.

4. Enter information for the following:
   - Mapping Number
   - Baseline Mapping
   - Declarative Statement
   - NIST Mapping
• Link URL
• Useful Link

5. Click **Save**.

**Editing a Maturity Declarative Statement**

To edit a Maturity Declarative Statement:

1. Select the Maturity Declarative Statement on **Maturity Declarative Statement** page.

2. Click **EDIT**.
   
   The **Add Maturity Declarative Statement** panel appears.

3. Modify the relevant information.

4. Click **Save**.

**Deleting a Maturity Declarative Statement**

To delete a Maturity Declarative Statement:

1. Select the Maturity Declarative Statement on **Maturity Declarative Statement** page.

2. Click **trash can**.
   
   A message appears “**Do you want to delete the Maturity Declarative Statement?**”.

3. Click **Delete**.
4 Internal Control

Internal Control assessment allows you to conduct an assessment of the system of internal control of an organization. You can perform Internal Control assessment for:

- **Principle**
- **Component**

Additionally, you can create [Internal Control Dashboard Reports](#) for Principle and Component.

4.1 Conducting Internal Control Assessment for Principle

To perform Internal Control Assessment for Principle, you can do the following:

- **Assign a task**
- **Conduct a task**
- **Review a task**

4.1.1 Assigning a Task

In Tardigrade, you can perform Internal Control Assessment analysis for Principle. The first step in the process involves a task assigner allocating a task to an assessor who performs it.

**Note:** A user whose role is defined as an **Assigner** can assign a task. To know more about roles and responsibilities, refer to [Roles and Responsibilities](#).

To assign an assessment task:

1. From the main menu, go to **Assessment » Internal Control » Principle » Principle Assign Task**. The **Principle Assessment** page appears.

2. Click [](#) The **Create Principle Assessment** panel appears.
Create Principle Assessment panel

3. From the Name drop-down list, select the user to whom you want to assign the assessment task.

4. From the Component drop-down list, select one of the following components:
   - Control Environment
   - Risk Assessment
   - Control Activities
   - Information and Communication
   - Monitoring Activities

Note: If you select a component that is already assigned for assessment, a message “Component already in progress!” appears, indicating that you cannot assign the same component for assessment.

5. Click Save.
   A message appears “Assessment is assigned”.

4.1.2 Conducting a Task

The second step in conducting Internal Control Assessment for Principle is performing the assigned task.

Note: In Tardigrade, a user whose role is defined as an Assessor can conduct a task. To know more about roles and responsibilities, refer to Roles and Responsibilities.

To conduct a task:

1. From the main menu, go to Assessment » Internal Control » Principle » Principle Conduct Task.
   The Principle Assessment page appears.
2. From the list of tasks, select a task. The details of the task appear in the **Conduct Internal Assessment** panel.

3. Enter all the data required to complete the task. Click **Next** or **Previous** to navigate the pages of the task.

4. [Optional] Click **Save & Continue** to save your current task.
5. [Optional] Click **Save & Exit** to resume the task later.

6. After entering the data required to complete the task, click **Finish** to complete the task. A message appears “**Assessment submitted for review**”. The assessment task is completed and it is sent to the Reviewer.

### 4.1.3 Reviewing a Task

The third and last step in conducting Internal Control Assessment for **Principle** is to review the task.

**Note:** In Tardigrade, a user whose role is defined as a **Reviewer** can review a task. To know more about roles and responsibilities, refer to [Roles and Responsibilities](#).

To review a task:

1. From the main menu, go to **Assessment » Internal Control » Principle » Principle Review Task**. The **Principle Assessment** page appears with a list of tasks to review.

2. From the list of tasks, select a task. The details of the task appear in the **Conduct Internal Assessment** panel.

3. Review the data. Click **Next** or **Previous** to navigate the pages of the task.

4. Select an **Assessment Response**.

5. [Optional] Enter your comments in **Reviewer Comment** text box.

6. [Optional] Click **Save & Continue** to save your current task.

7. [Optional] Click **Save & Exit** to resume your task later.

8. After reviewing the data required to complete the task, do one of the following:
   - Click **Approve**. A message appears “**Assessment is approved**” indicating that the assessment is complete.
   - Click **Reject**. The assessment is sent to the Assessor’s list of assigned tasks who must perform the assessment again.
4.2 Conducting Internal Control Assessment for Component

To perform Internal Control Assessment for Component, you can do the following:

- Assign a task
- Conduct a task
- Review a task

4.2.1 Assigning a Task

In Tardigrade, you can perform Internal Control Assessment analysis for Component. The first step in the process involves a task assigner allocating a task to an assessor who performs it.

**Note:** A user whose role is defined as an Assigner can assign a task.
To know more about roles and responsibilities, refer to Roles and Responsibilities.

To assign an assessment task:

1. From the main menu, go to Assessment » Internal Control » Component » Component Assign Task.
   The Component Assessment page appears.

   ![Component Assessment page]

2. Click .
   The Create Component Assessment panel appears.

   ![Create Component Assessment panel]
3. From the **Name** drop-down list, select the user to whom you want to assign the assessment task.

4. From the **Component** drop-down list, select one of the following components:
   - Control Environment
   - Risk Assessment
   - Control Activities
   - Information and Communication
   - Monitoring Activities

| Note: | If you select a component that is already assigned for assessment, a message “**Component already in progress!**” appears, indicating that you cannot assign the same component for assessment. |

5. Click **Save**.  
   A message appears “**Assessment is assigned**”.

### 4.2.2 Conducting a Task

The second step in conducting Internal Control Assessment for Component is performing the assigned task.

| Note: | In Tardigrade, a user whose role is defined as an **Assessor** can conduct a task. To know more about roles and responsibilities, refer to **Roles and Responsibilities**. |

To conduct a task:

1. From the main menu, go to **Assessment » Internal Control » Component » Component Conduct Task**.  
   The **Component Assessment** page appears.

2. From the list of tasks, select a task.  
   The details of the task appear in the **Conduct Internal Assessment** panel.
Conduct Internal Assessment panel – Conducting a task

3. Enter all the data required to complete the task.
   Click Next or Previous to navigate the pages of the task.

4. [Optional] Click Save & Continue to save your current task.

5. [Optional] Click Save & Exit to resume the task later.

6. After entering the data required to complete the task, click Finish to complete the task.
   A message appears “Assessment submitted for review”.
   The assessment task is completed and it is sent to the Reviewer.
4.2.3 Reviewing a Task

The third and last step in conducting Internal Control Assessment for Component is to review the task.

Note: In Tardigrade, a user whose role is defined as a Reviewer can review a task. To know more about roles and responsibilities, refer to Roles and Responsibilities.

To review a task:

1. From the main menu, go to Assessment » Internal Control » Component » Component Review Task.
   The Component Assessment page appears with a list of tasks to review.

2. From the list of tasks, select a task.
   The details of the task appear in the Conduct Internal Assessment panel.

3. Review the data.
   Click Next or Previous to navigate the pages of the task.

4. Select an Assessment Response.

5. [Optional] Enter your comments in Reviewer Comment text box.

6. [Optional] Click Save & Continue to save your current task.

7. [Optional] Click Save & Exit to resume your task later.

8. After reviewing the data required to complete the task, do one of the following:
   - Click Approve.
     A message appears "Assessment is approved" indicating that the assessment is complete.
   - Click Reject.
     The assessment is sent to the Assessor’s list of assigned tasks who must perform the assessment again.
4.3 Internal Control Dashboard Reports

For Internal Control Assessment, you can publish reports that can be viewed on the Tardigrade dashboard. You can also print the reports from the dashboard.

To publish a dashboard report:

1. From the main menu, go to Dashboard » Internal Control select a report from the following reports:
   - Component Compliance Result
   - Deficiency Result
   - Principle Compliance Result

2. In the dashboard page, use the respective date picker icons to enter the Start Date and the End Date.

3. Click Search. The relevant results are displayed.
4.3.1 Printing Internal Control Dashboard Reports

To print a report:

1. In the Cybersecurity Dashboard Reports search results page, click Proceed to download Report.
   A pop-up window displaying the PDF version of the report.

2. From the pop-up window, print the report or save it on your local system.
4.4 Internal Control Admin Panel

The Internal Control Admin panel allows you to add, edit and delete the following:

- Component
- Principle
- Point Of Focus
- Question

**Note:** You need to be logged on as the System Administrator to access the Internal Control Admin Panel.

To access the Internal Control Admin panel, expand System Maintenance in the left Administration panel and navigate to Application Administration » Internal Control.
4.4.1 Component

Adding a Component

To add a Component:

3. Expand System Maintenance in the left Administration panel and navigate to Application Administration » Internal Control » Add/Edit Component. The Add Component page appears.

4. To add a Component, click 🖋.
   The Add New Component panel appears.

5. Enter the name of the Component.

6. Click Save.

Editing a Component

To edit a Component:

1. Select the Component on Add Component page.

2. Click 🖋.
   The Add New Component panel appears.

3. Modify the name of the Component.

4. Click Save.
Deleting a Component

To delete a component:

1. Select the component on Add Component page.

2. Click .
   A message appears “Do you want to delete the Component?”.

3. Click Delete.

4.2 Principle

Adding a Principle

To add a Principle:

4. Expand System Maintenance in the left Administration panel and navigate to Application Administration » Internal Control » Add/Edit Principle. The Add Principle page appears.

![Add Principle page]

5. To add a Principle, click .
   The Add New Principle panel appears.

6. From the drop-down list, select a Component.
7. Enter the **Principle** and the **Description**.

8. Click **Save**.

**Editing a Principle**

To edit a Principle:

1. Select the Principle on **Add Principle** page.

2. Click **Edit**.  
   The **Add New Principle** panel appears.

3. Modify the following:
   - Name of the **Component**
   - The **Principle**
   - The **Description**

4. Click **Save**.

**Deleting a Principle**

To delete a Principle:

1. Select the Principle on **Add Principle** page.

2. Click **Delete**.  
   A message appears “**Do you want to delete the Principle?**”.

3. Click **Delete**.
4.4.3 Point Of Focus

Adding a Point of Focus

To add a Point of Focus:

1. Expand **System Maintenance** in the left **Administration** panel and navigate to **Application Administration » Internal Control » Add/Edit Point of Focus**. The **Point Of Focus** page appears.

```
<table>
<thead>
<tr>
<th>Principle</th>
<th>Point Of Focus</th>
<th>Parent</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1: Demonstrates</td>
<td>Commitment to Integrity</td>
<td>Sets the Tone at the Top and Ethical Values</td>
<td>The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.</td>
</tr>
</tbody>
</table>
```

2. To add a Point Of Focus, click 🖋. The **Add New Point Of Focus** panel appears.

3. From the drop-down lists, select a **Principle** and a **Parent**.

4. Enter the **Point Of Focus** and the **Description**.

5. Click **Save**.

Editing a Point Of Focus

To edit a Point Of Focus:

1. Select the Point Of Focus on **Point Of Focus** page.

2. Click 🖋. The **Add New Point Of Focus** panel appears.

3. Modify the following:
- The Principle
- The Parent
- The Point Of Focus
- The Description

4. Click **Save**.

**Deleting a Point Of Focus**

To delete a Point of Focus:

1. Select the Point Of Focus on **Point Of Focus** page.

2. Click 🗑️.
   A message appears “**Do you want to delete the Point Of Focus?**”.

3. Click **Delete**.

**4.4.4 Question**

**Adding a Question**

To add a Question:

1. Expand **System Maintenance** in the left **Administration** panel and navigate to **Application Administration » Internal Control » Add/Edit Question**.
   The **Add Question** page appears.

   ![](image)

   **Add Question page**

2. To add a Question, click 📝.
   The **Add New Question** panel appears.
3. From the drop-down list, select a **Component**.

4. Enter the **Question** and the **Description**.

5. Click **Save**.

**Editing a Question**

To edit a Question:

1. Select the Question on **Add Question** page.

2. Click 🖊.
The **Add New Question** panel appears.

3. Modify the following:
   - Name of the **Component**
   - The **Question**
   - The **Description**

4. Click **Save**.

**Deleting a Question**

To delete a Question:

1. Select the Question on **Add Question** page.

2. Click 🗑.
A message appears “**Do you want to delete the Question?**”.

3. Click **Delete**.
5 Security Requirement Traceability Matrix

Security Requirement Traceability Matrix (SRTM) allows you to select security controls from industry standards such as NIST 800-53 R4 and ISO 270001 for implementation. Additionally, System Administrators will be able to maintain various aspects of the module.

5.1 Security Requirement Traceability Matrix (SRTM) NIST 800-53

5.1.1 Creating Security Requirement Traceability Matrix for NIST 800-53 R4

To access Security Requirement Traceability Matrix for NIST 800-53:


NIST 800-53 R4 Security Control Selection page

In the NIST 800-53 R4 Security Control Selection page, you can create Security Requirement Traceability Matrix for the following options:

- All Control Family
- Individual Control Family (selected by default)
- Security Control Baselines

5.1.2 Creating SRTM NIST 800-53 R4 for All Control Family

To create SRTM NIST 800-53 R4 for All Control Family:

1. In the NIST 800-53 R4 Security Control Selection page, select All Control Family.
2. Select the Verification Method.
3. Click Save All Controls. A message "All NIST security controls have been successfully created." appears.
4. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.

5. From the list of Selected Controls, select All. The All indicates All Control Family. The Generate Report button appears.


8. Click Proceed to download Report. The Download Report pop-up window appears.

10. [Optional] Print the report or save it on your local system.

11. To close the PDF, click **Close**.
5.1.3 Creating SRTM NIST 800-53 R4 for Individual Control Family

To create SRTM NIST 800-53 R4 for Individual Control Family:

1. In the NIST 800-53 R4 Security Control Selection page, click Continue. Individual Control Family is selected by default. The Select Individual Control Family page appears.

Note: To create SRTM NIST 800-53 R4 for Individual Control Family from the main menu, navigate to Security Requirement Traceability Matrix (SRTM) » SRTM Standards » NIST Individual Control Family Selection. The Select Individual Control Family page appears. Then, follow the steps below.

Select Individual Control Family page

2. In the Select Individual Control Family page, select one or more individual control parameter checkboxes and then, from the drop-down list(s), select the corresponding Verification Method(s).

3. Click Save. A message “Individual NIST security controls have been successfully created.” appears.

4. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.

5. From the list of Selected Controls, select Individual. The Individual indicates Individual Control Family. The Generate Report button appears.
Select Individual Control Family

6. Click **Generate Report**.
   A message “**Report Generated Successfully!**” appears.

7. Click **View Report**.
   The **SRTM Report Details** page appears.

8. Click **Proceed to download Report**.
   The **Download Report** pop-up window appears.

9. In the pop-up window, click **Download Report**.
   The **NIST SRTM Report** appears as a PDF in a window.
10. [Optional] Print the report or save it on your local system.

11. To close the PDF, click Close.
5.1.4 Creating SRTM NIST 800-53 R4 for Security Control Baselines

To create SRTM NIST 800-53 R4 for Security Control Baselines:

1. In the NIST 800-53 R4 Security Control Selection page, select Security Control Baselines.


2. Click Continue. The Security Control Baselines page appears.

3. In the Security Control Baselines page, select one or more individual control parameter checkboxes and then, from the drop-down list(s), select the corresponding Verification Method(s).

4. Click Save. A message "Selected security controls have been successfully created." appears.

5. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.

6. From the list of Selected Controls, select Control Baseline. The Control Baseline indicates Security Control Baselines. The Generate Report button appears.
Select Security Control Baselines

7. Click Generate Report.
   A message “Report Generated Successfully!” appears.

8. Click View Report.
   The SRTM Report Details page appears.

9. Click Proceed to download Report.
   The Download Report pop-up window appears.

10. In the pop-up window, click Download Report.
    The NIST SRTM Report appears as a PDF in a window.
11. [Optional] Print the report or save it on your local system.

12. To close the PDF, click **Close**.
5.2 Security Requirement Traceability Matrix (SRTM) ISO 27001-2013

5.2.1 Creating Security Requirement Traceability Matrix for NIST 800-53 R4

To access Security Requirement Traceability Matrix for ISO 27001-2013:


ISO 27001-2013 Control Selection page

In the ISO 27001-2013 Control Selection page, you can create Security Requirement Traceability Matrix for the following options:

- All Control Family
- Individual Control Family (selected by default)

5.2.2 Creating SRTM ISO 27001-2013 for All Control Family

To create SRTM ISO 27001-2013 for All Control Family:

1. In the ISO 27001-2013 Control Selection page, select All Control Family.
2. Select the Verification Method.
3. Click Save All Controls. A message “All ISO security controls have been successfully created.” appears.
4. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.
5. From the list of Selected Controls, select All. The All indicates All Control Family. The Generate Report button appears.
6. Click **Generate Report**.  
A message "Report Generated Successfully!" appears.

7. Click **View Report**.  
The **SRTM Report Details** page appears.

8. Click **Proceed to download Report**.  
The **Download Report** pop-up window appears.

9. In the pop-up window, click **Download Report**.  
The **ISO SRTM Report** appears as a PDF in a window.
10. [Optional] Print the report or save it on your local system.

11. To close the PDF, click Close.

5.2.3 Creating SRTM ISO 27001-2013 for Individual Control Family

To create SRTM ISO 27001-2013 for Individual Control Family:

1. In the ISO 27001-2013 Control Selection page, click Continue. Individual Control Family is selected by default. The Select ISO Individual Control Family page appears.
2. In the **Select ISO Individual Control Family** page, select one or more individual control parameter checkboxes and then, from the drop-down list(s), select the corresponding **Verification Method(s)**.

3. Click **Save**.
   A message "**Individual ISO security controls have been successfully created.**" appears.

4. Click the "**Click Here to View Security Controls**" link.
   The **Security Control Requirement Selection View** page appears.

5. From the list of **Selected Controls**, select **Individual**. The **Individual** corresponds to Individual Control Family.
   The **Generate Report** button appears.

6. Click **Generate Report**.
   A message "**Report Generated Successfully!**" appears.

7. Click **View Report**.
   The **SRTM Report Details** page appears.

8. Click **Proceed to download Report**.
   The **Download Report** pop-up window appears.

9. In the pop-up window, click **Download Report**.
   The **NIST SRTM Report** appears as a PDF in a window.
ISO SRTM Report PDF Window

10. [Optional] Print the report or save it on your local system.

11. To close the PDF, click **Close**.
5.3 Security Requirement Traceability Matrix (SRTM) SOX

5.3.1 Creating Security Requirement Traceability Matrix for SOX

To access Security Requirement Traceability Matrix for SOX:

From the main menu, navigate to Security Requirement Traceability Matrix (SRTM) » SRTM Regulation & Law » SRTM SOX. The SOX Control Selection page appears.

SOX Control Selection page

In the SOX Control Selection page, you can create Security Requirement Traceability Matrix for the following options:

- All Control Family
- Individual Control Family (selected by default)

5.3.2 Creating SRTM SOX for All Control Family

To create SRTM SOX for All Control Family:

1. In the SOX Control Selection page, select All Control Family.
2. Select the Verification Method.
3. Click Save All Controls. A message “SOX Security Controls have been successfully created.” appears.
4. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.
5. From the list of Selected Controls, select All. The All indicates All Control Family. The Generate Report button appears.
Security Control Requirement Selection View page--Select All Control Family

6. Click **Generate Report**.
   A message “Report Generated Successfully!” appears.

7. Click **View Report**.
   The **SRTM Report Details** page appears.

8. Click **Proceed to download Report**.
   The **Download Report** pop-up window appears.

9. In the pop-up window, click **Download Report**.
   The **SOX SRTM Report** appears as a PDF in a window.

10. [Optional] Print the report or save it on your local system.
11. To close the PDF, click Close.

5.3.3 Creating SRTM SOX for Individual Control Family

To create SRTM SOX for Individual Control Family:

1. In the SOX Control Selection page, click Continue. Individual Control Family is selected by default. The Select SOX Individual Control Family page appears.

![Select SOX Individual Control Family page]

2. In the Select SOX Individual Control Family page, select one or more individual control parameter checkboxes and then, from the drop-down list(s), select the corresponding Verification Method(s).

3. Click Save. A message "Individual Security Controls have been successfully created." appears.

4. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.

5. From the list of Selected Controls, select Individual. The Individual corresponds to Individual Control Family. The Generate Report button appears.
Security Control Requirement Selection View - Select SOX Individual Family

6. Click **Generate Report**.
   A message “Report Generated Successfully!” appears.

7. Click **View Report**.
   The **SRTM Report Details** page appears.

8. Click **Proceed to download Report**.
   The **Download Report** pop-up window appears.

9. In the pop-up window, click **Download Report**.
   The **SOX SRTM Report** appears as a PDF in a window.
5.4 Security Requirement Traceability Matrix (SRTM) MAS

5.4.1 Creating Security Requirement Traceability Matrix for MAS

To access Security Requirement Traceability Matrix for MAS:

From the main menu, navigate to Security Requirement Traceability Matrix (SRTM) » SRTM Regulation & Law » Monetary Association of Singapore (MAS). The MAS Control Selection page appears.

MAS Control Selection page

In the MAS Control Selection page, you can create Security Requirement Traceability Matrix for the following options:

- All Control Family
- Individual Control Family (selected by default)

5.4.2 Creating SRTM MAS for All Control Family

To create SRTM MAS for All Control Family:

1. In the MAS Control Selection page, select All Control Family.

2. Select the Verification Method.

3. Click Save All Controls.
   A message "All MAS Security Controls have been successfully created." appears.

4. Click the “Click Here to View Security Controls” link.
   The Security Control Requirement Selection View page appears.

5. From the list of Selected Controls, select All. The All indicates All Control Family.
   The Generate Report button appears.
Security Control Requirement Selection View page--Select All Control Family

6. Click **Generate Report**.
   A message "Report Generated Successfully!" appears.

7. Click **View Report**.
   The SRTM Report Details page appears.

8. Click **Proceed to download Report**.
   The Download Report pop-up window appears.

9. In the pop-up window, click **Download Report**.
   The MAS SRTM Report appears as a PDF in a window.

10. [Optional] Print the report or save it on your local system.
11. To close the PDF, click Close.

5.4.3 Creating SRTM MAS for Individual Control Family

To create SRTM MAS for Individual Control Family:

1. In the MAS Control Selection page, click Continue. **Individual Control Family** is selected by default. The Select SOX Individual Control Family page appears.

2. In the Select MAS Individual Control Family page, select one or more individual control parameter checkboxes and then, from the drop-down list(s), select the corresponding Verification Method(s).

3. Click Save. A message “Individual MAS security controls have been successfully created.” appears.

4. Click the “Click Here to View Security Controls” link. The Security Control Requirement Selection View page appears.

5. From the list of Selected Controls, select Individual. The Individual corresponds to Individual Control Family. The Generate Report button appears.
Security Control Requirement Selection View - Select MAS Individual Family


7. Click **View Report**. The **SRTM Report Details** page appears.

8. Click **Proceed to download Report**. The **Download Report** pop-up window appears.

9. In the pop-up window, click **Download Report**. The **MAS SRTM Report** appears as a PDF in a window.

10. [Optional] Print the report or save it on your local system.
To close the PDF, click Close.

5.5 SRTM Reports

To generate a Security Requirement Traceability Matrix Report:

1. From the main menu, navigate to Security Requirement Traceability Matrix (SRTM) » SRTM Report.
   The Security Control Requirement Selection View page appears.

2. From the list of reports, select a report.
   The Generate Report button appears.

3. Click Generate Report.
   A message “Report Generated Successfully!” appears.

   The SRTM Report Details page appears.

5. Click Proceed to download Report.
   The Download Report pop-up window appears.

6. In the pop-up window, click Download Report.
   The report appears as a PDF in a window.

7. [Optional] Print the report or save it on your local system.

8. To close the PDF, click Close.
5.6  SRTM Admin Panel

The SRTM Admin panel allows you to:

- Edit the following:
  - NIST Control Baseline
  - NIST Control Family
- Upload NIST 800-53 R4 File
- Add, edit and delete the following:
  - ISO 27001-2013 Control
  - SOX Control
  - MAS Control
  - MAS Compliance

Note: You need to be logged on as the System Administrator to access the SRTM Admin Panel.

To access the SRTM Admin panel, expand System Maintenance in the left Administration panel and navigate to Application Administration » SRTM.
5.6.1 Editing NIST Control Baseline

To edit a NIST Control Baseline:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » SRTM » Edit NIST Control Baseline. The NIST Security Control Baseline page appears with a list of NIST Security Control parameters.

   ![NIST Security Control Baseline](image)

   **NIST Security Control Baseline page**

2. From the list, select a NIST Security Control. The NIST Security Control Baseline Details panel appears.

   **Note:** You can search for a NIST Security Control parameter by using the Search By Name or Control feature.
3. Modify the details.

4. Click Save.

### 5.6.2 Editing NIST Control Family

To edit a NIST Control Family:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » SRTM » Edit NIST Control Family. The NIST Control Family page appears with a list of NIST Control Family parameters.
2. From the list, select a NIST Control Family. The **View Sub Control Family** icon appears.

**Note:** You can search for a NIST Control Family parameter by using the **Search By Name or Control** feature.

![NIST Control Family](image)

**View Sub Control Family icon**

3. Click the **View Sub Control Family** icon. The **NIST Sub Control Family** page appears with a list of sub control families.

**Note:** You can search for a NIST Control Family by using the **Search By Name or Control** feature.

![NIST Sub Control Family](image)

**NIST Sub Control Family page**
4. Select a Sub Control Family.
The **Sub Control Details** panel appears.

```
Sub Control Details

Control Family: AC-1
Name: ACCESS CONTROL POLICY AND PROCEDURES

Guideline: The organization:
A. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls, and
B. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
C. Procedures to facilitate the implementation of the access control policy and associated access controls, and
D. Evaluates and updates the current:
   1. Access control policy [Assignment: organization-defined frequency]; and
   2. Access control procedures [Assignment: organization-defined frequency];
E. Access control policy [Assignment: organization-defined frequency]; and
F. Access control procedures [Assignment: organization-defined frequency].

Sub Control Details panel

5. In the **Sub Control Details** panel, modify the following:
   - Priority
   - Security Baseline

```

```
Sub Control Details panel – Details to update

6. Click **Save**.
```
5.6.3 Uploading NIST 800-53 R4 File

To upload a NIST 800-53 R4 File:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » SRTM » Upload NIST 800-53 R4 File. The following page appears.

![Page to upload NIST 800-53 R4 File](image)

This page allows you to upload NIST 800-53 R4 XML data file. Please note that the upload will delete previous NIST records in the database.

2. Click Import NIST 800-53 R4 Data. The File Upload pop-up window appears.

3. Click Browse and select a NIST 800-53 R4 File from your local system.

4. Click Upload. A message appears “NIST 800-53 R4 controls data has been uploaded successfully!”

**Note:** The NIST 800-53 R4 file that you want to upload must be an XML document or else, a message “Please upload nist standard .xml file extension” appears. Uploading the file automatically deletes the existing NIST 800-53 R4 file in the system. The upload process may take more time depending on the size of the XML file.
5.6.4 Adding ISO 27001-2013 Control

To add ISO 27001-2013 Control:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » SRTM » Add/Edit ISO 27001-2013 Control. The ISO Control Family page appears with a list of control families.

ISO Control Family page

2. Click . The Control Family Details panel appears.

3. Enter the Control Family and Name.

4. Click Save.

5.6.5 Editing ISO 27001-2013 Control

To edit ISO 27001-2013 Control:

1. In the ISO Control Family page, select a Control Family. The Control Family Details panel appears.

   **Note:** You can search for a Control Family by using the Search By Name or Control feature.

2. Modify the Control Family and Name.

3. Click Save.
5.6.6 Deleting ISO 27001-2013 Control

To delete ISO 27001-2013 Control:

1. In the **ISO Control Family** page, select a Control Family.

   **Note:** You can search for a Control Family by using the **Search By Name or Control** feature.

2. Click 🗑️. A message “**Do you want to delete Control Family?**” appears.

3. Click **Delete**.

5.6.7 Adding ISO 27001-2013 Sub Control Family

To add ISO 27001-2013 Sub Control Family:

1. In the **ISO Control Family** page, select a Control Family. The **View Sub Control Family** icon appears.

   **Note:** You can search for a Control Family by using the **Search By Name or Control** feature.

2. Click **View Sub Control Family** icon. The **ISO Sub Control Family** page appears.

3. Click 📄 The **Sub Control Details** panel appears.
4. Enter the details.

5. Click **Save**. A message "ISO Control Section is added successfully" appears.

6. Click **Back**. The ISO Control Family page appears.

### 5.6.8 Adding SOX Control

To add SOX Control:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » SRTM » Add/Edit SOX Control. The SOX Control Family page appears with a list of control families.
2. Click .
   The **Control Family Details** panel appears.

3. Enter the following information:
   - Control Family
   - COBIT Domain
   - Objective

4. Click **Save**.

### 5.6.9 Editing SOX Control

To edit SOX Control:

1. In the **SOX Control Family** page, select a Control Family.
   The **Control Family Details** panel appears.

**Note:** You can search for a Control Family by using the **Search By Control Family** feature.

2. Modify the details.

3. Click **Save**.
5.6.10 Deleting SOX Control

To delete SOX Control:

1. In the SOX Control Family page, select a Control Family.

   **Note:** You can search for a Control Family by using the **Search By Control Family** feature.

2. Click \(\text{Delete}\). A message “Do you want to delete Control Family?” appears.

3. Click **Delete**.

5.6.11 Adding SOX Control Activity

To add SOX Control Activity:

1. In the SOX Control Family page, select a Control Family.
   The **View Sub Control Family** icon appears.

   **Note:** You can search for a Control Family by using the **Search By Control Family** feature.

   ![SOX Control Family - View Sub Control Family icon]

2. Click **View Sub Control Family** icon.
   The SOX Control Activity page appears.

3. Click \(\text{ }\). The **Control Activity Details** panel appears.
SOX Control Activity Details panel

4. Enter the details.

5. Click **Save**. A message “**Control Activity is added successfully**” appears.

6. Click **Back**. The **SOX Control Family** page appears.

5.6.12 Adding MAS Control

To add MAS Control:

1. Navigate to **System Maintenance** in the left **Administration** panel and navigate to **Application Administration » SRTM » Add/Edit MAS Control**. The **MAS Control Family** page appears with a list of control families.
2. Click  
   The **Control Family Details** panel appears.

3. Enter the following information:
   - Control Family
   - Name

4. Click **Save**.

### 5.6.13 Editing MAS Control

To edit MAS Control:

1. In the **MAS Control Family** page, select a Control Family. 
   The **Control Family Details** panel appears.

   **Note:** You can search for a Control Family by using the **Search By Control Family** feature.

2. Modify the details.

3. Click **Save**.

### 5.6.14 Deleting MAS Control

To delete MAS Control:

1. In the **MAS Control Family** page, select a Control Family.

   **Note:** You can search for a Control Family by using the **Search By Control Family** feature.

2. Click  
   A message **“Do you want to delete Control Family?”** appears.

3. Click **Delete**.

### 5.6.15 Adding MAS Sub Control Family

To add MAS Sub Control Family:

1. In the **MAS Control Family** page, select a Control Family. 
   The **View Sub Control Family** icon appears.

   **Note:** You can search for a Control Family by using the **Search By Control Family** feature.
MAS Control Family - View Sub Control Family icon

2. Click **View Sub Control Family** icon.  
The **MAS Sub Control Family** page appears.

3. Click \[ icon.  
The **Control Family Details** panel appears.

MAX Sub Control Family - Sub Control Details panel

4. Enter the following:
   - Control Family
   - Name

5. Click **Save**.  
   A message “**Control Family is added successfully**” appears.

6. Click **Back**.  
The **MAS Control Family** page appears.
5.6.16 Adding MAS Family Section

To add MAS Family Section:

1. In the **MAS Control Family** page, select a Control Family. The **Control Family Details** panel appears.

**Note:** You can search for a Control Family by using the **Search By Control Family** feature.

![Control Family Details panel](image)

2. Click **View Control Family Section** button. The **MAS Family Section** page appears.
3. Click **File**. The **Control Section Details** panel appear.
4. Enter the following:
   - Control Section
   - Description
5. Click **Save**.
6. Click **Back**. The **MAS Control Family** page appears.

5.6.17 Editing MAS Family Section

1. In the **MAS Family Section** page, select a Family. The **Control Section Details** panel appear.

**Note:** You can search for a Control Family by using the **Search By Control Section** feature.

2. Modify the details.
3. Click **Save**.
4. Click **Back**. The **MAS Control Family** page appears.
5.6.18 Deleting MAS Family Section

1. In the MAS Family Section page, select a Family. The Control Section Details panel appear.

Note: You can search for a Control Family by using the Search By Control Section feature.

2. Click 🗑. A message "Do you want to delete Family Control?" appears.

3. Click Delete.

4. Click Save.

5. Click Back. The MAS Control Family page appears.

5.6.19 Adding MAS Compliance

To add MAS Compliance:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » SRTM » Add/Edit MAS Compliance. The MAS Compliance page appears with a list of compliances.

MAS Compliance page

2. Click 📝. The Compliance Details panel appears.

3. Enter the following information:

   • Compliance

4. Click Save.
5.6.20 Editing MAS Compliance

To edit MAS Compliance:

1. In the MAS Compliance page, select a Compliance. The Compliance Details panel appears.

   **Note:** You can search for a Control Family by using the Search By Compliance feature.

2. Modify the details.

3. Click **Save**.

5.6.21 Deleting MAS Compliance

To delete MAS Compliance:

1. In the MAS Compliance page, select a Compliance.

   **Note:** You can search for a Control Family by using the Search By Compliance feature.

2. Click 🗑️. A message “Do you want to delete Compliance?” appears.

3. Click **Delete**.
6 Reference Tables

The reference table feature allows you to maintain the Department and Line of Defense (LoD) data to be used in the application. The data is used to add drop-down list options to select from, when you create the various user (tenant) profiles in the application.

Using Reference Tables, you can:

- Add a Department
- Edit a Department
- Delete a Department
- Add a Line of Defense
- Edit a Line of Defense
- Delete a Line of Defense

6.1 Adding a Department

To add a department:

1. Navigate to System Maintenance in the left Administration panel and navigate to Application Administration » Reference Tables » Add/Edit Department. The Department Maintenance page appears with a list of departments.

   ![Department Maintenance page]

   Department Maintenance page

2. Click

   The Department Information panel appears.

3. Enter the following information:
6.2 Editing a Department

To edit a department:

1. In the Department Maintenance page, select a Department Name. The Department Information panel appears.

   **Note:** You can search for a department by using the Search By department name feature.

2. Modify the details.

3. Click **Save**.

6.3 Deleting a Department

To delete a department:

1. In the Department Maintenance page, select a Department Name.

   **Note:** You can search for a department by using the Search By department name feature.

2. Click **Trashbin**. A message “Do you want to delete a department with ID = Id Number?” appears.

3. Click **Delete**.

6.4 Adding a Line of Defense

To add a line of defense:

2. Click 
   The **Lod Function Information** panel appears.

3. From the drop-down list, select a Line of Defense.

4. Enter the **Line of Defense Function**.

5. Click **Save**.

### 6.5 Editing a Line of Defense

To edit a department

1. In the **Line of Defense Maintenance** page, select a Line of Defense. The **Lod Function Information** panel appears.

   **Note:** You can search for a department by using the **Search By lod name** feature.

2. Modify the details.

3. Click **Save**.
6.6 Deleting a Line of Defense

To delete a department:


| Note: You can search for a department by using the Search By lod name feature. |

2. Click 🗑. A message “Do you want to delete a lod function with ID = Id Number?” appears.

3. Click Delete.
7  My Account

The My Account feature allows you to edit your user-account information, reset your password, and logs you out of Tardigrade.

Using My Account, you can:

• Update your profile
• Reset your password
• Log out of Tardigrade

7.1 Updating Your Profile

To update user profile:

1. From the main menu, go to My Account » My Profile. The My Account Profile page appears.

My Account Profile page

2. Select a user.
   The Personal Information panel appears.
3. Modify the details.

4. Click **Save**. A message “The user profile is updated” appears.

### 7.2 Resetting your Password

To reset your password:

1. From the main menu, go to **My Account » Password Reset**. The **My Account Profile – Password Reset** page appears.

2. Enter your email address.
3. Enter the password.

4. Enter the password again.
   Depending on the complexity of the password, Tardigrade displays the **Password Strength** as the following:
   - Weak
   - Medium
   - Strong

5. Click **Save**.

### 7.3 Logging Out of Tardigrade

To log out of Tardigrade:

1. From the main menu, go to **My Account » Logout**.
   The application logs you out.
8 User Administration

The User Administration feature allows you to manage access authorizations depending on groups, roles and permissions, tenant and user administration profiles across the modules of Tardigrade. As a system admin, you can reset the password for other users.

Note: You need to be logged on as the System Administrator to access the User Administration module.

Using the following sub-features in User Administration, you can:

- **Authorization**
  - Edit a group
  - Add a role
  - Edit a role
  - Edit a permission
- **Reset a user's password**
- **Tenant**
  - Add a tenant
  - Edit a tenant
  - Delete a tenant
- **User Admin**
  - Add a user
  - Edit a user’s account
  - Delete a user
8.1 Authorization

With Authorization, you can manage groups, roles and permissions for users who access Tardigrade.

8.1.1 Editing a group

To edit a group:

1. From the main menu, go to User Administration » Authorization. The Authorization Management page appears with the Groups tab selected by default.

2. In the Groups tab, select a Group. The Group Information panel appears.

Note: You can search for a group by using the Search group feature.
3. Modify the information.
4. Click Save. A message “Group is saved” appears.
8.1.2 Adding a Role

1. In the Authorization Management page, select Roles tab. The Roles and Permission Management page appears.

2. From the Module drop-down list, select one of the following:
   - Cybersecurity
   - Internal Control
   - SRTM

3. From the Role drop-down list, select one of the following:
   - ADMINISTRATOR
   - CYBERSECURITY ASSIGNER
   - CYBERSECURITY ASSESSOR
   - CYBERSECURITY REVIEWER
   - CYBERSECURITY ADMINISTRATOR

The New Role text field appears.
New Role text field

4. Enter a role and click **Add**.
The role is added to the list of roles.

### 8.1.3 Editing a Role

1. In the **Roles and Permission Management** page, from the **Module** drop-down list select a module.

2. From the **Role** drop-down list, select a role.

3. From the panel below, you can do the following:
   
   - Click to select the required checkbox(es)
   
   - Click to remove the selected checkbox(es)
4. Click Update. A message “Role updated successfully” appears.

8.1.4 Editing a Permission

To edit a permission:

1. In the Authorization Management page, select Permissions tab. The Permissions page appears with a list of permissions.
Permissions page

2. Select a Permission. The **Permission Information** panel appears.

**Note:** You can search for a group by using the **Search permission** feature.

![Permission Information panel](image)

**Figure 80: Permission Information panel**

3. Modify the information.

4. Click **Save**. A message **"Permission is saved"** appears.
8.2 Resetting a User's Password

As a system administrator, you can reset a user’s password by using the User Administration module.

To reset a user’s password:

1. From the main menu, go to User Administration » Password Reset. The My Account Profile page appears with the Password Reset panel.

   ![User Administration – Password Reset page](image)

   2. Enter the user’s Email address.

   3. Enter the password.

   4. Enter the password again. Depending on the complexity of the password, Tardigrade displays the Password Strength as the following:

   - Weak
   - Medium
   - Strong

   5. Click Save.
8.3 Tenant

With Tenant, you can add, edit and delete tenant profiles in Tardigrade.

8.3.1 Adding a Tenant

To add a tenant:

1. From the main menu, go to User Administration » Tenant. The Tenant Profile page appears with a list of tenants.

   ![Tenant Profile page]

   2. Click 📋. The Company Information panel appears.

   ![Company Information panel]

   3. Enter the information.
4. Click **Save**.

### 8.3.2 Editing a Tenant

To edit a tenant:

1. In the **Tenant Profile** page, select a tenant profile. The **Company Information** panel appears.

   ![Editing a tenant - Company Information panel](image)

   *Note: You can search for a group by using the **Search by tenant name** feature.*

2. Modify the details.

3. **Click** **Save**.

   A message “**The tenant profile is updated**” appears.
8.3.3 Deleting a Tenant

To delete a tenant:

1. In the **Tenant Profile** page, select a tenant profile.

   **Note:** You can search for a group by using the **Search by tenant name** feature.

2. Click 🗑. A message “Do you want to delete a tenant with ID = Id Number?” appears.

3. Click **Delete**.

8.4 User Admin

With **User Admin**, you can add and delete a user in Tardigrade. You can also edit the following information for the users in Tardigrade:

- Personal
- Contact
- Other
- Role
- Group

8.4.1 Adding a user

To add a user:

1. From the main menu, go to **User Administration » User Admin**. The **Account Profile** page appears with a list of user profiles.
Account Profile page

2. Click 
   The **Personal Information** panel appears.
### Personal Information panel

3. Enter the information.
4. Click **Save**.

8.4.2 Editing a user's account

To edit a user's account information:

1. In the **Account Profile** page, select a user. The **Personal Information** panel appears.

   **Note:** You can search for a group by using the **Search** feature.

2. Modify the following as required:
   - Personal Information
   - Contact Information
   - Other Information
   - Role Information
   - Group Information

3. Click **Save**. A message “**The user profile is updated**” appears.

8.4.3 Deleting a user

To delete a user:

1. In the **Account Profile** page, select a user.

   **Note:** You can search for a group by using the **Search** feature.

2. Click . A message “**Do you want to delete user with ID: User Id?**” appears.

3. Click **Delete**.
9 Help

To access the Help module:

From the main menu, go to Help » Help Guides. The User Guide and Help Document page appears with a list of documents.

The documents are available as hyperlinks which open in a new tab as an online PDF document.

User Guide and Help Document page

In the Help module, you can view the following documents:

- Inherent Risk Profile Guide
- Domain Maturity Guide
- Cybersecurity Overview and User Guide
- NIST 800-53 R4 Publication Guide
9.1 Accessing a Help Document


Note: You can search for a document by using the Search by document name feature.

Document opens in a new tab
## 10 Appendix A: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSO</td>
<td>The Committee of Sponsoring Organizations of the Treadway Commission</td>
</tr>
<tr>
<td>FFIEC</td>
<td>Federal Financial Institutions Examination Council</td>
</tr>
<tr>
<td>ISO 27001-2013</td>
<td>International Organization for Standardization 27001-2013</td>
</tr>
<tr>
<td>NIST 800-53 R4</td>
<td>National Institute of Standards and Technology 800-53 R4</td>
</tr>
<tr>
<td>MAS</td>
<td>Monetary Authority of Singapore</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
</tbody>
</table>
Bibliography


Vita

Alexis Shook was born in New Orleans, LA. She received her Bachelor’s degree in writing for production from the University of New Orleans in 2016. She returned to the university to earn her Master’s in English and plans on pursuing a career in technical writing.