Using ORM

Using the Remediation Experience for ORM

The Operational Risk Management Solution uses the Remediation Experience within the Workiva Platform to support Incident and Event Loss Management.

When you open up the remediation experience, you will see a list view of incidents and events that are being monitored in the workspace. You can either open up a current incident, or you can create a new incident by clicking on the create button. I will go ahead and open an existing incident that was created around data security.

When I open up and incident I see my data form. Consistent with the other forms within the database, the incident and event loss form is fully customizable to ensure that each organization can track required data elements and relationships within their operational risk structure.

In this example, we have properties such as IDs and Descriptions. We have the ability to assign ownership of these incidents and events as well as track the "type" of incident that is being created as well as specific dates the incident has occurred.

We can tie incidents or events directly to business units, risks, and control. We can also specially record the financial gain or loss of a specific incident or event. The amount can then be aggregated by business unit or process for evaluation by senior management. We have also created sections within the form.

When looking at a Root Cause analysis, we can create drop downs of options for consistent reporting, or free text fields can also be incorporated. Calculated fields can also be incorporated into the incident and event form in the case an organization wants to evaluate incident severity or some other calculated measure into the form. In this instance, I can select levels of severity and a cumulative severity will calculate. These calculations can help drive further review or analysis.

Also incorporated into the form is the ability to build review plans for each incident or event. These review plans drive workflow across the organization so individuals can review and approve each incident or even prior to closure. You can add one level of review, or multiple levels of review to each incident or event. The system will use this review plan to create tasks and notify individuals that their review is required. Review logs will show all the activity within the review plan.

The Workiva Request functionality is also used within the remediation experience. Incident owners can request supporting documentation to other individuals within the

organization. The system will notify these individuals of the request and assignees will have the opportunity to upload direct.

Workflow within the platform is also used to create tasks, track outstanding requests, and provide back and forth communication activities to ensure the support being provided is accurate. Each request will be linked directly to the incident form for tracking status and easy navigation. Each incident or event allows for the creation of one, or multiple action plans.

The action plan form is very similar to that of the incident form where form is fully customizable to ensure that each organization can track required data elements and relationships. The action plan form allows for the same request functionality to occur for gathering support data around the action plan. Each action plan is directly linked to the incident or event in which it has been created.

Going back to the incident form I can easily see all action plans and requests that have been created as part of managing this incident within the workspace.

Testing Operational Controls

The Operational Risk Management Solution allows Risk Management and Compliance Teams the ability to perform detailed testing of controls within the Checklists Experience.

The Checklists Experience is built on our Audit functionality.

When creating a new checklist, the user can choose between creating a Blank Checklist and creating an Existing Checklist structure that has already been used from a previous audit.

Within the list view, you can see the Title of the review, the objective, the auditor, the reviewer, as well as the status of the audit being performed.

I will go ahead and open up an audit that is currently in progress. By doing so, this will launch the checklist form.

Checklist forms are very similar to other testing and remediation forms in the database. Checklist forms are fully customizable to ensure that each organization can track required data elements and audit information within their operational risk structure. Organizations can track key data elements of each audit such as objectives, locations, start and end dates, as well as the overall health and status. Organizations can budget hours for each audit, and track time against that budget.

Review plans can be established that will generate tasks and notifications to reviews to when the audit is completed and ready for review. The review history is also stored directly in the audit form. Any ongoing issues associated with an audit will also be identified and status of the remediation plans will be displayed. This provided the reviewers a holistic view of the audit prior to final sign off.

Based on the risk information that is being audited, organizations can create their own test phases and procedures. In this example, we are performing test procedures on multiple controls.

From the main checklist form, I can see the results and status of each of these test procedures. If I drill into a test procedure, another form will open. As already noted, test procedure forms are fully customizable to ensure that each organization can track required data elements and audit information within their operational risk structure.

In this example, I can see the controls that I am testing. I can track status, attach relevant files and conclude on the test. Review plans can be built for each test procedure that allows that some tasking and workflow capabilities as testing and remediation forms within the platform.

Specific test steps and attributes can be built within each procedure. These test steps and attributes then support out sample based testing matrix so auditors or testers are able to pass or fail each sample tested.

Similar to our control testing forms, testers are able to request supporting documentation for each sample. That supporting documentation can then be marked up to support the test that was performed. If any Issues that are identified as part of the audit procedures performed can easily be created from the audit form, and that issue can be tracked through the remediation experience within the platform.

Using checklists as part of operational risk management increases efficiency by managing the testing of operational controls inside a single, secure cloud platform. Aggregate testing observations can be easily shared with risk committees, or senior management can drill down into specific test results in real-time.

Risk Assessments

Operational Risk Assessments can be performed using the Assessments experience in the Workiva platform.

Assessments are used to collect information about a particular object of data in the database. In this case, we want to collect data around a particular risk.

Video Transcript

The Operational Risk Management Solution uses the Remediation Experience within the Workiva Platform to support Incident and Event Loss Management.

When you open up the remediation experience, you will see a list view of incidents and events that are being monitored in the workspace. You can either open up a current incident, or you can create a new incident by clicking on the create button.

I will go ahead and open an existing incident that was created around data security. When I open up and incident I see my data form.

Consistent with the other forms within the database, the incident and event loss form is fully customizable to ensure that each organization can track required data elements and relationships within their operational risk structure.

In this example, we have properties such as IDs and Descriptions. We have the ability to assign ownership of these incidents and events as well as track the "type" of incident that is being created as well as specific dates the incident has occurred.

We can tie incidents or events directly to business units, risks, and control. We can also specially record the financial gain or loss of a specific incident or event. The amount can then be aggregated by business unit or process for evaluation by senior management. We have also created sections within the form.

When looking at a Root Cause analysis, we can create drop downs of options for consistent reporting, or free text fields can also be incorporated. Calculated fields can also be incorporated into the incident and event form in the case an organization wants to evaluate incident severity or some other calculated measure into the form.

In this instance, I can select levels of severity and a cumulative severity will be calculated. These calculations can help drive further review or analysis. Also incorporated into the form is the ability to build review plans for each incident or event. These review plans drive workflow across the organization so individuals can review and approve each incident or even prior to closure.

You can add one level of review, or multiple levels of review to each incident or event. The system will use this review plan to create tasks and notify individuals that their review is required. Review logs will show all the activity within the review plan.

The Workiva Request functionality is also used within the remediation experience. Incident owners can request supporting documentation to other individuals within the organization. The system will notify these individuals of the request and assignees will have the opportunity to upload direct.

Workflow within the platform is also used to create tasks, track outstanding requests, and provide back and forth communication activities to ensure the support being provided is accurate. Each request will be linked directly to the incident form for

tracking status and easy navigation. Each incident or event allows for the creation of one, or multiple action plans.

The action plan form is very similar to that of the incident form where form is fully customizable to ensure that each organization can track required data elements and relationships. The action plan form allows for the same request functionality to occur for gathering support data around the action plan. Each action plan is directly linked to the incident or event in which it has been created.

Going back to the incident form I can easily see all action plans and requests that have been created as part of managing this incident within the workspace.

The qualitative risk assessment is the most common form of risk assessment. We will use this type of risk assessment as our example in the operational risk model.

Here is how an example risk assessment could be structured:

Consistent with the other forms within the database the risk assessment form is fully customizable to ensure that each organization can track and assess required data elements for their operational risk structure and regulatory requirements.

In our example, each risk assessment form would detail the assessed risk, the assessor, as well as the risk description. Additional properties of the risk could be included in requested by the customer.

Within this form, we have built a navigation link to a user-centric report when the risk owner could see a full population of assigned risks. We have yes / no certification questions that can be answered by each assessor. Through configuration, we can build conditional fields that populate when an answer is provided that require additional information.

In this case, if the assessor were no longer the risk owner, a conditional field would populate to provide additional information.

These forms have the ability to support the qualitative components of the risk assessment. The form has built calculations to calculate the Inherent and Residual Risk rating of the risk. By selecting Risk Likelihood, Severity, Velocity, and Management effeteness, these qualitative ratings will populate on the form.

Once the assessor is complete, they would submit the assessment for review and completion. The completed date and the status will automatically updated once submitted.

Managing these risk assessment is a seamless process using the Assessments experience.

When the assessment forms are created the relationship of the piece of day we want to assess and the assessor is identified. With our example of risk assessments, the risk owner, or risk owners are tied directly to each risk.

When I want to create the new assessment I click on the create button in the upper portion of the screen. When I do that the New Assessment creation pops up on the screen. I select the particular template I want to assess. In this case the RCSA Operation Risk Assessment. I select the period that I want to assess. And then I select the due date of the assessment.

Once those items are selected I hit the preview button. The preview loads and I can see the number of risk/assignees relationships and forms I will be sending to users. I can review this list and if I find issues I can go back or cancel, or if I am good with this list, I can hit the create button.

Upon hitting the create, 94 new assessments will be created. They are defaulted to not being sent. I can select all of my assessments and send, or I can individually send out each assessment when I am ready.

When an assessment is sent, a task will be created for that user. They will get an email notification when sent. A follow up email will be generated the day before it is due if it is not compete, the day that it is due if it not compete, and the day after it is due if it is not complete. Status of the assessments is tracked in the list view from not sent, in progress, in review, returned, as well as completed. I can also drill further into the list view by status. And if I need to send reminders, I can do that directly from this screen.

Using the assessments experience within the Workiva platform makes creating and tracking the status of your assessments easy and efficient.

KRI Data Gathering

Gathering Key Risk Indicator (KRI) data from organizational leaders can be done using the Assessments experience in the Workiva platform.

Assessments are used to collect information about a particular object of data in the database. In this case, we want to collect data around a particular KRI. As an example, I have opened up a KRI related to IT Incidents.

Consistent with the other forms within the database the KRI form is fully customizable to ensure that the each organization can track and assess required data elements for their risk structure and regulatory requirements.

Video Transcript

In our example, we have identified three key components around the KRI. The KRI Threshold Warning Direction, whether it is ascending or descending in nature, the Cautionary Threshold Warning Level of the KRI, the Escalation Threshold Warning Level of the KRI. We can identify the active ratings from previous periods in which the KRI gathering process occurred.

In this instance, and active rating of 5 was identified and the status is set to cautionary. Escalated KRIs and be identified easily in charts and dashboard to help guide management and determine if additional risk assessment measures are needed.

KRI gathering is a seamless process using the Workiva Assessments experience. When the assessment forms are created the relationship of the piece of day we want to assess and the assessor is identified.

With our example of KRIs, the KRI owner, or KRI owners are tied directly to each Key Risk Indicator. When I want to create the new assessment I click on the create button in the upper portion of the screen. When I do this, the new assessments pop up appears on the screen. I select the particular template I want to assess. In this, case the KRI Assessment. I select the period that I want to assess. And then I select the due date of the assessment.

Once those items are selected I hit the preview button. The preview loads and I can see the number of KRIs/assignees relationships and forms I will be sending to users. I can review this list and if I find issues I can go back or cancel, or if I am good with this list, I can hit the create button.

Upon hitting the create, 4 new assessments will be created. They are defaulted to not being sent. I can select all of my assessment and send or I can individually send out each assessment when I am ready.

When an assessment is sent, a task will be created for that user. They will get an email notification when sent. A follow-up email will be generated the day before it is due if it is not compete, the day that it is due if it not compete, and the day after it is due if it is not complete.

Status of the assessments is tracked in the list view from not sent, in progress, in review, retuned, as well as completed. I can also drill further into the list view by status. And if I need to send reminders, I can do that directly from this screen.

Using the assessments experience within the Workiva platform makes KRI data gathering and tracking the status of your assessments easy and efficient.