TRACELINK UNIVERSITY

Indirect Supplier Incident

Indirect supplier incidents originate from suppliers you do not contract with directly, but who provide materials or services to your direct suppliers.

What is a indirect supplier incident

Indirect supplier incidents arise from suppliers without a direct contractual relationship, but who provide materials or services to a company's direct suppliers. For e.g. raw material contamination, process changes, regulatory or legal action, or supply chain disruption.

Types of indirect supplier incidents

- **Raw Material Contamination:** Introduction of adulterated, counterfeit, or unsafe raw materials that compromise product safety and quality.
- **Process Changes at Tier-2:** Unapproved modifications to raw material synthesis, formulation, or processing methods that introduce risks to quality or safety.
- **Regulatory or Legal Action at Tier-2:** Actions by regulatory or legal authorities against a Tier-2 supplier that disrupt availability, compliance, or

© TraceLink Inc. 2009 - 2025 All Rights Reserved

certification status.

- **Supply Chain Disruption:** Interruptions in the flow of materials due to external events beyond the supplier's direct control, impacting continuity and timelines.

How to configure the indirect supplier incident marketplace solution

Before using the batch record review marketplace solution, Solution Designers must first configure the solution in Opus Solution Environment (OSE) by following the steps listed below:

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.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

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.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

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.

For more information about configuring or customizing marketplace solutions as per your business needs, see OPUS Solution Environment Help Center.

Add a indirect supplier incident

Add a indirect supplier incident

By default, an indirect supplier incident is created by a set of basic fields, which are widely used. However, depending on your business needs, you may need to include additional fields in the indirect supplier incident. To include additional fields, edit the indirect supplier incident to view all available fields and update the required fields.

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 Indirect Supplier Incident from the left menu.
7. Select New.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

8. In the General section fill in the following fields:
    a. Title field – The title of the new indirect supplier incident.
    b. Description field – The description of the indirect supplier incident.
9. Select Save.
   The indirect supplier incident is created in the Draft state.
10. To move the indirect supplier incident to To Do state, select Move to.

Modify a indirect supplier incident

Edit a indirect supplier incident

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 Indirect Supplier Incident from the left menu.
7. Select the Display Identifier of the indirect supplier incident to edit.
8. Select Edit.
   In addition to the fields updated when creating the indirect supplier incident, additional fields will be displayed which can be updated if required.
9. In the General section update the following fields:
    a. Display Identifier field – The display identifier of the indirect supplier incident.
    b. Title field – The title of the indirect supplier incident.
    c. Category field – The type of the indirect supplier incident. For example: Raw Material Contamination, Process Changes at Tier-2/ Supplier, Supply Chain Disruption, etc.
        i. If you selected Raw Material Contamination in the Category drop-down, add the required sub-category information:

© TraceLink Inc. 2009 - 2025 All Rights Reserved

a. Sub-category field – The sub-category of the selected category. For example: Adulterated Raw Materials, Counterfeit Raw Materials.
b. Material Name field – The name of the contaminated raw material.
c. Source of Material field – The supplier or region of origin.
d. Contaminant Identified field – The name of the contaminant.
e. Severity of Contamination field – The severity of the contamination. For example: Low, Medium, High, Critical.
f. Lab Test Performed field – Indicates if lab testing was done.

ii. If you selected Process Changes at Tier-2 in the Category drop-down, add the required sub-category information:
a. Sub-category field – The sub-category of the selected category. For example: Unapproved Solvent Change, Unapproved Synthesis Change.
b. Tier-2 Supplier Name field – The name of the indirect supplier.
c. Change Description field – The description of the process change.
d. Date of Change field – The date when the process change occurred.
e. Risk of Impurity Introduced field – Indicates whether the change introduced new risk.
f. Impurity Type (if any) field – The description of impurity introduced.
g. Regulatory Notification Sent field – Indicates whether this was reported to the authorities.

iii. If you selected Regulatory or Legal Action at Tier-2 in the Category drop-down, add the required sub-category information:
a. Sub-category field – The sub-category of the selected category. For example: License Suspension, Warning Letter, Facility

© TraceLink Inc. 2009 - 2025 All Rights Reserved

Shutdown.

b. Regulatory Body Involved field – The regulatory body involved in the legal action. For example: FDA, EMA, CDSCO, etc.
c. Action Type field – The type of legal action taken.
d. Effective Date field – The date when the action was taken.
e. Impacted Materials or Products field – List of affected materials.
f. Alternate Source Identified field – Indicates whether a backup supplier exists.

iv. If you selected Supply Chain Disruption in the Category drop-down, add the required sub-category information:
    a. Sub-category field – The sub-category of the selected category. For example: Natural Disaster, Geopolitical Issue, Transportation Breakdown.
    b. Disruption Type field – The type of disruption. For example: Flood, Earthquake, Border Closure, etc.
    c. Region Affected field – The country or region of disruption.
    d. Date of Disruption field – The date when the disruption occurred.
    e. Business Continuity Plan Triggered field – Indicates whether business continuity plan was activated.
    f. Estimated Delay (Days) field – The number of days of delay expected.
    g. Alternative Route Available field – Indicates whether backup logistics are in place.

d. Incident Date field – The date when the indirect supplier incident occurred.
e. Due Date field – The due date of the indirect supplier incident.
f. Business Priority field – The level of priority for the indirect supplier incident. Select from Low, Medium, High, and Critical.
g. Description field – The detailed description of the indirect supplier

© TraceLink Inc. 2009 - 2025 All Rights Reserved

incident.

10. If you require to collaborate with an external partner, enter the details under the Participants section:
    a. Initiator Company field – The name of the company that created the indirect supplier incident. This field is automatically populated with the logged-in user.
    b. Assignee Company field – The name of the Partner company that is assigned to take action on the indirect supplier incident.
11. In the Product Information section, add information about the impacted product in the following fields:
    a. Product Name field – The name of the impacted product.
    b. Item Code Type field – The item code type of the impacted product.
    c. Item Code Value field – The item code value of the impacted product.
    d. Product GTIN field – The GTIN of the impacted product.
    e. Batch/Lot Number field – (Optional) The batch or lot number of the impacted product.
12. In the Locations Affected section, add location information in the following fields:
    a. Business Name field – The business name of the location affected
    b. Identifier Type field – The identifier type of the location affected
    c. Identifier Value field – The identifier value of the location affected
    d. Risk Level field – The level of risk associated with the indirect supplier incident. For example: None, Low, Medium, High, Critical.
13. Select Save.

    The indirect supplier incident is updated.

Owners can edit the Assignee Details section while the batch record review is in the Draft state. Once the work item moves to the To Do state, the Assignee Details section can be edited only once.

Indirect supplier incidents workflow

© TraceLink Inc. 2009 - 2025 All Rights Reserved

The following workflow states are used to track the progress of a indirect supplier incident:

Base State	Workflow State	Description
Draft	Draft	The indirect supplier incident has been created and is in its initial state. It remains editable by the user who created it until it is submitted for action.
To Do	To Do	The indirect supplier incident has been assigned for review or action and is awaiting follow-up. When applicable, the relevant partner is notified.
In Progress	Under Investigation	The indirect supplier incident is actively being investigated. Authorized users can update the record while the issue is assessed, the root cause is identified, and appropriate resolution actions are initiated.
In Progress	Under Resolution	The resolution activities have been completed and are being verified to confirm that the incident has been addressed effectively.
Done	Done	The indirect supplier incident has been resolved, verified, and formally closed. No further action is required.

Monitor indirect supplier incident

A high level understanding of the state of all indirect supplier incidents that you have access to.

View the dashboard (Owner)

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 Indirect Supplier Incidents Dashboard from the left menu.
   View the widgets in the dashboard, which display pre-defined queries to demonstrate the state of all indirect supplier incidents at a high level.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

Metric	Description
Status	Indirect supplier incidents classified according to workflow status (Draft, To Do, In Progress, Done).
Business Priority	Indirect supplier incidents classified according to business priority (Critical, high, medium, low) combined with workflow status.
Category	Indirect supplier incidents classified by exception category.
Sub-Category	Indirect supplier incidents classified by exception sub-category.
Created by Owner Vs Partner	Indirect supplier incidents classified by creator (Owner vs Partner).
Due Date Monitoring	
Indirect Supplier Incidents Overdue	Indirect supplier incidents past Due Date by currentState. Escalates compliance and execution risks.
Indirect Supplier Incidents Due in Next 24 Hours	Indirect supplier incidents due within 24 hours by currentState. Highlights items requiring immediate executive attention.
Indirect Supplier Incidents Due in Next 7 Days	Indirect supplier incidents due within 7 days by currentState. Supports short-term workload planning.
Indirect Supplier Incidents Due in Future	Indirect supplier incidents due beyond 7 days by currentState. Supports capacity forecasting.

View the dashboard (Partner)

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 Indirect Supplier Incidents Dashboard from the left menu.
   View the widgets in the dashboard, which display pre-defined queries to demonstrate the state of all indirect supplier incidents at a high level.

Metric	Description
Business Priority	Indirect supplier incidents classified according to business priority (Critical, high, medium, low) combined with workflow status.
Status	Indirect supplier incidents classified by state (To Do, In Progress, Done).
Category	Indirect supplier incidents classified by exception category.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

Metric	Description
Sub-Category	Indirect supplier incidents classified by exception sub-category.
Due Date	Indirect supplier incidents classified by due date combined with workflow status.
Due Date and Business Priority	Indirect supplier incidents classified by due date and business priority.
Resolution Time by Category	Indirect supplier incidents classified by the time required to resolve incidents grouped by category.
Due Date Monitoring	
Indirect Supplier Incidents Overdue	Indirect supplier incidents past Due Date by currentState. Escalates compliance and execution risks.
Indirect Supplier Incidents Due in Next 24 Hours	Indirect supplier incidents due within 24 hours by currentState. Highlights items requiring immediate executive attention.
Indirect Supplier Incidents Due in Next 7 Days	Indirect supplier incidents due within 7 days by currentState. Supports short-term workload planning.
Indirect Supplier Incidents Due in Future	Indirect supplier incidents due beyond 7 days by currentState. Supports capacity forecasting.

Search indirect supplier incident

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 Indirect Supplier Incident from the left menu.
7. Select Filter.
8. In the Filters panel, fill in one or more of the following fields to filter the results:
    a. State field – The state of the indirect supplier incident.
    b. Title field – The title of the indirect supplier incident.
    c. Incident Date field – The date when the indirect supplier incident occurred.
    d. Display Identifier field – The display identifier of the indirect supplier

© TraceLink Inc. 2009 - 2025 All Rights Reserved

incident.

e. Category drop-down – The category of the indirect supplier incident. For example: Quality Issues, Regulatory, etc.
f. Subcategory drop-down – The sub-category of the indirect supplier incident.
g. Business Priority field – The business priority of the indirect supplier incident.
h. Last Modified Time field – The last modified date and time of the indirect supplier incident.
i. Due Date field – The due date of the indirect supplier incident.
j. Initiator Company field – The company which initiated the indirect supplier incident.
k. Assignee Company field – The company which was assigned the indirect supplier incident.

9. Select Apply.

   All indirect supplier incidents matching the filter criteria are displayed.

© TraceLink Inc. 2009 - 2025 All Rights Reserved