

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 is the Resolver logo and navigation bar. Below the navigation bar, the 'My Tasks' tab is selected. The main content area is divided into two panels. The left panel, titled 'My Tasks', lists two assigned risks: 'Cyber Security' (ID R-1.1) and 'Data Quality' (ID R-2.1), both assigned on Mar 25th, 2020. Each risk has a 'RISK ASSESSMENT' button. The right panel, titled 'Risk', shows a 'Workflow State' bar chart with a scale from 0 to 3. A blue bar indicates the current state is 2, labeled '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

×

Business Unit

Corporate

Risk Sub Category

Regulatory

The Risk form in the Inherent Risk Assessment section.

- In the **Inherent Risk** tab, select the relevant ratings from the **Inherent Impact** and **Inherent Likelihood** fields to generate an inherent risk score.
- 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.
- Optional:** Click the **Historical Trending** tab to view a chart showing how the inherent risk score has changed over time.

The screenshot shows the 'Inherent Risk' section of the Resolver interface. It features a tabbed navigation bar with 'Inherent Risk' selected. Below the tabs, a text box explains: 'Determine the inherent risk. Inherent risk reflects any risk to the organization before considering risk management activities that the organization puts in place to mitigate risk.' There are two dropdown menus: 'Inherent Impact' set to 'Critical' (indicated by a red dot) and 'Inherent Likelihood' set to 'Remote' (indicated by a green dot). Below these, definitions are provided: 'Critical: Financial loss of \$X million or more; Significant external reputational impact; game-changing loss of market share; Significant prosecution and fines' and 'Remote: Once in 20 years or less'. At the bottom, the 'Inherent Risk Score' is displayed as 'High' in a yellow box.

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.

The screenshot shows the 'ADD EXISTING CONTROLS' dialog. It has a blue header with the title and a close button. Below the header is a search bar with the placeholder text 'Start typing to find an existing Control'. A message states: 'Showing 50 most recently created Control. If you don't see what you were searching for, try searching from all Controls above.' Two control entries are listed: 'C-121 Vendor review of COVID procedures' and 'C-127 Update Test'. Each entry has an 'ACTIVE' status and a '+ ADD' button. The description for the first control is 'Vendor review of COVID procedures' and for the second is 'This is a test'.

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](#).

CONTROL

Disclosure of personal information to third parties

C-58.4

ASSIGN CONTROL OWNER

Details

History

Communications

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 ⓘ

Q Start typing to find Use...

Q Start typing to find Use...

Control Delegate

Q Start typing to find Use...

Frequency

Annually

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																														
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.																																		
Controls <table border="1"> <thead> <tr> <th>Unique ID</th> <th>Name</th> <th>Description</th> <th>Control Self Assessment</th> <th>Workflow State</th> <th></th> </tr> </thead> <tbody> <tr> <td>C-97.3</td> <td>Mandatory privacy training</td> <td>Mandatory privacy training</td> <td>Weak</td> <td>Assign Control Owner</td> <td>✕</td> </tr> <tr> <td>C-58.4</td> <td>Disclosure of personal information to third parties</td> <td>The entity's privacy policies address the disclosure of personal information to third parties.</td> <td>Excellent</td> <td>Assign Control Owner</td> <td>✕</td> </tr> <tr> <td>C-57.3</td> <td>Personal information policy</td> <td>Personal information is relevant to the purposes for which it is to be used.</td> <td>Strong</td> <td>Assign Control Owner</td> <td>✕</td> </tr> <tr> <td>C-56.14</td> <td>Sensitive information policy</td> <td>A process is in place that protects sensitive information from unauthorized users.</td> <td>Medium</td> <td>Assign Control Owner</td> <td>✕</td> </tr> </tbody> </table> ADD EXISTING 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	✕
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	✕																													

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								
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. Related Incidents: The number of incidents related to the contributing factors that are related to this risk. Potential Incidents: The number of incidents related to the incident type(s) that are related to this risk. Net Loss from Related Incidents \$0.00 Incident Type <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">No data to display</td> </tr> </tbody> </table> ADD EXISTING INCIDENT TYPE					Unique ID	Name	Total Incidents	Net Loss	No data to display			
Unique ID	Name	Total Incidents	Net Loss									
No data to display												
Related Incidents 0 RELATED INCIDENTS												

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.

Inherent Risk Control Effectiveness **Residual Risk** Risk Treatment Historical Trending

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 you 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.

11. **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.

12. **Optional:** Add [comments](#), as needed.
13. 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.