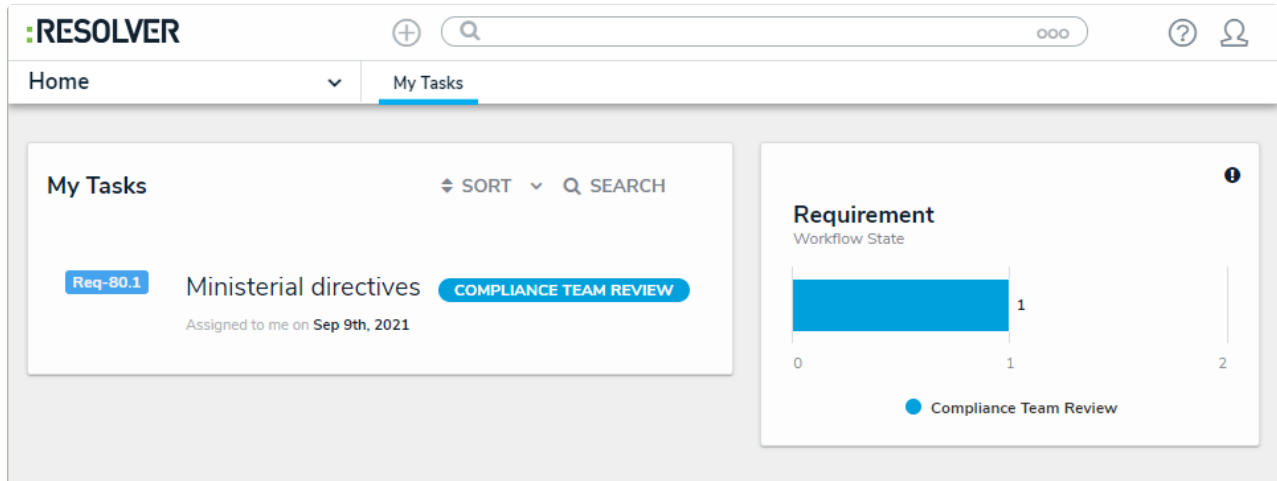


Review Requirements

Last Modified on 12/21/2021 12:09 pm MST

After the [Requirement Owner](#) has reviewed a requirement or a requirement has been [updated](#), they return it to the **Compliance Team**, who will assess it for residual risk. As the Compliance Team, requirements that have been submitted for your review will appear either on the [My Tasks](#) page or the [Assess Risk](#) activity.



The screenshot shows the RESOLVER application interface. At the top, there is a navigation bar with the RESOLVER logo, a search bar, and user profile icons. Below the navigation bar, there are two tabs: 'Home' and 'My Tasks', with 'My Tasks' being the active tab. The main content area is divided into two panels. The left panel, titled 'My Tasks', contains a list of tasks. One task is visible: 'Req-80.1 Ministerial directives', which is assigned to the user and has a 'COMPLIANCE TEAM REVIEW' button. The right panel, titled 'Requirement', shows a 'Workflow State' bar chart. The bar chart has a scale from 0 to 2, and the 'COMPLIANCE TEAM REVIEW' state is represented by a blue bar reaching the value of 1.

Assigned requirements on the My Tasks page.

To assess risk:

1. Log into a user account that's been added to the **Compliance Team** user group to open the **My Tasks** page.
2. Click a requirement in the **Compliance Team Review** state to open the **Compliance Team Review** form.

Compliance Assessment - Requirement Workflow **Compliance Team Review**

Compliance Team Review Req-80.1 ...

Review the requirement, inherent risk, controls, and residual risk documented by the Requirement Owner to determine whether the requirement is in compliance or requires additional remediation.

Requirement Name
Ministerial directives

Description
A bank must comply and must ensure that its foreign subsidiaries that carry on activities similar to a reporting entity comply with directives issued by the Minister in respect of transactions with certain foreign states or entities.

Requirement Owner **Requirement Delegate**
Compliant Consuela

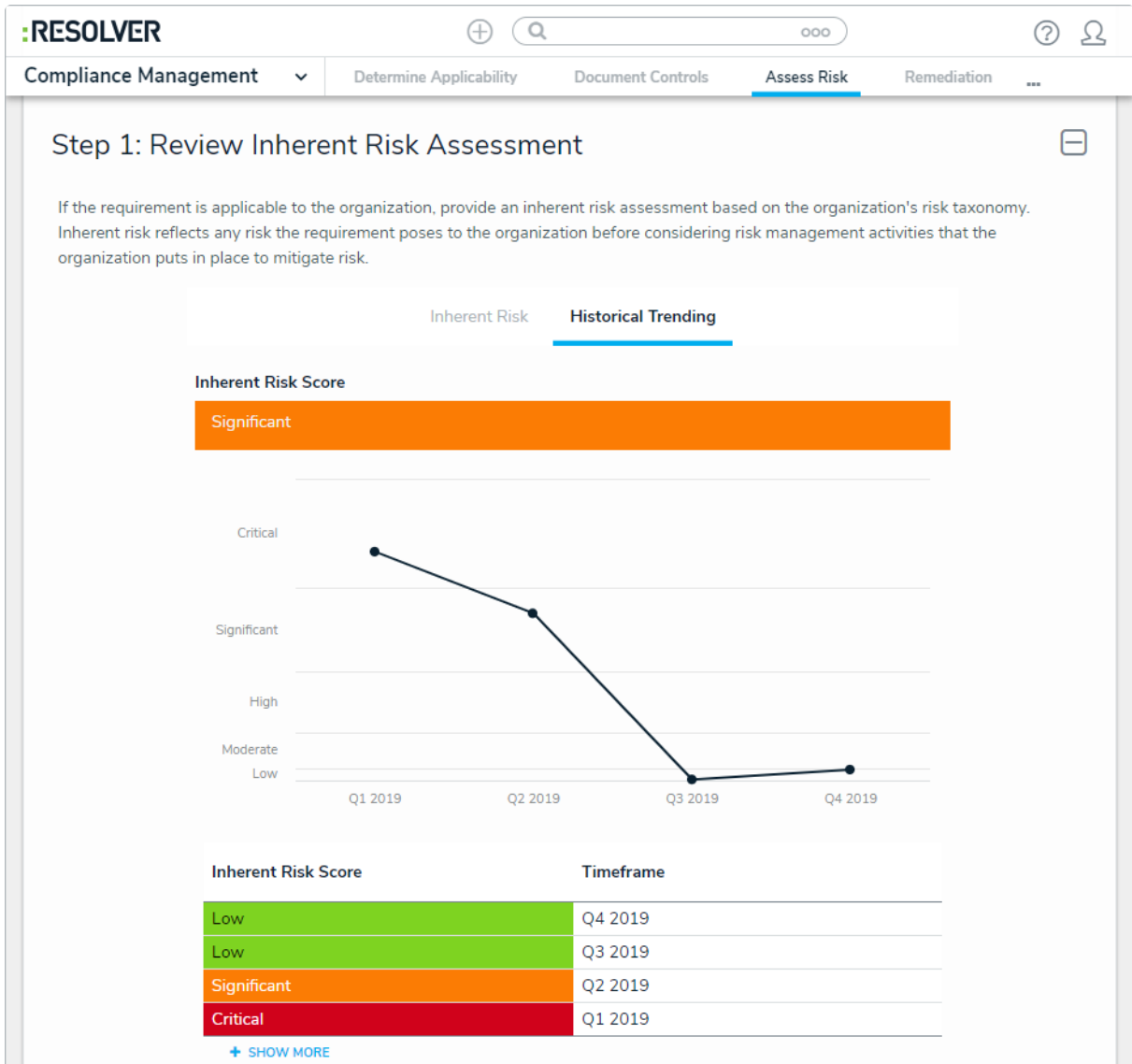
Sub Topic
Oversight

Source of Requirement
PCMLTFA section 11.42 (<http://laws-lois.justice.gc.ca/eng/acts/P-24.501/section-11.42.html>) PCMLTFA section 11.44 (<http://laws-lois.justice.gc.ca/eng/acts/P-24.501/section-11.44.html>) FINTRAC Guidance: Foreign Branches, Subsidiaries and affiliate requirements <https://www.fintrac-canafe.gc.ca/guidance-directives/branches-succursales/1-eng>

Date Updated **Effective Date**
December 11, 2017 December 11, 2017

Viewing a requirement in the Compliance Team Review form.

3. **Optional:** Navigate to the **Review Inherent Risk Assessment** section to review the inherent risk. Clicking the **Historical Trending** will display a chart showing how the inherent risk score has changed over time.



The Historical Trending tab of the Review Inherent Risk Assessment section.

4. In the Review Control Documentation section:

- a. Click the name of a control to open the Control Review palette. Add any additional details, as needed.
- b. Select the rating that best describes the control in the Control Effectiveness field.

Step 2: Review Control Documentation

Review the requirement and document all relevant controls. To find existing controls from the control library, start typing the control name at the bottom of the table. If a new control is required, click **Create New** at the bottom of the table.

Unique ID	Name	Description	Control Self Assessment	Design Effectiveness	Operating Effectiveness	Workflow State
C-101.2	Protection of personal information stored on portable media or devices	Personal information stored on portable media or devices is protected from unauthorized access.		● Not Tested	● Not Tested	Self Assessment

[ADD EXISTING CONTROLS](#) [CREATE NEW](#)

Control Effectiveness
● Medium

Medium: Control is not consistently effective

The Review Control Documentation section

5. In the Residual Risk Assessment section:

- a. Click the **Residual Impact** dropdown menu to select the impact of the risk after the controls have been put in place.
- b. Click the **Residual Likelihood** dropdown menu to select how likely the risk is to occur after the controls have been put in place.

Step 3: Residual Risk Assessment

Residual risk refers to the remaining level of risk once risk management activities have been put in place. The residual risk is determined based on the degree to which the controls reduce the level of inherent risk.

Residual Risk | Historical Trending

Residual Impact | **Residual Likelihood**

● High | ● Rare

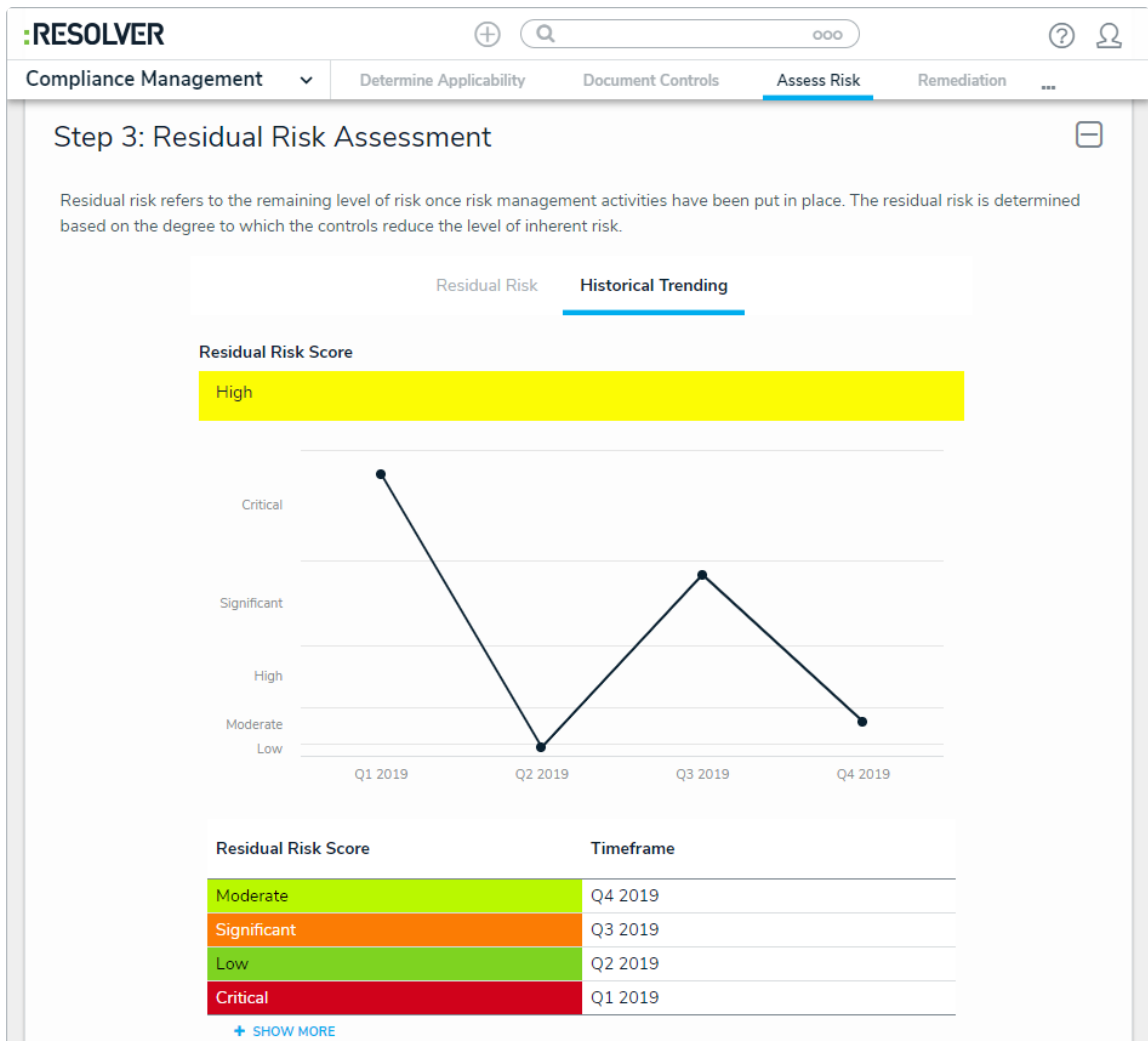
High: Financial loss of \$X million up to \$X million; Limited external reputational impact; Report of breach to regulator with immediate correction to be implemented

Rare: Once in 10 years up to once in 20 year

Residual Risk Score
High

The Residual Risk tab of the Residual Risk Assessment section.

- c. Click the **Historical Trending** tab to view how the residual risk score has fluctuated over time.



The Historical Trending tab of the Residual Risk Assessment section.

6. Optional: In the Document Issues section:

- Click the name of an issue to make any changes or to close the issue as needed.
- Begin typing keywords in the search bar to display a list of existing issues. Click on an appropriate issue to add it to the requirement.
- Click + to open the **Create a New Issue** palette. Fill in the fields as required.

The screenshot shows a web application window titled "Issue Status Creation". The main heading is "Create a New Issue". In the top right corner, there is a red button labeled "I-XXX". Below the heading, there are several input fields: "Issue Name" (a single-line text box), "Description" (a multi-line text area), "Issue Owner" (a dropdown menu with the placeholder "Start typing to find Us..."), "Reviewed By" (a dropdown menu with the placeholder "Start typing to find Us..."), "Issue Delegate" (a dropdown menu with the placeholder "Start typing to find Us..."), and "Priority" (a dropdown menu with the placeholder "Select one...").

The Create a new Issue palette.

7. In the **Determine Level of Compliance** section:
 - a. Select the requirement's level of compliance in the **Compliance Level** select list.
 - b. Enter any comments on the requirement's compliance level in the **Comments on Level of Compliance** field.

Step 5: Determine Level of Compliance

Review the requirement, controls, residual risk, and issues to determine whether the requirement is compliant, partially compliant, or not compliant.

Compliance Level

Select one...

Comments on Level of Compliance

VIEW REQUIREMENT PROFILE

The Determine Level of Compliance section.

- Optional: Expand the **Related Assessments** section to view the assessments related to the risk. Clicking on an assessment will display its **Requirement Review** form.

RESOLVER

Compliance Management Determine Applicability Document Controls **Assess Risk** Remediation

Related Assessments


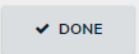
Residual Risk Score

High

Assessment Name	Inherent Risk Score	Control Effectiveness	Residual Risk Score
Shared Services Compliance Assessment	Significant	Medium	Moderate

Comments

Type here to add a comment

VIEW RELATIONSHIP GRAPH  

The Related Assessments section.

- Add [comments](#), as needed.
- Click one of the following buttons:

:RESOLVER

- **Remediation Required:** Send the requirement back to the Requirement Owner if further input is required.
- **Send to Monitoring:** Transition the requirement to the **Monitoring** state.