Software Requirement Specification Document to

LANKAPAY

Risk Module

Version 1.2

October 13, 2025

Table of Contents

Revision History

Created By	Date	Reason	Version	Reviewed by	Approved by
Nehan Naidabadu	30.09.2025	Initial Creation	Version 1.0	Amanda Illankoon	
Nehan Naidabadu	09.10.2025	Requested Changes	Version 1.1	Amanda Illankoon	
Nehan Naidabadu	13.10.2025	Requested Changes	Version 1.2	Amanda Illankoon	

1 Introduction

1.1 Objective

This Software Requirements Specification (SRS) document defines the key specifications, functional requirements, and process overview diagrams of the **Risk Module**, which has been designed to support risk assessment and related processes at **Lankapay**. It provides clear guidance for stakeholders involved in the design, development, implementation, and utilization of the Risk Module solution.

The proposed solution aims to streamline and optimize existing risk management practices by improving efficiency and accuracy in risk identification, assessment, and monitoring. It also strengthens internal controls over processes that are currently handled manually, while promoting greater transparency, accountability, and consistency in the overall risk management framework.

Furthermore, this document serves as a comprehensive reference guide that outlines the essential features, capabilities, and functionalities incorporated into the system. It ensures a common understanding among stakeholders and supports effective decision-making throughout the solution lifecycle.

1.2 Intended Audience

The intended audience of this document includes Pre-Sales Engineers, Sales Managers, Project Managers, System Engineers, Product Developers, Software Developers, System Administrators, HODs, and Other End Users of the Risk Module.

1.3 Document Conventions

The Document uses the standard SRS template published by IEEE. The template standards are published under “IEEE Standards Collection”.

1.4 Solution Scope

The solution will be implemented covering the following scope:

1. **Risk Assessment Initiation** – capturing and recording identified risks and vulnerabilities.
2. **Risk Control and Current Risk Evaluation** – assessing existing controls and evaluating current risk levels.
3. **Risk Treatment Strategy and Action Planning** – defining treatment strategies and assigning action plans.
4. **Carry Forward Risks from Previous Year** - carry forward risks from the previous year into the current year to ensure continuity
5. **Report Generation** - Enables users to view comprehensive risk registry details for each process’s risk assessments and export the information to Excel.
6. **Dashboard view** - The Dashboard view is part of the project scope, but its details are not included in this SRS and a separate addendum document will be provided for the dashboard requirements.
7. **Automated Notifications and Reminders** – ensuring timely updates and follow-ups.

8. **Administrative Configurations** – managing users, parameters, and system settings for flexibility and control.

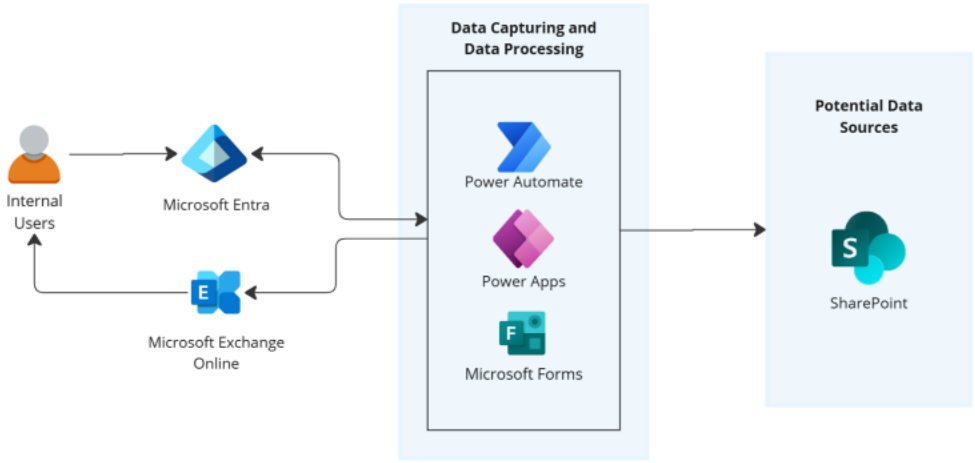
1.5 Out of Scope

- Any scope other than mentioned in the design document will be considered out of scope.
- Any Integrations to the system.
- Migration of any existing data will not be considered.
- Risk status updates and Finalizing are fully handled by the Risk Team and will not be automated by the system.

1.6 Assumptions & Limitations

- Standard Limitations applicable for the Power Platform & Share Point shall be applicable for the development of the solution. (Refer - Power Automate Limitations)

2 System Architecture

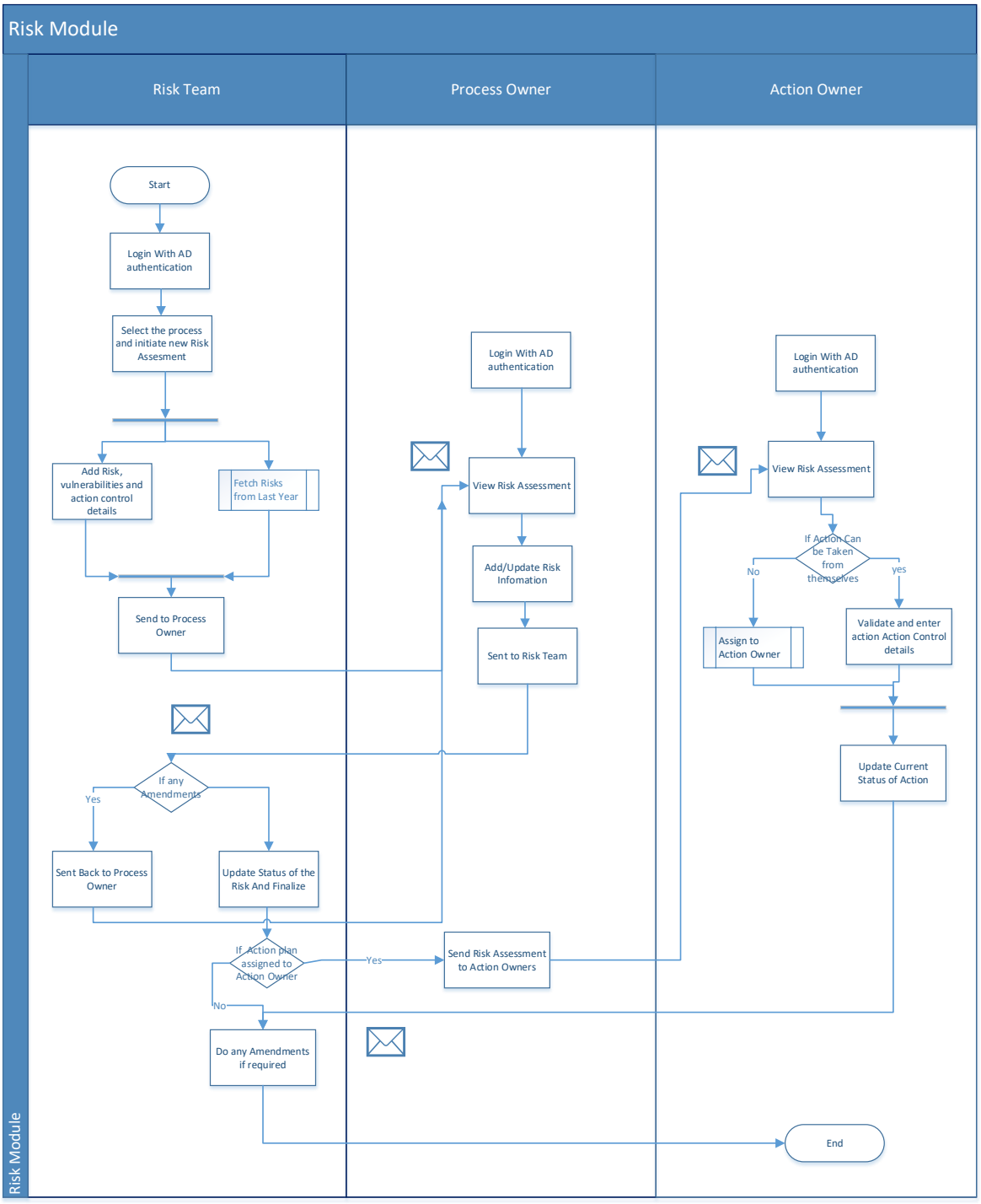


The figure above illustrates a high-level overview of how the solution architecture would be for the workflow solution. This system is designed on the **Microsoft Power Platform** to ensure seamless integration with the existing M365 environment, effectively leveraging widely used tools such as Outlook and **Microsoft Entra (Active Directory).** Internal users within LankaPay can access these solutions, with their authentication managed through Microsoft Entra to maintain security and streamlined access.

The data capture and processing for internal users will be facilitated through **Microsoft Power Automate and Power Apps**, enabling a robust and user-friendly interface for efficient data handling. All data gathered will be stored securely in **Share Point**, which will act as the central data repository for the solution, providing a reliable and organized structure for information storage.

Additionally, for effective notification management, Microsoft Exchange will be utilized to automate and send emails to relevant parties, ensuring that stakeholders remain informed of important updates and actions.

3 Proposed workflow for Risk Module Solution



Process No	Process	Pre-Condition	User	Action	Post Condition	Output
01	System Login	The user should be an Active Directory registered Role Based Access User within the System.	Any authorized user.	1. Enter a valid O365 username and a password.	A logged-in user.	Users should be able to log into the System and should land on the home page.
02	Initiate New Risk Assessment	1. The user should have logged in to the system and Should have access to Initiate Risk Assessment Module	Risk Team	1. Navigate to the **Initiate Risk Assessment** module. 2. Select a Financial year and process Note: Default will be Current Financial Year 3. Add risk-capturing information, Vulnerability Details and Action Control Details. 4. Save Assessment as Draft if required. 5. Send Risk Assessment to Process Owner. Note: System should automatically identify the Process Owner/s of the particular Process considering Admin Module configuration.	1. IF Inherent Risk Details Entered, **Inherent Risk Rating** is automatically calculated based on the entered *impact* and *likelihood*. 2. IF Current Risk Details Entered, **Current Risk Rating** is automatically calculated based on the current *impact* and *likelihood*. 3. IF Residual Risk Details Entered, The **Residual Risk Rating** is calculated based on the *impact* and *likelihood* after applying treatment strategies. 4. If Risk added, Risk status defaults to **"Open"**. 5. If Action Control added, each Current Status	1. Each risk assessment should be generated with a unique identification number that includes the process and financial year. 2. Once Assessment Sends to Process Owner , It should visible in **Process Owner's summary view**. Generate the Email Template 6.1 Note: there will be pool of Process Owners. 3. Request should be visible in summary view of the risk team as well. 4. If Drafted the Assessment, it should visible in Draft section

					defaults to **"Not Started"**.	for further amendments.
03	Fetch Risks from Previous Financial year to current year	1. The user should have logged in to the system and Should have access to Initiate Risk Assessment Module	Risk Team	1. Click on the **"Fetch from Previous Year"** button. 2. A list of risks from the **previous financial year** will be displayed in grid view. 3. Select one or multiple risks. 4. A "Select All" option should also be available. 5. Confirm the selection to add the chosen risks to the current year's assessment.		1. The selected risks from the previous year will be fetched into the current year's assessment in **editable mode**, allowing users to update details as required.
04	Process Owner Response to Risk Assessment Form	1. The user must be logged into the system and have access rights as a **Process Owner.** 2. Risk Assessment should be Submitted to Process Owner by Risk Team	Process Owner /HOD	1. Navigate to **Risk Assessment Summary** section. 2. Review the risk details entered by the Risk Team. 3. Add/ Update Risk Details, Vulnerability Details and Action Control Details if necessary. 4. Forward Risk Assessment to Risk Team.	1. IF Inherent Risk Details Entered, **Inherent Risk Rating** is automatically calculated based on the entered *impact* and *likelihood*. 2. IF Current Risk Details Entered, **Current Risk Rating** is automatically calculated based on the current *impact* and *likelihood*. 3. IF Residual Risk Details Entered, The **Residual Risk Rating** is calculated based on	1. Once Assessment Forwarded to Risk Team , It should visible in **Risk Team summary view**. Generate the Email Template 6.2.

					the *impact* and *likelihood* after applying treatment strategies. 4. If Risk added, Risk status defaults to **"Open"**. 5. If Action Control added, each Current Status defaults to **"Not Started"**.	
05	Finalizing Risk Assessment	1. The user must be logged into the system and should have access rights to the *Risk Assessment Summary* module. 2. A risk assessment should be Submitted by Process Owner.	Risk Team	1. Navigate to the ***Risk Assessment Summary*** module. Note: Each member of risk team have access to each assessment. 2. Navigate to Pending Section. 3. Select a specific risk assessment and open the detailed view. 4. Update previously entered risk details or add if required. 5. If required, Send Back to Process Owner for amendments. 6. Finalize Risk Assessment.		1. If Send Back to Process Owner for Amendments, It should Sent Back to **Process Owner's summary view**. Generate the Email Template 6.1. 2. Once Assessment Finalized, Tasks should be send to each Action Owners **summary view**. Generate the Email Template 6.3./ 6.4/6.5
06	Action Owner Response to Risk Assessment Form	1. The user must be logged into the system and have access rights as an **Action Owner**. 2. Risk Assessment should be Finalized from Risk Team	Action Owner	1. Navigate to **Risk Assessment Summary** section.		1. If the **Action Owner** updates a control status directly, Risk Team should be notified.

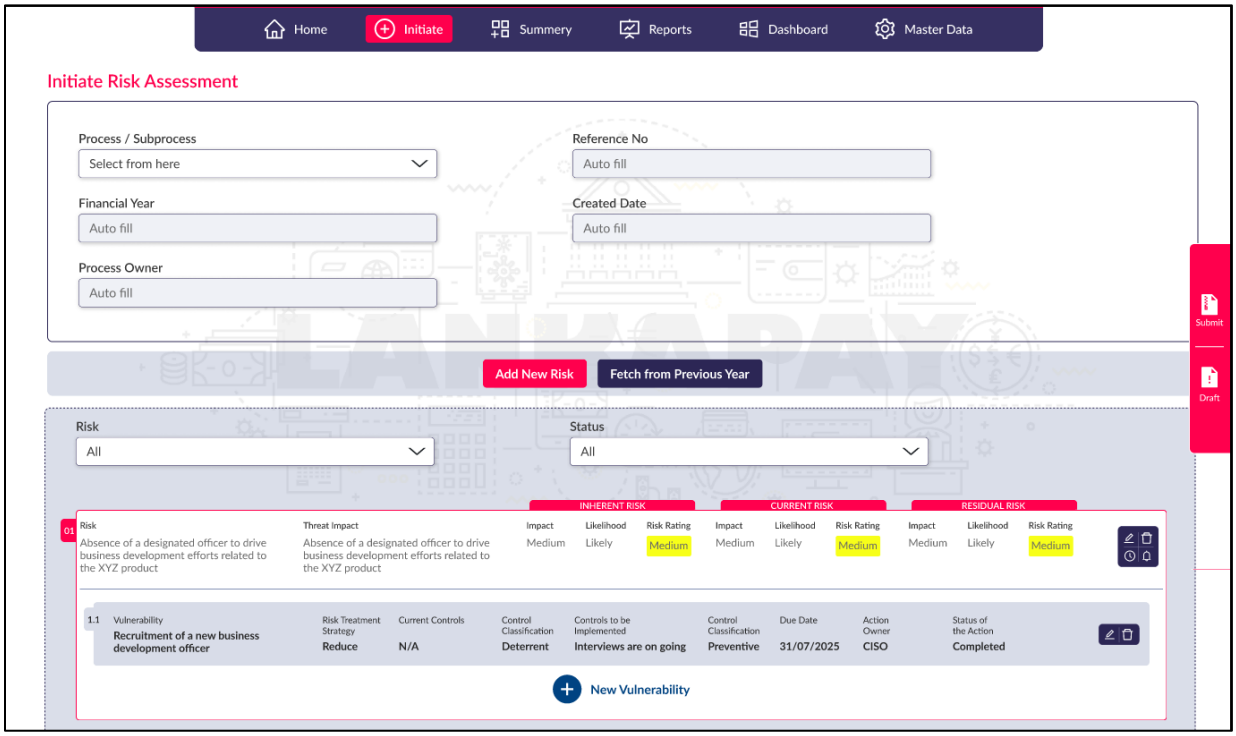
				2. Review the risk details entered by the Risk Team/Process Owner. 3. Edit or update the control details, current status or remark. 4. If required, assign to an other Action Owner. Note: there can be up to three levels of assignment. 5. Submit the Assessment.		Generate the Email Template 6.6. 2. If the Action **Owner** assigns an Other, the assessment is sent to that **Action Owner's summary view** for response. Generate the Email Template 6.3./ 6.4/6.5
07	Report Module	The user should have logged in to the system and Should have access to Report Module	Corporate Management/ Risk Team	1. Navigates to the **Report Module**. 2. Applies filters (e.g., process, risk category, financial year, status, etc) to retrieve specific risks. 3. The system displays the **Risk Registry** based on the applied filters. 4. Exports the selected assessment to the Excel worksheet.	1. The **Risk Registry** shall display all relevant risks, vulnerabilities, and control details according to the applied filtering criteria. 2. The selected Risk Assessment shall be successfully exported into the Excel format.	

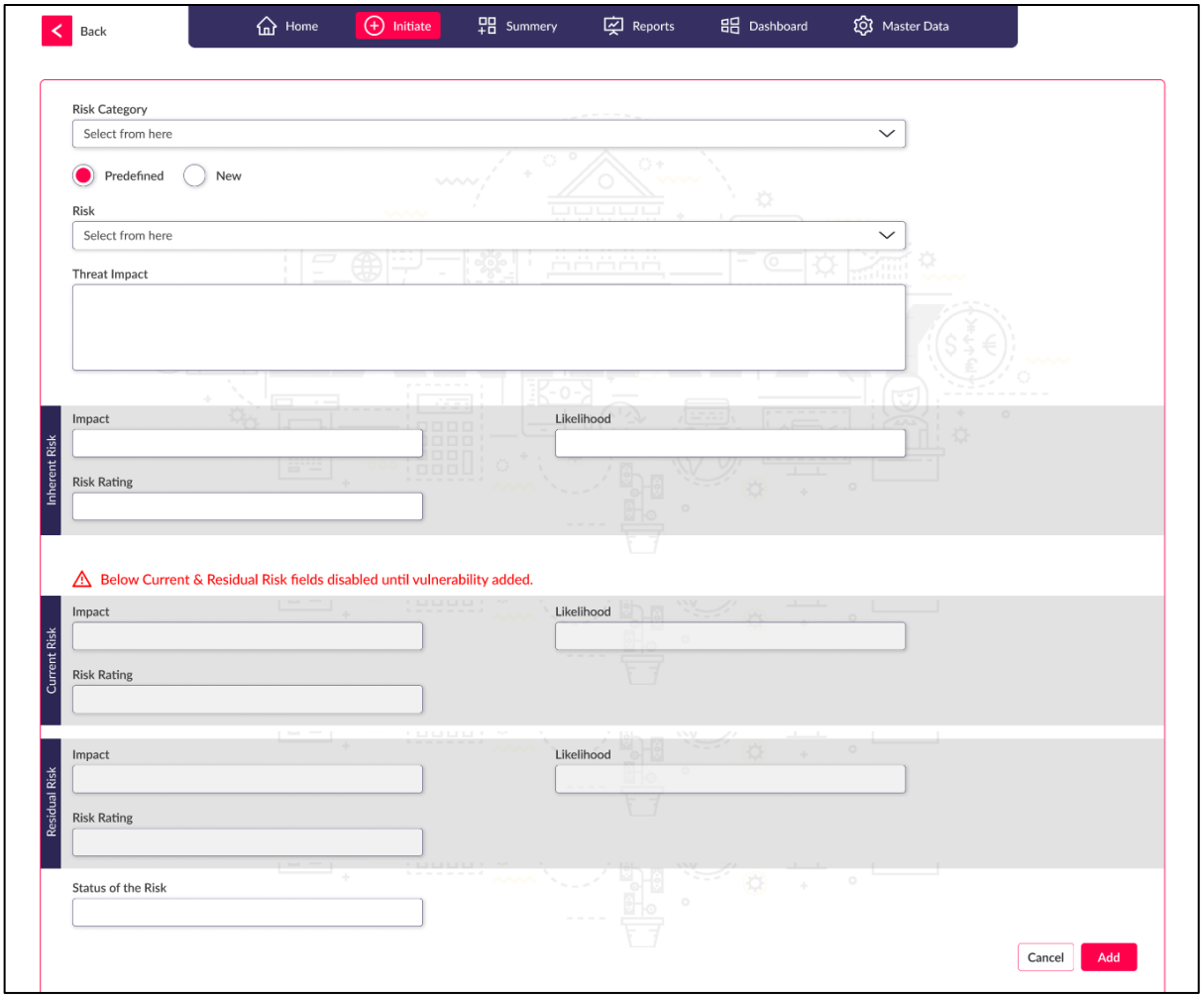
4 Wireframes

4.1 Home Screen

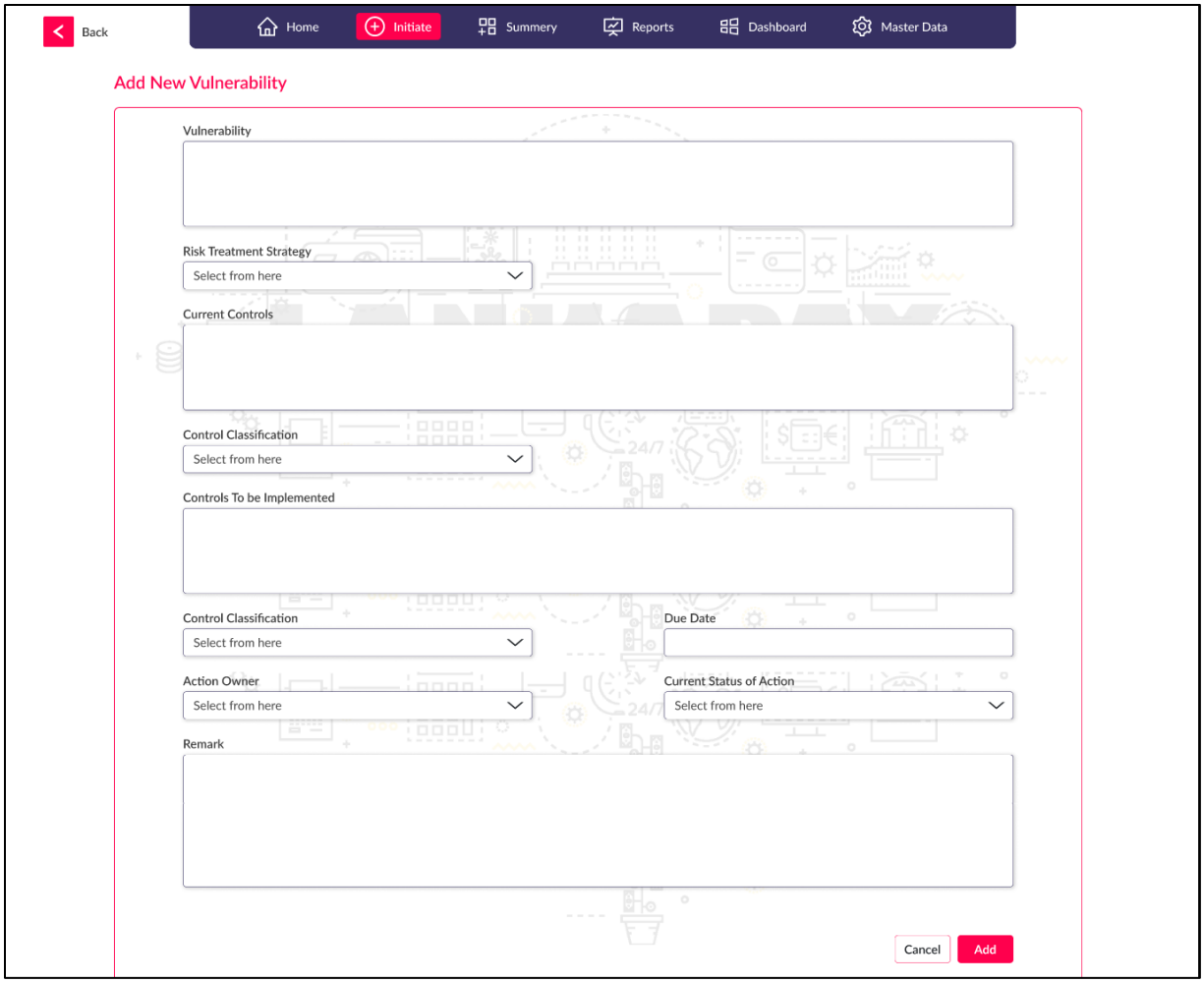

Back
lanka pay
Initiate Risk Assessment
Risk Assessment Summary
Reports
Dashboard
Master Data
© 2025 LankaPay. All rights reserved.
lanka pay

4.2 New Risk Assessment Initiation





Note: Inherent Risk , Current Risk Rating details, Residual Rate Details and Risk Status Enable after Vulnerability added.


Back
Home
Initiate
Summery
Reports
Dashboard
Master Data
Add New Vulnerability
Vulnerability
Risk Treatment Strategy
Select from here
Current Controls
Control Classification
Select from here
Controls To be Implemented
Control Classification
Select from here
Due Date
Action Owner
Select from here
Current Status of Action
Select from here
Remark
Cancel
Add

Fetch From Previous Year UI

Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Process	Drop Down	M	N/A	Drop down values from Share Point list
Process Owner	Auto Filled	N/A	N/A	Autofill the process owner/s mapped to the particular Process. If multiple process owners exist, show comma separately.
Risk Assessment Reference	Auto Generated	N/A	N/A	The system shall generate a unique risk assessment reference number in the format: **<ProcessCode>-<Financial Year>-<Sequence Number>** The sequence number shall be auto-incremented for each new risk assessment created.
Financial Year	Drop Down	M	N/A	The financial year dropdown should display only a range of years spanning from five years prior to the current financial year up to five years ahead. Format- (2025-2026) Current Financial Year should be default selected.
Created Date	Auto Filled	N/A	N/A	
Risk No	Auto Filled	N/A	N/A	Auto increment number (ex-1)
Risk Category	Drop Down	M	N/A	Drop Down Values from Share Point list
Predefined Risk/ New Risk	Radio Button	M	N/A	
Risk	Dependent	Dependent	N/A	if “Predefined Risk” = TRUE This should be a Drop Down. Drop Down Values from Share Point list If the risk is **already added** to the assessment or fetched from the previous year, warning message should display

				if “New Risk” = TRUE This should be a Text Area Once entered this should be added to Risk Share Point list
Threat Impact	Text Area	M	100	
Risk Status	Drop Down	M	N/A	Open (Default) Closed Accepted Avoided Transferred Not Applicable Once Risk Added this should be default to “Open”
Fetch From Previous Year	Button	N/A	N/A	When the user clicks on the *Fetch from Previous Year* button, all risks from the previous financial year related to the selected process shall be displayed in grid view. User should be able to filter by Risk status. The user shall have the ability to multi-select risks and add them to the current year’s assessment. A *Select All* option shall also be available
Inherent Risk Impact	Drop Down	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable. • **Critical (5):** Severe consequences causing critical disruption, major financial losses, significant legal/regulatory breaches, or irreparable reputational damage. • **High (4):** Serious consequences causing notable disruption, considerable financial losses, regulatory non-compliance, or significant reputational harm. • **Moderate (3):** Manageable consequences with moderate financial, operational, or reputational impact that can be addressed with planned controls. • **Low (2):** Minor consequences with limited impact on operations, finances, or reputation; easily manageable. • **Insignificant (1):** Negligible impact with little to no effect on operations, finances, or reputation. Note: Show the description in tooltip

<table>
<tr>
<td>Inherent Risk Likelihood</td>
<td>Drop Down</td>
<td>M</td>
<td>N/A</td>
<td>Note: until at least one vulnerability added for the particular Risk, this filed should be disable.

• Almost Certain (5): Events with a very high likelihood of occurring, supported by strong historical evidence or current circumstances.
• Likely (4): Events with a high probability of occurring based on historical trends or current circumstances.
• Moderate (3): Events with a moderate chance of occurrence based on available data and expert judgment.
• Unlikely (2): Events that are improbable but have occurred sporadically in the past and/or based on expert judgment.
• Rare (1): Highly improbable events with minimal historical occurrence and expert judgment.

Note: Show the description in tooltip</td>
</tr>
<tr>
<td>Inherent Risk Rating</td>
<td>Auto Filled</td>
<td>M</td>
<td>N/A</td>
<td>Inherent Risk Rate should be calculate considering Impact and Likelihood according to Below Formula.

<table>
<tr><th>Impact ↓ / Probability →</th><th>Rare (1)</th><th>Unlikely (2)</th><th>Moderate (3)</th><th>Likely (4)</th><th>Almost Certain (5)</th></tr>
<tr><td>Insignificant (1)</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>Low (2)</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>Moderate (3)</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>High (4)</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>Critical (5)</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>

Category Mapping
• Frozen = Score 1–2
• Chilling = Score 3-6
• Heating = Score 8-9
• Flaming = Score 10-16
• Buring = Score 20-25</td>
</tr>
<tr>
<td>Current Risk Impact</td>
<td>Drop Down</td>
<td>M</td>
<td>N/A</td>
<td>Note: until at least one vulnerability added for the particular Risk, this filed should be disable.

• Critical (5): Severe consequences causing critical disruption, major financial losses, significant legal/regulatory breaches, or irreparable reputational damage.
• High (4): Serious consequences causing notable disruption, considerable financial losses, regulatory non-compliance, or significant reputational harm.</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td>

Moderate (3): Manageable consequences with moderate financial, operational, or reputational impact that can be addressed with planned controls.
Low (2): Minor consequences with limited impact on operations, finances, or reputation; easily manageable.
Insignificant (1): Negligible impact with little to no effect on operations, finances, or reputation.

</td></tr>
<tr><td>Current Risk Likelihood</td><td>Drop Down</td><td>M</td><td>N/A</td><td>
Note: until at least one vulnerability added for the particular Risk, this filed should be disable.

Almost Certain (5): Events with a very high likelihood of occurring, supported by strong historical evidence or current circumstances.
Likely (4): Events with a high probability of occurring based on historical trends or current circumstances.
Moderate (3): Events with a moderate chance of occurrence based on available data and expert judgment.
Unlikely (2): Events that are improbable but have occurred sporadically in the past and/or based on expert judgment.
Rare (1): Highly improbable events with minimal historical occurrence and expert judgment.

</td></tr>
<tr><td>Current Risk Rating</td><td>Auto Filled</td><td>N/A</td><td>N/A</td><td>
Current Risk Rate should be calculate considering Impact and Likelihood according to Below Formula.

<table>
<tr><th>Impact ↓ / Probability →</th><th>Rare (1)</th><th>Unlikely (2)</th><th>Moderate (3)</th><th>Likely (4)</th><th>Almost Certain (5)</th></tr>
<tr><td>Insignificant (1)</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>Low (2)</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>Moderate (3)</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>High (4)</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>Critical (5)</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>

Category Mapping

Frozen = Score 1–2
Chilling = Score 3-6
Heating = Score 8-9
Flaming = Score 10-16
Buring = Score 20-25

</td></tr>
<tr><td>Residual Risk Impact</td><td>Drop Down</td><td>M</td><td>N/A</td><td>Note: until at least one vulnerability added for the particular Risk, this filed should be disable.</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td>

- **Critical (5):** Severe consequences causing critical disruption, major financial losses, significant legal/regulatory breaches, or irreparable reputational damage.
- **High (4):** Serious consequences causing notable disruption, considerable financial losses, regulatory non-compliance, or significant reputational harm.
- **Moderate (3):** Manageable consequences with moderate financial, operational, or reputational impact that can be addressed with planned controls.
- **Low (2):** Minor consequences with limited impact on operations, finances, or reputation; easily manageable.
- **Insignificant (1):** Negligible impact with little to no effect on operations, finances, or reputation.

</td></tr>
<tr><td>Residual Risk Likelihood</td><td>Drop Down</td><td>M</td><td>N/A</td><td>

Note: until at least one vulnerability added, this filed should be disable.

- **Almost Certain (5):** Events with a very high likelihood of occurring, supported by strong historical evidence or current circumstances.
- **Likely (4):** Events with a high probability of occurring based on historical trends or current circumstances.
- **Moderate (3):** Events with a moderate chance of occurrence based on available data and expert judgment.
- **Unlikely (2):** Events that are improbable but have occurred sporadically in the past and/or based on expert judgment.
- **Rare (1):** Highly improbable events with minimal historical occurrence and expert judgment.

</td></tr>
<tr><td>Residual Risk Rating</td><td>Auto Filled</td><td>N/A</td><td>N/A</td><td>

Residual Risk Rate should be calculate considering Impact and Likelihood according to Below Formula.

<table>
<tr><th>Impact ↓ / Probability →</th><th>Rare (1)</th><th>Unlikely (2)</th><th>Moderate (3)</th><th>Likely (4)</th><th>Almost Certain (5)</th></tr>
<tr><td>Insignificant (1)</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>Low (2)</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>Moderate (3)</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>High (4)</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>Critical (5)</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>

Category Mapping

- Frozen = Score 1–2
- Chilling = Score 3-6

</td></tr>
</table>

				• Heating = Score 8-9 • Flaming = Score 10-16 • Buring = Score 20-25
Vulnerability No	Auto Filled	N/A	N/A	Auto increment number (ex-1.1) Numbering format should be <Risk No>.< Vulnerability No>
Vulnerability	Text Area	M	255	To add a risk, its mandatory to add at least one vulnerability. Else show an error message For each risk there can be up to maximum 30 vulnerabilities
Risk Treatment Strategy	Drop Down	M	N/A	• Mitigate • Accept • Avoid • Transfer If Accept, Avoid or Transfer below Fields should be auto filled as Not Applicable **Current Controls, Control Classifications, Controls to be implemented, Control Classification, Due Date, Action Owner, Current Status of action**
Current Controls	Text Area	M	255	
Control Classification	Drop Down	M	N/A	• Preventive • Detective • Corrective • Deterrent
Controls To be Implemented	Text Area	M	255	
Control Classification	Drop Down	M	N/A	• Preventive • Detective • Corrective • Deterrent
Due Date	Date Picker	M	N/A	Due Date cant be a day before current date
Action Owner	Drop Down	M	N/A	Dropdown user who defined as Action owners in User Share Point List Single Selection
Current Status of Action	Drop Down	M	N/A	• Not Started (Default) • In progress • Completed Once Vulnerability Added this should be default to “Not Started”
Remark	Text Area	O	255	

Draft	Button	N/A	N/A	Assessment should be visible in Summery view, Draft Section
Submit	Button	N/A	N/A	To submit the Assessment to process owner, its mandatory to enter all fields except remark. Assessment should be send to Process Owner Summery View. Generate the Email Template 6.1.
Cancel Button	Button	N/A	N/A	

4.3 Risk Assessment Summary View – Process Owner

- Process Owner Will **receive the risk assessment** of their assigned process.
- The assignment is determined based on the **mapping between process and process owner** defined in the Admin Module.
- The Risk Team Assessment Summary View shall consist of two sections:

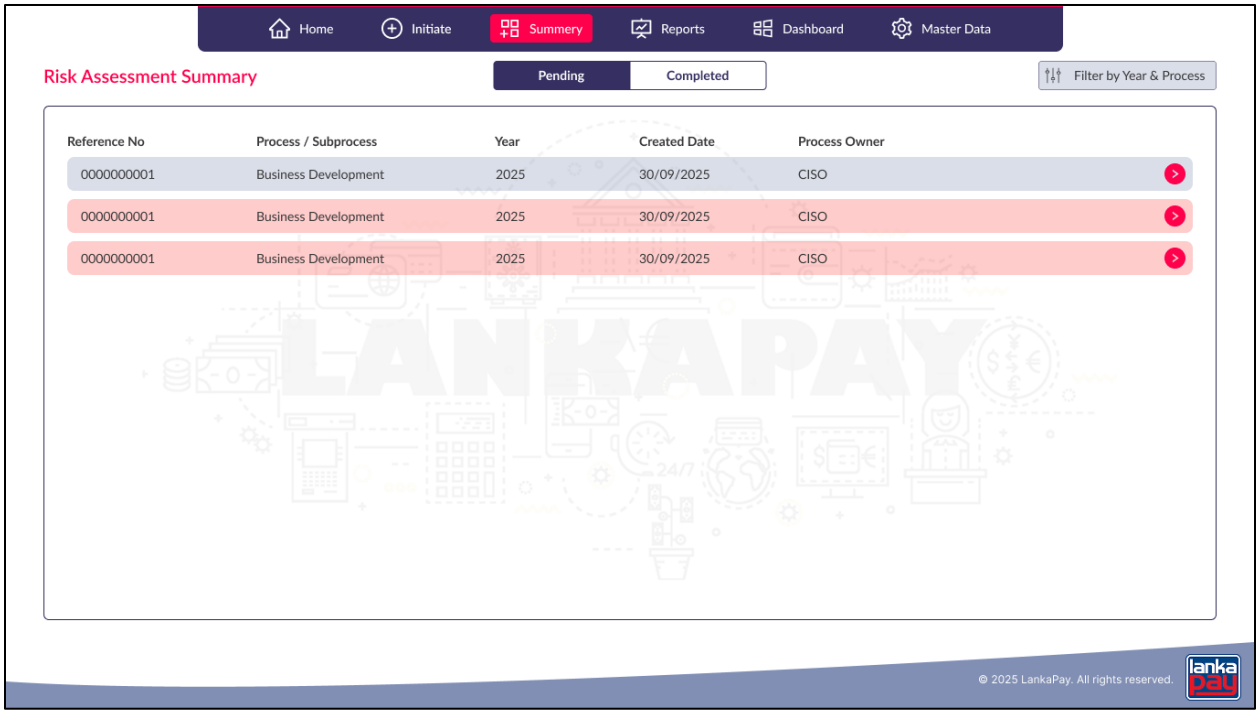
    1. **Pending** – Displays risk assessments that are awaiting action from the risk team. fields in this section shall be editable.

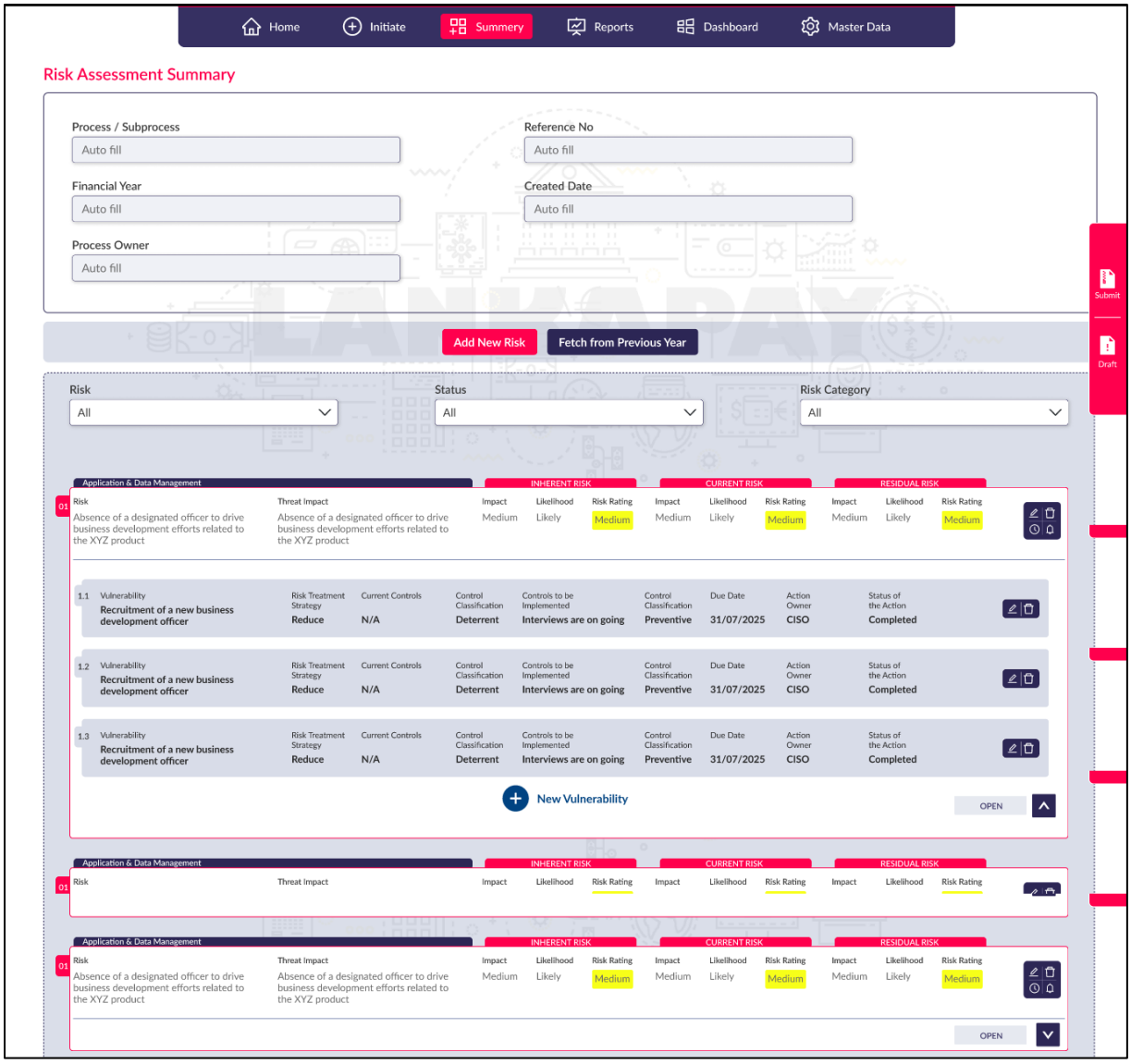
        Note: In scenarios where a user holds dual roles (e.g., Process Owner and Action Owner), the system shall display pending actions for both roles within the Pending section, differentiated by distinct colors for easy identification.

    2. **Completed** – Displays risk assessments that have been completed by the risk team. Fields in this section shall be non-editable.

- The system shall allow the **Process Owner** to perform the following actions within the Pending section:

    1. **Update Details of identified Risks** – Address and update risks identified by the Risk Team.
    2. **Add New Risks and Vulnerabilities** – Record and manage new risks or vulnerabilities directly identified by the Process Owner.


Home
Initiate
Summery
Reports
Dashboard
Master Data
Risk Assessment Summary
Pending
Completed
Filter by Year & Process
Reference No
Process / Subprocess
Year
Created Date
Process Owner
0000000001
Business Development
2025
30/09/2025
CISO
0000000001
Business Development
2025
30/09/2025
CISO
0000000001
Business Development
2025
30/09/2025
CISO
© 2025 LankaPay. All rights reserved.



Note: if new risk added by process owner Inherent Risk details, Current Risk Rating details, Residual Rate Details and Risk Status Enable after Vulnerability added.

Please note the inherent, current and residual risk details of the risks added by process owner should be mandatory before submission, else display an error message.

Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Process	Auto Filled	N/A	N/A	
Process Owner	Auto Filled	N/A	N/A	
Risk Assessment Reference	Auto Filled	N/A	N/A	
Financial Year	Auto Filled	N/A	N/A	
Created Date	Auto Filled	N/A	N/A	
Risk No	Auto Filled	N/A	N/A	
Risk Category	Auto Filled/Editable	M	N/A	
Predefined Risk/ New Risk	Auto Filled/Editable	M	N/A	
Risk	Auto Filled/Editable	M	N/A	
Threat Impact	Auto Filled/Editable	M	N/A	
Risk Status	Auto Filled/Editable	O	N/A	
Inherent Risk Impact	Auto Filled/Editable	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable.
Likelihood	Auto Filled/Editable	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable.
Inherent Risk Rating	Auto Filled	N/A	N/A	

Current Risk Impact	Auto Filled/Editable	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable.
Likelihood	Auto Filled/Editable	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable.
Current Risk Rating	Auto Filled	N/A	N/A	
Residual Risk Impact	Auto Filled/Editable	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable.
Likelihood	Auto Filled/Editable	M	N/A	Note: until at least one vulnerability added for the particular Risk, this filed should be disable.
Residual Risk Rating	Auto Filled	N/A	N/A	
Vulnerability No	Auto Filled	N/A	N/A	
Vulnerability	Auto Filled/Editable	M	N/A	To add a, risk its mandatory to add at least one vulnerability, else display an error message
Risk Treatment Strategy	Auto Filled/Editable	M	N/A	• Mitigate • Accept • Avoid • Transfer If Accept, Avoid or Transfer below Fields should be auto filled as Not Applicable **Current Controls, Control Classifications, Controls to be implemented, Control Classification, Due Date, Action Owner, Current Status of action**
Current Controls	Auto Filled/Editable	M	N/A	
Control Classification	Auto Filled/Editable	M	N/A	
Controls To be Implemented	Auto Filled/Editable	M	N/A	
Control Classification	Auto Filled/Editable	M	N/A	
Due Date	Auto Filled/Editable	M	N/A	
Action Owner	Auto Filled/Editable	M	N/A	Dropdown user who defined as Action owners in User Share Point List Single Selection

Current Status of Action	Auto Filled/Editable	M	N/A	• Not Started (Default) • In progress • Completed Once Vulnerability Added this should be default to “Not Started”
Remark	Auto Filled/Editable	O	N/A	
Draft	Button	N/A	N/A	Save the updated details and keep the Assessment in pending section itself for later submission to Risk Team
Submit	Button	N/A	N/A	Assessment should be send to Risk Team Summery View. Generate the Email Template 6.2.
Cancel Button	Button	N/A	N/A	

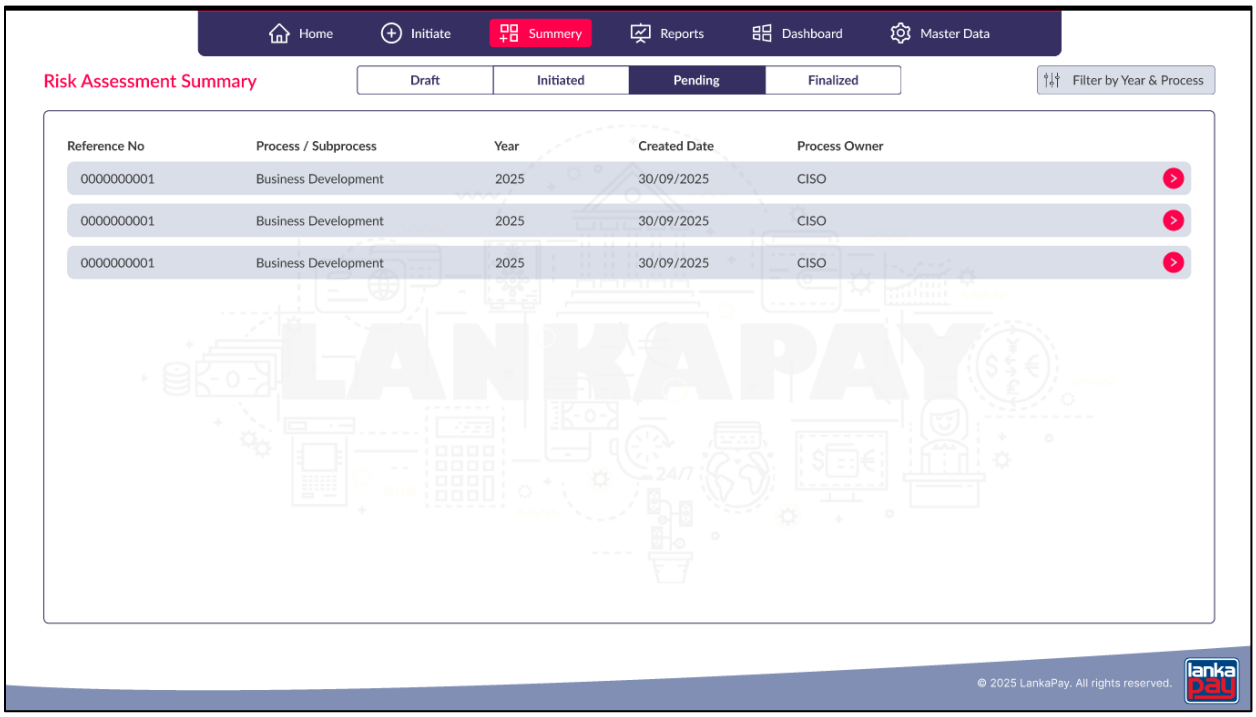
4.4 Risk Assessment Summary View – Risk Team

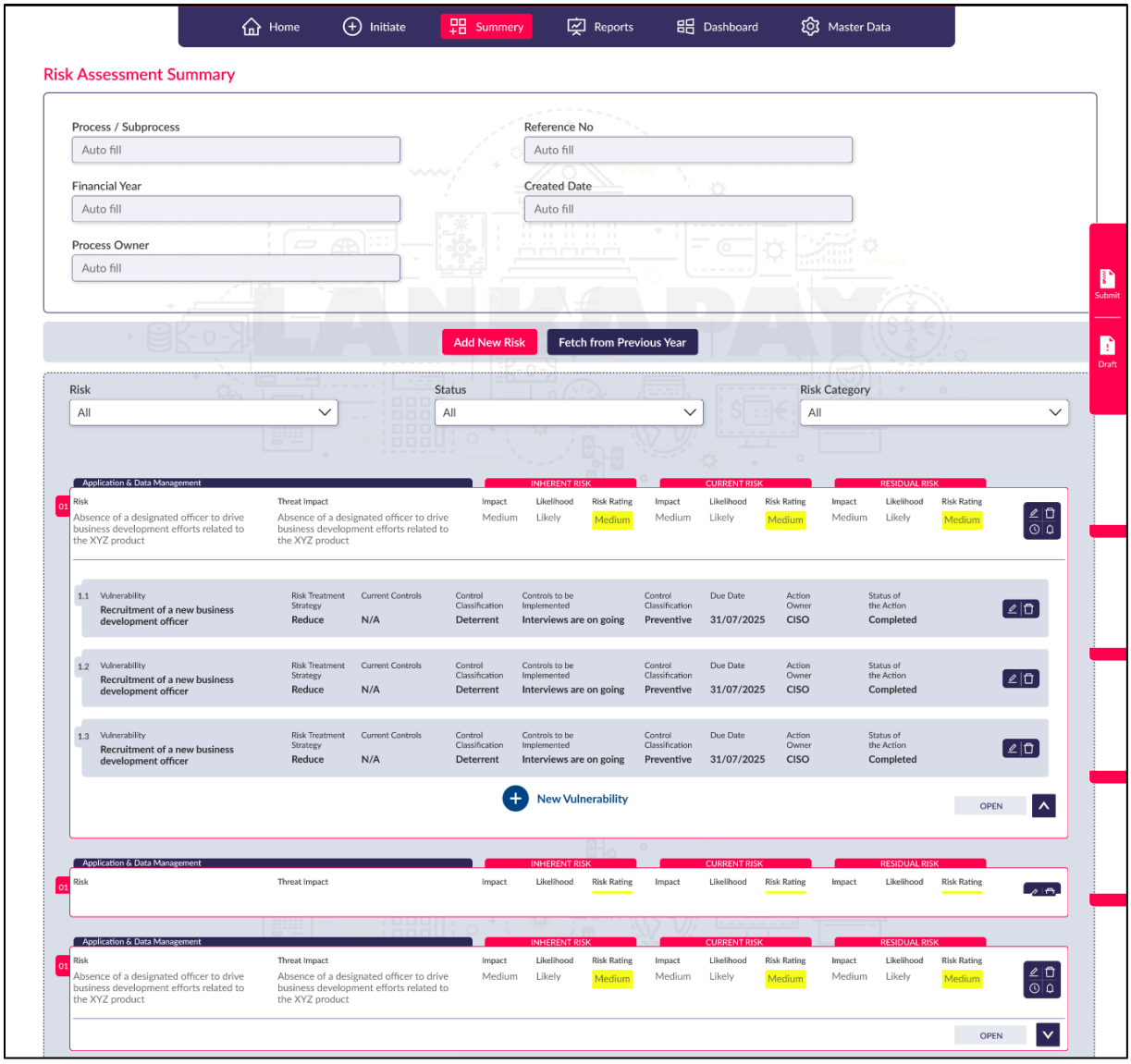
The Risk Team's Summary View is organized into four sections, each reflecting the status of risk assessments and their respective permissions:

1. **Draft**
    - Displays drafted assessments that are yet to be submitted.
    - All fields remain **editable** for further updates or changes.
2. **Submitted**
    - Displays assessments already submitted to the Process Owner.
    - Fields are **read-only (non-editable)** while awaiting Process Owner's action.
3. **Pending**
    - Displays assessments completed and submitted by the Process Owner.
    - Currently pending Risk Team action to finalize.
    - Fields remain **editable** for the Risk Team.
    - The system shall allow users to update details periodically, and draft changes and later Finalization.
4. **Finalized**
    - Displays assessments that have been finalized and are awaiting Action Owner updates.
    - Since, Risk Team has the full Authority to Risk Assessment. They should be able to edit required details if necessary even after Finalized.

Note: In the summary views, risk cards shall remain collapsed by default, hiding their associated vulnerabilities. When the 'Expand' icon is clicked, the system shall **expand** specific risk card to display their vulnerabilities.

4.4.1 Risk Assessment Summary Pending Finalization Section




Home
Initiate
Summery
Reports
Dashboard
Master Data
Risk Assessment Summary
Process / Subprocess
Auto fill
Reference No
Auto fill
Financial Year
Auto fill
Created Date
Auto fill
Process Owner
Auto fill
Submit
Draft
Add New Risk
Fetch from Previous Year
Risk
All
Status
All
Risk Category
All
Application & Data Management
INHERENT RISK
CURRENT RISK
RESIDUAL RISK
01
Risk
Absence of a designated officer to drive business development efforts related to the XYZ product
Threat Impact
Absence of a designated officer to drive business development efforts related to the XYZ product
Impact
Likelihood
Risk Rating
Medium
Likely
Medium
1.1
1.2
1.3
Vulnerability
Recruitment of a new business development officer
Risk Treatment Strategy
Reduce
Current Controls
N/A
Control Classification
Deterrent
Controls to be Implemented
Interviews are on going
Control Classification
Preventive
Due Date
31/07/2025
Action Owner
CISO
Status of the Action
Completed
New Vulnerability
OPEN

Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Process	Auto Filled	N/A	N/A	
Process Owner	Auto Filled	N/A	N/A	
Risk Assessment Reference	Auto Filled	N/A	N/A	
Financial Year	Auto Filled	N/A	N/A	
Created Date	Auto Filled	N/A	N/A	
Risk No	Auto Filled	N/A	N/A	
Risk Category	Auto Filled/Editable	M	N/A	
Predefined Risk/ New Risk	Auto Filled/Editable	M	N/A	
Risk	Auto Filled/Editable	M	N/A	
Threat Impact	Auto Filled/Editable	M	N/A	
Risk Status	Auto Filled/Editable	M	N/A	Open Closed Accepted Avoided Transferred Not Applicable
Fetch From Previous Year	Button	N/A	N/A	When the user clicks on the *Fetch from Previous* button, all risks from the previous financial year related to the selected process shall be displayed in grid view. Should be able to filter by Risk Status

				The user shall have the ability to multi-select risks and add them to the current year's assessment. A *Select All* option shall also be available
Inherent Risk Impact	Auto Filled/Editable	M	N/A	
Likelihood	Auto Filled/Editable	M	N/A	
Inherent Risk Rating	Auto Filled	N/A	N/A	
Current Risk Impact	Auto Filled/Editable	M	N/A	
Likelihood	Auto Filled/Editable	M	N/A	
Current Risk Rating	Auto Filled	N/A	N/A	
Residual Risk Impact	Auto Filled/Editable	M	N/A	
Likelihood	Auto Filled/Editable	M	N/A	
Residual Risk Rating	Auto Filled	N/A	N/A	
Vulnerability No	Auto Filled	N/A	N/A	
Vulnerability	Auto Filled/Editable	M	N/A	For each risk at least one vulnerability should be added before finalize.
Risk Treatment Strategy	Auto Filled/Editable	M	N/A	• Mitigate • Accept • Avoid • Transfer If Accept, Avoid or Transfer below Fields should be autofill as Not Applicable **Current Controls, Control Classifications, Controls to be implemented, Control Classification, Due Date, Action Owner, Current Status of action**
Current Controls	Auto Filled/Editable	M	N/A	
Control Classification	Auto Filled/Editable	M	N/A	

Controls To be Implemented	Auto Filled/Editable	M	N/A	
Control Classification	Auto Filled/Editable	M	N/A	
Due Date	Auto Filled/Editable	M	N/A	
Action Owner	Auto Filled/Editable	M	N/A	
Current Status of Action	Auto Filled/Editable	N/A	N/A	• Not Started (Default) • In progress • Completed
Remark	Auto Filled/Editable	O	N/A	
Draft	Button	N/A	N/A	Save the updated details and keep the Assessment in pending section itself for later submission
Finalize	Button	N/A	N/A	If Finalize check all of fields except Current Status/Remark is filled, if not display error message. Once finalize Tasks should be visible in each Action owners summary view. Generate the Email Template 6.3,6.4,6.5. If Update Risk Status as "Accepted, Avoided, Not Applicable or Transferred", Generate the Email Template 6.8. If Update Risk Status as "Closed", Generate the Email Template 6.9.
Sent Back	Button	N/A	N/A	Assessment should be send Back to Process Owner Summery View for Amendments.
Cancel Button	Button	N/A	N/A	

4.4.2 Risk Assessment Summary Finalized Section

Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Process	Auto Filled	N/A	N/A	
Process Owner	Auto Filled	N/A	N/A	
Risk Assessment Reference	Auto Filled	N/A	N/A	
Financial Year	Auto Filled	N/A	N/A	
Created Date	Auto Filled	N/A	N/A	
Risk No	Auto Filled	N/A	N/A	
Risk Category	Auto Filled	N/A	N/A	
Predefined Risk/ New Risk	Auto Filled	N/A	N/A	
Risk	Auto Filled	N/A	N/A	
Threat Impact	Auto Filled	N/A	N/A	

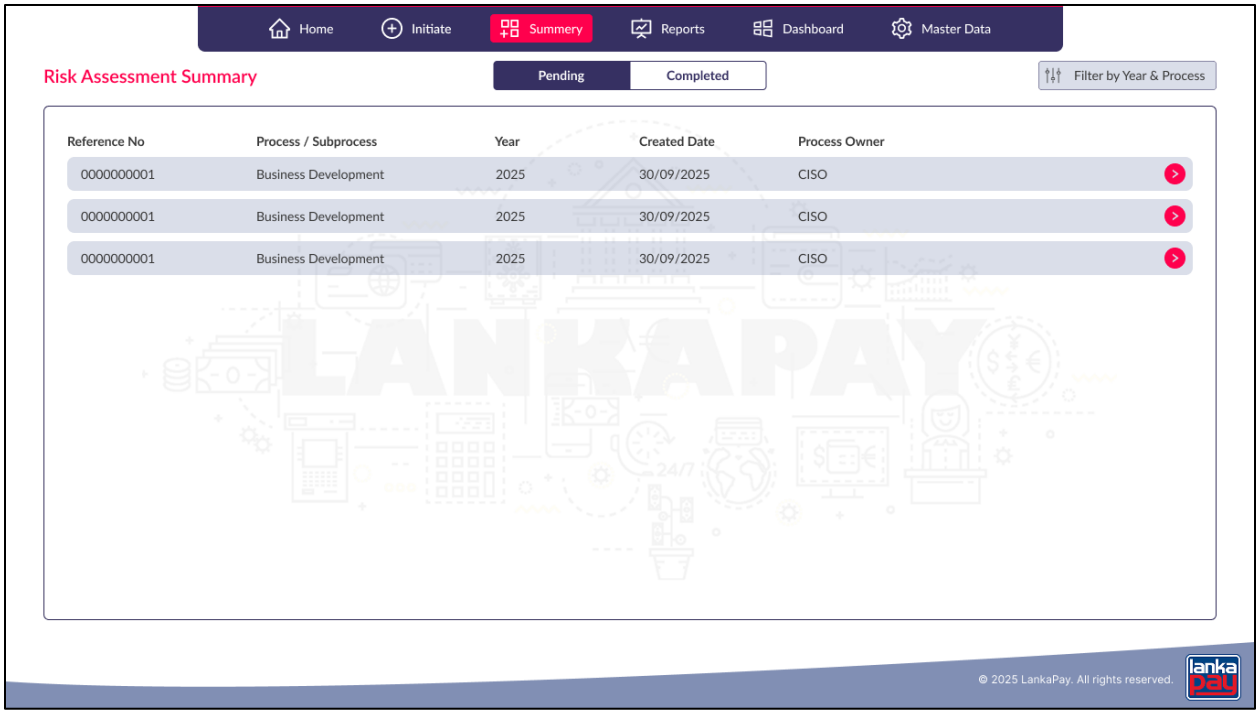
Risk Status	Auto Filled	N/A	N/A	
Inherent Risk Impact	Auto Filled	N/A	N/A	
Likelihood	Auto Filled	N/A	N/A	
Inherent Risk Rating	Auto Filled	N/A	N/A	
Current Risk Impact	Auto Filled	N/A	N/A	
Likelihood	Auto Filled	N/A	N/A	
Current Risk Rating	Auto Filled	N/A	N/A	
Residual Risk Impact	Auto Filled	N/A	N/A	
Likelihood	Auto Filled	N/A	N/A	
Residual Risk Rating	Auto Filled	N/A	N/A	
Vulnerability No	Auto Filled	N/A	N/A	
Vulnerability	Auto Filled	N/A	N/A	
Risk Treatment Strategy	Auto Filled	N/A	N/A	
Current Controls	Auto Filled	N/A	N/A	
Control Classification	Auto Filled	N/A	N/A	
Controls To be Implemented	Auto Filled	N/A	N/A	
Control Classification	Auto Filled	N/A	N/A	
Due Date	Auto Filled	N/A	N/A	There should be an icon to view due date revision history after finalization
Action Owner	Auto Filled	N/A	N/A	
Current Status of Action	Auto Filled	N/A	N/A	
Remark	Auto Filled	N/A	N/A	

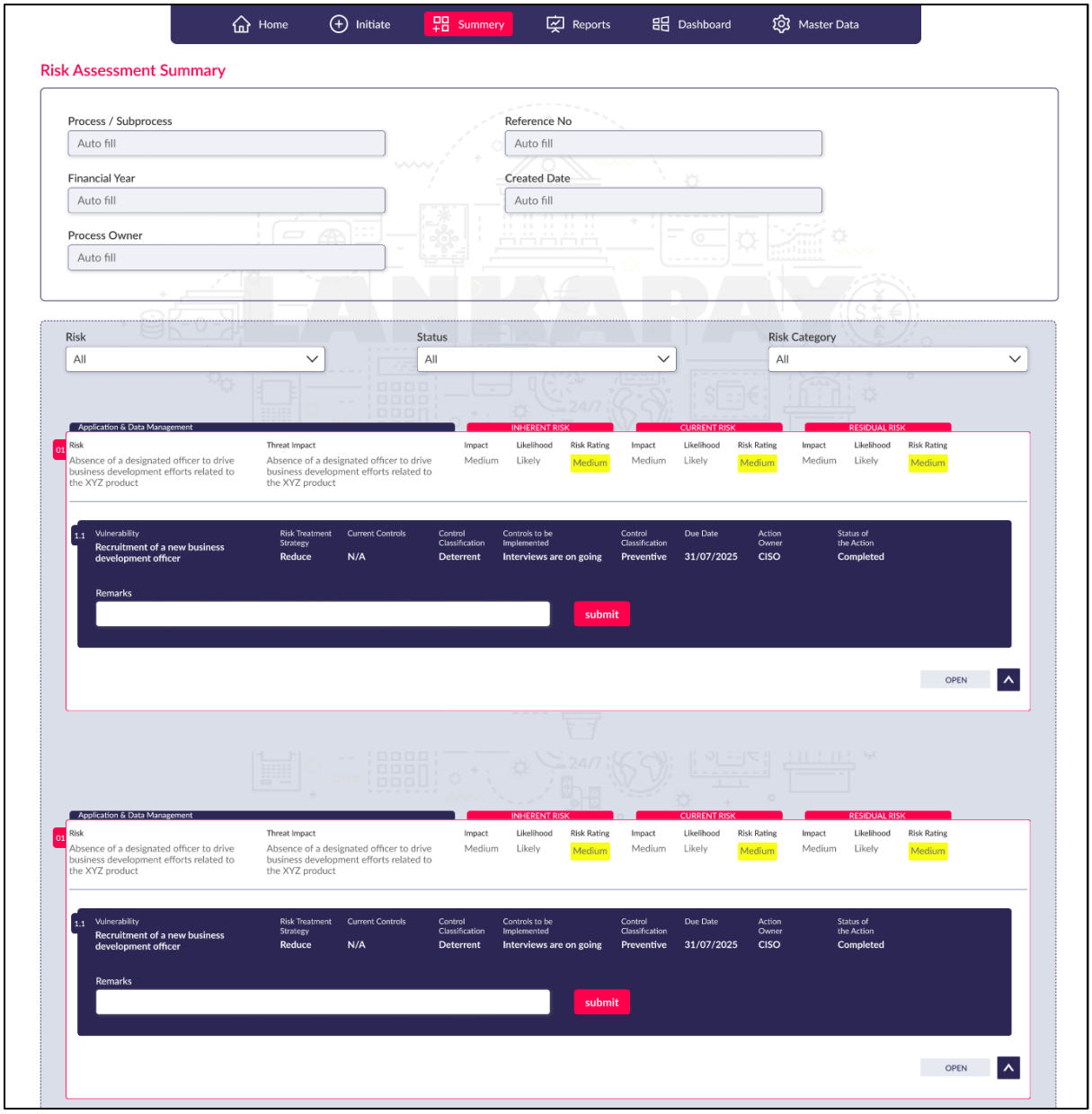
Edit	Icon	N/A	N/A	When the user clicks on 'Edit,' all fields shall be editable except for the fields listed below. The Risk Team shall be able to update any of the editable fields. Process, Process owner, Assessment Reference, Financial Year, Created date, Risk No, Inherent/Current/Residual Risk Rating, Vulnerability No Action owner editable only if action not been taken yet. All Changes should capture in Audit log. IF Action Owner Updated, Generate the Email Template 6.3,6.4,6.5, 6.10. IF Due Date, Control to be implemented Updated Generate the Email Template 6.10.
Remind icon	Icon	N/A	N/A	If risk team click on remind icon, if Current Status != Completed Generate the Email Template 6.3.

4.5 Risk Assessment Summary View – Action Owner

- The Action Owner Assessment Summary View shall consist of two sections:

    1. **Pending** – Displays risk assessments that are pending action from the Risk Team. Action Owners can view/Take Action only the risks or vulnerabilities assigned specifically to them.
    2. **Completed** – Displays risk assessments that have been completed by the Action Owner. Fields in this section shall be non-editable.




Home
Initiate
Summery
Reports
Dashboard
Master Data
Risk Assessment Summary
Process / Subprocess
Auto fill
Reference No
Auto fill
Financial Year
Auto fill
Created Date
Auto fill
Process Owner
Auto fill
Risk
All
Status
All
Risk Category
All
Application & Data Management
INHERENT RISK
CURRENT RISK
RESIDUAL RISK
01
Risk
Absence of a designated officer to drive business development efforts related to the XYZ product
Threat Impact
Absence of a designated officer to drive business development efforts related to the XYZ product
Impact
Likelihood
Risk Rating
Medium
Likely
1.1
Vulnerability
Recruitment of a new business development officer
Risk Treatment Strategy
Reduce
Current Controls
N/A
Control Classification
Deterrent
Controls to be Implemented
Interviews are on going
Control Classification
Preventive
Due Date
31/07/2025
Action Owner
CISO
Status of the Action
Completed
Remarks
submit
OPEN

Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Process	Auto Filled	N/A	N/A	
Process Owner	Auto Filled	N/A	N/A	
Risk Assessment Reference	Auto Filled	N/A	N/A	
Financial Year	Auto Filled	N/A	N/A	
Created Date	Auto Filled	N/A	N/A	
Risk No	Auto Filled	N/A	N/A	
Risk Category	Auto Filled	N/A	N/A	
Predefined Risk/ New Risk	Auto Filled	N/A	N/A	
Risk	Auto Filled	N/A	N/A	
Threat Impact	Auto Filled	N/A	N/A	
Risk Status	Auto Filled	N/A	N/A	
Inherent Risk Impact	Auto Filled	N/A	N/A	
Likelihood	Auto Filled	N/A	N/A	
Inherent Risk Rating	Auto Filled	N/A	N/A	
Current Risk Impact	Auto Filled	N/A	N/A	

Likelihood	Auto Filled	N/A	N/A	
Current Risk Rating	Auto Filled	N/A	N/A	
Residual Risk Impact	Auto Filled	N/A	N/A	
Likelihood	Auto Filled	N/A	N/A	
Residual Risk Rating	Auto Filled	N/A	N/A	
Vulnerability No	Auto Filled	N/A	N/A	
Vulnerability	Auto Filled	N/A	N/A	
Risk Treatment Strategy	Auto Filled	N/A	N/A	
Current Controls	Auto Filled/Editable	M	N/A	
Control Classification	Auto Filled/Editable	M	N/A	
Controls To be Implemented	Auto Filled/Editable	M	N/A	
Control Classification	Auto Filled/Editable	M	N/A	
Due Date	Auto Filled	N/A	N/A	There should be an icon to view due date revision history after finalization
Action Owner	Auto Filled/ Editable	M	N/A	If Action Owner want to Assign the control to another user, they can edit and select the Next Action Owner. There can be up to maximum 3 levels of assignments Dropdown user who defined as Action owners in User Share Point List
Current Status of Action	Drop Down	M	N/A	Not Started In Progress Completed If Action owner update status as “In-progress”, keep the control action in pending section itself to complete later.
Remark	Text Area	O	255	

Submit	Button	N/A	N/A	If assign to Other Action Owner, Tasks should be visible in Action owners summary view. Generate the Email Template 6.3,6.4,6.5 If current status of action = Complete, Generate the Email Template 6.6.
Cancel Button	Button	N/A	N/A	

4.6 General Functional Requirements

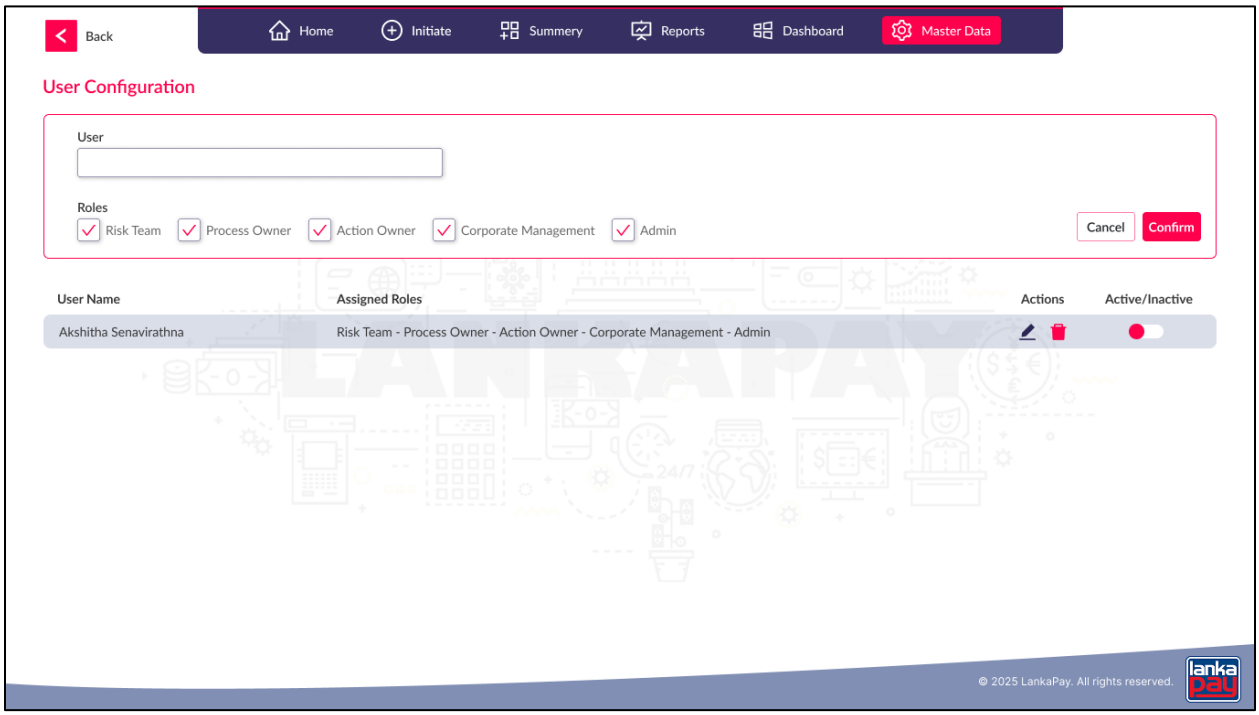
Functional Requirements	Description
Risk Assessment Reference Number Generation	• The system shall generate a unique risk assessment reference number in the format: **<ProcessCode>-<Financial Year>-<Sequence Number>** • The sequence number shall be auto-incremented for each new risk assessment created.
Mandatory Fields in Assessment	• All mandatory fields shall be clearly marked with an asterisk (*) symbol. • If a user attempts to submit the form without completing the mandatory fields, the system shall display an error message.
Request Search and Retrieval	• In the **Risk Summary View**, users shall be able to filter and retrieve requests based on the following parameters: Financial Year, Process, Risk Category, Risk, Risk Status
Activity Log and Audit Log	An **Activity Log** shall be maintained within the system. • Any user can access the activity log by clicking the history icon provided. • The activity log shall display user actions and relevant details, Action, Action Date Time, Action Taken By • If a risk is fetched from the previous financial year, the activity log should indicate it with the original Risk Assessment Reference Number. An **Audit Log** shall be available within the **Admin Module** only. • The audit log shall be exportable in CSV format. • Access shall be restricted to admin users only.
Notification Management	The system shall automatically trigger email notifications for actions, reminders, and escalations as defined in the SRS. Email Template Body wording should be configurable in Admin module. If the same user is assigned multiple roles (e.g., a Process Owner also acting as an Action Owner), the system shall ensure that email notifications are not duplicated for that user.
Color Coding in Risk Summary View	In the **Risk Summary View**, inherent, current, and residual risk ratings shall be color-coded for quick identification: • Frozen→ Light Blue • Chilling→ Light Purple • Heating→ Dark Orange • Flaming→ Red • Burning→ Maroon

4.7 Master Data Management

The configurations for the **Admin Module** are outlined in the following figure, providing a detailed overview of its setup and functionality.

4.7.1 User Configuration

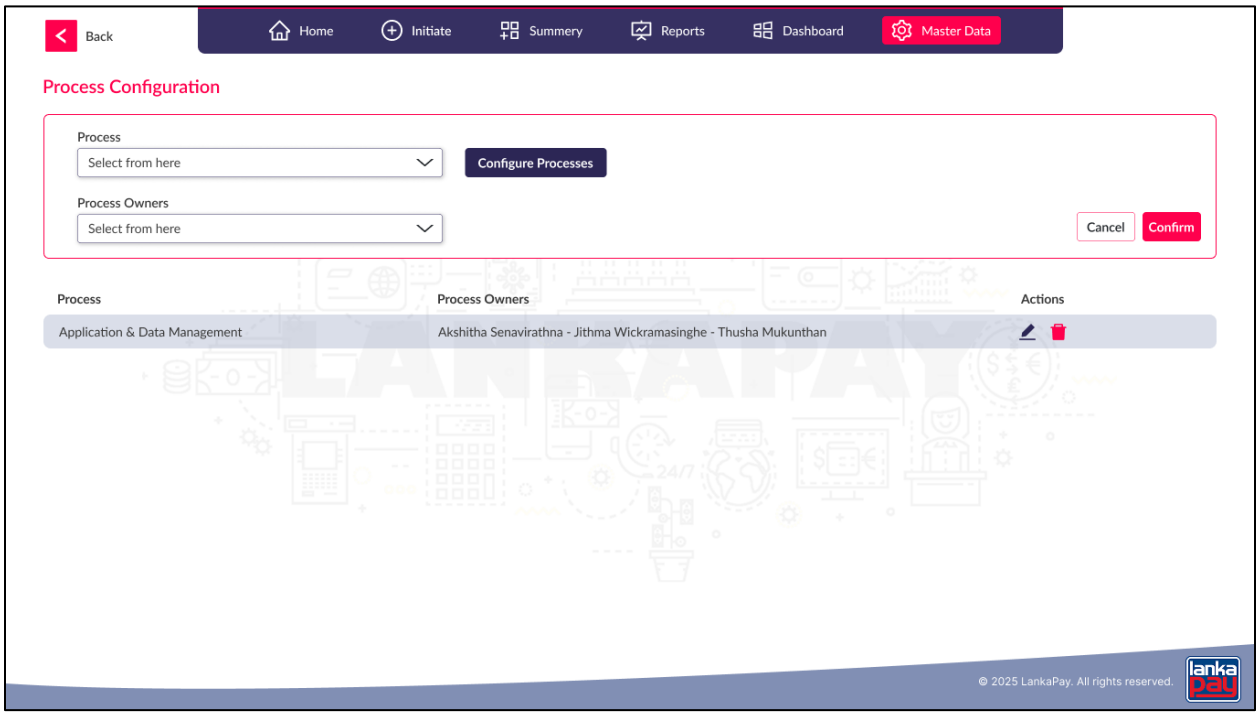
- Admin can create, edit, and delete user accounts.

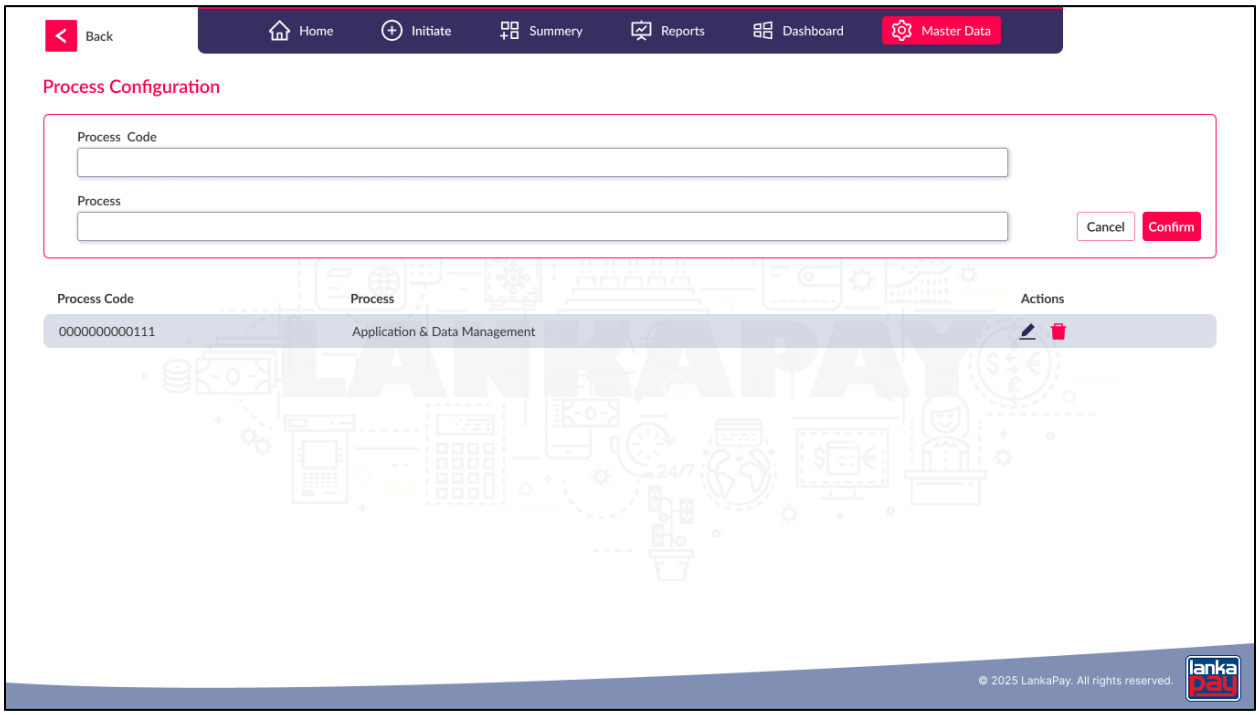


Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
User	AD Search	M	N/A	Drop down users from AD
Roles	Check Box	M	N/A	Should tick at least one Role. Multiple can be selected. Values: Risk Team, Process Owner, Action Owner, Corporate Management, Admin
Active/Inactive	Radio Button	M	N/A	By Default user should be Active.

4.7.2 Process Configuration

- Admin can add, edit, and delete organizational processes.

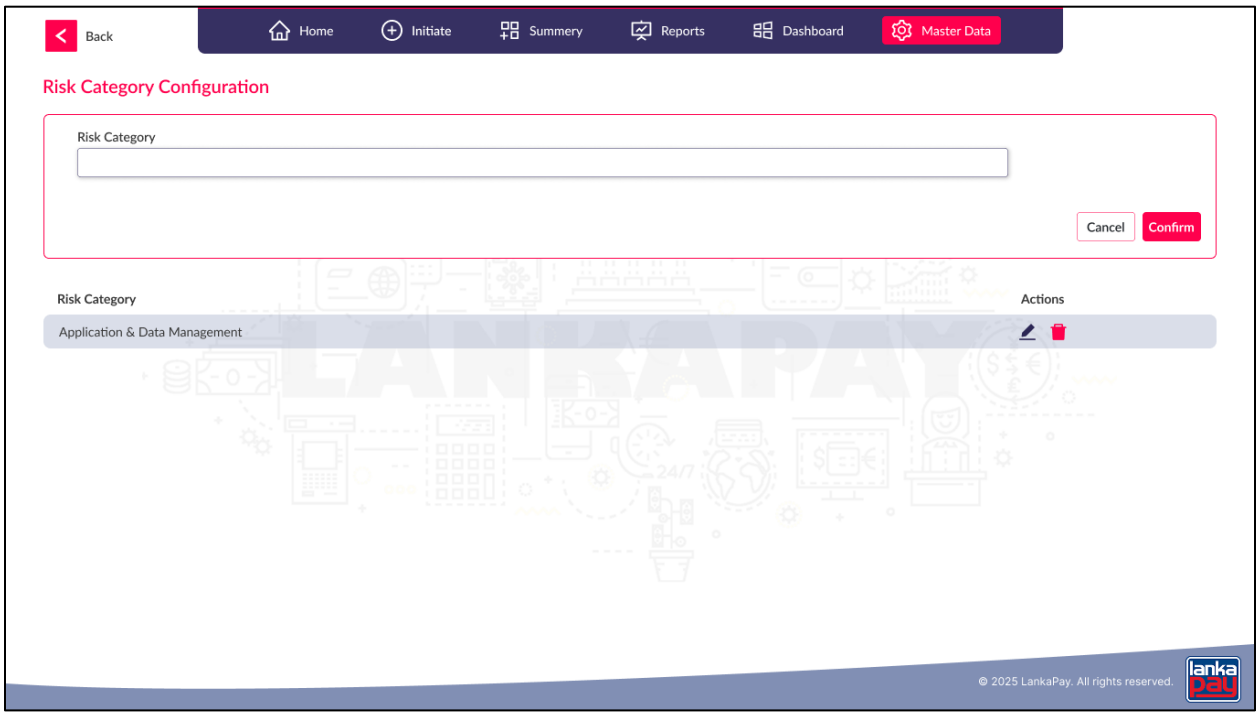




Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Process Code	Text Field	M	20	
Process	Text Field	M	100	
Process Owner	AD Search	M	N/A	• For each process, up to three (3) Process Owners can be assigned.

4.7.3 Risk Category Configuration

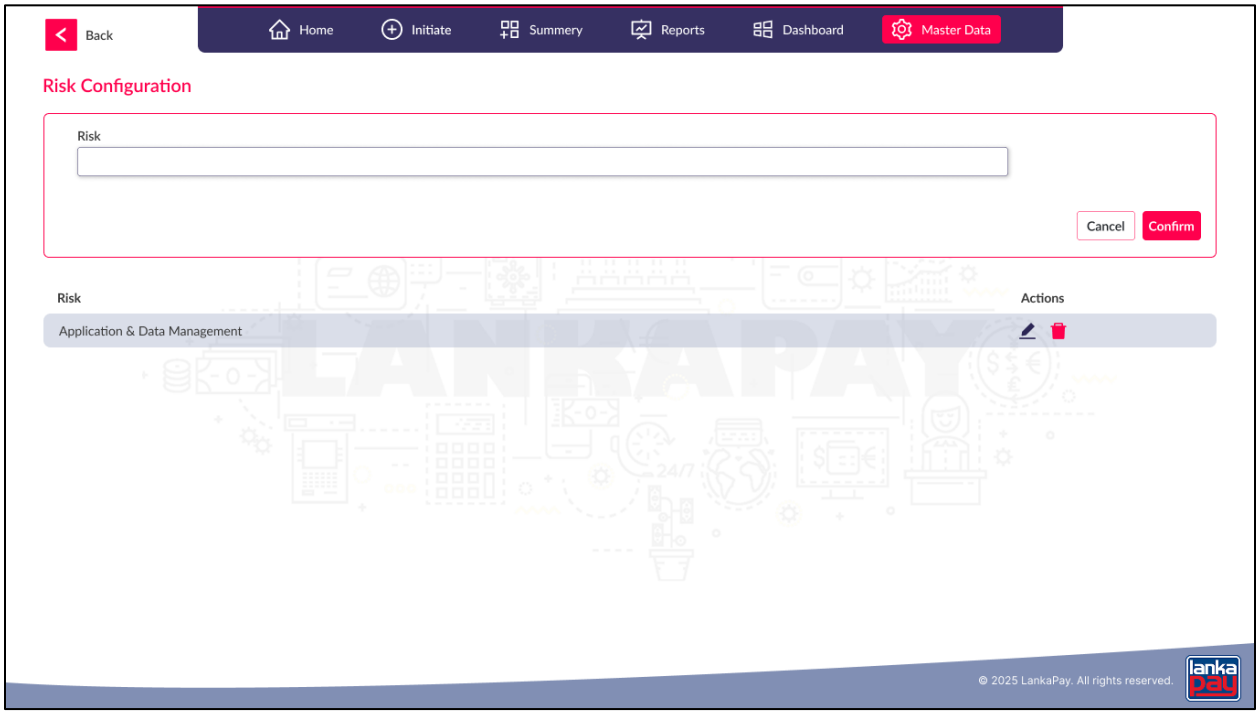
- Admin can manage risk categories by adding, editing, or deleting them



Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Risk Category	Text Field	M	100	

4.7.4 Risk Configuration

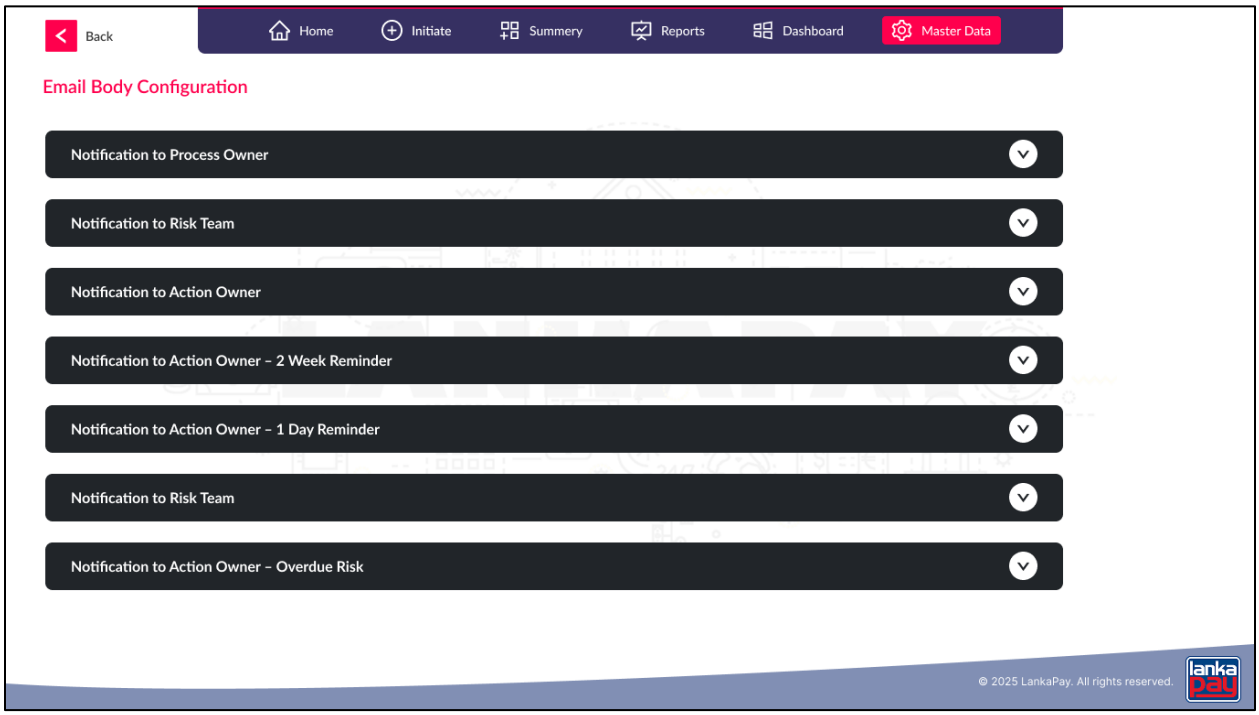
- Admin can add, edit, and delete risks.



Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Risk	Text Area	M	255	

4.7.5 Email Body Configuration

- The Admin should have the ability to add and edit the content of email body templates. For system-generated emails, the configured email body should be used when triggering notifications.
- There should be revision history to view changes done for each template.



Field Name	Controller Type	Mandatory/ Optional	Character Length	Remarks if any
Email Body	Text Area	M	255	

4.7.6 Audit Log

The system should maintain an audit log that records all actions taken within the platform. This log must capture the following details for each risk assessment and vulnerability:

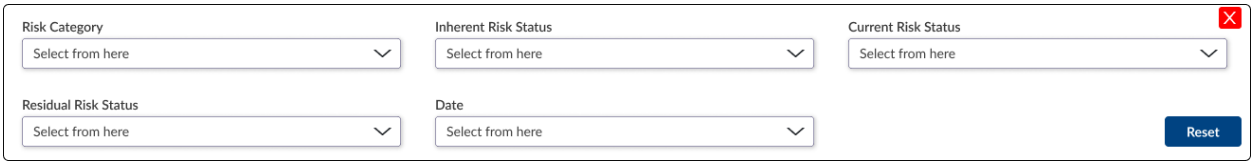
- **User:** The individual who performed the action.
- **Date and Time:** The timestamp of when the action was performed.
- **Activity:** A description of the activity or change made.

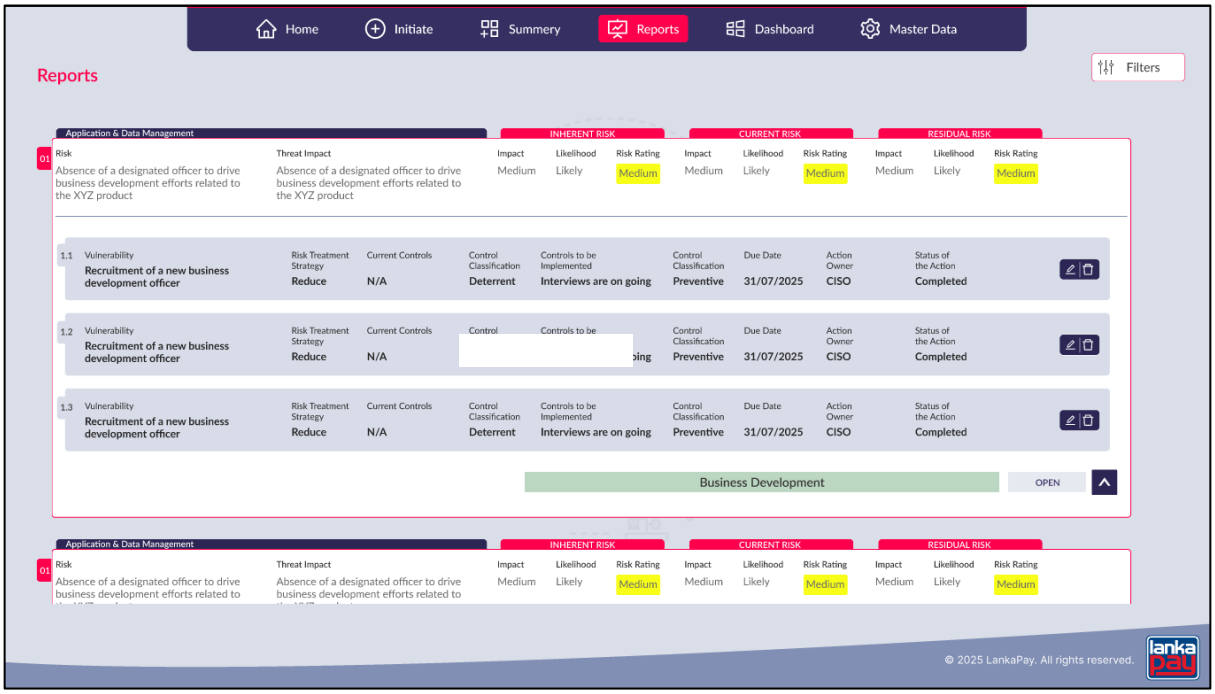
This audit log should be accessible for review and provide a clear history of all interactions with risk assessments and vulnerabilities.

- Format should be CSV

4.8 Report : Risk Registry

- The system shall maintain a centralized **Risk Registry** that consolidates all identified risks and associated vulnerability details for every process.
- **Filters:** Process (multiselect), Risk Category, Financial Year, Inherent Risk Rating, Current Risk Rating, Residual Risk Rating, Risk Status, Action Status, Created Date Range
- **Report Fields:** Fields same as summary view
- The records should be sorted in descending order based on the creation date and time, ensuring that the most recent records appear at the top of the list for easy access and review.
- The system should provide the functionality for users to export detailed request data into a excel file. All the Risk, vulnerability and Action details should be exported to the excel.





5 User Permission Matrix

User Role	Initiate Risk Assessment	Risk Assessment Summary	Dashboard	Report	Master Data
Risk Team	✓	✓	✓	✓	X
Process Owner/HOD	X	✓ [Their process only]	X	X	X
Action Owner	X	✓ [Assigned Actions Only]	X	X	X
Corporate Management	X	X	✓	✓	X
Admin	X	X	X	X	✓

- Same user can be in multiple user roles
- The system shall implement a role-based permission matrix. Once a user is assigned to a specific role, all functions and permissions associated with that role shall automatically be granted to the user.

6 Email Alert Templates

6.1 Notification to Process Owner

To : <Process Owner Email Address> Cc : Subject : Risk Assessment Assignment - <Reference Number>
Dear < Process Owner Name> *(fetch from email address)*, < Email Body> Process/Department: < xxxxxxx> Year: < xxxxxxx>   <Link to the workflow> Thank you!

6.2 Notification to Risk Team

To : <Risk initiator Email Address>
Cc :
Subject : Risk Assessment Completion - <Reference Number>

Dear < Risk Initiator Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>
Process Owner: < xxxxxxx>
Year: < xxxxxxx>

<Link to the workflow>

Thank you!

6.3 Notification to Action Owner

To : <Action Owner Email Address>
Cc :
Subject : New Action Assigned Notification - <Reference Number>

Dear < Action Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>

Risk Category	Risk	Vulnerability	Action	Due Date	Current Status
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- If Due date is prior to 2 weeks, this notification should be triggered immediately after Risk Finalization.
- If multiple controls are assigned with the same due date, they should be grouped and displayed in a single email notification, instead of sending separate emails.

6.4 Notification to Action Owner – 2 Week Reminder

To : <Action Owner Email Address>
Cc :
Subject : Reminder: Upcoming Action Due in 2 Weeks - <Reference Number>

Dear < Action Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>

Risk Category	Risk	Vulnerability	Action	Due Date	Current Status
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- The system shall automatically send **timely follow-up reminder emails** only for Action controls that remain in **Not Started, In Progress** statuses.
- Time period is 2weeks.
- If multiple controls are assigned with the same due date, they should be grouped and displayed in a single email notification, instead of sending separate emails.

6.5 Notification to Action Owner – 1 Day Reminder

To : <Action Owner Email Address>
Cc :
Subject : Reminder: Action Item Due Tomorrow - <Reference Number>

Dear < Action Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>

Risk Category	Risk	Vulnerability	Action	Due Date	Current Status
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- The system shall automatically send **timely follow-up reminder emails** only for Action controls that remain in **Not Started, In Progress** statuses.
- Time period is 1day.
- If multiple controls are assigned with the same due date, they should be grouped and displayed in a single email notification, instead of sending separate emails.

6.6 Notification to Risk Team – Action Completed

To : <Risk initiator Email Address>
Cc :
Subject : List of Open Actions Completed as of <Todays Date> - <Reference Number>

Dear < Risk Initiator Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>
Date: < xxxxxxx>

Risk	Vulnerability	Action	Action Owner
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- Daily Batch job should be scheduled at each day end to trigger **a single consolidated email notification** to the Risk Team mentioning Completed actions.

6.7 Notification to Action Owner – Overdue Risk

To : <Action Owner Email Address> <Process Owner Email Address>
Cc :
Subject : Overdue Actions Notification- <Reference Number>

Dear < Action/Process Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>

Risk Category	Risk	Vulnerability	Action	Action Owner	Due Date	Current Status
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- If an action status remains in **not started/In Progress** status beyond its assigned due date, the system shall trigger an **overdue email notification**
- If multiple controls are overdue with the same due date, they should be grouped and displayed in a single email notification, instead of sending separate emails.

6.8 Notification to Process Owner - Updated Risk Status

To : <Process Owner Email Address>
Cc :
Subject : Update on Risk Status - <Reference Number>

Dear < Process Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>

Risk	Status
< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- This email should be triggered, When a risk item status is Accepted, Avoided, Not Applicable or Transferred is done

6.9 Notification of Closed Risk

To : <Action Owner Email Address> <Process Owner Email Address>
Cc :
Subject : Congratulations – Risk is Successfully Mitigated- <Reference Number>

Dear < Action/Process Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>
Year: < xxxxxxx>

Risk	Status
< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- This email should be triggered, When a risk item status is Closed is done
- Only send to Action Owners associated with particular Risk Only

6.10 Notification of Action/Due Date Updates

To : < Previous Action Owner Email Address> <New Action Owner Email Address> <Process Owner Email Address>
Cc :
Subject : Notification of Changes- <Reference Number>

Dear < Action/Process Owner Name> *(fetch from email address)*,

< Email Body>

Process/Department: < xxxxxxx>

Control	Action Owner	Due Date
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>
< xxxxxxx>	< xxxxxxx>	< xxxxxxx>

<Link to the workflow>

Thank you!

- This email should be triggered, When an update is done (to Control to be implemented, Action Owner or Due Date) from Risk Team after finalizing.
- If Action owner changed, need to notify previous Action Owner As well.

7 Approval for Software Requirement Specification Document

We have read and understood this **Software Requirement Specification Document V1.2** for Risk Module Solution Implementation for **Lankapay**. The expected solution design needs to be as prescribed above.

LANKAPAY	**Tech One Global Lanka (Pvt) Ltd.**
Signed by: **Name:** H.G.A.R.Senavirathna **Designation:** Assistant Manager-Risk & Compliance Akshitha Senavirathna Digitally signed by Akshitha Senavirathna Date: 2025.10.13 17:39:44 +05'30' **Signature with Company Stamp:** **Date:** 13/10/2025 Name : K. V. Srimali Premalal Designation : Chief Information Systems Audit Officer K. V. S. Premalal Digitally signed by K. V. S. Premalal Date: 2025.10.13 17:57:20 +05'30'	**Signed by:** **Name: Sandunika Daniel** **Designation: Lead – Project Management** **Signature with Company Stamp:** **Date: 13th October 2025**