



TRACELINK UNIVERSITY

Home

Resources

TraceLink University

Supplier Risk Assessment

Supplier Risk Assessment enables organizations to evaluate, classify, mitigate, and monitor risks associated with suppliers across their lifecycle.

What is a supplier risk assessment

A supplier risk assessment is a structured evaluation used to identify potential operational, regulatory, financial, and compliance risks associated with a supplier relationship. The process enables organizations to assess supplier risks, determine mitigation actions, and monitor supplier performance across the lifecycle.

1. **Assessment Initiation:** Establish the assessment scope, ownership, and supplier being evaluated.
2. **Information Collection:** Gather supplier responses and supporting documentation.
3. **Risk Evaluation:** Analyze supplier data to identify risk categories and impacts.
4. **Risk Classification:** Determine the overall supplier risk level.
5. **Mitigation Planning:** Define mitigation actions and responsible owners.
6. **Monitoring:** Track mitigation progress and reassess supplier risk posture.
7. **Closure:** Complete the assessment and document outcomes.

Types of supplier risk assessments

- **Operational Risk Assessments** – Evaluate operational stability and supply chain reliability.
- **Compliance Risk Assessments** – Evaluate regulatory and compliance risks.
- **Financial Risk Assessments** – Assess supplier financial stability.
- **Cybersecurity Risk Assessments** – Evaluate cybersecurity posture and information security practices.
- **ESG Risk Assessments** – Evaluate environmental, social, and governance risks.

How to configure the supplier risk assessment marketplace solution

Before using the supplier risk assessment marketplace solution, configure it in the Opus Solution Environment (OSE).

Save the marketplace solution as a company solution in OPUS Solution Environment

Solution Designers must first save the latest version of the marketplace solution from the marketplace catalog as a company solution.

1. Select the Main Menu  icon.
2. Select OPUS Solution Environment.
3. Select Catalog from the left menu.
4. Select Marketplace Solutions.
5. On the Search Solutions page, filter the list of solutions to find the required solution.
6. Find the latest version of the solution and select the Solution Name to open the solution.
7. On the Solution Details page, select Save As.
8. On the Save As panel, fill in the following fields:
 - a. Solution Name field – The name of the solution that will be saved as a

company solution.

b. Description field - (Optional) The description of the solution.

9. Select Apply.

The marketplace will be saved as a company solution in the Available tab on the left menu.

Create a network for the solution in OPUS Administration

After saving the solution as a Company Solution, Solution designers must create a network for the solution from OPUS Administration.

1. Select the Main Menu  icon.
2. Select Administration.
3. Select Network and Apps from the left menu.
4. Select New.
5. In the Network Information section, fill in the following fields:
 - a. Application drop-down - Select the application for which you want to configure the marketplace solution. For e.g. Process Orchestration for Empowered Teams.
 - b. Network Name field - The name of the network being created.
 - c. Network Description field - (Optional) The description of the network being created.
6. In the Solution section, fill in the following fields:
 - a. Standard Solution toggle - This value must be no as the solution for which the network is being created is a marketplace solution.
 - b. Company Solution field - Select the solution that you saved as a company solution in the previous procedure.
7. Select Save.

The new network is created and the solution is ready for use.

Configure roles for the new network in OPUS Administration

After creating a network for the solution, Solution Designers must define roles for

accessing the network.

1. Select the Main Menu  icon.
2. Select Administration.
3. Select Users from the left menu.
4. Select Network Members from the left menu.
5. On the Search Network Members page, filter the list of network members by the network created in the previous procedure.
6. Select the user email of the user who created the network.
7. Select Edit.
8. In the Roles section, select the role required to access the network.
9. Select Save.

The role to access the new network is configured.

Add a supplier risk assessment

Add a supplier risk assessment

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Supplier Risk Assessment from the left menu.
7. Select New.
8. In the General section fill in the following fields:
 - a. Title field – Provide a clear and descriptive title for the supplier risk assessment.
 - b. Description field – Briefly describe the reason or scope of the assessment.

9. Select Save.

The supplier risk assessment is created in Draft state.

10. Select Move to to progress the assessment.

Modify a supplier risk assessment

Edit a supplier risk assessment

1. Select the Main Menu  icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Supplier Risk Assessment from the left menu.
7. Select the required assessment.
8. Select Edit.
9. In the General section update the following fields:
 - a. Title – Name of the supplier risk assessment.
 - b. Supplier Name – Supplier being assessed.
 - c. Business Function – Business function engaging the supplier.
 - d. Priority – Assessment priority.
 - e. Due Date – Target completion date.
10. In the Participants section update the following fields:
 - a. Supplier Owner – Owner responsible for supplier relationship.
 - b. Assessment Owner – Primary coordinator of the assessment.
 - c. Risk Reviewers – Users responsible for evaluating risks.
 - d. Approvers – Governance decision makers for high-risk assessments.
11. In the Description section update the following fields:
 - a. Assessment Description – Description of the assessment scope and purpose.

- b. Attachments – Supporting documents.
12. In the Information Collection section update the following fields:
- a. Online Risk Assessment – URL to supplier questionnaire.
 - b. Offline Risk Assessment Attachment – Uploaded supplier questionnaire.
 - c. Additional Supplier Responses – Summary of supplier-provided information.
 - d. Clarifications – Notes from follow-ups with the supplier.
13. In the Risk Evaluation section update the following fields:
- a. Identified Risks – Description of key supplier risks.
 - b. Risk Categories – Applicable risk categories such as compliance, operational, financial, cybersecurity, ESG, and supply chain.
 - c. Potential Impacts – Business impact of identified risks.
14. In the Risk Classification section update the following fields:
- a. Overall Risk Level – Classified risk level (Low, Medium, High, Critical).
 - b. Classification Rationale – Justification for risk classification.
 - c. Reviewer Comments – Consolidated reviewer input.
15. In the Risk Mitigation Plan section update the following fields:
- a. Mitigation Actions – Steps defined to reduce supplier risk.
 - b. Target Completion Date – Expected mitigation completion date.
16. In the Monitoring and Review section update the following fields:
- a. Monitoring Approach – How supplier risk will be monitored.
 - b. Review Frequency – Frequency of reassessment.
 - c. Open Issues – Outstanding risks or actions.
 - d. Due Date – Monitoring deadline.
17. In the Assessment Closure & Attachments section update the following fields:
- a. Assessment Closure Comments – Summary of assessment outcome.
 - b. Attachments – Supporting evidence.
 - c. Related Records – Link related records.

Monitor supplier risk assessments

Search supplier risk assessments

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Supplier Risk Assessment from the left menu.
7. Select Filter.
8. In the Filters panel fill one or more of the following fields:
 - a. Title – Search by full or partial assessment title.
 - b. Supplier Name – Filter by supplier being assessed.
 - c. Owner – Filter by internal assessment owner.
 - d. Business Function – Filter by business function engaging the supplier.
 - e. Assessment Trigger – Filter by reason for initiating the assessment.
 - f. Overall Risk Level – Filter by classified supplier risk level.
 - g. Status – Filter by workflow state.
 - h. Priority – Filter by assessment priority.
 - i. Created Date – Filter by assessment creation date.
 - j. Last Updated Date – Filter by most recent update.
9. Select Apply.

Matching supplier risk assessments are displayed.