

Assess Risks

Last Modified on 04/05/2023 5:13 pm EDT

Risk Owners and their delegates are responsible for assessing risks and ensuring that they are properly mitigated by attaching controls, Key Risk Indicators (KRIs), and issues. Once users in the group have completed their tasks, the risks are then sent to the [Risk Team](#) for review. All assigned risks appear on the [My Tasks](#) page.

The screenshot shows the Resolver application interface. At the top, there is a navigation bar with the Resolver logo, a search bar, and user profile icons. Below the navigation bar, there are two tabs: 'Home' and 'My Tasks', with 'My Tasks' being the active tab. The main content area is divided into two panels. The left panel, titled 'My Tasks', contains a list of two risks: 'Cyber Security' (ID R-1.1) and 'Data Quality' (ID R-2.1). Both risks are assigned to the user on March 25th, 2020, and each has a 'RISK ASSESSMENT' button. The right panel, titled 'Risk', shows a 'Workflow State' chart. The chart is a horizontal bar chart with a scale from 0 to 3. A blue bar extends to the value 2, and a legend below indicates that this bar represents 'Risk Assessment'.

Assigned risks on the My Tasks page.



The Risk Team can also complete these steps from the **Risk Assessment** section of the **Assess & Treat** tab. However, it's recommended that the Risk Owner is the one who assesses risks.

To assess risks:

1. Log into a user account from the **Risk Owner & Delegate** user group to display the **My Tasks** page.
2. Click the relevant **Risk** to display it.

Privacy Risk R-5.1 RISK ASSESSMENT

Details | Assessments | Relationship Graph | History | Communications

Risk Details

The risk profile provides a comprehensive understanding of your risk, including risk assessments, controls, and issues. Review all risk information to determine how the risk should be treated.

Description

Ensuring privacy/identity management and information security/system protection may require significant resources for us

Risk Owner

Q Jane Smith x

Business Unit

Corporate

Risk Sub Category

Regulatory

The Risk form in the Inherent Risk Assessment section.

- a. In the **Inherent Risk** tab, select the relevant ratings from the **Inherent Impact** and **Inherent Likelihood** fields to generate an inherent risk score.
- b. **Optional:** Click the **Contributing Factors** tab to review any contributing factors currently attached to this risk.
 - To add an existing contributing factor, click **Add Existing Contributing Factor**, type its name in the search bar, and select it.
 - To create a new factor from scratch, click **+ Create New** and fill in the required fields.
- c. **Optional:** Click the **Historical Trending** tab to view a chart showing how the inherent risk score has changed over time.

The Inherent Risk section.

3. In the **Document Controls and Determine Control Effectiveness** section:
 - a. Click **Add Existing Controls** and begin typing in the search bar to search for existing controls.
 - b. Click **Add** next to each appropriate control to add it to the risk.
 - c. **Optional:** To add the version of a control used by an assessment in another application or business unit, click **Assessments** and then **Add** next to the relevant assessment.

Searching for existing controls in the Add Existing Controls dialog.



If there are no controls appropriate to this risk, a Risk Owner can personally [submit a new risk](#), but the Risk Team must approve it.

- d. Click any controls in this section to display the **Control Assessment** dialog.
- e. Begin typing in the **Control Owner** and **Control Delegate** fields and click to select the relevant user.
- f. Fill in the remaining fields as required. Read more here: [Assess a Control](#).

The screenshot shows a 'CONTROL' dialog box with a blue header. The title is 'Disclosure of personal information to third parties'. Below the title, there is a green pill with 'C-58.4' and a grey pill with 'ASSIGN CONTROL OWNER'. A tabbed interface has 'Details' selected. The form contains the following fields:

- Control Name:** Disclosure of personal information to third parties
- Description:** The entity's privacy policies address the disclosure of personal information to third parties.
- Business Unit:** Corporate
- Control Owner:** A search field with a yellow border and a yellow information icon, containing the text 'Start typing to find Use...'
- Reviewed By:** A search field containing the text 'Start typing to find Use...'
- Control Delegate:** A search field containing the text 'Start typing to find Use...'
- Frequency:** A dropdown menu with 'Annually' selected.

The Control dialog box.

- g. Select the relevant rating from the **Control Self-Assessment** list in the **Control Effectiveness** section.

Inherent Risk	Control Effectiveness	Residual Risk	Risk Treatment	Historical Trending
<p>Document controls or risk management activities that the organization has in place to reduce risk. To find existing controls from the control library, click Add Existing Controls at the bottom of the table. If a new control is required, please navigate to the library to create the control first. Once you have documented all controls, form a manual determination on the overall control effectiveness for the risk.</p>				
Controls				
Unique ID	Name	Description	Control Self Assessment	Workflow State
C-97.3	Mandatory privacy training	Mandatory privacy training	● Weak	● Assign Control Owner ✕
C-58.4	Disclosure of personal information to third parties	The entity's privacy policies address the disclosure of personal information to third parties.	● Excellent	● Assign Control Owner ✕
C-57.3	Personal information policy	Personal information is relevant to the purposes for which it is to be used.	● Strong	● Assign Control Owner ✕
C-56.14	Sensitive information policy	A process is in place that protects sensitive information from unauthorized users.	● Medium	● Assign Control Owner ✕
Q ADD EXISTING CONTROLS				

The Document Controls and Determine Control Effectiveness section.

- Optional:** Click the **Related Incidents** tab to review any incident types attached to this risk. An existing incident type can be added by typing its name in the search bar and selecting it.

Issues & Actions	Key Risk Indicators	Loss Events	Contributing Factors	Related Incidents								
<p>Consider what types of corporate security incidents might have an impact on this particular risk. To search for incident types, start typing at the bottom of the table.</p> <p>Related Incidents: The number of incidents related to the contributing factors that are related to this risk.</p> <p>Potential Incidents: The number of incidents related to the incident type(s) that are related to this risk.</p> <p>Net Loss from Related Incidents</p> <p>\$0.00</p> <p>Incident Type</p> <table border="1"> <thead> <tr> <th>Unique ID</th> <th>Name</th> <th>Total Incidents</th> <th>Net Loss</th> </tr> </thead> <tbody> <tr> <td colspan="4" style="text-align: center;">No data to display</td> </tr> </tbody> </table> <p style="text-align: center;">Q ADD EXISTING INCIDENT TYPE</p>					Unique ID	Name	Total Incidents	Net Loss	No data to display			
Unique ID	Name	Total Incidents	Net Loss									
No data to display												
<p>Related Incidents</p> <p>0</p> <p>RELATED INCIDENTS</p>												

The Related Incidents tab.

5. **Optional:** Click the **Key Risk Indicators** tab to review any KRIs attached to this risk. An existing KRI can be added by clicking **Add Existing Key Risk Indicators**, or a new one can be created from scratch by clicking **Create New**. Read more here: [Create KRIs](#).



While this may vary between organizations, it is recommended that the Risk Team create KRIs and assign them to indicator owners. However, the Risk Owner also has this capability.

6. In the **Residual Risk** section: Select the relevant ratings from the **Residual Impact** and **Residual Likelihood** fields to generate a residual risk score.
7. **Optional:** Click the **Loss Events** tab to review any loss events attached to this risk. An existing loss event can be added by clicking **Add Existing Loss Events** or a new one can be created from scratch by clicking **Create New**. Read more here: [Submit a Loss Event](#).
8. **Optional:** Click the **Historical Trending** tab to view a chart showing how the inherent risk score has changed over time.

Residual risk refers to the remaining level of risk once risk management activities have been put in place. Consider any related events that may increase your level of risk exposure.

Residual Impact
● Moderate

Residual Likelihood
● Unlikely

Moderate: Financial loss of \$X million up to \$X million; Limited reputational impact; Reportable incident to regulator, no follow up

Unlikely: Once in 5 years up to once in 10 years

Residual Risk Score
High

The Residual Risk section.

9. In the **Risk Treatment** section:
 - a. Select one of these treatment options in the **Risk Response Plan** dropdown:
 - **Tolerate - Accept:** The risk owner accepts the risk as is and no further action is taken.
 - **Treat - Reduce:** Corrective action must be performed on this risk to mitigate its impact on the organization.
 - **Transfer - Share:** Corrective action must be performed on the risk, but it must be transferred to or shared with another individual and/or group within the organization.

- **Terminate - Avoid:** This risk can be avoided and should be removed from the library.
- **Not Applicable:** This risk is not applicable to the organization.

b. Enter a description of the treatment in the **Comments on Disposition** field.

The Risk Treatment section.



The **Document Issues and Corrective Actions** section will not appear if the user chose **Tolerate - Accept** or **Not Applicable**. If either of these options were selected, skip to the next step.

10. In the **Issues & Actions** section, an existing contributing issue can be added by clicking **Add Existing Issue**, typing its name in the search bar, and selecting it. To create a new issue from scratch, click **+ Create New** and fill in the required fields. Read more here: [Review an Issue](#) and [Review a Corrective Action](#).

Issues & Actions | Key Risk Indicators | Loss Events | Contributing Factors | Related Incidents

When transferring the risk, document any issues associated to the risk or control. This may include any corrective actions required to transfer the risk to another party. To find existing issues, click **Add Existing Issue** at the bottom of the table. If a new issue is required, click **Create New** at the bottom of the table.

Issues

Unique ID	Name	Description	Priority	Due Date	Workflow State
No data to display					
Q ADD EXISTING ISSUES		+ CREATE NEW			

The Document Issues and Corrective Actions section.

- Optional:** Expand the **Related Assessments** section to view the assessments related to the risk.

Related Assessments

Use this table to review assessments of this risk across the organization.

Residual Risk Score
High

Assessment Name	Inherent Risk Score	Control Effectiveness	Residual Risk Score	Related Incidents
Operations BU Risk Assessment	Low	N/A	Invalid Result	0

The Related Assessments section.

- Optional:** Add [comments](#), as needed.
- Click one of the following buttons:
 - **View Risk Profile:** Opens a report that shows a high-level summary of the risk, including its scores, its trending data, and the controls, issues, and KRI's attached to the risk.
 - **Escalate Risk:** Sends the risk back to the risk team for further review. This button will only appear for the **Treat - Reduce** and **Transfer - Share** treatment options.
 - **Submit For Review:** Completes the risk assessment and sends it to the risk team for review.