

Create & Monitor KRIs

To aid organizations in monitoring the status of risks, Risk Management allows for the creation of key risk indicators (KRIs). KRIs track the levels of specific aspects of a risk (eg. profit loss, percentage of employees who have completed training, etc.) and sends an alert when these levels cross acceptable thresholds. KRIs can be created by the risk team in risks that are in the **Review** and **Monitoring** workflow state.

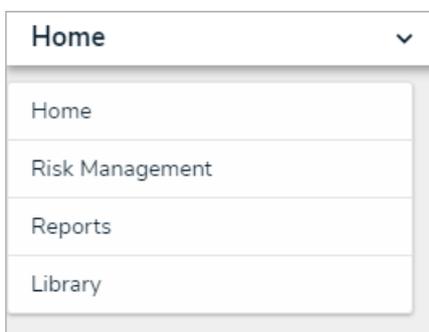


KRI's can also be created by risk owners in risks that are in **Assess Risk** workflow state. While the exact procedure will vary from organization to organization, it is recommended that KRIs are created by the risk team.

Once the indicator owner has updated the KRI, it is moved to the **Monitoring** workflow state. Members of the risk team can then monitor the KRI to ensure it is still being followed and they can return the KRI to the indicator owner for further updates.

To create a KRI:

1. Log into a user account that's been added to the **Risk Team** user group.
2. Click the dropdown in the nav bar > **Risk Management**.



The nav bar.

3. Navigate to the **Review & Monitor** tab and click a risk in the **Review Risks** or **Risk Monitoring** section.

The screenshot displays the RESOLVER Risk Management interface. At the top, there is a navigation bar with the RESOLVER logo, a search bar, and icons for settings, help, and user profile. Below the navigation bar, the 'Risk Management' section is active, with sub-tabs for 'Identify Risks', 'Launch Risk Assessment', and 'Assess & Treat'. The main content area is titled 'Review & Monitor' and contains a sub-section 'Review & Monitor' with the text 'Review and monitor risks through reports and trending.' Below this is a 'Review Risks' section with the text 'The following risks have been submitted for review by the risk owners.' Three risk items are listed: 'Information Risk' (R-26.2), 'IT Infrastructure Risk' (R-27.1), and 'Cyber Security' (R-29.1). Each item includes a description, a 'CORPORATE' tag, and a 'Review' button.

RESOLVER (+) (Q) (ooo) (gear) (?) (user)

Risk Management (v) Identify Risks Launch Risk Assessment Assess & Treat ...

Review & Monitor

Review & Monitor

Review and monitor risks through reports and trending.

Review Risks

The following risks have been submitted for review by the risk owners.

- R-26.2** Information Risk [Review](#)
Aliquam etiam erat velit scelerisque in. Sed risus pretium quam vulputate dignissim. Pellentesque elit ullamcorper dignissim cras tincidunt lobortis feugiat vivamus.
CORPORATE
- R-27.1** IT Infrastructure Risk [Review](#)
Lorem sed risus ultricies tristique nulla aliquet enim tortor. Egestas pretium aenean pharetra magna ac placerat vestibulum.
CORPORATE
- R-29.1** Cyber Security [Review](#)
Pellentesque dignissim enim sit amet venenatis urna cursus eget.
CORPORATE

The Monitor & Review tab.

4. Click Key Risk Indicators in the **Determine Residual Risk** section.

Step 3: Determine Residual Risk



Residual risk refers to the remaining level of risk once risk management activities have been put in place. Consider any contributing factors to the risk, including but not limited to key risk indicators or related incidents that may increase your level of risk exposure.

Residual Risk Related Incidents **Key Risk Indicators** Loss Events Historical Trending

Consider any metrics that may provide useful insight into the potential exposure to this risk. To create a new Key Risk Indicator ("KRI"), click **Create New** at the bottom of the table. Otherwise, search for an existing KRI.

Key Risk Indicators

Unique ID	Name	Target Value	Current Value	Indicator Rating	Workflow State
IND-11	Number of patents filed during period, range	5	10	● Out of Tolerance	Monitoring ×

[Q ADD EXISTING KEY RISK INDICATORS](#) [+ CREATE NEW](#)

The Key Risk Indicators tab of the Determine Residual Risk section.

5. Click **+ Create New** to open the **Create a New Indicator** dialogue.

Indicator Status **Creation** ✕

Create a New Indicator I-XXX

Indicator Name

Description

Indicator Owner

Start typing to find Us... ▼

Indicator Details +

CREATE AND SAVE AS

DRAFT

CANCEL

The Create a New Indicator dialogue

6. Enter a name in the **Indicator Name** field, then add a description of the indicator to the **Indicator Description** field.
7. Begin typing keywords in the **Indicator Owner** field to display a list of available users, then click to select an appropriate user. Multiple indicator owners can be assigned to a single KRI.
8. Click **Create and Save as Draft**.
9. In the **Determine Residual Risk** section, click the KRI in the **Draft** workflow state to open the **Draft Indicator** dialogue.

Indicator Status **Draft**
🗨️ ✕

Percentage of employees who have completed annual cyber security training IND-16

Indicator Name

Description

How many employees are up to date with their training on mitigating these risks?

Indicator Owner ⓘ

👤
Indicator Owner (Limited User) ✕
▼

Key Dates

Define the entry due date and the reporting cutoff date for the Indicator Owner. The Due Date should be before the Reporting Date.

Any values entered after the Reporting Date will be recorded in the following time period for historical trending.

Due Date ⓘ

📅

▼

Reporting Date ⓘ

📅

▼

The Draft Indicator dialogue.

10. In the **Key Dates** section:

- a. Enter the date that the indicator should be updated by in the **Due Date** field.
- b. Enter the date by which the indicator update should be finalized by in the **Reporting Date** field.

11. In the **Indicator Details** section:

- a. Select how frequently the indicator should be updated in the **Frequency of Update** select list.
- b. Select what the indicator is current, leading, or lagging in the **Classification** select list.
- c. Select what kind of limit range the indicator should have in the **Type** select list. For example, if the indicator's value cannot go above a certain level, select **Increasing Range**. If it cannot go below a certain level, select **Decreasing Range**. If the value must stay between two levels, select **Range**.

If the user selects **Increasing Range** or **Decreasing Range**, the **Indicator**



Limits section below will only have the **Target Limit** and **Threshold Limit** fields available.

- d. Select how the indicator should be measured in the **Unit of Measurement** select list.

Indicator Details

Frequency of Update	Classification
Annually	Current
Type ⓘ	Unit of Measurement
Range	%

The Indicator Details section.

12. In the **Indicator Limits** section:

- Enter the ideal value that the indicator should have by default in the **Target Value** field.
- Enter how low or high the value can go before being out of tolerance in the **Threshold Lower Limit** and **Threshold Upper Limit** fields.
- Enter how low or high the value can go before being considered off-target but still within tolerance in the **Target Lower Limit** and **Target Upper Limit** fields.

Indicator Limits

Set lower and upper limits for the Indicator, based on the type selected above.

Target Value

Range: Values between or at the target limits are "On Target". Values between the target and threshold limits, or at the threshold limits are "Within Tolerance". All other values are "Out of Tolerance".

Lower Limit	Target Lower Limit	Target Upper Limit	Upper Limit
5	10	15	20

The Indicator Limits section.

13. **Optional:** Expand the **Related Data** section to view the risks and objectives the KRI is attached to.

Related Data

Risks

Monogram	Unique ID	Name	Description	
R	R-1.1	Cyber Security	The probability of exposure or loss resulting from a cyber-attack or data breach.	×

Objectives

Monogram	Unique ID	Name	Description
No data to display			

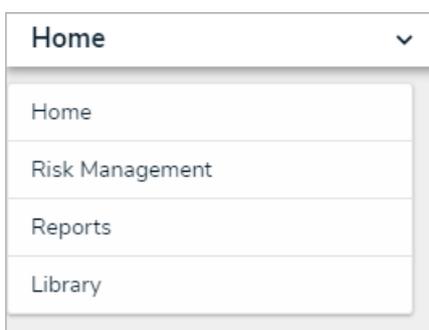
The Related Data section.

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

15. Click **Send to Indicator Owner**.

To monitor a KRI:

1. Log into a user account that's been added to the **Risk Team** user group.
2. Click the dropdown in the nav bar > **Risk Management**.



The nav bar.

3. Navigate to the **Indicators** tab and scroll down to the **Monitor Indicators** section.

The screenshot shows the Resolver Risk Management interface. At the top, there is a navigation bar with the Resolver logo, a search bar, and user icons. Below the navigation bar, the 'Risk Management' section is active, with sub-tabs for 'Identify Risks', 'Launch Risk Assessment', and 'Assess & Treat'. The main content area is titled 'Monitor Indicators' and includes a search bar. Below the title, a message states: 'The following indicators are in monitoring. They should be updated as changes emerge throughout the organization.' Three indicators are listed:

- IND-1** Number of negative news events **Monitoring**
- IND-2** Percentage of completion of BCP training **Monitoring**
- IND-3** Spend due to health & safety incidents **Monitoring**

The Monitor Indicators section of the Indicators tab.

4. Click a KRI in the **Monitoring** workflow state to open the **Monitor Indicator** form.

The screenshot shows the 'Monitor Indicator' form. At the top, the 'Indicator Status' is 'Monitoring'. The form title is 'Monitor Indicator' with the ID 'IND-11'. Below the title, a message states: 'The following indicator is in a monitoring state. It will remain available to edit and review by the Risk Team until the next update period.' The form contains the following fields:

- Indicator Name:** Number of patents filed during period, range
- Description:** (Empty text area)
- Indicator Owner:** Start typing to find Us... (Dropdown menu)
- Key Dates:** Define the entry due date and the reporting cutoff date for the Indicator Owner. The Due Date should be before the Reporting Date. Any values entered after the Reporting Date will be recorded in the following time period for historical trending.
 - Due Date:** (Calendar icon, dropdown menu)
 - Reporting Date:** (Calendar icon, dropdown menu)

The Monitor Indicator form.

5. Edit the fields as required. See the [Update a KRI](#) article for more information on filling in the rest of the form.
6. **Optional:** If the KRI requires further updates from the indicator owner, click **Send for Update**.