

Assess Risk on a Requirement

Last Modified on 12/10/2021 6:26 pm EST

Requirement owners are responsible for documenting issues and ensuring their business unit complies with their assigned requirements by creating new controls or selecting existing controls from the library. Once users in the group have completed their tasks, the requirements are then sent to the [Compliance Team](#) for review.

All assigned requirements appear on the [My Tasks](#) page.

The screenshot displays the Resolver application interface. At the top, the 'RESOLVER' logo is on the left, and a search bar with a magnifying glass icon is on the right. Below the logo, a navigation bar shows 'Home' and 'My Tasks' (which is selected and underlined). The main content area is divided into two panels. The left panel, titled 'My Tasks', contains a list of assigned requirements. Each entry includes a requirement ID in a blue box, the requirement name, the assignment date, and an 'ASSESS RISK' button. The right panel, titled 'Requirement', shows a 'Workflow State' chart. The chart is a horizontal bar graph with a scale from 0 to 3. A blue bar extends to the value 2, and a legend below it indicates that the blue color represents 'Assess Risk'.

Requirement ID	Requirement Name	Assigned to me on	Action
Req-85.1	Obligation to Comply with Audit	Sep 9th, 2021	ASSESS RISK
Req-79.1	Reporting and Delegation	Sep 9th, 2021	ASSESS RISK

Requirement Workflow State

0 1 2 3

Assess Risk

Assigned requirements on the My Tasks page.

To review requirements:

1. Log into a user account that's been added to the **Requirement Owner & Delegate** user group to display the **My Tasks** page.
2. Click a requirement to display the **Assess Risk** form.

RESOLVER

+

Q

ooo

?

u

Applications

▼

Compliance Assessment - Requirement Workflow
Assess Risk

Assess Risk

Req-85.1

...

The compliance team has assigned you to the following requirement and associated requirement details. Review the requirement and its associated requirement details. Determine the inherent risk level, document all relevant controls, and evaluate residual risk.

Requirement Name
Obligation to Comply with Audit

Description
An employer that is subject to an audit under the Act, must assist with the carrying out of such audit. Where an assessment has been made that an employer has breached their obligations under the Act, an employer must take steps to comply with the notice received by the Minister or take the necessary steps to seek a review of the assessment.

Requirement Owner
Compliant Consuela

Requirement Delegate

Q Start typing to find Us...

Sub Topic

Compliance

Source of Requirement
Employment Equity Act s. 23 and 38 (<http://laws-lois.justice.gc.ca/eng/acts/e-5.401/FullText.html>)

Date Updated
April 16, 2020

Effective Date
April 16, 2020

The Assess Risk form.

- Click + in the **Review Requirement Details** section to review the requirement's details.

Review Requirement Details

☰

Review associated requirement details to gain a better understanding of the regulatory requirement.

Requirement Detail

Q Search Table...

Unique ID	Name	Description	
RD-25.1	Privacy Officer	An organization must designate an individual who is accountable for the organization's compliance with the list of privacy principles that must be implemented by the organization (Privacy Officer). The Privacy Officer will be held accountable for dealing with complaints about the organization's compliance with its obligations under the PIPEDA.	×
RD-24.1	Policies and Procedures for Complaint Management	An organization must establish policies and procedures to receive and respond to complaints or inquiries about the organization's policies and procedures relating to the appropriate collection and handling of personal information. The complaints procedure must be easily accessible and easy to use. Front-line staff and managers should be aware of these policies and procedures, and able to distinguish between an inquiry and a complaint. They should be able to refer individuals to the designated privacy officer or to other staff assigned to handle inquiries or complaints.	×

The Review Requirement Details section.

- In the **Review Inherent Risk Assessment** section, select the appropriate rating in

4. In the **REVIEW INHERENT RISK ASSESSMENT** section, select the appropriate rating in the **Inherent Impact** field. Repeat this process for the **Inherent Likelihood** field to generate an **Inherent Risk Score**.

Step 1: Review Inherent Risk Assessment

Provide an inherent risk assessment based on the organization's risk scale. Select the impact of the risk materializing and the likelihood that the risk would occur. When evaluating inherent risk, consider the risk level of the requirements poses with no controls in place.

Inherent Risk

Historical Trending

Inherent Impact

Inherent Likelihood

Significant

Unlikely

Significant: Financial loss of \$X million up to \$X million; External reputation affected; significant loss of market share; Report to regulator requiring major project for corrective action

Unlikely: Once in 5 years up to once in 10 years

Inherent Risk Score

Significant

The Review Inherent Risk Assessment section.

5. In the **Control Documentation** section:
 - a. Click **Add Existing Controls** to open the **Add Existing Controls** dialog.
 - b. Begin typing in the search bar to search for existing controls. If any of the controls are applicable to the requirement, click **Add**.
 - c. **Optional:** If you wish to add the version of a control that being used by an assessment in another application or business unit, click **Assessments** and then **Add** next to the assessment you wish to share with.

ADD EXISTING CONTROLS

Q implementation

C-55 Post-implementation reviews

ACTIVE

Post-implementation reviews are performed to verify that controls are operating effectively.

+ ADD

ASSESSMENTS

Internal Controls Ass...

CORPORATE

CONTROL OWN...

+ ADD

Searching for existing controls in the Add Existing Controls dialog.

- d. Select the combined effectiveness of the controls from the **Control Effectiveness**

select list.

Step 2: Control Documentation

Review the requirement and document all relevant controls. To find existing controls from the control library, click **Add Existing Controls** at the bottom of the table. Controls may exist in multiple parts of the business. If the control exists in another business unit, expand the assessment tab and select the relevant version of the control, but clicking **Link to Existing**. Once the controls have been documented, determine the control effectiveness score.

Unique ID	Name	Description	Control Self Assessment	Workflow State
C-11.2	Sensitive information policy	A process is in place that protects sensitive information from unauthorized users.	Medium	Assign Control Owner

ADD EXISTING CONTROLS

Control Effectiveness

Strong

Strong: Effectively mitigates risk most of the time

The Control Documentation section.

6. In the **Residual Risk** section, select the appropriate rating in the **Residual Impact** field. Repeat this process for the **Residual Likelihood** field to generate an **Residual Risk Score**.

Step 3: Residual Risk

Provide a residual risk assessment based on the organization's risk scale. Select the impact of the risk materializing and the likelihood that the risk would occur with controls in place. When evaluating residual risk, consider whether the controls have reduced the inherent risk level.

Residual Risk

Historical Trending

Residual Impact

Residual Likelihood

Low

Remote

Low: Financial loss up to \$X million; Negligible reputational impact; Not reportable to regulator

Remote: Once in 20 years or less

Residual Risk Score

Low

The Residual Risk section.

7. In the **Document Issues** section:
 - a. Click **Add Existing Issues**, begin typing keywords in the search bar to display a list of existing issues, then click **+Add** next to each desired issue.

Step 4: Document Issues

Document any known issues associated to the requirement or the control. To find existing issue, click **Add Existing Issues** at the bottom of the table. If a new issue is required, click **Create New** at the bottom of the table.

Unique ID	Name	Description	Priority	Due Date	Workflow State
I-8	Noncompliance with policies or other best practices	The key controls or procedures are not in compliance with organizational policies or generally accepted best practices	High	October 26, 2020	Overdue

[ADD EXISTING ISSUES](#)
[+ CREATE NEW](#)

VIEW REQUIREMENT PROFILE

The Document Issues section.

- b. **Optional:** To create a new issue from scratch, click **+ Create New** to open the **Create a New Issue** palette and fill in the required fields. See the [Review an Issue](#) article for more information.

Issue Status Creation

Create a New Issue

I-XXX

Issue Name

Description

Issue Owner

Start typing to find Us...

Reviewed By

Start typing to find Us...

Issue Delegate

Start typing to find Us...

Priority

Select one...

The Create a New Issue palette.

8. **Optional:** Click **View Requirement Profile** to view this requirement's **Requirement**

Profile report. This report summarizes all information about the requirement as well as its attached controls and issues.

9. Click one of the following buttons:

- **Submit for Compliance Team Review:** Send the completed requirement to the Compliance Team. The Compliance Team will receive an email notifying them that the requirement has been sent to them for review.
- **Return to Compliance Team:** If the requirement was assigned to you in error, add comments to the **Comments** box, then click this button to return the requirement to the Compliance Team.