QAD Adaptive Applications

User Guide

QAD EQMS Applications: Risk Management

70-3375-2025

QAD QMS Applications version 2025

March 2025

Copyright

QAD Inc.

100 Innovation Place

Santa Barbara, CA 93108

Phone: + 1 (805) 566-6100

http://www.qad.com

Risk Management User Guide Change Summary

The following table summarizes significant differences between this document and previous versions.

Date/Version	Description	Reference	Changed By
AUG 2019/v2019	Initial upload	--	RQT
OCT 2020/v2020.1	Updated versioning	--	RQT
MAR 2021/v2021	Updated linkage	--	RQT
MAY 2021/v2021	Added a section for Commands	p.70	RQT
MAY 2021/v2021.1	Updated versioning	--	RQT
FEB 2022/v2022	Updated versioning	--	RQT
SEPT 2022/v2022.1	Updated versioning	--	RQT
MAR 2023/v2023	Updated versioning; Modified Risks	p. 31	RQT
MAR 2024/v2024	Updated versioning	--	RQT
SEPT 2024/v2024.1	Updated versioning	--	RQT
MAR 2025/v2025	Updated versioning	--	RQT

Chapter 1

Introduction

Overview

Many recent global events have disrupted manufacturing organizations, demonstrating the impact of failing to properly address risk. Recalls, financial crises, natural disasters, distressed suppliers, and knowledge erosion all contribute to a greater need to evaluate and mitigate risks across the organization. Customer demands, internal challenges, and supplier constraints, combined with the accelerating pace of new product introductions, make real-time visibility into possible risks and potential remediation more critical than ever.

Risk-based thinking now appears in quality standards and has become a key initiative for most industries. Most executives see the new risk focus in standards and the module of risk-based thinking as a positive change that can lead to improved operations and higher margins. Industry leaders view the uncertainty associated with the new standards as a chance to introduce novel ideas and embrace new opportunities.

About This Guide

This user guide focuses on:

- Setup required for the Risk Management module
- Different forms of document organization in the Risk Management module
- Security and roles for the Risk Management module
- Instructions for the various Risk Management tasks

Note: This guide does not provide field descriptions for the Risk Management module fields. Field help is provided in the software.

Risk Management Module Setup Guide

This section describes the processes of the Risk Management module. The list below is arranged by the order in which the processes should be completed, starting with the setup operations and continuing with the main functions.

Setting Up the Risk Management Module

Color Indicators

Use Color Indicators to set up a list of different colors that are used throughout the Risk Management module and other modules. See "Color Indicators" on page 14.

Risk Acceptability Types

Use Risk Acceptability Types to identify how the company feels about each Likelihood and Consequence combination in a Risk or Risk Acceptability Matrix record. See "Risk Acceptability Types" on page 15.

Risk Ratings

Use Risk Ratings to define a list of ratings for risks and the risk acceptability matrix. See "Risk Ratings" on page 17.

Risk Treatment Types

Use Risk Treatment Types to categorize risk treatments and risk library controls. See "Risk Treatment Types" on page 18.

Risk Acceptability Matrix

Use the Risk Acceptability Matrix to define the general acceptability of the combination of two risk ratings. See "Risk Acceptability Matrix" on page 19.

Risk Drivers

Use Risk Drivers to identify aspects of a business that effect changes on another aspect of the business and create risk for the organization. See "Risk Drivers" on page 23.

Risk Events Sources

Use Risk Events Sources to identify areas form which a risk may potentially originate. See "Risk Events Sources" on page 25.

Risk Library Controls

Use Risk Library Controls to categorize controls that are able to treat multiple risks so that they may be selected on additional risks. See "Risk Library Controls" on page 27.

Using The Risk Management Module

Risk Library

Use Risk Library to maintain a list of known risks that are associated with a particular context within the software. See "Risk Library" on page 30.

Risks

Use Risks to document the effect of uncertainty on objectives that are an integral part of many risk management standards. See "Risks" on page 31.

Risk Assessments

Use Risk Assessments to group the identification, analysis, and evaluation of risks into a group for easier management. See "Risk Assessments" on page 36.

Risk Treatment

Use Risk Treatments to mitigate risks and, later, become risk controls. See "Risk Treatments" on page 39.

Risk Controls

Use Risk Controls to identify and document treatments that have been implemented as controls for a risk. See "Risk Controls" on page 40.

Risk Events

Use Risk Events to document incidents that have actually occurred that need to be resolved to prevent future consequences to the organization. See "Risk Events" on page 42.

Risk Actions

Use Risk Actions to support the adding and tracking of actions related to a risk or risk assessment. See "Risk Actions" on page 45.

Risk Bow Tie Analysis

Use the Risk Bow Tie Analysis to determine the likelihood and consequence for a risk. See "Risk Bow Tie Analysis" on page 49.

Risk Bow Tie Analysis Cause

Use the Risk Bow Tie Analysis Cause to determine why a risk happened or could potentially happen. See "Risk Bow Tie Analysis Cause " on page 50.

Risk Bow Tie Analysis Consequence

Use the Risk Bow Tie Analysis Consequence to determine the possible outcomes of a risk. See "Risk Bow Tie Analysis Consequence" on page 51.

Getting Started

Before you can begin using the Risk Management module, it is important to understand the basics of how to navigate and use the QMS system. The system is intuitive, but some layouts, features, and best practices require a more thorough understanding. See the User Interface user guide for additional information about the QMS software.

Chapter 2

Setting Up the Risk Management Module

Introduction

Some preparation is required before you can create, assess, or treat risks.

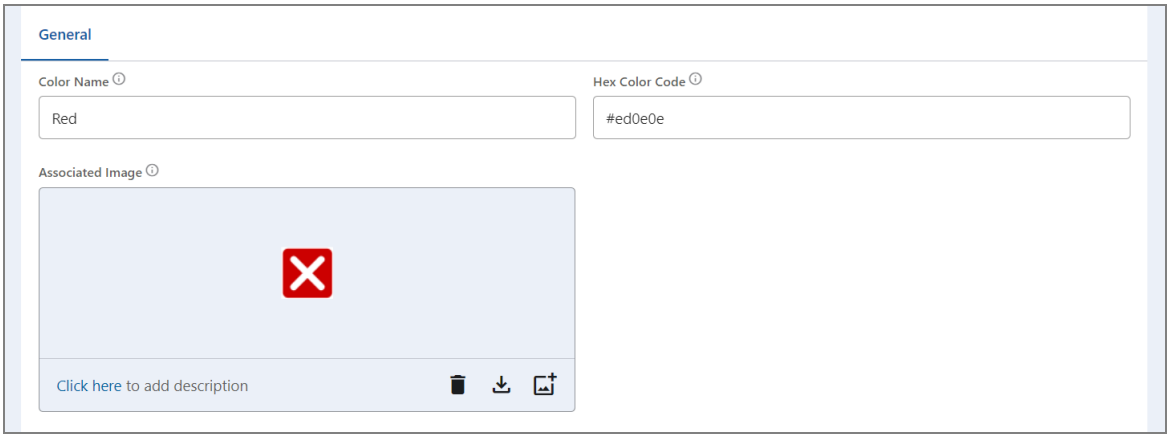
Risk preparation involves setting up the organization of risk acceptability and treatment, supplying drivers and ratings, and more. These tasks are generally performed by the risk administrator, risk champion, or the risk management maintenance role.

Color Indicators

Color indicators set up a list of different colors that are used in risk acceptability types. See "Risk Acceptability Types" on the next page.

You can add an image to the color indicator that represents what the indicator will be used for. For example, red is typically used in negative situations (unacceptable, error, stop, etc.) so an image of a red X may be best suited to a red color indicator.

Fig. 1: Color Indicators process screen

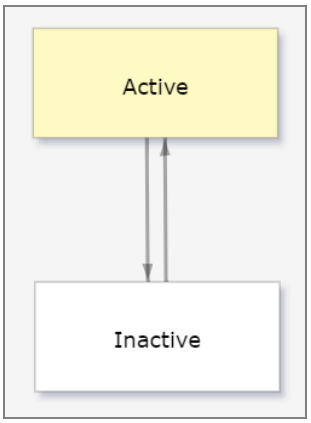


Color Indicators States

This section defines each state available in the workflow for the Risk Management process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A color indicator that is actively used.

Inactive. A color indicator that is no longer in use.



Color Indicators Tasks

Adding a New Color Indicator

1. Select Color Indicators from the left navigation panel. Then, click the Add Item button in the toolbar.
2. Enter the color name and its corresponding hex color code number.

   Note: The hex color code number is a six digit number made up of numerals and letters that, when preceded by the octothorpe (#) symbol, signifies a specific shade. Hex color code numbers can be found in various places online, such as https://imagecolorpicker.com.

3. Click the Browse button in the Associated Image field to select an image that best represents what the color indicator will be used for. A new window appears.
4. Navigate to the image file. Select it, then click Open. The image uploads.
5. Click Save to save the new record. When selecting the next state, click Active.

   Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the indicator cannot be used for new records.

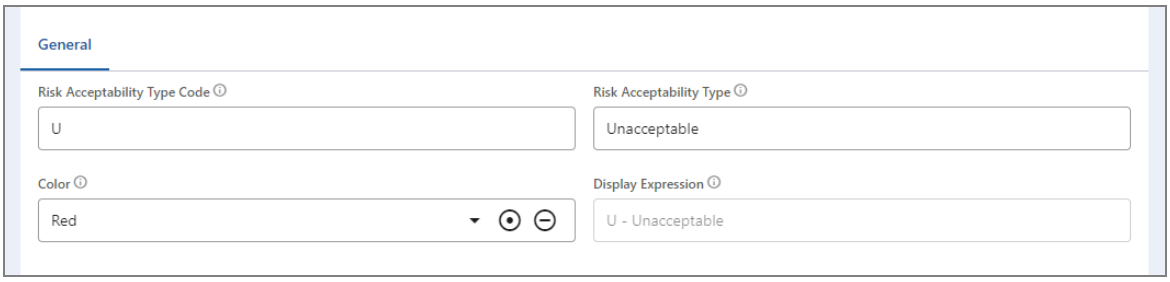
Risk Acceptability Types

Generally, there are three to five acceptability types. The default data is Acceptable, Unacceptable, and As Low As Reasonably Practicable. These types are used on the risk acceptability matrix to identify how the company feels about the intersection of each Likelihood and Consequence combination. For example, if the intersection is low likelihood and low consequence, then the organization will most likely find that acceptable.

Risk acceptability types are used in the following processes of the Risk Management module:

- By the Risk Acceptability Matrix to define the acceptability of a likelihood-consequence combination. See "Risk Acceptability Matrix" on page 19.
- By Risks to evaluate the acceptability of a risk during the Identification/Analysis state. See "Risks" on page 31.

Fig. 2: Risk Acceptability Types process screen

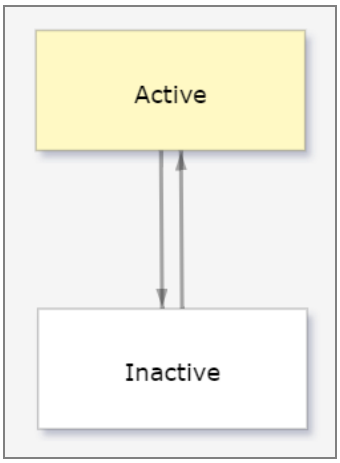


Risk Acceptability Types States

This section defines each state available in the workflow for the Risk Acceptability Types process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk acceptability type that is actively used.

Inactive. A risk acceptability type that is no longer in use.



Risk Acceptability Types Tasks

Adding a New Risk Acceptability Type

1. Select Risk Acceptability Types from the left navigation panel. Then, click the Add New button in the toolbar.
2. Enter values for the risk acceptability type code and name. Notice how the Display Expression field combines the two values; this is how users will look up this acceptability type.
3. Select a color to represent this specific type; for example, an Acceptable type may be represented by the color green while an Unacceptable type may be represented by the color red.
4. Click Save to save the new record. When selecting the next state, click Active.

Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the acceptability type cannot be used for new records.

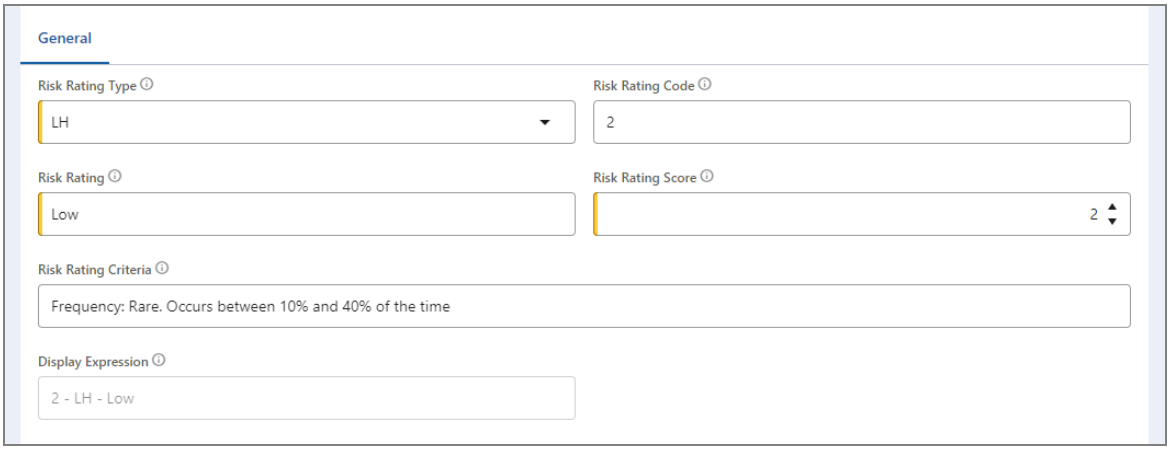
Risk Ratings

Risk ratings allow you to define a list of ratings for risks and the risk acceptability matrix. The typical example of risk rating types are Likelihood (LH) and Consequence (CON). Risk ratings are often between one and five, where five is the most likely to occur or the highest consequence if it does occur. A matrix can then be established between the two criteria and a definition of risk acceptance defined for each value.

Risk ratings are used in the following processes of the Risk Management module:

- By Risk Acceptability Matrix to define intersecting parameters. See "Risk Acceptability Matrix" on page 19.
- By Risk to determine the likelihood that a risk will occur. See "Risks" on page 31.

Fig. 3: Risk Ratings process screen

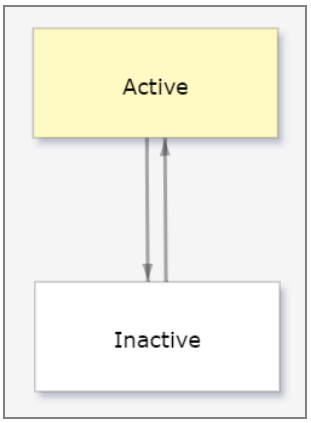


Risk Ratings States

This section defines each state available in the workflow for the Risk Ratings process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk rating that is actively used.

Inactive. A risk rating that is no longer in use.



Risk Ratings Tasks

Adding a New Risk Rating

1. Select Risk Ratings from the left navigation panel. Then, click the Add New button in the toolbar.
2. Select a risk rating type: LH (likelihood) or CON (consequence).
3. Create a code and name for the risk rating.
4. Assign a numerical score associated with the risk rating; typically, this number is between 1 and 5 or 10.
5. Document all of the risk rating's criteria to help users decide whether or not they should select this risk rating.
6. Click Save to save the new record. When selecting the next state, click Active.

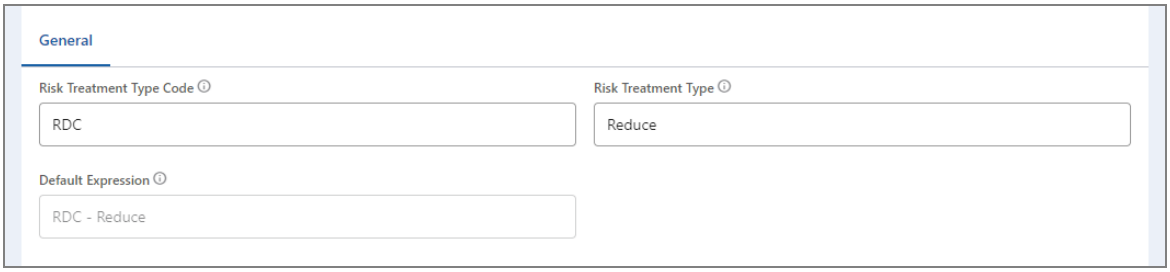
   Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the rating cannot be used for new records.

Risk Treatment Types

Risk treatment types are categories for risk treatments. Generally, there are five different treatment types: Share, Reduce, Avoid, Transfer, or Tolerate/Accept.

Risk treatment types are used in the Risk Library Controls and Risk Treatment processes for categorization. See "Risk Library Controls" on page 27 and "Risk Treatments" on page 39.

Fig. 4: Risk Treatment Types process screen

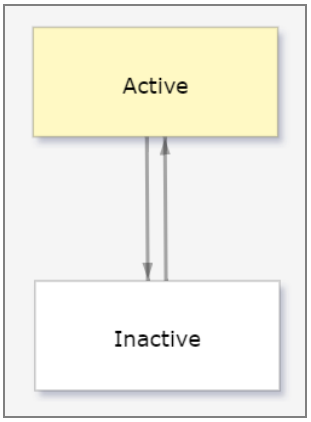


Risk Treatment Types States

This section defines each state available in the workflow for the Risk Treatment Types process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk treatment type that is actively used.

Inactive. A risk treatment type that is no longer in use.



Risk Treatment Types Tasks

Adding a New Risk Treatment Type

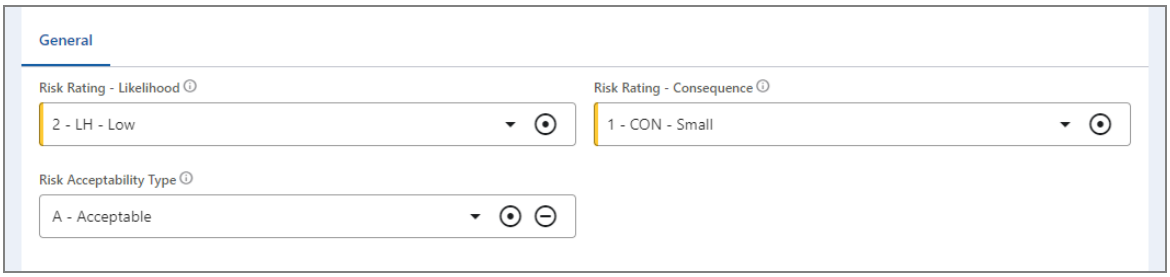
1. Select Risk Treatment Types from the left navigation panel. Then, click the Add New button in the toolbar.
2. Enter values for the risk treatment type code and name. Notice how the Display Expression field combines the two values; this is how users will look up this treatment type.
3. Click Save to save the new record. When selecting the next state, click Active.

Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the treatment type cannot be used for new records.

Risk Acceptability Matrix

The risk acceptability matrix defines the general acceptability of the combination of two risk ratings. In most cases, the risk ratings would be Likelihood and Consequence, therefore a matrix line item would set the acceptability level for the selected combination of Likelihood and Consequence.

Fig. 5: Risk Acceptability Matrix process screen

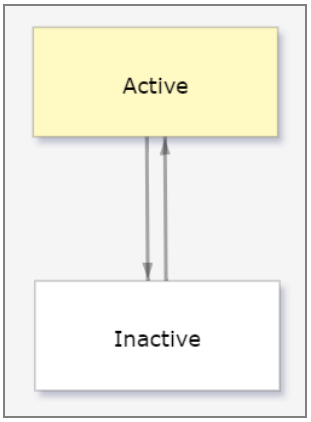


Risk Acceptability Matrix States

This section defines each state available in the workflow for the Risk Acceptability Matrix process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk acceptability matrix that is actively used.

Inactive. A risk acceptability matrix that is no longer in use.



Risk Acceptability Matrix Tasks

Adding a Risk Acceptability Matrix Field

Once complete, the Risk Acceptability Matrix is viewed as a report. Before the report can be seen, you must set up the fields that populate the matrix.

1. Select Risk Acceptability Matrix from the left navigation panel. Then, click the Add New ⊞ button in the toolbar.
2. Select the risk rating likelihood and consequence.

   Note: The Likelihood and Consequence make up the x and y axes. By selecting a specific likelihood and consequence, you are identifying one specific square within the matrix. See the examples below.

3. Select the risk acceptability type.
4. Click Save to save the new record. When selecting the next state, click Active.

Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the matrix field cannot be used for new records.

Fig. 6: Risk Acceptability Matrix parameters

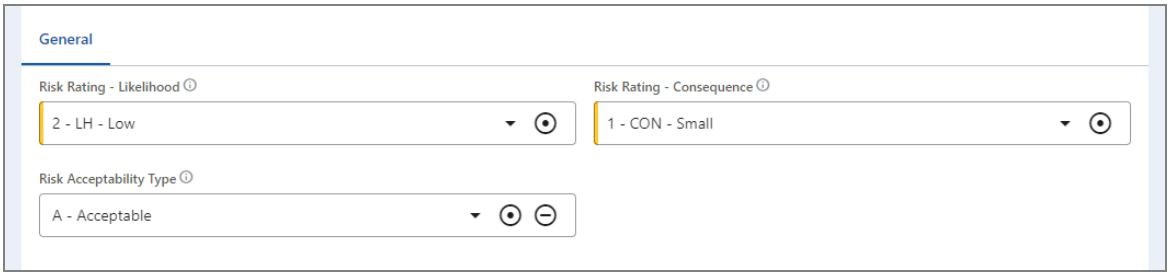
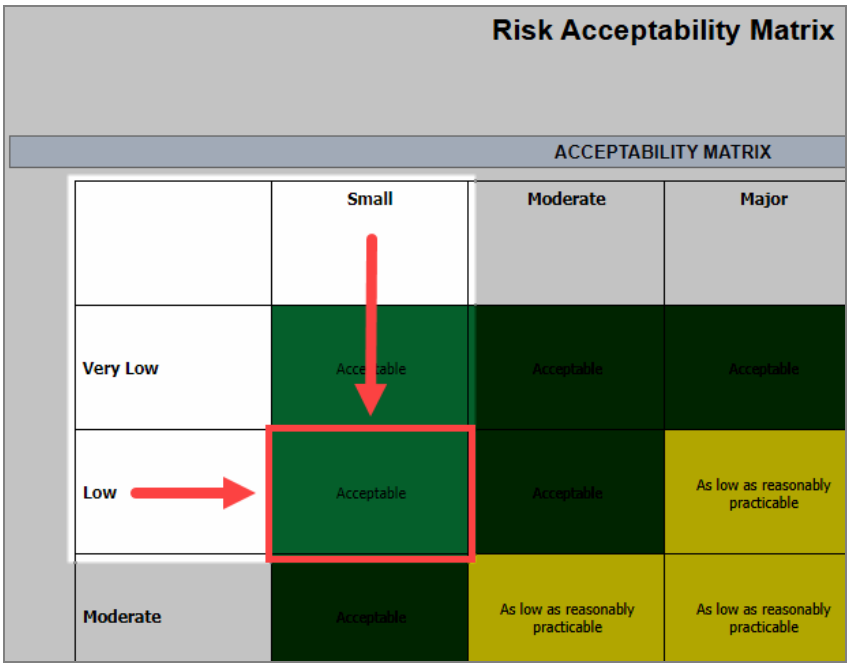


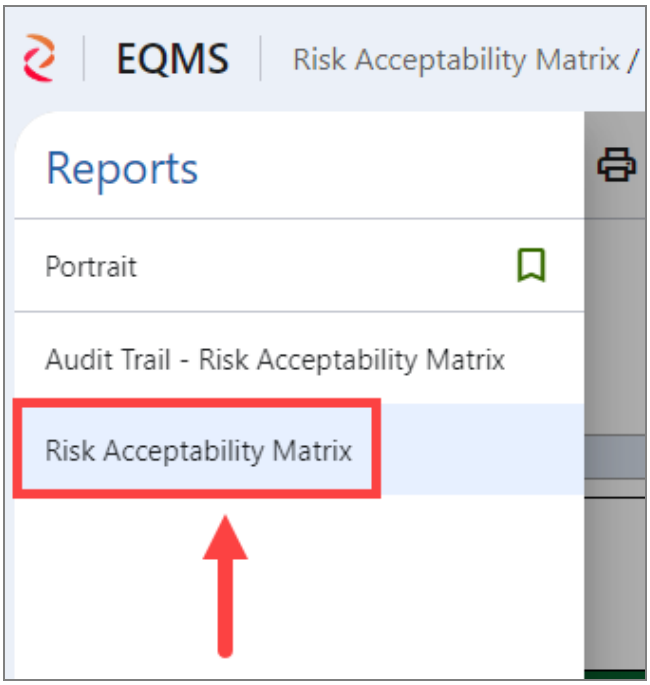
Fig. 7: Risk Acceptability Matrix field result



View the Risk Acceptability Matrix

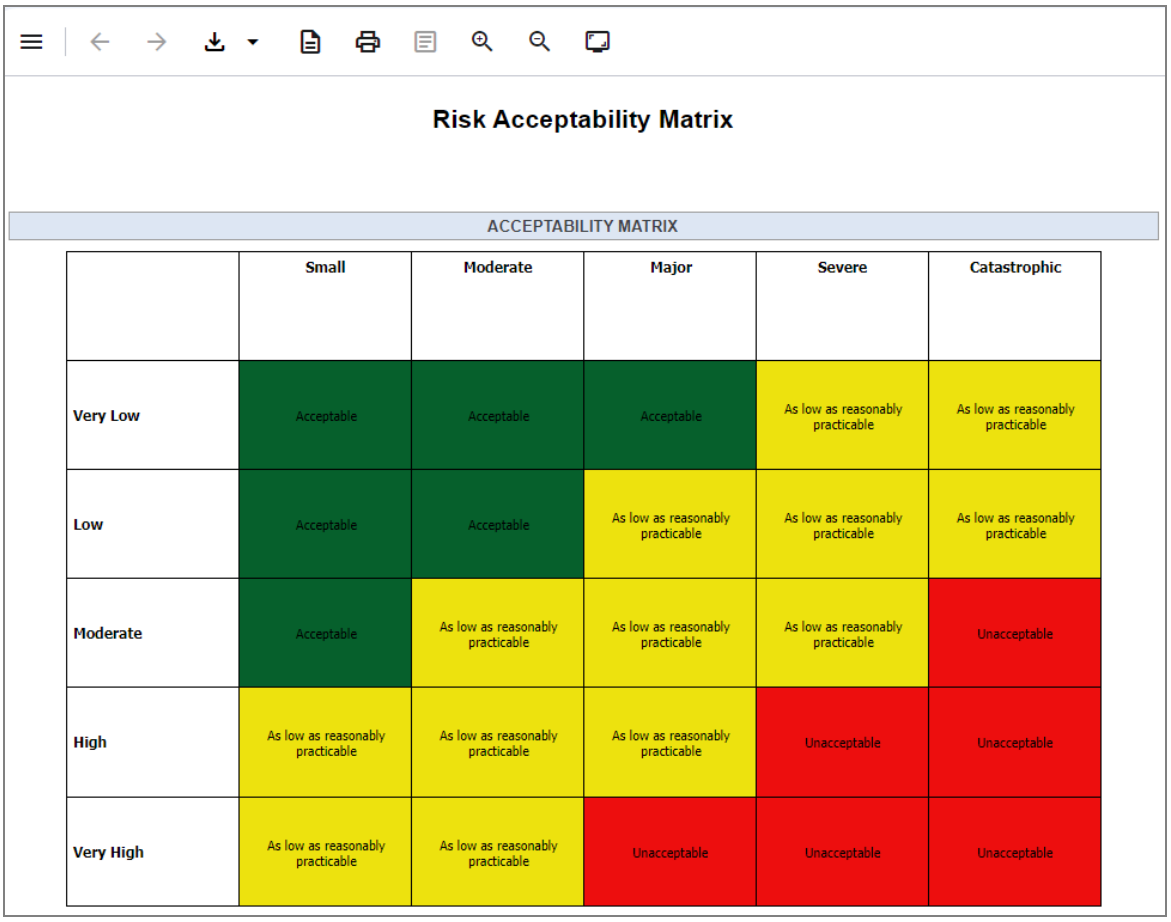
1. Select Risk Acceptability Matrix from the left navigation panel.
2. Click the Reports icon in the toolbar. The Report Viewer screen opens, and the Reports list expands on the left.
3. In the Reports list, select the Risk Acceptability Matrix report.

Fig. 8: Report Viewer



4. Once the report has loaded, you can view the matrix.
    - Scroll past the matrix to view the rating descriptions for likelihood ratings and consequence ratings.
    - Use the Report Viewer toolbar to export, print, or toggle the view of the report.
5. When finished, click the Close button at the bottom right of the screen.

Fig. 9: Risk Acceptability Matrix parameters



Risk Acceptability Matrix

ACCEPTABILITY MATRIX

	Small	Moderate	Major	Severe	Catastrophic
Very Low	Acceptable	Acceptable	Acceptable	As low as reasonably practicable	As low as reasonably practicable
Low	Acceptable	Acceptable	As low as reasonably practicable	As low as reasonably practicable	As low as reasonably practicable
Moderate	Acceptable	As low as reasonably practicable	As low as reasonably practicable	As low as reasonably practicable	Unacceptable
High	As low as reasonably practicable	As low as reasonably practicable	As low as reasonably practicable	Unacceptable	Unacceptable
Very High	As low as reasonably practicable	As low as reasonably practicable	Unacceptable	Unacceptable	Unacceptable

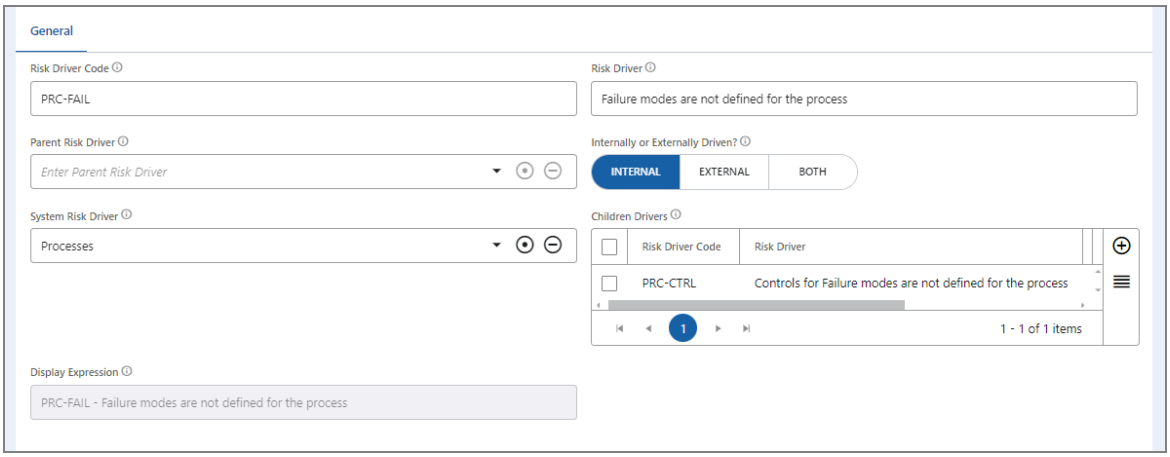
Risk Drivers

If a driver is an aspect of a business that affects a change on another aspect of the business, then risk drivers are drivers that create risk for the organization. Some high-level drivers include Reputation, Market, Infrastructure, and Finance. Risk drivers can also include sub-categories. Some examples of sub-categories for Infrastructure might include Internal Processes, IT Systems, Suppliers, or Natural Disasters.

Note that this process contains a field titled System Risk Driver. This is a list maintained by the system to identify what risk drivers (and therefore, what risks) are associated with specific parts of the system. The current list of system risk drivers includes APQP Projects, Change Requests, Complaints, Objectives, Processes, and Suppliers.

Risk drivers are used in the Risks and Risk Library processes for categorization purposes. See "Risks" on page 31 and "Risk Library" on page 30.

Fig. 10: Risk Drivers process screen

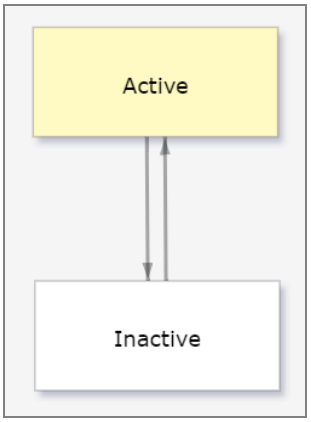


Risk Drivers States

This section defines each state available in the workflow for the Risk Drivers process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk driver that is actively used.

Inactive. A risk driver that is no longer in use.



Risk Driver Tasks

Adding a New Risk Driver

1. Select Risk Drivers from the left navigation panel. Then, click the Add New ⊞ button in the toolbar.
2. Enter values for the risk driver code and name. Notice how the Display Expression field combines the two values; this is how users will look up this risk driver.
3. To create a hierarchy of risk drivers, you can select a parent risk driver and create children drivers.

Note: Parent risk drivers are higher in the hierarchy, while children drivers branch off from the current risk driver.

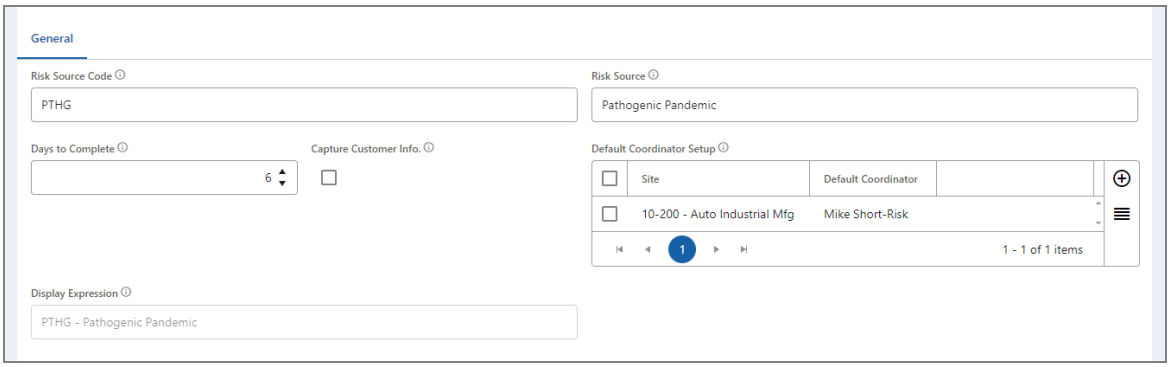
4. Select a system risk driver to establish a system context for the risk driver. This field pulls from a system-built list.
5. Select whether the risk driver is driven by internal or external forces.
6. Click Save to save the new record. When selecting the next state, click Active.

Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the risk driver cannot be used for new records.

Risk Events Sources

Risk events sources are areas from which a risk may potentially originate, such as Customer, Supplier, or Environment. Use this process to assign a risk event source-specific coordinator, add customer information fields to a risk event, and determine the number of days to complete events that originate from this source. See "Risk Events" on page 42.

Fig. 11: Risk Events Sources process screen

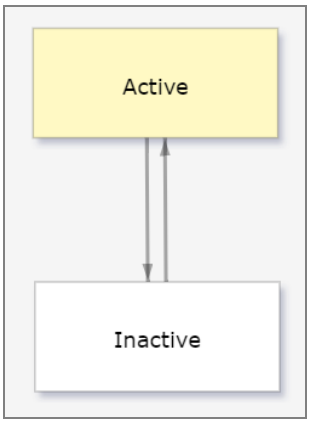


Risk Events Sources States

This section defines each state available in the workflow for the Risk Events Sources process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk event source that is actively used.

Inactive. A risk event source that is no longer in use.

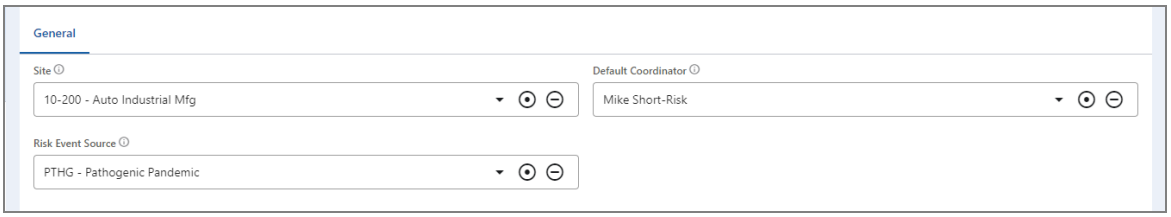


Risk Events Sources Tasks

Adding a New Risk Events Source

1. Select Risk Events Sources from the left navigation panel. Then, click the Add New button in the toolbar.
2. Enter values for the risk event source code and name. Notice how the Display Expression field combines the two values; this is how users will look up this risk event source.
3. Select the number of days to complete events that originate from this source. This number will be added to the initiated date within a risk event to determine that event's target completion date.
4. Select the "Capture Customer Info" check box to add customer contact fields to a risk event.
5. Assign a default coordinator for events that originate from this source. You may designate coordinators for each site.
    a. Click the Add New Item button. A new screen opens.
    b. Select the site and default coordinator.
    c. Click Save. When selecting the next state, click Active.

Fig. 12: Risk Event Sources Coordinator screen



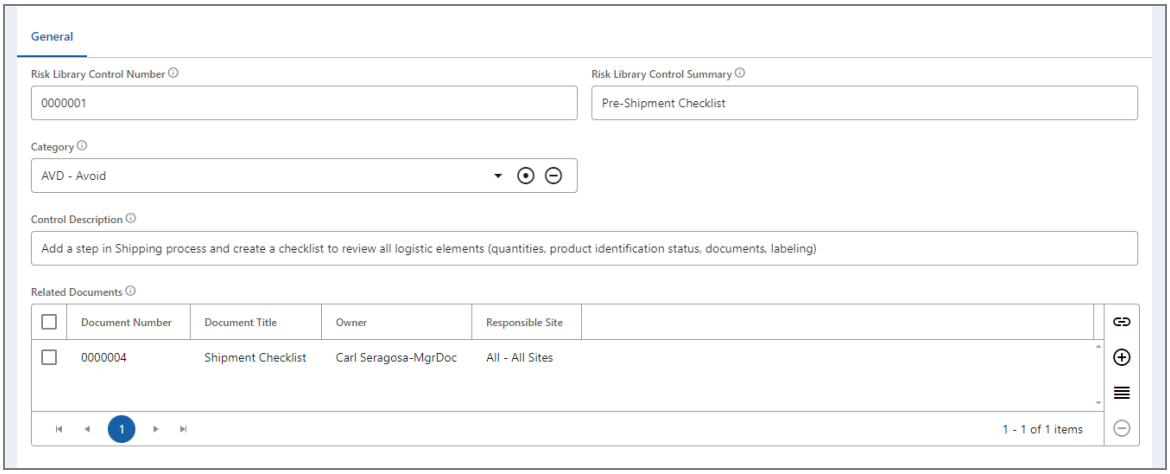
6. Back in the main process screen, click Save to save the new record. When selecting the next state, click Active.

Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the risk event source cannot be used for new records.

Risk Library Controls

Risk library controls are known controls used to help treat risk. Once a treatment has been implemented, it becomes a control; since one control may be able to treat multiple risks, users can add those controls to the library for easy selection on additional risks.

Fig. 13: Risk Library Controls process screen

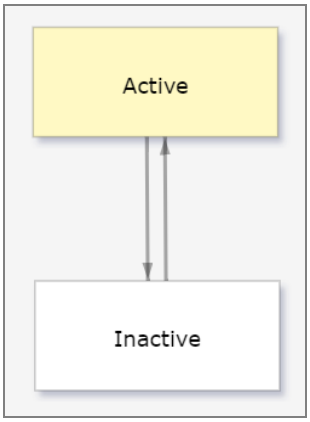


Risk Library Control States

This section defines each state available in the workflow for the Risk Library Control process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk library control that is actively used.

Inactive. A risk library control that is no longer in use.



Risk Library Control Tasks

Adding a New Risk Library Control

1. Select Risk Library Controls from the left navigation panel. Then, click the Add New button in the toolbar.
2. Create a summary that briefly describes the library control.
3. Select a category. This drop-down field pulls from the Risk Treatment Types process.
4. Enter a thorough description of the library control.
5. Select or add documents related to the library control.
6. Click Save to save the new record. When selecting the next state, click Active.

   Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the library control cannot be used for new records.

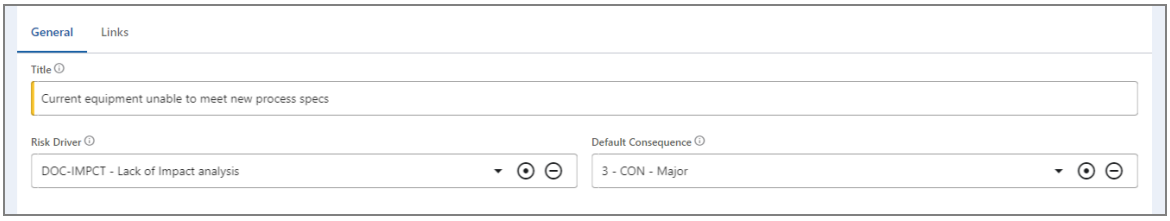
Chapter 3

Using the Risk Management Module

Risk Library

A risk library is an area to keep a list of known risks associated with a particular context within the software. The library provides a great way to help automate lessons learned regarding risk; when a new risk is identified that should apply to everything within a context, it can be added to the library. The setup of library items that should be evaluated during each assessment allows users to focus on the assessment of standardized risks versus trying to remember what risks to identify.

Fig. 14: Risk Library screen, General tab



The General tab is used to define the basic details of a risk library.

Fig. 15: Risk Library screen, Links tab

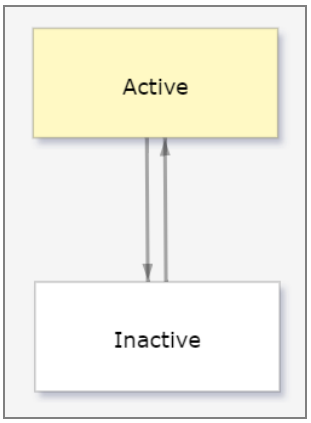
The Links tab connects the risk library to a change request type. Note that this is only valid for risk library items that apply to a risk driver that affects the system risk driver of change requests.

Risk Library States

This section defines each state available in the workflow for the Risk Library process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk library item that is actively used.

Inactive. A risk library item that is no longer in use.



Risk Library Tasks

Adding a New Risk Library

1. Select Risk Library from the left navigation panel. Then, click the Add New button in the toolbar.
2. Enter a title for the library.
3. Select a risk driver and default consequence for the library item.
4. Navigate to the Links tab. Select a change request type.

   Note: This is only valid for risk library items that apply to a risk driver that affects the system risk driver of change requests.

5. Click Save to save the new record. When selecting the next state, click Active.

   Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the library cannot be used for new records.

Risks

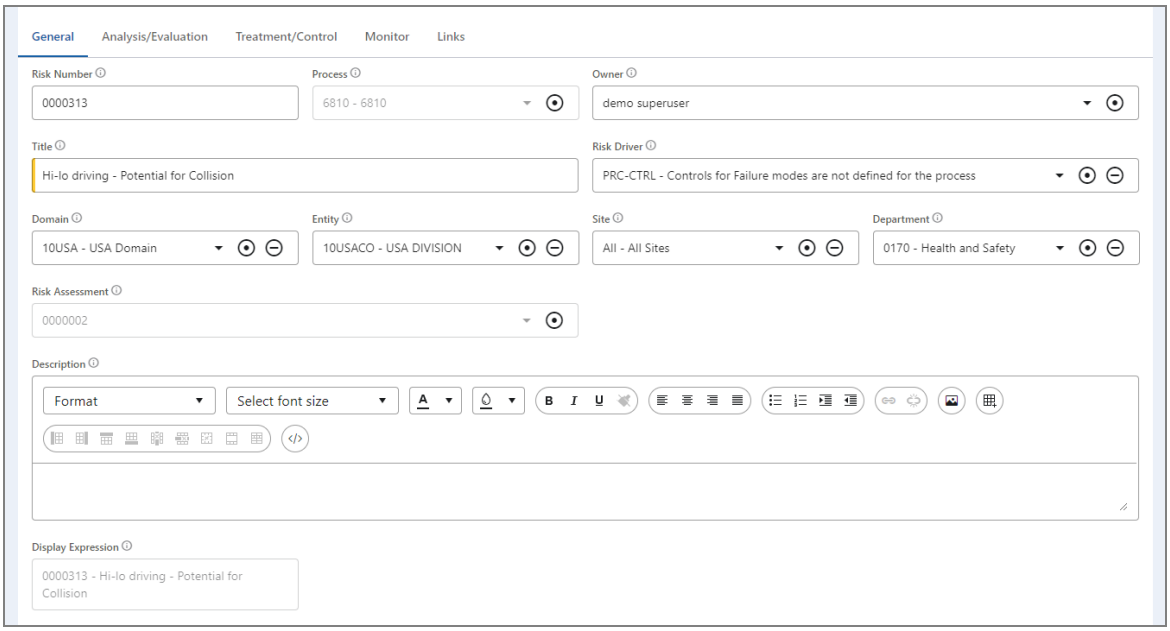
Risk is not inherently bad; it is defined as the "effect of uncertainty on objectives", with effect being a deviation from the expected – positive or negative. A company may calculate the risk of expanding the company, switching suppliers, or altering a process, to name a few neutral risks.

The Risks process is used to document risks, which are generally in reference to potential events and consequences (though risks may include actual events as well). After identifying the appropriate risks, you can then analyze and evaluate the risk to determine if their particular state warrants additional risk treatment or controls to be put in place.

Risks are used in the following processes to document the risks that have been identified as a part of the individual process:

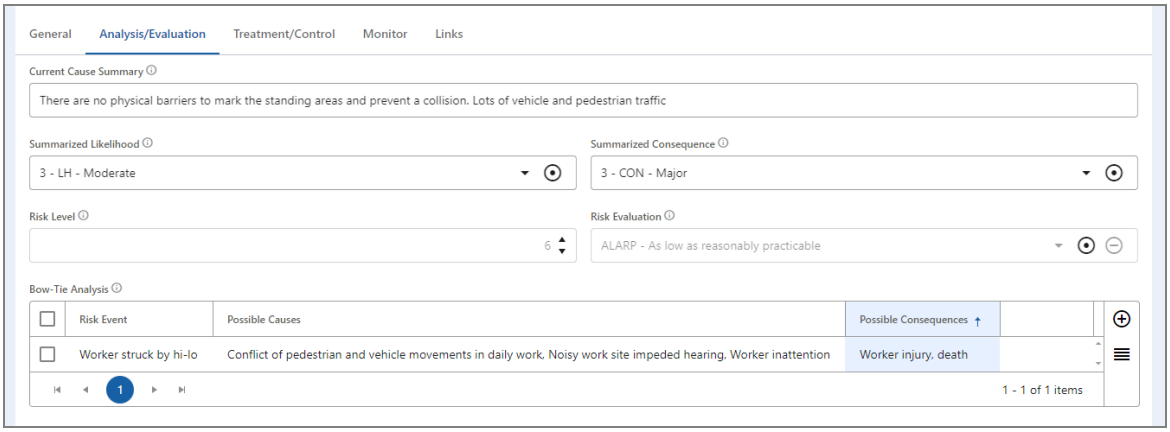
- Risk Assessments. Learn more on page 36.
- Risk Treatment. Learn more on page 39.
- Risk Controls. Learn more on page 40.
- Risk Events. Learn more on page 42.
- Risk Actions. Learn more on page 45.

Fig. 16: Risk screen, General tab



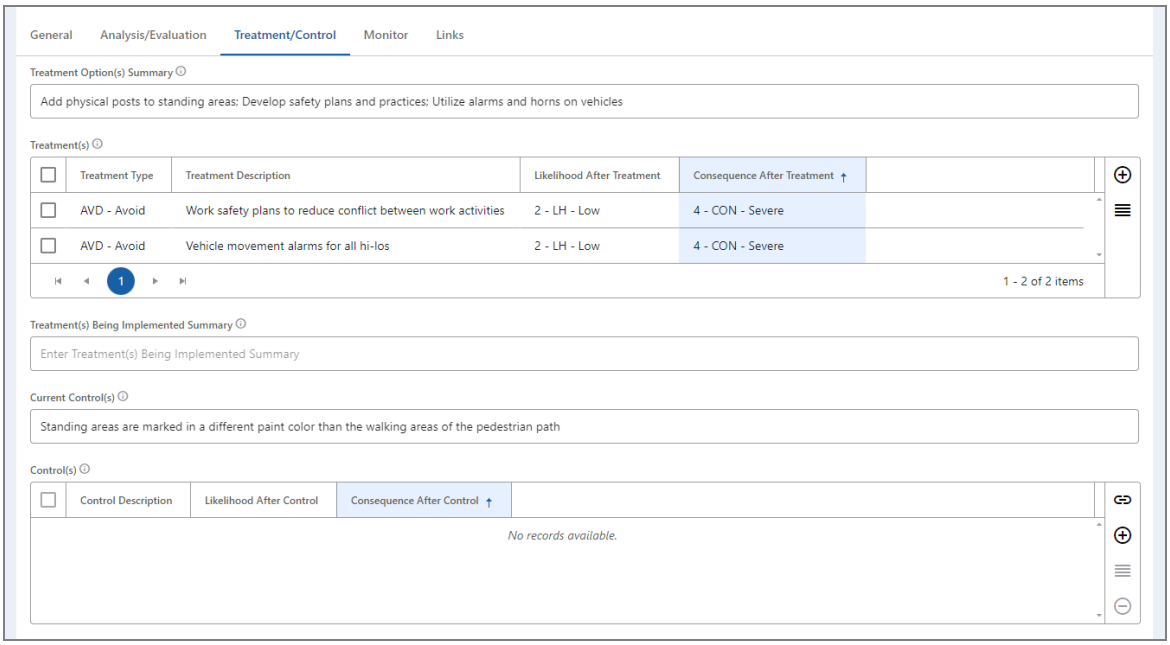
The General tab is used to define the basic details of a risk.

Fig. 17: Risk screen, Analysis/Evaluation tab



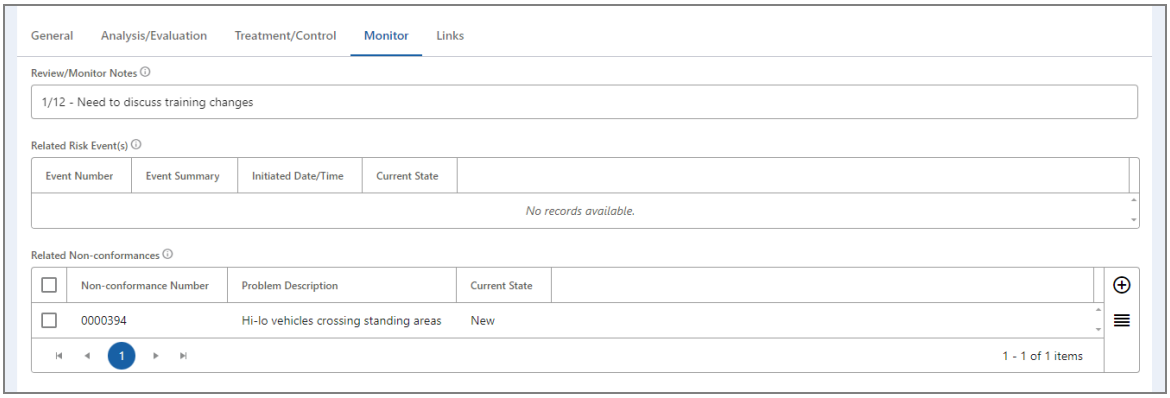
Use the Analysis/Evaluation tab to describe any known causes of a risk and determine the likelihood and consequence levels of that risk. This tab also contains the bow-tie analysis.

Fig. 18: Risk screen, Treatment/Control tab



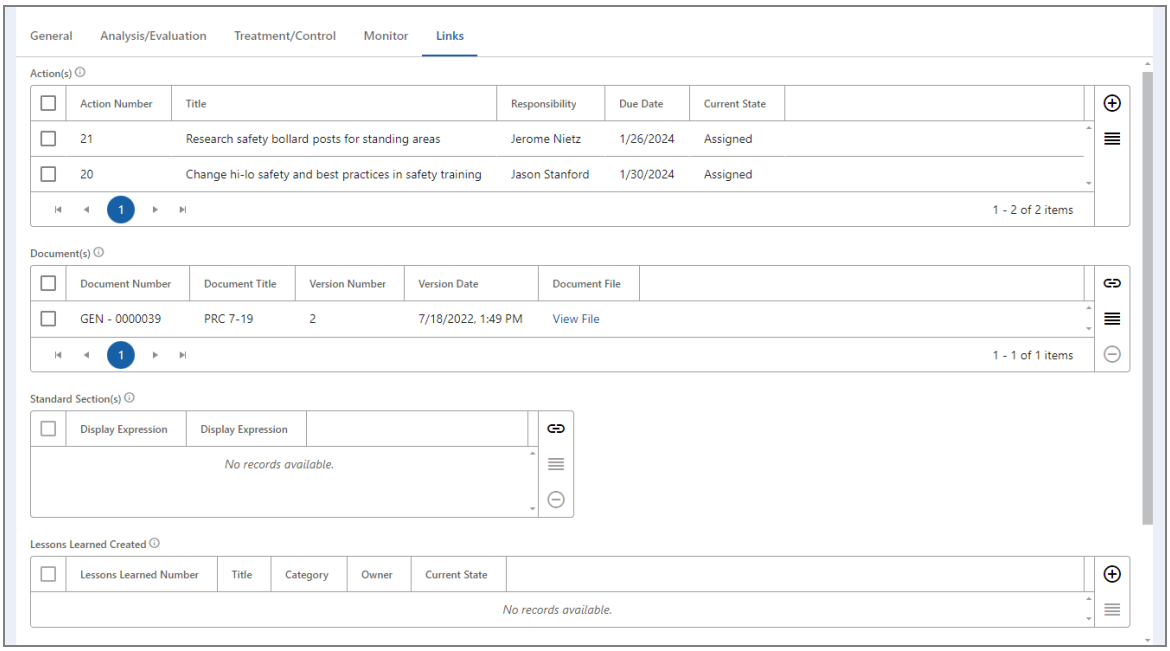
The Treatment/Control tab contains the treatment plans and risk controls for risks that require treatment.

Fig. 19: Risk screen, Monitor tab



Use the Monitor tab to document risk notes when reviewing or monitoring the risk. You can also link related risks and non-conformances to this tab.

Fig. 20: Risk screen, Links tab



Use the Links tab to link related actions, documents, lessons learned, and more.

Risk States

This section defines each state available in the workflow for the Risk process. See "State Change Security" on page 65 to learn more about how these states transition.

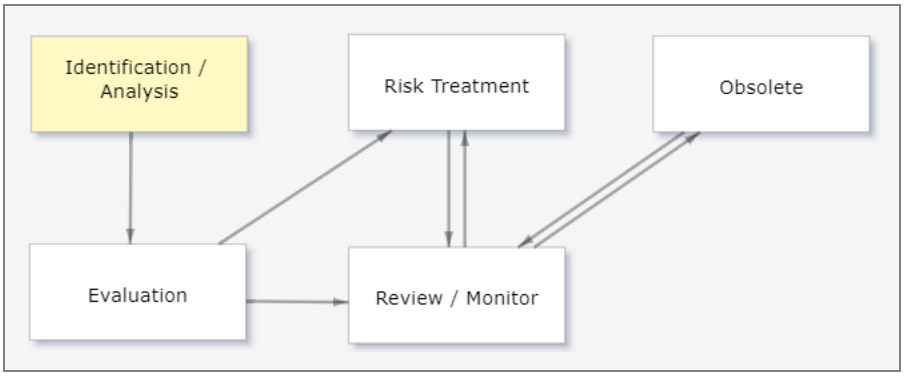
Identification/Analysis (Default). Identify and analyze the risk.

Evaluation. Evaluate the risk and determine the risk level.

Risk Treatment. Apply one or more risk treatments to bring the risk into an acceptable range.

Review/Monitor. Risk is being monitored and reviewed for changes.

Obsolete. Risk is no longer applicable to the organization.



Risk Tasks

Adding a New Risk

1. Select Risks from the left navigation panel. Then, click the Add New button in the toolbar.
2. Enter a title for the risk. The title should be a brief description of the risk so that it can be easily identified in a list.
3. Use the following drop-down fields as needed:
    - Risk Driver
    - Domain
    - Entity
    - Site
    - Department
    - Assessments
    - Process
    - Project
    - Change Request
    - Complaint
4. Enter a thorough description of the risk.
5. Navigate to the Analysis/Evaluation tab. Describe any known causes of the risk in the Current Cause Summary field.
6. Click Save to save the new record. When selecting the next state, click Evaluation.

Completing a Risk Evaluation and Treatment

1. In the Risk detail screen, navigate to the Analysis/Evaluation screen.
2. Use the Summarized Likelihood and Consequence drop-down fields to determine the current likelihood and consequence of the risk. The Risk Level and Risk Evaluation fields automatically calculate.
3. Create a bow tie analysis in the Bow-Tie Analysis field. See "Risk Bow Tie Analysis" on page 1 for more information.
4. Back in the Risk detail screen, click the Save button to save the record. When selecting the next state, click Risk Treatment.

Completing a Risk

1. In the Risk detail screen, navigate to the Treatment/Control tab.
2. Enter a summary of treatment options in the Treatment Options Summary field.
3. Create risk treatments in the Treatments field. See "Risk Treatments" on page 39 for more information.
4. In the fields that follow, summarize any treatments and controls currently being implemented.
5. Create or link risk controls in the Controls field. See "Risk Controls" on page 40 for more information.
6. Click Save to save the record.
7. Navigate to the Monitor tab. Enter any review or monitor notes. Add a related non-conformance, if applicable.

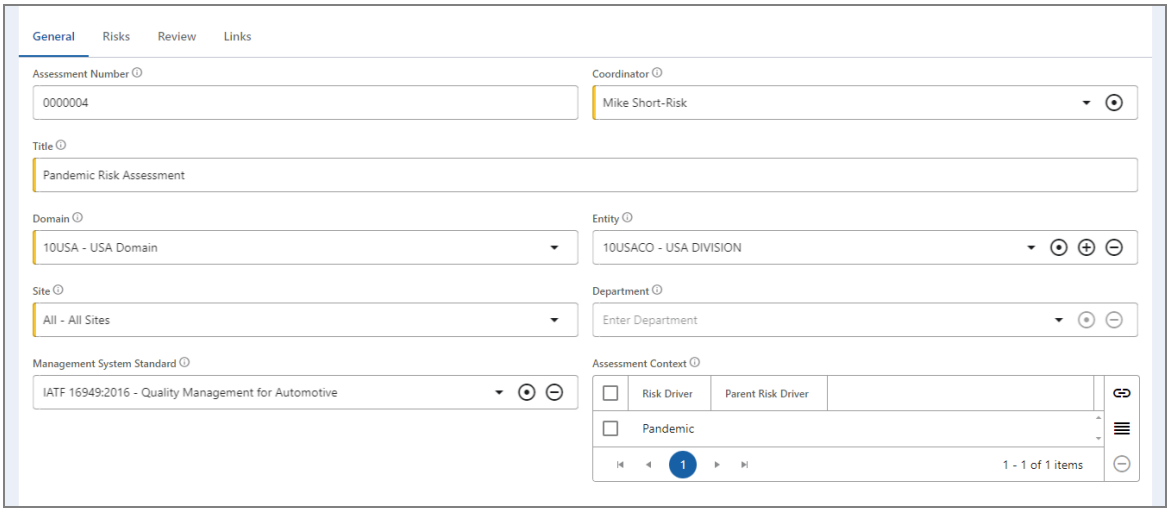
8. Navigate to the Links tab. Create or link any actions, documents, standard sections, or lessons learned as needed. See "Risk Actions" on page 45 for more information.
9. Click Save to save the record. When selecting the next state, click Review/Monitor.

Risk Assessments

Risk assessments allow you to combine the identification, analysis, and evaluation of risks into a group for easier management. A risk assessment could be for varying levels within the organization, from an overall organization perspective down to the assessment of an individual process.

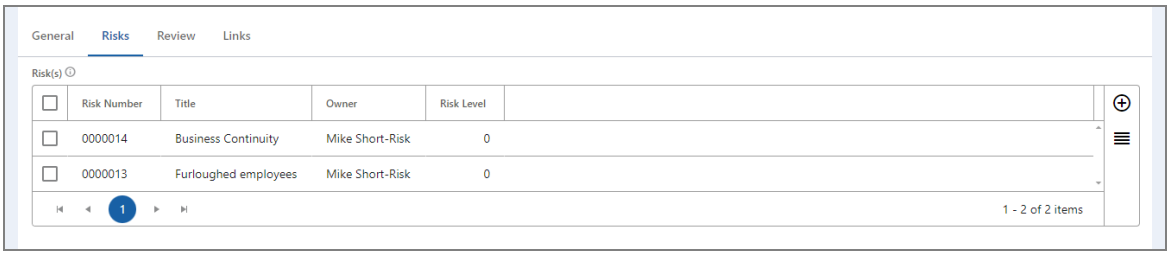
Risk assessments can identify a risk, and are therefore connected to that process. See "Risks" on page 31. Risk assessments are also linked to risk actions. See "Risk Actions" on page 45.

Fig. 21: Risk Assessments screen, General tab



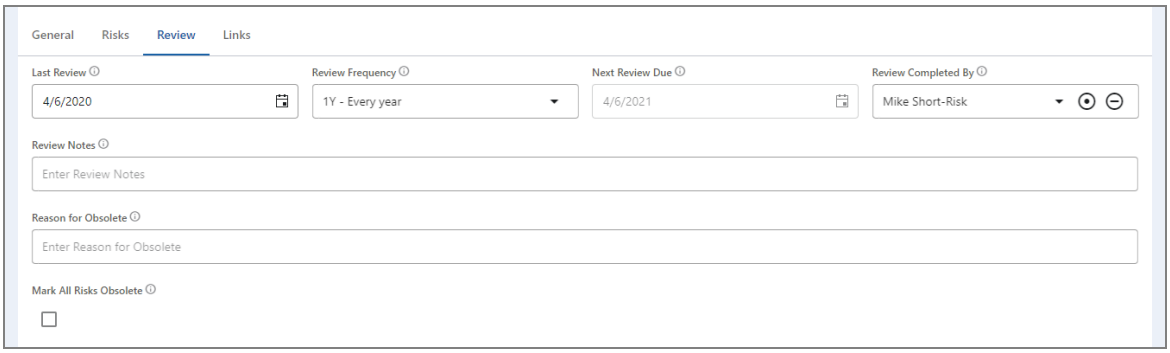
The General tab is used to define the basic details of a risk assessment.

Fig. 22: Risk Assessments screen, Risks tab



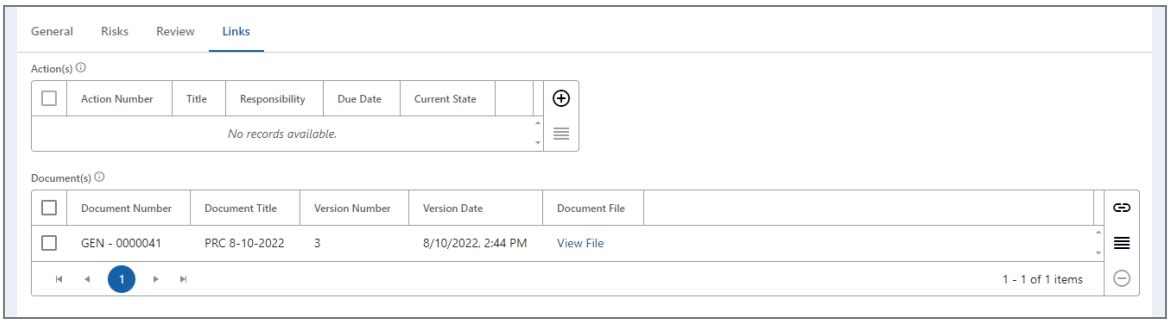
If a risk has been identified as part of the risk assessment, then create or link that risk to the Risks tab.

Fig. 23: Risk Assessments screen, Review tab



Use the Review tab to assign a user to review the risk assessment at a scheduled frequency. This tab also allows you to mark risks as Obsolete.

Fig. 24: Risk Assessments screen, Links tab



Use the Links tab to create actions and link documents to the risk assessment.

Risk Assessment States

This section defines each state available in the workflow for the Risk Assessment process. See "State Change Security" on page 65 to learn more about how these states transition.

Identification (Default). Risks are being identified for the risk assessment.

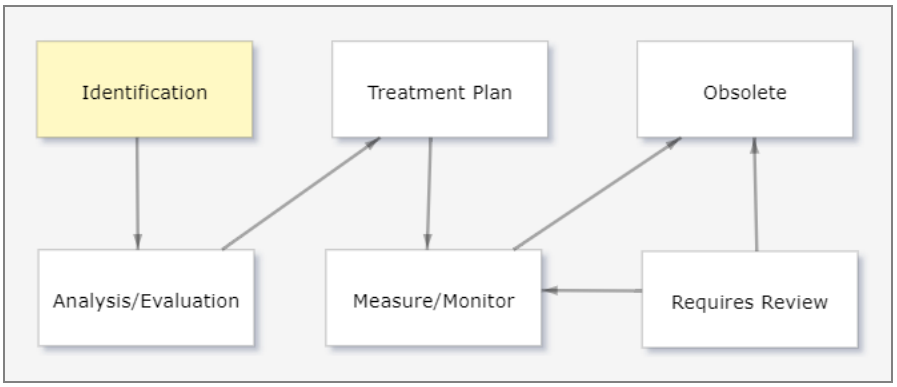
Analysis/Evaluation. For each risk identified, the risks are being evaluated to determine the risk priority.

Treatment Plan. For risks whose current risk priority is beyond our current risk appetite, treatment plans are being devised.

Measure/Monitor. Risks are being measured and monitored, the initial assessment is complete.

Requires Review. The risk assessment requires review.

Obsolete. The risk assessment is no longer applicable.



Risk Assessment Tasks

Adding a New Risk Assessment

1. Select Risk Assessments from the left navigation panel. Then, click the Add New button in the toolbar.
2. Enter a title for the assessment.
3. Select a department that the assessment applies to. The Coordinator, Domain, Entity, and Site fields default to the current user's settings.
4. Select the management system standard that this assessment is intended to analyze for risks.
5. In the Assessment Context field, click the Link button. A new window appears.
6. Select one or more risk drivers that define the context for the assessment. Click OK.
7. Click Save to save the new record. When selecting the next state, click Identification.

Completing a Risk Assessment

1. In the Risk Assessment detail screen, navigate to the Risks tab.
2. Click the Add New Item button to add any risks that have been identified as part of the assessment. See "Risks" on page 31 to learn more about added risks.
3. Navigate to the Review tab. Select a review frequency and assign a user to complete the review.
4. Navigate to the Links tab. Add actions that should be completed to close out the assessment. See "Risk Actions" on page 45 to learn more about adding actions.
5. If pertinent, link any documents related to the risk assessment.
6. Click Save to save the record. When selecting the next state, click Measure/Monitor.

Reviewing a Risk Assessment

A review frequency is set when the risk assessment is created. When the Next Review Due field matches the current date, the coordinator receives a notification that they must review the assessment.

1. Double-click the risk assessment to be modified or open the file from the Assignment tab of the inbox.
2. Once the changes have been made, navigate to the Review tab and update the information to reflect the latest review date and reviewer.

3. Update the review notes based on the changes. Previous review notes are captured in the audit trial.
4. Click Save to save the risk assessment. When selecting the next state, click Measure/Monitor.

Obsoleting a Risk Assessment

1. In the risk assessment detail screen, navigate to the Review tab.
2. Document the reason or any notes for the risk assessment becoming obsolete.
3. Select the "Mark All Risks Obsolete" check box. This will move the state of all associated risks to Obsolete, as well as the current risk assessment.
4. Click Save to save the risk assessment. When selecting the next state, click Obsolete.

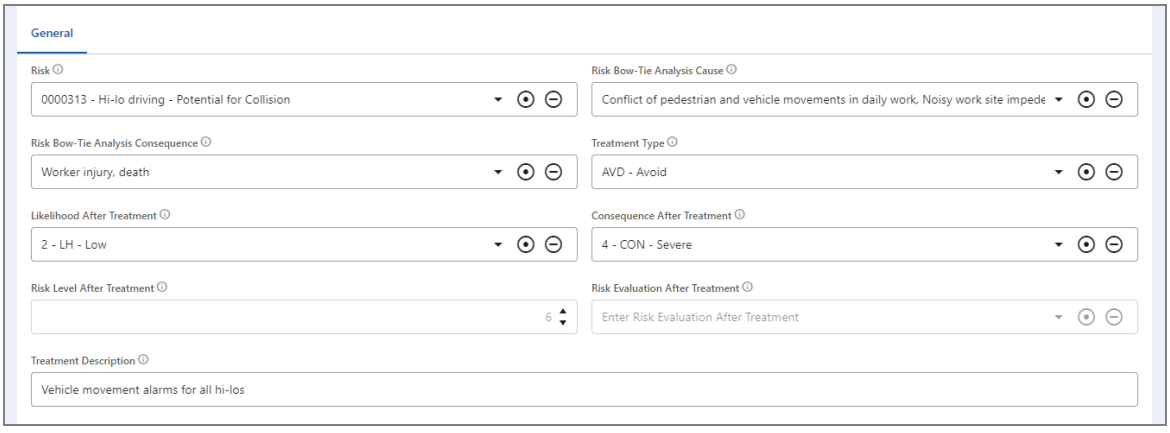
Risk Treatments

Risk treatment is the way an organization decides to treat or modify a risk. Sometimes an organization may accept the risk, or even share the risk with another organization, such as a supplier. A risk may have more than one treatment, as the best treatment may be an expensive long-term plan that must still be mitigated in the short term. Once a treatment has been implemented, it becomes a risk control.

Risk treatments are used in the following processes of the Risk Management module:

- Risks. Learn more on page 31.
- Risk Controls. Learn more on page 40.
- Risk Bow Tie Analysis Cause. Learn more on page 50.
- Risk Bow Tie Analysis Consequence. Learn more on page 51.

Fig. 25: Risk Treatments process screen

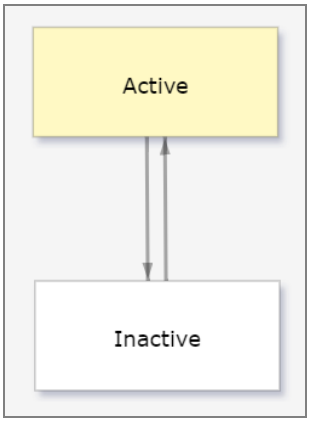


Risk Treatments States

This section defines each state available in the workflow for the Risk Treatments process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk treatment that is actively used.

Inactive. A risk treatment that is no longer in use.



Risk Treatments Tasks

Adding a New Risk Treatment

1. In a Risk record detail screen, click the Add New Item button in the Treatments field. A new screen opens.
2. Select the associated risk. If you created this treatment from a Risk record, then the Risk field is automatically populated.
3. Select the associated risk bow tie analysis cause or consequence.

   Note: These fields are only applicable if the risk contains a bow tie analysis.

4. Select the appropriate treatment type.
5. Select the estimated likelihood and consequence for the risk if this treatment is implemented.
6. Enter a description of the treatment.
7. Click Save to save the new record. When selecting the next state, click Active.

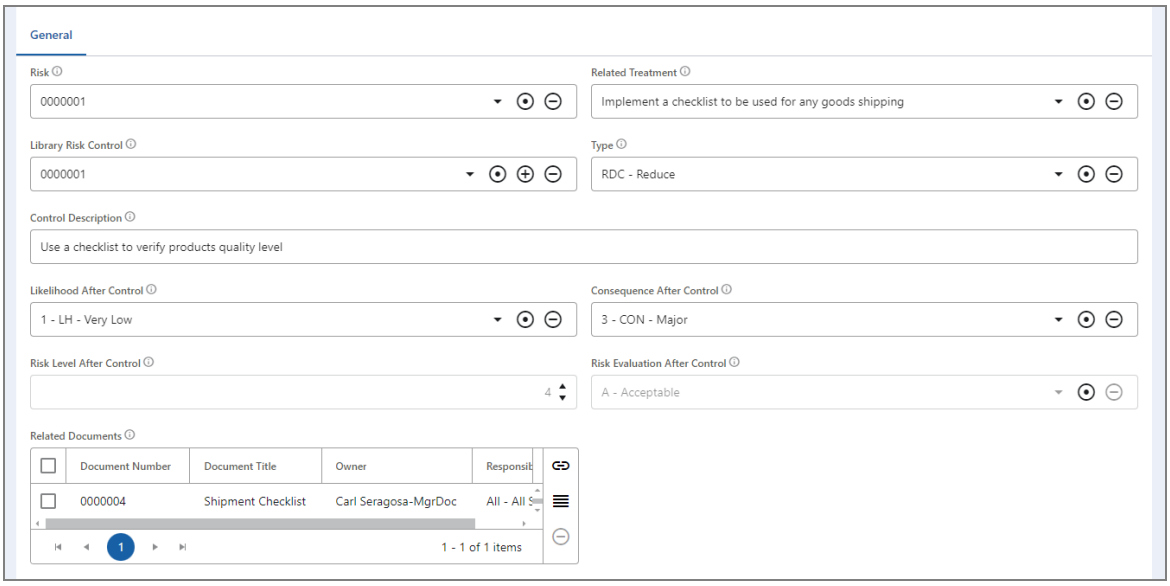
   Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the treatment cannot be used for new records.

Risk Controls

Risk controls identify and document treatments that have been implemented as controls for a risk. Controls also identify what the new likelihood and consequence are, based on that control being in place.

Risk controls are used in the Risk process. See "Risks" on page 31.

Fig. 26: Risk Controls process screen

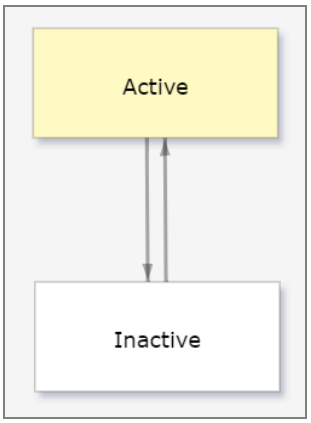


Risk Controls States

This section defines each state available in the workflow for the Risk Controls process. See "State Change Security" on page 65 to learn more about how these states transition.

Active (Default). A risk control that is actively used.

Inactive. A risk control that is no longer in use.



Risk Controls Tasks

Adding a New Risk Control

1. In a Risk record detail screen, click the Add New Item button in the Control field. A new screen opens.
2. Select a related risk, treatment, type, and library risk control.

Note: If you created this control from a Risk record, then the Risk field is automatically populated.

3. Enter a description of the control.
4. Determine the likelihood and consequence of the risk as a result of the control being in place.
5. Select the risk evaluation as a result of the control.
6. Select documents related to the control.
    a. Click the Link button. A new window opens.
    b. Select the check box beside each document you want to include.
    c. Click OK.
7. Click Save to save the new record. When selecting the next state, click Active.

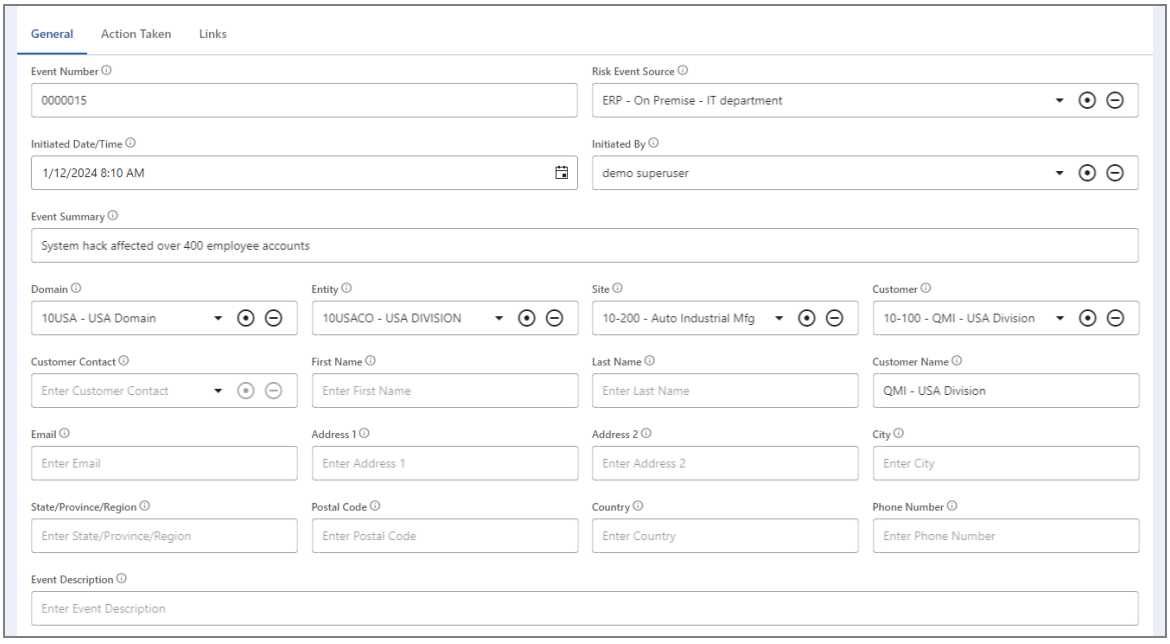
Note: You can toggle between Active and Inactive as needed. When the state is Inactive, the control cannot be used for new records.

Risk Events

Risk events, often referred to as incidents, are events that have occurred and must be resolved to prevent future consequences to the organization. As an example, if an earthquake strikes and affects three of the top suppliers, a risk event details what the customer must do to prevent additional consequences, such as find new suppliers, make the parts that the suppliers were supplying internally, and so on.

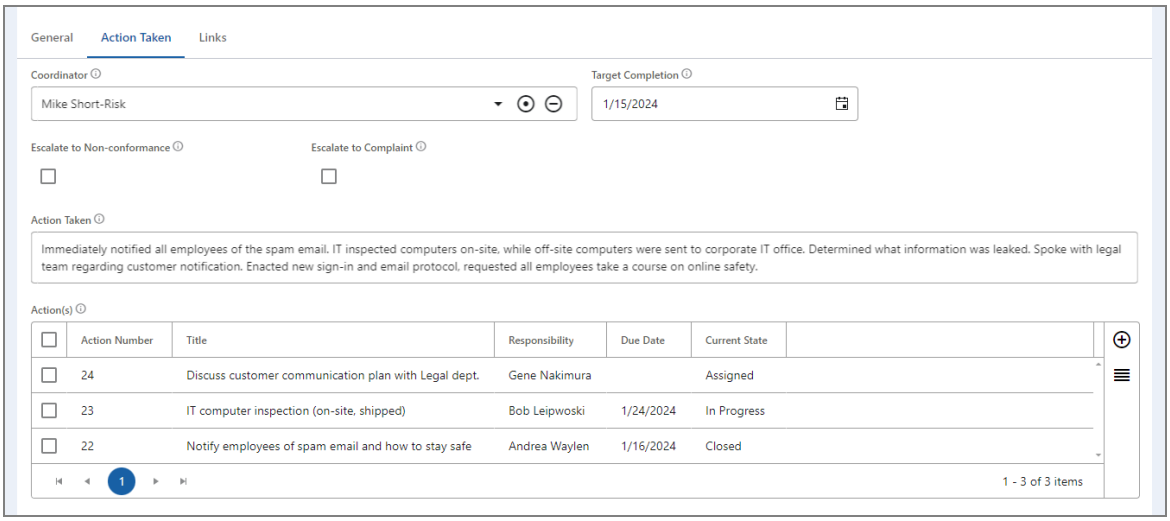
Risk events are used by risks as part of the monitoring process. See "Risks" on page 31. Risk events link to risk actions, which track the completion of the risk event. See "Risk Actions" on page 45.

Fig. 27: Risk Events screen, General tab



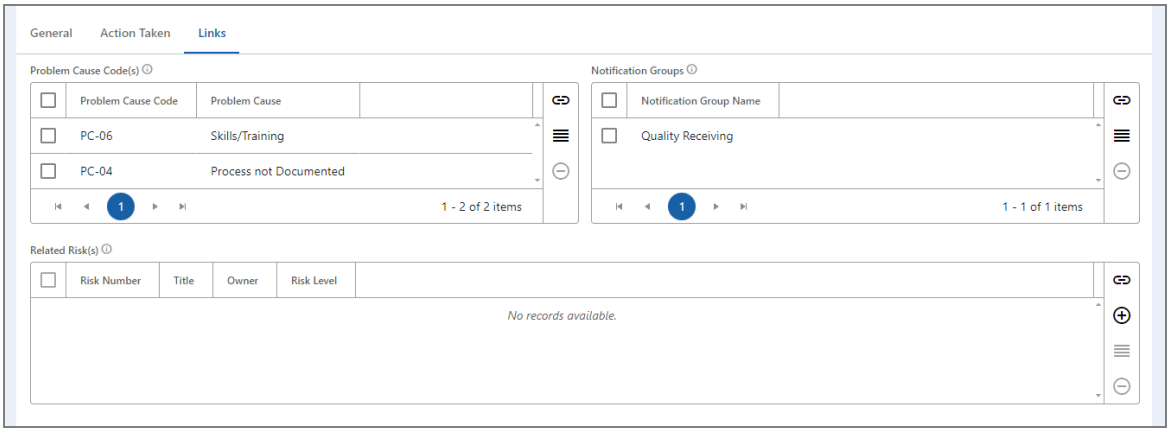
The General tab is used to define the basic details of a risk event.

Fig. 28: Risk Events screen, Action Taken tab



Use the Action Taken tab to assign actions to remedy the situation and determine if the event needs to be escalated to a non-conformance or complaint.

Fig. 29: Risk Events screen, Links tab



Use the Link tab to associate problem cause codes, notification groups, and related risks with the risk event.

Risk Events States

This section defines each state available in the workflow for the Risk Events process. See "State Change Security" on page 65 to learn more about how these states transition.

New (Default). The default state for a newly created incident.

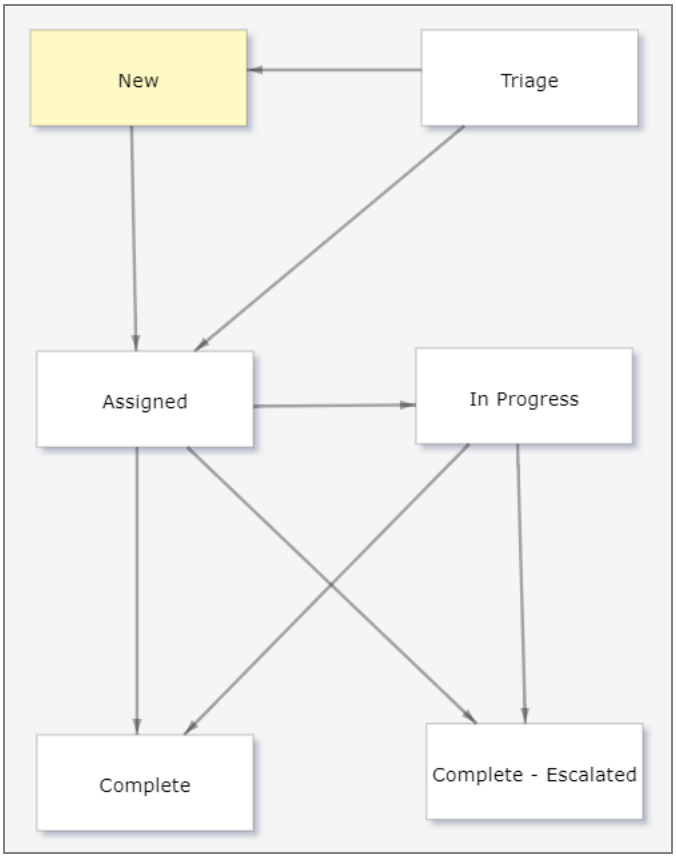
Triage. The default state for incidents created outside of the QMS system. This allows the incident to be triaged before moving to Assigned.

Assigned. The incident is ready to be actioned.

In Progress. Select this state when you have begun work on the incident.

Complete. All actions have been completed to resolve the incident.

Complete – Escalated. Select this state to escalate the incident to one of the escalation options.



Risk Events Tasks

Adding a New Risk Event

1. Select Risk Events from the left navigation panel. Then, click the Add New button in the toolbar.
2. Select a risk event source.
3. Enter a summary of the event.
4. Select a customer and customer contact. If the customer contact does not exist, then you can enter their name and contact information in the fields that follow.
5. Enter more details of the event in the Event Description field.
6. Navigate to the Links tab. Select any relevant problem cause codes.
7. Select one or more groups to notify of the new risk event and when it is complete.
8. Select one or more risks associated with this event.
9. Click Save to save the new record. When selecting the next state, click Assigned.

Completing a Risk Event

1. In the Risk Event detail screen, navigate to the Action Taken tab.
2. Click the Add New Item ⊕ button in the Actions field to assign actions to resolve the risk event. See "Risk Actions" below for more information on adding a new action.
3. If necessary, select the "Escalate to Non-conformance" or "Escalate to Complaint" check box.
4. Click Save to save the record. When selecting the next state, click In Progress.
5. Once the actions are completed, enter a description of what actions were taken.
6. Click Save to save the record. When selecting the next state, click Complete. If you selected either of the escalation check boxes, then click Complete – Escalated.

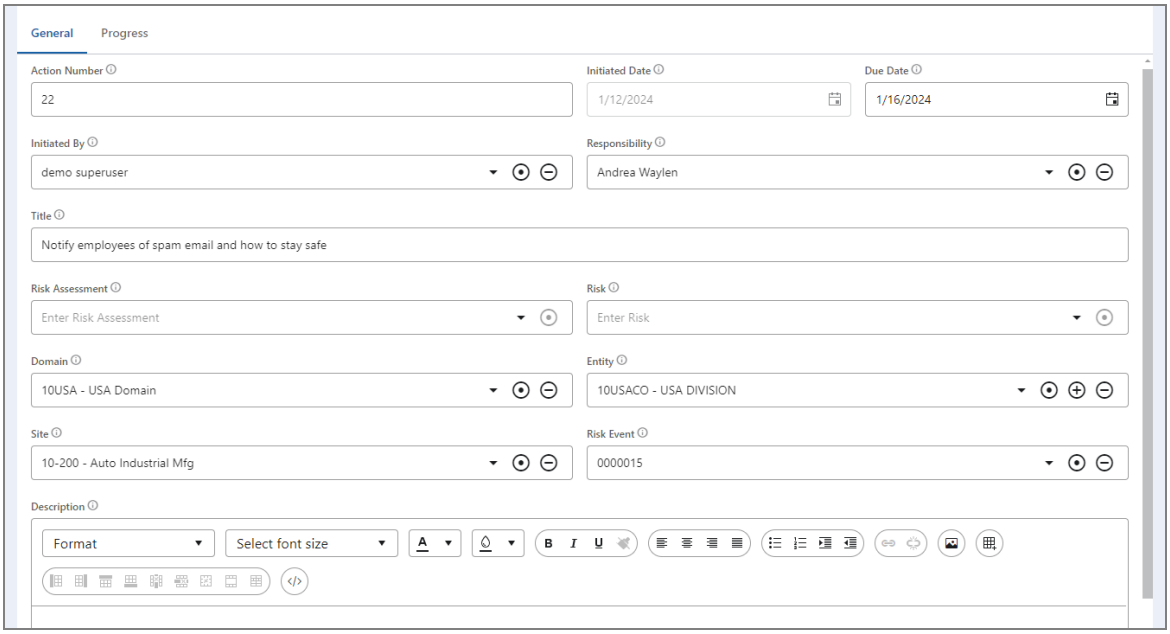
Risk Actions

Risk actions support the adding and tracking of actions related to a risk or risk assessment. Actions allow users to define items that must be completed to close out a particular risk or assessment.

Risk actions are used in the following processes of the Risk Management module:

- Risks. Learn more on page 31.
- Risk Assessments. Learn more on page 36.
- Risk Events. Learn more on page 42.

Fig. 30: Risk Actions screen, General tab



The General tab is used to define the basic details of a risk action.

Fig. 31: Risk Actions screen, Progress tab

The Progress tab shows the completed date an any progress notes made.

Risk Actions States

This section defines each state available in the workflow for the Risk Actions process. See "State Change Security" on page 65 to learn more about how these states transition.

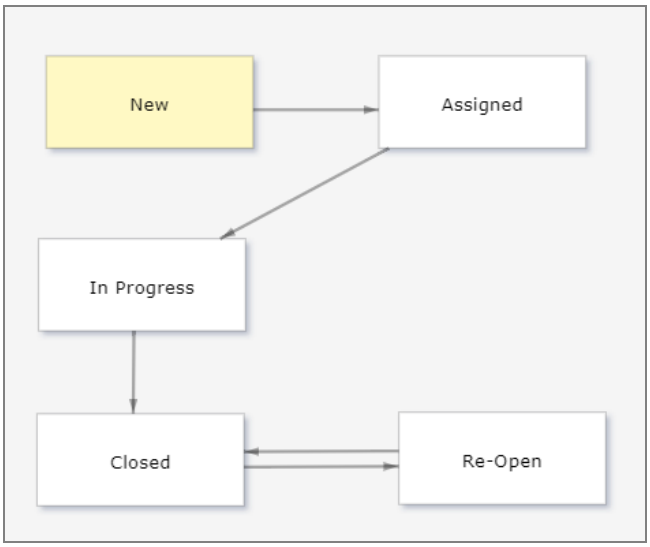
New (Default). A newly created risk action that has not yet been evaluated.

Assigned. A risk action that has not been assigned for completion yet.

In Progress. The risk action is in progress but not yet complete.

Closed. The risk action has been completed and closed.

Re-Open. The risk action has been re-opened for reassessment.



Risk Actions Tasks

Adding a New Risk Action

1. There are two ways to add a risk action:
    a. Select Risk Actions from the left navigation panel. Then, click the Add New button in the toolbar.
    b. In a Risk, Risk Events, or Risk Assessments detail screen, click the Add New Item button in the Actions field.
2. If you created the risk action through another process, then that process is indicated in the Risk Assessment, Risk, or Risk Event field.
3. Select the due date.
4. Select the person responsible for completing the risk action.
5. Enter a title for the risk action.
6. Enter a thorough description of the risk action.
7. Click Save to save the new record. When selecting the next state, click Assigned.

Completing a Risk Action

1. Open the risk action, either from the navigation panel or from the Inbox.
2. Navigate to the Progress tab. As you work on the risk action, track your progress in the Progress Notes field. When saving changes, select the state In Progress.
3. When you are finished with the risk action, select the date of completion.
4. Click Save to save the record. When selecting the next state, click Closed.

Note: If the risk action requires an update, click the state Re-Open.

Chapter 4

Risk Bow Tie Analysis

Risk Bow Tie Analysis

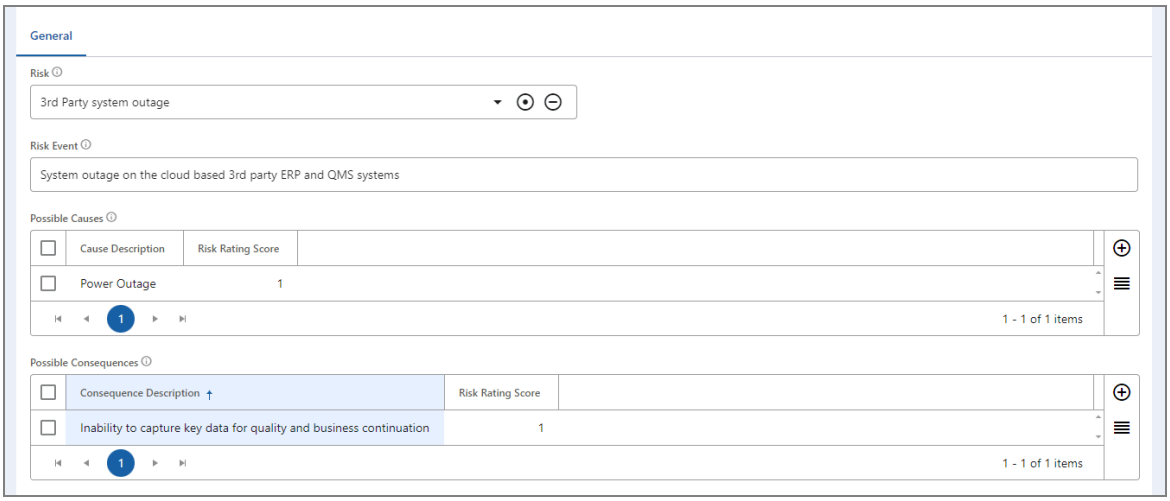
A bow tie analysis is conducted to help determine the likelihood and consequence for a risk. It asks:

- What causes could lead to this outcome occurring?
- What consequences could ensue if the outcome does occur?
- What treatments could possibly help achieve our goal?

The analysis organizes the content into a three-part diagram resembling a bow tie. Causes are grouped together in a triangle shape on the left. The risk event is alone in the center. Consequences are organized into a triangle on the right. Treatments are listed alongside each cause and each consequence. It gives a striking visual picture of the risk and what is being done to treat that risk.

The risk bow tie analysis is used in the Risks process as part of the analysis and evaluation state. See "Risks" on page 31.

Fig. 32: Risk Bow Tie Analysis process screen



Risk Bow Tie Analysis States

This section defines each state available in the workflow for the Risk Bow Tie Analysis process.

There are no states identified.

Risk Bow Tie Analysis Tasks

Adding a New Risk Bow Tie Analysis

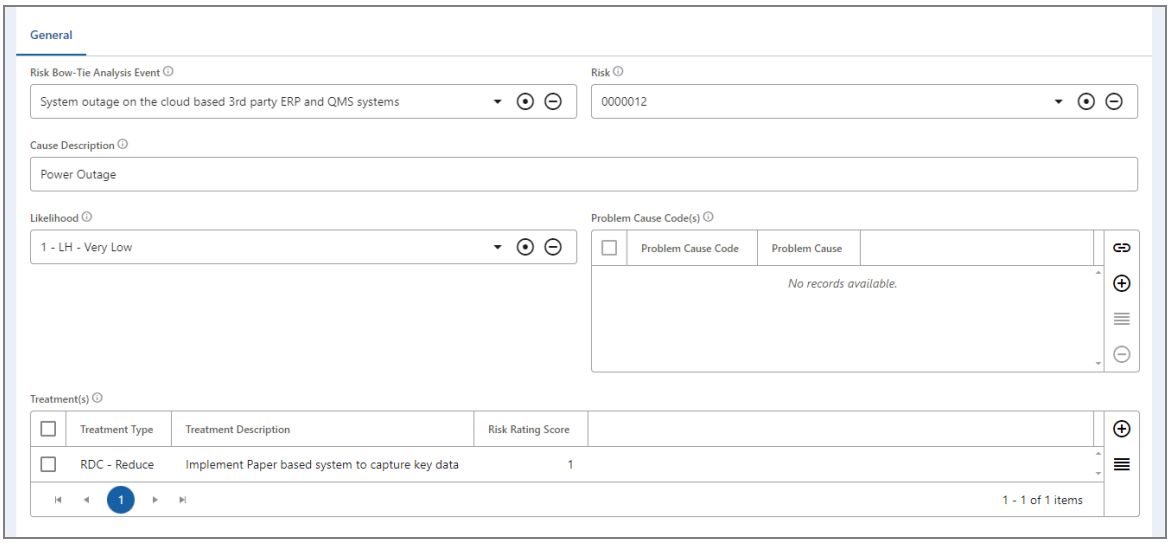
1. In a Risk record, navigate to the Analysis/Evaluation tab and click the Add New Item ⊕ button in the Bow-Tie Analysis field.
2. Enter a title description in the Risk Event field.

3. Click Save to save the record. The screen returns to the Risk record; navigate back to the bow tie analysis detail screen.
4. Click the Add New Item button in the Possible Causes and Possible Consequences fields. To learn more about adding causes and consequences, see "Risk Bow Tie Analysis Cause " below and "Risk Bow Tie Analysis Consequence" on the facing page.
5. Click Save to save the new record. When selecting the next state, click Active.

Risk Bow Tie Analysis Cause

In a risk bow tie analysis, the cause determines why the risk happened or potentially could happen. It is assigned a likelihood and may be designated a treatment. See "Risk Bow Tie Analysis" on the previous page and "Risk Treatments" on page 39.

Fig. 33: Risk Bow Tie Analysis Cause process screen



Risk Bow Tie Analysis Cause States

This section defines each state available in the workflow for the Risk Bow Tie Analysis Cause process.

There are no states identified.

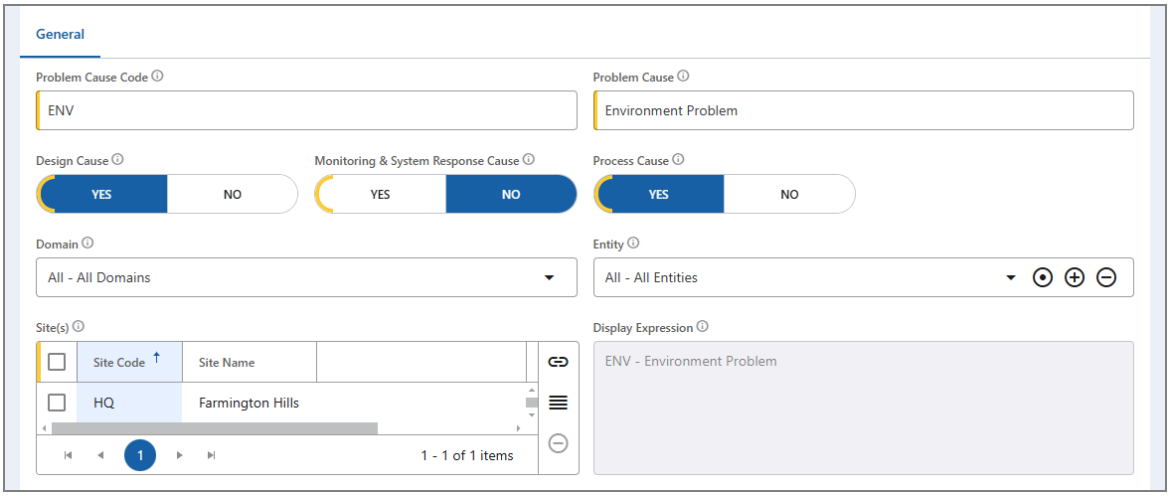
Risk Bow Tie Analysis Cause Tasks

Adding a New Risk Bow Tie Analysis Cause

1. In a Risk Bow Tie Analysis detail screen, click the Add New Item button in the Possible Causes field. A new screen opens.
2. Enter a cause description.
3. Select the likelihood of this cause.
4. Select or add problem cause codes.

5. If adding a new problem cause code:
    a. In the new screen, enter a problem cause code and name.
    b. Click the Link button and select any sites that apply. Then click OK.
    c. Click Save to save the record. When selecting the next sate, click Active.

Fig. 34: Problem Causes screen

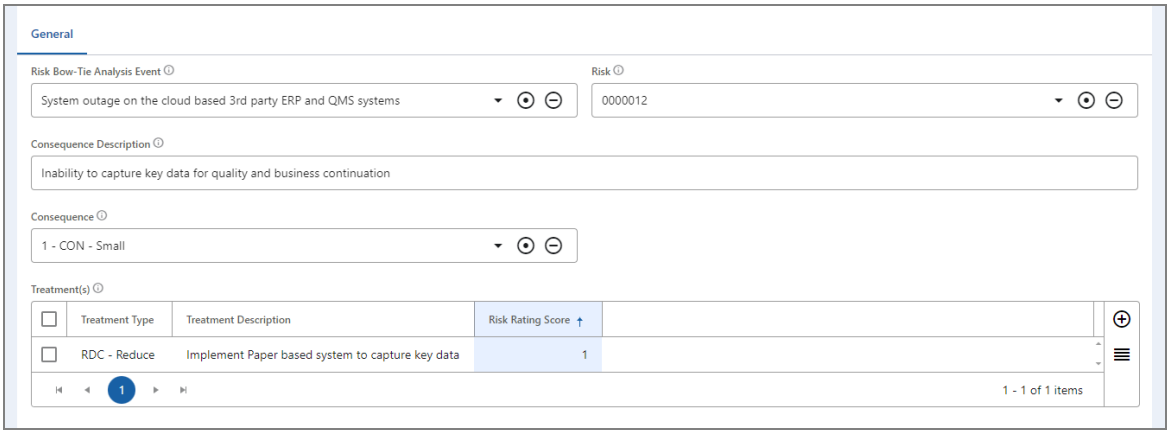


6. Back in the main detail screen, click Save to save the record. The screen returns to the Risk Bow Tie Analysis record; navigate back to the cause record.
7. Click the Add New Item button in the Treatments field. See "Risk Treatment Types" for more information on how to fill out a treatment record.
8. Click Save to save the new record.

Risk Bow Tie Analysis Consequence

In a risk bow tie analysis, the consequence determines the possible outcomes of a risk. It is assigned a likelihood and may be designated a treatment. See "Risk Bow Tie Analysis" on page 49 and "Risk Treatments" on page 39.

Fig. 35: Risk Bow Tie Analysis Consequence process screen



Risk Bow Tie Analysis Consequence States

This section defines each state available in the workflow for the Risk Bow Tie Analysis Consequence process.

There are no states identified.

Risk Bow Tie Analysis Consequence Tasks

Adding a New Risk Bow Tie Analysis Consequence

1. In a Risk Bow Tie Analysis detail screen, click the Add New Item button in the Possible Consequences field. A new screen opens.
2. Enter a consequence description.
3. Select a consequence rating.
4. Click the Add New Item button in the Treatments field. See "Risk Treatments" on page 39 for information on how to fill out a treatment record.
5. Click Save to save the new record.

Chapter 5

Inbox Messages

Introduction to Inbox Messages

Most processes in the system require multiple people, departments, or groups to coordinate on completing a process. The inbox automates notifications sent to the appropriate users at specific times in the process.

An individual inbox action item represents a single task, approval, or notification that has been sent to you. This task will remain in your inbox until the necessary steps have been taken for completion.

Inbox messages can be separated into three different action types:

- **Assignment.** You are required to take some action in the system to move it beyond your workflow.
- **Approval.** Your approval is requested. You must approve or reject the process item.
- **Acknowledgment.** This is only for your information. You can acknowledge the notification to remove it from your inbox.

See the User Interface user guide to learn how to access inbox messages.

Inbox Messages

The table below describes each inbox action item involved in the Risk Management module. In addition to title and description, the table indicates which process each item comes from, who receives the message, and when it is sent. See the User Interface user guide to learn more about inbox messages.

Process	Title	Message	Action Type	Sent To / Sent When
Risk Assessments	Coordinator – Active Assessment	This message is to notify you that the following risk assessment is still active. When the risk assessment is complete, please move the state to Measure/Monitor. Title: {Title_f}	Assignment	Sent to the Coordinator when the current state is NOT Measure/Monitor or Obsolete.
Risk Assessments	Coordinator – Review Required	This message is to notify you that the following risk assessment requires review. When the review is complete, please update the last completed date and document any notes and move the state to Measure/Monitor or Obsolete. Title: {Title_f}	Assignment	Sent to the Coordinator when the current state moves to Requires Review.

Process	Title	Message	Action Type	Sent To / Sent When
Risk Events	Notification Groups – New Event	This is a notification that the following new Risk Event has been created: Risk Event Source: {RiskEventSource_f} Initiated Date/Time: {InitiatedDateTime_f} Initiated By: {InitiatedBy_f} Event Summary: {EventSummary_f}	Assignment	Sent to the notification groups after the record's first save.
Risk Events	Notification Groups – Event Complete	This is a notification that the following Risk Event has been completed: Risk Event Source: {RiskEventSource_f} Initiated Date/Time: {InitiatedDateTime_f} Initiated By: {InitiatedBy_f} Event Summary: {EventSummary_f} Action Taken: {ActionTaken_f}	Assignment	Sent to the notification groups when the current state moves to Complete or Complete – Escalated.
Risk Actions	Responsibility – Assigned	A risk action has been assigned to you, please complete the action and then set it to closed: Title: {Title_f} Due Date: {DueDate_f}	Assignment	Sent to the Responsibility when the current state is Assigned.
Risk Actions	Responsibility – Past Due	The following risk action is past due, please complete this action as soon as possible and then set it to close: Title: {Title_f} Due Date: {DueDate_f}	Assignment	Sent to the Responsibility when the current state is NOT Closed and the current date is beyond the due date.

Chapter 6

Metrics and Reports

Introduction to Metrics and Reports

The QMS system includes reporting and metric features that let you analyze the data in each process, measuring efficiency and effectiveness. The metrics and reports available differ between each process.

Report are generated within each process, either from the search screen or the detail screen. Metrics and key process indicators (KPIs) are gadgets that can be placed on one of your dashboards.

See the User Interface user guide to learn how to generate reports, metrics, and KPIs.

Reports

Pre-set reports have been set up to be pulled on a process by process basis, though not every process has a pre-set report. Certain reports require additional parameters in order to be previewed. The parameters are listed on the right side of the preview window. If a report requires parameters, then this pane will automatically appear. Once you have selected the desired parameters, click the Preview button to see the report preview.

Below is a table that describes each report available in the Risk Management module. In addition to title and description, the table indicates which process each report comes from and whether it is pulled from the search screen or detail screen. Lastly, if the report requires specific parameters in order to be generated properly, a description of those parameters is included below that report. See the User Interface user guide to learn how to access reports.

Process	Pulls From	Title	Description
Color Indicators	Detail Screen	Audit Trail – Color Indicators	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Acceptability Types	Detail Screen	Audit Trail – Risk Acceptability Types	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Ratings	Detail Screen	Audit Trail – Risk Ratings	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Treatment Types	Detail Screen	Audit Trail – Risk Treatment Types	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Acceptability Matrix	Detail Screen	Audit Trail – Risk Acceptability Matrix	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Acceptability Matrix	Search Screen	Risk Acceptability Matrix	Allows you to view the completed risk acceptability matrix.

Risk Drivers	Detail Screen	Audit Trail – Risk Drivers	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Events Sources	Detail Screen	Audit Trail – Risk Events Sources	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Library Controls	Detail Screen	Audit Trail – Risk Library Controls	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Library	Detail Screen	Audit Trail – Risk Library	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risks	Detail Screen	Audit Trail – Risks	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Assessments	Detail Screen	Audit Trail – Risk Assessments	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Assessments	Detail Screen	Risk Assessment Summary	This report is a summary of the risk assessment, including a list of risks identified and evaluated during the assessment.
Risk Treatments	Detail Screen	Audit Trail – Risk Treatment	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Controls	Detail Screen	Audit Trail – Risk Controls	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Events	Detail Screen	Audit Trail – Risk Events	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Actions	Detail Screen	Audit Trail – Risk Actions	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Bow Tie Analysis	Detail Screen	Audit Trail – Risk Bow Tie Analysis	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Bow Tie Analysis Cause	Detail Screen	Audit Trail – Risk Bow Tie Analysis Cause	Provides a path of how the record has progressed over time with changes (who, what, and when).
Risk Bow Tie Analysis Consequence	Detail Screen	Audit Trail – Risk Bow Tie Analysis Consequence	Provides a path of how the record has progressed over time with changes (who, what, and when).

Metrics

Below is a table that describes each metric available in the Risk Management module. In addition to title and description, the table indicates which process each metric comes from. Lastly, if the metric requires specific parameters in order to be generated properly, a description of those parameters is included below that metric. See the User Interface user guide to learn more about metrics.

Process	Pulls From	Title	Description
Risks	Gadgets	Number of Open Risks (Not in Review/Monitor state) by Risk Driver & by Site	A count of open risks that are not in the Review/Monitor state, organized by risk driver and by the user-specified site.
Risk Events	Gadgets	Number of Risk Events Ready for Review by Site	A count of risk events in the Triage state that are grouped by site so the user can see relative site counts of risk events to be reviewed.
Risk Events	Gadgets	Risk Events for a Site for a Given Date Range	A count of total risk events for a user-specified site and date range.
Risk Actions	Gadgets	Number of Open Risk Actions by Site	A count of risk actions that are **not** in the Closed state for the user-specified site.
Risk Actions	Gadgets	Number of Past Due Actions by Site and Responsibility	A count of risk actions **not** in the Closed state that are past their date, grouped by site and responsibility.

KPIs

See the User Interface user guide to learn more about KPIs.

There are no KPIs available for this module.

Chapter 7

Security Settings

Security Roles

Security roles define how various users access and control different types of processes and data. These roles are then assigned to each user. Some roles are used by many users, while others may only be applied to one or two individuals.

The following security roles apply in the Risk Management module.

All Roles

System controlled All Roles value. Any security applied to this special system role grants that security access to all users of the system.

Record Administrator

This security role allows you to add and edit new records. The Record Administrator also has the ability to edit any record as if he or she were the owner of the record.

Risk Administrator

This security role allows you to add, edit, and remove records in any process in the Risk module.

Risk Assessment Add/Edit

This security role allows you to add new and edit risk assessments and risks. Upon adding a risk assessment or risk, you will become the risk assessment or risk owner by default. The owner and the Risk Administrator security role are the only users who will be able to edit the risk assessment or risk.

Risk Champion

This security role allows you to add records in any process in the Risk Management module.

Risk Maintenance

This security role allows you to add, edit, and remove risk ratings, risk types, and risk acceptance matrix. Typically this maintenance account is only given to one or two individuals responsible for setting up this data for others to use.

Risk Management Maintenance

This security role allows you to add and remove risk ratings, risk types, and risk acceptance matrix. Besides being able to add and remove items for those processes, you can also view and edit all of the fields of the processes noted. Typically this maintenance account is only given to one or two individuals responsible for setting up this data for others to use.

Risk Navigation

This security role allows you to navigate to the Risk module.

System Administrator

This maintenance security role allows you to add and remove security roles, domains, entities, sites, locations, generalized code types and codes, product lines, item groups, item types, review frequencies, company types, cost accounts, and units of measure.

Besides being able to add and remove items, you can also view and edit all of the fields for the processes noted. Typically, this maintenance security role is only given to one or two individuals who are responsible for setting up the data for others to use.

System View

System view is a generic role that most users and modules use. This role allows you to view (but in most cases not edit) much of the non-sensitive data in the system. Being able to view the data is still subject to you having the ability to navigate to and open a process.

Every user should have this security role because it allows users to view non-secure data for most processes. For users who typically only have to approve data, but do not have to add or edit data, this System View role is what they need.

Process Security Roles

Each list below displays the security roles that provide you with permissions to add items for the indicated individual process.

Color Indicators

- Risk Administrator
- Risk Champion

Risk Acceptability Types

- Risk Administrator
- Risk Champion

Risk Ratings

- Risk Administrator
- Risk Champion
- Risk Maintenance

Risk Treatment Types

- Risk Administrator
- Risk Champion

Risk Acceptability Matrix

- Risk Administrator
- Risk Champion
- Risk Maintenance

Risk Drivers

- Risk Administrator
- Risk Champion

Risk Events Sources

- Risk Administrator
- Risk Champion

Risk Library Controls

- Risk Administrator
- Risk Champion

Risk Library

- Documents Administrator
- Documents Champion
- Risk Administrator
- Risk Champion

Risks

- APQP Administrator
- APQP Champion
- Complaints Administrator
- Complaints Specialist
- Documents Administrator
- Documents Champion
- Investigations Add/Edit
- Performance Management Administrator
- Performance Management Champion
- Risk Administrator
- Risk Assessment Add/Edit
- Risk Champion
- Supplier Quality Administrator
- Supplier Quality Champion

Risk Assessments

- Risk Administrator
- Risk Assessment Add/Edit
- Risk Champion

Risk Treatments

- Risk Administrator
- Risk Champion
- Supplier Quality Champion
- Supply Chain Manager

Risk Controls

- Risk Administrator
- Risk Champion
- Supplier Quality Champion
- Supply Chain Manager

Risk Events

- Risk Administrator
- Risk Champion

Risk Actions

- Risk Administrator
- Risk Champion
- Supplier Quality Champion
- Supply Chain Manager

Risk Bow Tie Analysis

- Risk Administrator
- Risk Champion
- Supplier Quality Champion
- Supply Chain Manager

Risk Bow Tie Analysis Cause

- Risk Administrator
- Risk Champion

Risk Bow Tie Analysis Consequence

- Risk Administrator
- Risk Champion

State Change Security

As you complete tasks in the system, changes occur based on your activities (such as changing a record's state) and when other events occur (such as a specific amount of time passing). The changes based on your activities are called **actions**, while the event-based changes are called **transactions**. The main difference between the two is the initiator: actions are performed by users, and transactions are managed by the system.

Each system change may depend on a number of factors, including where you are in the system, who is involved, which fields are populated, and more. It is important to know the actions and transactions for each process because these affect your ability to complete a task.

The state change security for each process is separated into two sections:

1. **Security.** Which users (by security role or field role) can change the state of a record. Field roles are indicated with an asterisk*.
2. **Transactions.** The conditions that must be met to initiate a transaction.

Security

Color Indicators

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risk Acceptability Types

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risk Treatment Types

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risk Acceptability Matrix

Transitions	Risk Maintenance
Active >> Inactive	✓
Inactive >> Active	✓

Risk Drivers

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risk Events Sources

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risk Library Controls

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	✓

Risk Library

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risks

Transitions	Owner*	Risk Administrator
Evaluation >> Review/Monitor	✓	✓
Evaluation >> Risk Treatment	✓	✓
Identification/Analysis >> Evaluation	✓	✓
Obsolete >> Review/Monitor	✓	✓
Review/Monitor >> Obsolete	✓	✓
Review/Monitor >> Risk Treatment	✓	✓
Risk Treatment >> Review/Monitor	✓	✓

Risk Assessments

Transitions	Coordinator*	Risk Administrator
Analysis/Evaluation >> Treatment Plan	✓	✓
Identification >> Analysis/Evaluation	✓	✓
Measure/Monitor >> Obsolete	✓	✓
Requires Review >> Measure/Monitor	✓	✓
Requires Review >> Obsolete	✓	✓
Treatment Plan >> Measure/Monitor	✓	✓

Risk Treatments

Transition	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	X

Risk Controls

Transitions	Risk Administrator	Risk Champion
Active >> Inactive	✓	✓
Inactive >> Active	✓	✓

Risk Events

Transitions	Record Administrator	Risk Champion
Assigned >> Complete	✓	X
Assigned >> Complete – Escalated	✓	X
Assigned >> In Progress	X	X
In Progress >> Complete	✓	X
In Progress >> Complete – Escalated	✓	X
New >> Assigned	✓	✓
Triage >> Assigned	✓	X
Triage >> New	✓	X

Risk Actions

Transitions	Risk Administrator	Risk Champion
Assigned >> In Progress	✓	X
Closed >> Re-Open	✓	X
In Progress >> Closed	✓	X
New >> Assigned	✓	✓
Re-Open >> Closed	✓	X

Transactions

Risks

Hide Complaint when Null

The Complaint field is hidden when empty.

Hide Incident Investigation when ITAR Restricted

The Incident Investigation field is hidden when the investigation is ITAR restricted and the user is not ITAR compliant.

Hide Incident Investigation when Null

The Incident Investigation field is hidden when empty.

Hide Process when Null

The Process field is hidden when empty.

Hide Risk Assessment when Null

The Risk Assessment field is hidden when empty.

Hide Supplier Risk Assessment when Null

The Supplier Risk Assessment field is hidden when empty.

Summarized Likelihood or Summarized Consequence is Changed

When the Summarized Likelihood or Summarized Consequence fields are changed, the Risk Evaluation field is updated to reflect the changes.

Risk Assessments

Measure/Monitor and Past Next Review Date

When the current state is Measure/Monitor and the current date is past the next review date, the system updates the current state to Requires Review.

Not Measure/Monitor or Obsolete

When the current state is not Measure/Monitor or Obsolete, a notification is sent to the coordinator to inform them that they have an active risk assessment.

This action will remain on your list until you move the state of the risk assessment to either Measure/Monitor or Obsolete.

Obsolete and Mark All Risks Obsolete

When the current state changes to Obsolete and the "Mark All Risks Obsolete" check box is selected, the state of all associated risks is also changed to Obsolete.

Requires Review

When the current state changes to Requires Review, a notification is sent to the Coordinator to inform them that a review of the risk assessment is required.

Review Frequency = None

When the risk assessment does not have a review frequency, the following fields are hidden:

- Last Review
- Next Review Due
- Review Completed By

Risk Controls

Changes in Likelihood After Control or Consequence After Control

When the Likelihood After Control or Consequence After Control fields are changed, the Risk Evaluation After Control field is updated to reflect the changes.

Risk Events

Added Rule Customer or Contact Changed

When the Customer or Contact fields change, the system updates any fields that populated on default based on these fields.

Complete – Escalated State and Escalate to Complaint is Checked

When the current state moves to Complete – Escalated and the "Escalate to Complaint" check box is selected, a Complaint record is created based on the Risk Event information. The following fields carry over to the new Complaint record:

- Address 1
- Address 2
- City
- First Name
- Last Name
- Phone Number
- State/Province/Region
- Postal Code
- Event Description (populates Event/Problem Description field)

Complete – Escalated State and Escalate to Non-conformance is Checked

When the current state moves to Complete – Escalated and the "Escalate to Non-conformance" check box is selected, a Non-conformance record is created based on the Risk Event information. The following fields carry over to the new Non-conformance record:

- Event Description (populates Problem Description field)
- Initiated By
- Initiated Risk Event

Complete or Complete – Escalated State

When the current state changes to Complete or Complete – Escalated, a notification is sent to the Notification Groups to inform them that the risk event has been completed.

First Save

When the record is saved for the first time, a notification is sent to the Notification Groups to inform them that a new risk event has been created.

The Site Field Has Been Selected

When the Site field is selected for the first time, the system links the appropriate notification groups to the record.

Risk Actions

Assigned

When the current state is Assigned, a notification is sent to the Responsibility to inform them that a risk action has been assigned to them.

Past Due

When the current state is **not** Closed and the Current Date field is beyond the due date, a notification is sent to the Responsibility to informt hem that the risk action is past due.

Commands

Some processes utilize command buttons to perform pre-defined actions. Commands can be found under the Actions icon in the top toolbar of the appropriate process.

Below is a table that describes each command available in the Risk Management module. In addition to title and description, the table indicates which process each command comes from, the roles that can execute the command, and the states when the command can be executed.

There are no commands for this module.

Chapter 8

Module Frequently Asked Questions

Frequently Asked Questions

Why shouldn't I delete items?

Records should only be deleted when you are sure that they are no longer needed. Even though records use a soft delete mechanism, there is still work that must be done to restore an item once it has been deleted.

The best thing to do with an item that is no longer needed is to set it to Inactive, Retired, or Obsolete, whichever state is applicable. This way, the item historically remains in the system but cannot be used.

If you do need to delete an item for good, then use the Trash button in the toolbar. Typically, only the system administrator can delete items.

I just changed the state of a process. What happens now?

When a process' state makes a transition, the system typically takes some automated steps. Details about these steps are listed in the State Transitions section of each process in this user guide.

Typically, state transition steps perform one of three functions:

1. **Notifications.** Notifications are sent to the users that are responsible for the next state of a process.
2. **Field Update.** Fields that depend on a state, date, or action are updated.
3. **Another State Transition**. A process' state may be transitioned automatically by the system, depending on a state, date, or action update.

Some processes may not have any automatic state transitions. In that case, it is useful to check the States section to view the process' state map and read the definitions of each state.

You can also review the Task list for that process. Each list typically describes which state to select when saving a process record.