IBM OpenPages with Watson
Version 9.0.0

Solutions Guide

IBM

Note

Before using this information and the product it supports, read the information in .

Product Information

This document applies to IBM OpenPages with Watson Version 9.0.0 and may also apply to subsequent releases.

Contents

x

Introduction

The *IBM OpenPages with Watson Solutions Guide* is intended for users who need to use the solutions that are provided with OpenPages with Watson. The content describes the object types for each solution. It also identifies subcomponents, computed fields, helpers, notifications, reports, triggers, profiles, role templates, views, and workflows that are supported by each solution.

IBM OpenPages with Watson documentation

IBM® maintains one set of documentation serving IBM OpenPages® with Watson™, IBM OpenPages for IBM Cloud Pak for Data, and IBM OpenPages with Watson on Cloud deployments. The IBM OpenPages with Watson documentation describes certain features and functions which may not be available on the cloud.

If you have any questions about the functionality available in the product version that you are using, contact IBM OpenPages Support by using the IBM Support portal.

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. OpenPages documentation has accessibility features. PDF documents are supplemental and include no added accessibility features.

Object type licensing

You are licensed to use the object types for each IBM OpenPages with Watson solution that you purchased.

For a full list of object types provided with each solution, see Chapter 3, "Object types," on page 29. Use of any other object types is prohibited without prior written approval from IBM.

Solution acronyms

The following solution acronyms are used throughout this guide:

- BCM = IBM OpenPages Business Continuity Management
- DPM = IBM OpenPages Data Privacy Management
- ESG = IBM OpenPages Risk Management for ESG
- FCM = IBM OpenPages Financial Controls Management
- ITG = IBM OpenPages IT Governance
- IAM = IBM OpenPages Internal Audit Management
- MRG = IBM OpenPages Model Risk Governance
- ORM = IBM OpenPages Operational Risk Management
- PCM = IBM OpenPages Policy Management
- RCM = IBM OpenPages Regulatory Compliance Management
- TPRM = IBM OpenPages Third Party Risk Management

Chapter 1. IBM OpenPages GRC solutions

IBM OpenPages with Watson contains the following solutions.

OpenPages Financial Controls Management

IBM OpenPages Financial Controls Management (FCM) reduces the time and resource costs that are associated with ongoing compliance for financial reporting regulations.

IBM OpenPages Financial Controls Management combines powerful document and process management with rich interactive reporting capabilities in a flexible, adaptable easy-to-use environment. This feature provides CEOs, CFOs, managers, independent auditors, and audit committees the ability to perform all activities for complying with financial reporting regulations in a simple and efficient manner.

It allows users to easily see the status of their financial controls documentation project, and provides a secure repository for the storage of their internal controls documentation.

Key features include:

- A Financial Controls Management Repository, which logically presents processes, risks and controls in many-to-many and shared relationships at multiple levels, and enables file attachment capability and action plans for processes, risks, controls, and tests at all levels.
- Flexible automation, which provides notification and completion of financial controls management activities, such as design review, operating review, and certification.
- Reporting, monitoring, and analytics.
- Pre-built workflows create an automated, consistent, and repeatable approach to reduce the complexity of an organization's internal sub-certification process.
- Greater visibility for the oversight function into the health of the organization's internal control and process frameworks.
- Actionable, on-demand reports enable users to identify, remediate, and report risks sooner.

Show me how: FCM Overview

This video provides an overview of FCM.

https://youtu.be/5_1xZhQZcV4

OpenPages Model Risk Governance

IBM OpenPages Model Risk Governance (MRG) supports organizations in organizing and centralizing their Model Inventory.

As a solution IBM OpenPages Model Risk Governance provides a configurable and customizable platform, allowing firms to:

- Organize, document, and maintain an enterprise-wide inventory of models and their usages
- Document and track issues that are associated with models in a central location
- Record Model Change management governance activities
- Schedule, track, and manage Model Reviews and Validations
- Conduct periodic model attestations and model risk assessments
- Assign appropriate roles and responsibilities for model ownership and model risk management
- Monitor performance and status of their Model Risk Management program
- View the relationships between their Model Inventory and the relevant aspects of their Policy and Compliance obligations

IBM Watson OpenScale Integration

IBM OpenPages Model Risk Governance (MRG) includes an out-of-the-box integration with IBM Watson® OpenScale.

IBM Watson OpenScale is a tool that monitors and measures outcomes from AI Models across their lifecycle and performs ongoing validations of AI Models. Organizations can include AI models in their Model Inventory and send the results of the performance monitoring directly to OpenPages.

Show me how

This video provides an overview of how OpenPages is integrated with IBM Watson OpenScale:

https://youtu.be/JOGffAHGreQ

Fields

The following fields are used in the integration with IBM Watson OpenScale:

- MRG-Model field group
  - Machine Learning Model
  - Monitored with Watson Studio
- MRG-Metric-Shared field group
  - Metric Type
  - Watson Studio Category
  - Watson Studio Description
  - Watson Studio Metric
  - Watson Studio Metric Value
  - Watson Studio Subscription Name
  - Watson Studio Subscription Type
  - Watson Studio Sub-Category

Sample calculation

The Metric Value Update calculation is used in the integration with IBM Watson OpenScale.

Public Filter

A public filter for the Model object is used by IBM Watson OpenScale to locate Models in OpenPages that have the Monitored with Watson Studio field set to Yes.

User profiles

MRG profiles included the fields that support the integration.

OpenPages Operational Risk Management

IBM OpenPages Operational Risk Management (ORM) combines document and process management with a monitoring and decision support system. IBM OpenPages Operational Risk Management enables organizations to analyze, manage, and mitigate risk in a simple and efficient manner.

IBM OpenPages Operational Risk Management helps automate the process of measuring and monitoring operational risk. It combines all risk data, including risk and control self assessments, loss events, scenario analysis, external losses, and key risk indicators (KRI), into a single integrated solution.

IBM OpenPages Operational Risk Management includes the following key features:

- Loss Events to track, assess, and manage internal and external events that might result in operational loss.
- Risk and Control Self Assessments (RCSA) to identify, measure, and mitigate risk.
- Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), which can track performance metrics to potentially show the presence or state of a risk condition or trend.
- Scenario Analysis, which is an assessment technique that is used to identify and measure specific kinds of risks, in particular, low frequency, high-severity events.
- External Loss Events to import loss data from IBM FIRST Risk Case Studies, ORX, and ORIC loss databases
- Issue Management and Remediation (IMR)
- Reporting, monitoring, and analytics

IBM FIRST Risk Case Studies

The IBM FIRST Risk Case Studies database is a collection of external, public operational risk loss events in the form of risk case studies.

IBM FIRST Risk Case Studies events are targeted at the financial sector and contain over 20 years of events, which have been indexed to 13 keyword hierarchies, including Basel category and business line. Other hierarchies include control factor, event trigger, business unit type, and entity type. IBM FIRST Risk Case Studies cases include detailed descriptions that break down the event to analyze root cause, identify control breakdowns, lessons learned, management response and aftermath of the event. Events can also include sections with supporting detail that provide a timeline for the event, relevant information about the institution that it happened to, or other detail about loss impacts.

Most events in IBM FIRST Risk Case Studies capture quantitative information as well as detailed qualitative analysis. This quantitative information takes the form of loss amounts that are captured at the time of the event.

IBM FIRST Risk Case Studies offers a subscription to a data add-on refreshed daily with the IBM FIRST Risk Case Studies database in a format that is compatible with the FastMap feature.IBM OpenPages with Watson customers can use the IBM FIRST Risk Case Studies FastMap data add-on to provide end users with access to IBM FIRST Risk Case Studies case studies within the OpenPages with Watson application. After the data is loaded into OpenPages with Watson, end users can browse and associate IBM FIRST Risk Case Studies case studies to objects like Scenario Analyses, Risks, and Loss Events. Consult your IBM account representative for details on obtaining the IBM FIRST Risk Case Studies data add-on for OpenPages with Watson.

If you subscribe to the IBM FIRST Risk Case Studies database service, IBM FIRST Risk Case Studies provides a compatible FastMap file for a seamless load of IBM FIRST Risk Case Studies data to IBM OpenPages Operational Risk Management.

By default, IBM OpenPages Operational Risk Management includes the OpenPages FIRST Loss profile. Users with this profile can load FIRST Loss data through the IBM OpenPages FastMap feature. For more information about this profile, see Chapter 8, "Profiles," on page 89.

OpenPages Policy Management

IBM OpenPages Policy Management (PCM) is an enterprise compliance management software solution that reduces the cost, complexity, and cumbersome nature of compliance with multiple regulatory mandates and corporate policies.

IBM OpenPages Policy Management allows companies to manage and monitor compliance activities through a full set of integrated functionality including:

- Regulatory Libraries and Change Management
- Risk and Control Assessments
- Policy Management, including Policy Creation, Review & Approval and Policy Awareness

- Control Testing and Issue Remediation
- Regulator Interaction Management
- Incident Tracking
- Key Performance Indicators
- Reporting, monitoring, and analytics

PCM supports three approaches to initially load policy data and establish how it is organized and viewed in the Policy objects:

Datacentric
> Policy attributes are stored as metadata in the Policy object. Policy and Procedure content is created, stored, edited, and reviewed in Policy Viewers. Red-lined track changes within draft iterations are not supported.

Docucentric
> Policy attributes are stored as metadata in the Policy object. Policy and Procedure content is created outside of OpenPages with Watson and the entire document is attached to the Policy Object. Policy and Procedure content is never imported nor stored in OpenPages with Watson.

Hybrid
> Policy attributes are stored as metadata in the Policy object. Policy and Procedure content is created and edited in Microsoft Word documents then imported and stored in OpenPages with Watson. The Track Changes functionality available in Microsoft Word is used for tracking red-line changes within draft iterations.

After the policy data is loaded, a pre-built workflow allows organizations to advance a Policy object through a policy review and approval process. A Policy progresses through each stage based on the values of the approval and publication status.

OpenPages IT Governance

IBM OpenPages IT Governance (ITG) aligns IT services, risks, and policies with corporate business initiatives, strategy, and operational standards.

IBM OpenPages IT Governance allows you to manage internal IT control and risk according to the business processes they support. In addition, it unites multiple silos of IT risk and compliance to deliver improved visibility, better decision support, and ultimately enhanced corporate performance.

Key features include:

- IT Regulatory and Policy Compliance
- Risk and Control Assessments
- Control Testing and Issue Remediation
- IT Resource Management
- Incident tracking
- Vulnerability tracking and scoring
- Key Performance and Key Risk Indicators
- Reporting, monitoring, and analytics

RiskLens connector

IBM OpenPages IT Governance includes an integration with the cyber risk quantification analysis platform RiskLens.

Within the RiskLens platform, users record the Assets and Threats included within Scenarios and populate these objects in accordance with the FAIR method using data helpers provided in RiskLens for guidance. The integration with OpenPages enables an OpenPages user to push a record for inclusion within a Risk Assessment in RiskLens. The object can be associated to one or more Scenarios within RiskLens and Monte Carlo simulations are performed. After completing the simulation, and in accordance with the

scheduled job in OpenPages, the loss exposure metrics generated by the Monte Carlo simulations are pulled into OpenPages for use throughout the application. The scheduled job in OpenPages also pulls updated data from RiskLens when Risk Assessments are modified.

For information about how to configure the RiskLens connector, see the *IBM OpenPages with Watson Administrator's Guide*.

OpenPages Internal Audit Management

IBM OpenPages Internal Audit Management (IAM) provides internal auditors with a uniquely configured view into organizational governance, risk, and compliance (GRC), affording audit the chance to supplement and coexist with broader risk and compliance management activities.

IBM OpenPages Internal Audit Management is completely integrated with financial controls management, IT governance, policy management efforts and operational risk management programs. The internal audit team has the capability to work as a fully integrated partner to business stakeholders, completely independently, or anywhere in between, as determined by the specific needs of the audit department or a particular audit being undertaken.

Key features include:

- The capability to risk rank the audit universe, configured according to your audit methodology
  - Powerful support for your risk assessment methodology.
  - Full reporting across the entire audit universe.
- The ability to define, plan, execute, and report on audits across your business
  - Track and manage audits, audit sections, workpapers, and audit resource requirements and allocations.
  - Automate operations through fully configurable reporting.
- The ability to provide independent assurance to the business or work as an integrated part of GRC efforts
  - Opine on management's GRC efforts independently.
  - Control access to confidential audits, fields, and audit-only views.

Issue Management and Remediation

The Issue Management and Remediation (IMR) process is an essential component to any risk management program. A sound IMR framework provides awareness, validation, and transparency to the risk management program that it supports.

When successfully implemented, it provides high value with minimal overhead and serves as the underlying stimulus for the continuous improvement of a risk management program. An effective IMR framework effectively documents, monitors, remediates, and audits identified issues.

Issues are events that negatively affect the ability to accurately manage and report risk. The issues are identified against the documented IMR framework. Issues can be associated with objects within the framework and commonly have attributes, such as ownership, scheduling, or remediation status that identify the area of focus. An issue can be associated with multiple parents. For example, if an issue is discovered through a loss event, the issue can be associated with the loss event, the risk that occurred, and any failing controls that are documented.

The IMR process operates in the following key activities:

1. Issue Creation and Assignment
2. Action Creation and Assignment
3. Remediation Performance
4. Issue closedown
5. Reporting

Issue Creation and Assignment

Issues arise as a result of various risk management activities, such as a loss event, KRI threshold breach, or control weakness identification. Throughout these activities, users can create an issue within IBM OpenPages with Watson.

When an issue is created, the Issue review workflow starts automatically. For more information, see "Issue review workflow" on page 107.

Action Creation and Assignment

It is the responsibility of the issue owner to establish and record the appropriate actions to resolve the identified issue.

When an action is created, the Action Item workflow starts automatically. For more information, see "Action Item Approval workflow" on page 105.

The following data is captured on an action item: description, assignee, start date, due date, actual closure date, status (read-only) and comments.

Action assignees are notified that they must complete an action.

Remediation Performance

After being notified, the assignee completes the assigned action. Some actions can take time to complete, so the assignee adds comments to track progress.

When the action is complete, the assignee selects **Actions** > **Submit for Approval**.

Issue Closedown

The issue owner accesses a list of actions to approve for closure.

If the action is rejected and saved, the status reverts to open and the action returns to the action assignee. If the action is accepted for closure and saved, the action status changes to closed and the field **Closure date** is populated with the current date.

When actions are completed, the issue owner reviews the issue and updates the status to **Closed**.

Reporting

A selection of issue and action reports is available to all users. In addition, all email notifications are included in a consolidated issue and action bulletin to users, including the following information:

- Issues assigned to the recipient in the past X days.
- Actions assigned to recipient in the past X days.
- Issues due for closure in the next X days.
- Actions due for closure in the next X days.
- Overdue issues.
- Overdue actions.
- Actions awaiting closure approval.

Key Risk Indicators and Key Performance Indicators (KRIs and KPIs)

Key Risk Indicators (KRIs) and Key Performance Indicators (KPis) are available to the following solutions: IBM OpenPages Operational Risk Management, IBM OpenPages IT Governance, and IBM OpenPages Business Continuity Management.

The main stages within the Key Indicator life cycle are definition, value creation, value capture, and reporting. The following automation is provided in these stages for both KRIs and for KPIs in support of a metrics management program:

Indicator definition
Indicators can be created from scratch or can be created based on standard indicators in an indicator library.

Value creation
KRI and KPI Value objects are created automatically by the KRI Value Creation workflow, which runs on a scheduled basis. The workflow can also be run by an administrator.

Value capture
The KRI Value Entry workflow assigns KRI Values to users and provides a process for KRI Value approval. Notifications that a value needs to be entered are automatically sent to the value Collector of Active indicators which are close to their collection date. When the value has been entered and saved, calculations automatically calculate Breach and other status values, persist them on the value and on the indicator. You might need to click another tab and then return to the view to see the latest KRI or KPI values. If the KRI Breach Status is Red, a child Issue is created.

Indicator reporting
KRI and KPI dashboards display summary indicator information for the selected Business Entity and its descendants, with the ability to drill-through to detail and trend information for the indicator values.

OpenPages Third Party Risk Management

IBM OpenPages Third Party Risk Management (TPRM) supports firms in assessing and analyzing risks that are associated with the vendors they do business with.

IBM OpenPages Third Party Risk Management brings transparency into operational and security activities for vendors and the subcontractors they hire. It provides a scalable way to manage third-party compliance and risk. Firms can use it to understand more clearly how individual vendors or engagements relate to business processes.

IBM OpenPages Third Party Risk Management allows firms to complete the following tasks:

- Create, maintain, and document all vendors and engagements
- Classify or "tier" vendors as low, medium, or high criticality
- Manage contracts with third-party vendors
- Understand how third-party engagements support your business
- Use standard risk assessments to identify and mitigate risk in a specific way for individual vendors
- Leverage the questionnaire assessment capability to conduct vendor or engagement tiering using information you gather with risk or compliance questionnaire assessments.
- Collect and store evidence in a central location
- Import vendor details and ratings from third-party data providers
- Remediate and mitigate risks after they are identified
- Build key performance and key risk indicators
- Monitor and report risks on an ongoing basis

In previous releases, IBM OpenPages Third Party Risk Management was named Vendor Risk Management. The original name and the acronym, VRM, still exist in internal names for profiles and role templates.

RapidRatings connector

OpenPages Third Party Risk Management includes a connector for RapidRatings.

The RapidRatings connector enables you to import vendor details and financial ratings from RapidRatings into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

For information about how to configure the Supply Wisdom connector, see the *IBM OpenPages with Watson Administrator's Guide*.

RiskRecon connector

OpenPages Third Party Risk Management includes a connector for RiskRecon.

The RiskRecon connector enables you to import vendor details and ratings from RiskRecon into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

For information about how to configure the RiskRecon connector, see the *IBM OpenPages with Watson Administrator's Guide*.

SecurityScorecard connector

OpenPages Third Party Risk Management includes a connector for SecurityScorecard.

The SecurityScorecard connector enables you to import security ratings from SecurityScorecard into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

For information about how to configure the SecurityScorecard connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Supply Wisdom connector

OpenPages Third Party Risk Management includes a connector for Supply Wisdom.

The Supply Wisdom connector enables you to import vendor details, ratings, alerts, and locations from Supply Wisdom into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

For information about how to configure the Supply Wisdom connector, see the *IBM OpenPages with Watson Administrator's Guide*.

OpenPages Regulatory Compliance Management

IBM OpenPages Regulatory Compliance Management (RCM) supports organizations in breaking down regulations into a catalog of requirements, evaluating its impact to the business, and creating actionable tasks.

As a solution it allows firms to:

- Maintain a repository of regulations and requirements that they must comply with
- Identify and create a catalog of requirements that fulfill the regulations
- Map regulatory requirements to their internal control framework
- Create groupings of requirements into Compliance Themes
- Conduct assessments of regulatory requirements under Compliance Plans
- Ingest, direct, and respond to regulatory events supplied by third-party data providers
- Record, organize, and respond to regulator interactions, including regulatory inquiries and examinations

Ascent connector

IBM OpenPages Regulatory Compliance Management includes a connector for Ascent Reg Tech.

The Ascent connector enables the direct ingestion of regulatory feeds from Ascent Reg Tech into RCM.

IBM OpenPages with Watson enables the direct ingestion of new rules, rule changes, and obligations from Ascent Reg Tech into the Mandate, Sub-Mandate, and Requirement objects in OpenPages. For Requirements, past and future versions of the regulatory text are available.

For information about how to configure the Ascent connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Reg-Track connector

IBM OpenPages Regulatory Compliance Management includes a connector for Reg-Track.

The Reg-Track Regulatory Event object enables the direct ingestion of regulatory event feeds from Reg-Track into RCM, and the automated generation of workflows assigned to users based on supplied data points. This automation helps to assign tasks to users efficiently, enabling them to effectively respond to, and prepare for, regulatory change.

Taxonomy mapping

Users can associate their own taxonomy to the Reg-Track taxonomy that is used for Regulatory Events.

Users can populate fields on a Regulatory Event record that are more consistent with other values that are used in IBM OpenPages with Watson. The converted data points are available for use in the same way as existing data points on the Regulatory Event record, such as for setting conditions within the Rules Engine or in a workflow.

Reg-Track Rules Engine

The IBM OpenPages with Watson Rules Engine helps users to handle the daily influx of regulatory events, automatically route them to the right users in their organization, and start any necessary workflows.

The data from the Reg-Track feeds is loaded into OpenPages, and then passes through the Rules Engine. One regulatory event can trigger multiple rules if more than one rule's conditions are met.

Users can access the Rules Engine via a link on the **Reg-Track Regulatory Events** page.

Sample workflows

IBM OpenPages with Watson includes sample workflows for processing Reg-Track Regulatory Events. For more information, see "Sample workflows" on page 105.

Out-of-the-box rules for Reg-Track Regulatory Event processing

IBM OpenPages with Watson includes example rules for the incoming Reg-Track Regulatory Events. These rules can be modified to match an organization's methodology for processing alerts published by regulatory agencies.

For information about how to configure the Reg-Track connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Thomson Reuters connector

IBM OpenPages Regulatory Compliance Management includes a connector for Thomson Reuters Regulatory Intelligence (TRRI).

The TRRI Regulatory Event object enables the direct ingestion of regulatory event feeds from Thomson Reuters into RCM, and the automated generation of workflows assigned to users based on supplied data points, as well as documents impacted by regulatory change. This helps to efficiently assign tasks to users to effectively respond to, and prepare for, regulatory change.

Taxonomy mapping

Users can associate their own taxonomy to the Thomson Reuters taxonomy that is used for Regulatory Events.

Users can populate fields on a Regulatory Event record that are more consistent with other values that are used in IBM OpenPages with Watson. The converted data points are available for use in the same way as existing data points on the Regulatory Event record, such as for setting conditions within the Rules Engine or in a workflow.

TRRI Rules Engine

The IBM OpenPages with Watson Rules Engine helps users to handle the daily influx of regulatory events, automatically route them to the right users in their organization, and start any necessary workflows.

The data from the Thomson Reuters Regulatory Intelligence (TRRI) feed is loaded into OpenPages, and then passes through the Rules Engine. One regulatory event can trigger multiple rules if more than one rule's conditions are met.

Users can access the Rules Engine via a link on the **TRRI Regulatory Events** page.

Sample workflows

IBM OpenPages with Watson includes sample workflows for processing TRRI Regulatory Events. For more information, see .

Out-of-the-box rules for TRRI Regulatory Event processing

IBM OpenPages with Watson includes example rules for the incoming TRRI Regulatory Events. These rules can be modified to match an organization's methodology for processing alerts published by regulatory agencies.

Regulatory Library
IBM OpenPages with Watson enables the direct ingestion of a regulatory library feed from Thomson Reuters into RCM's Sub-Mandate object. In instances where Thomson Reuters identifies regulations impacted by a Regulatory Event, the impacted Sub-Mandate is automatically associated upon ingestion.

For information about how to configure the Thomson Reuters connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Wolters Kluwer connector

IBM OpenPages Regulatory Compliance Management includes a connector for Wolters Kluwer (WK).

The WK Regulatory Event object enables the direct ingestion of regulatory event feeds from Wolters Kluwer into RCM, and the automated generation of workflows assigned to users based on supplied data points, as well as documents impacted by regulatory change. This helps to efficiently assign tasks to users to effectively respond to, and prepare for, regulatory change.

Taxonomy mapping

Users can associate their own taxonomy to the Wolters Kluwer taxonomy that is used for Regulatory Events.

Users can populate fields on a Regulatory Event record that are more consistent with other values that are used in IBM OpenPages with Watson. The converted data points are available for use in the same way as existing data points on the Regulatory Event record, such as for setting conditions within the Rules Engine or in a workflow.

WK Rules Engine

The Rules Engine helps users to handle the daily influx of regulatory events, automatically route them to the right users in their organization, and start any necessary workflows.

The data from Wolters Kluwer is loaded into OpenPages, and then passes through the Rules Engine. One regulatory event can trigger multiple rules if more than one rule's conditions are met.

Users can access the Rules Engine via a link on the **WK Regulatory Events** page.

Sample workflows

IBM OpenPages with Watson includes sample workflows for processing WK Regulatory Events. For more information, see the *IBM OpenPages with Watson Solutions Guide*.

Out-of-the-box rules for WK Regulatory Event processing

IBM OpenPages with Watson includes example rules for the incoming WK Regulatory Events. These rules can be modified to match an organization's methodology for processing alerts published by regulatory agencies.

Regulatory Library

IBM OpenPages with Watson enables the direct ingestion of a regulatory library feed from Wolters Kluwer into RCM's Mandate and Sub-Mandate objects. In instances where Wolters Kluwer identifies regulations impacted by a Regulatory Event, the impacted Mandates and Sub-Mandates are automatically associated upon ingestion.

For information about how to configure the Wolters Kluwer connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Using OpenPages Business Continuity Management

IBM OpenPages Business Continuity Management (BCM) is used by an organization, or group, to maintain or resume a predetermined level of operations during or after a disruptive event. All risks that can potentially impact the business during or following an event are identified.

Using BCM, organizations can build a framework for identifying critical assets and processes and creating company-wide business continuity plans.

BCM helps organizations to:

- Centralize business continuity data
- Establish, monitor, and test impact tolerance thresholds for identified important businesses services
- Perform business impact analyses to determine criticality of people, processes, and assets
- Develop business continuity plans, including, but not limited to, preparedness for disaster recovery, communication plans, equipment checklists, emergency readiness, employee logistics, and vendor checklists
- Test the effectiveness of your business continuity plan and identify and mitigate key risks
- Run workflows on a scheduled basis to ensure reviews of business services, business impact analyses, dependency mappings, and testing is conducted at regular intervals
- Visualize key management activities and monitor key performance and risk indicators with a user-friendly dashboard

BCM has built-in calculations to help organizations determine the criticality of processes to their business and to ensure alignment of recovery time and point objectives across assets and vendors that support critical business processes. Pre-built workflows allow organizations to draft, review, approve, and publish plans with triggers for expiry and archival. These plans can be mapped to the client's business impact analyses, policies, procedures, processes, locations, events, issues, and tests.

Show me how: BCM Overview

This video provides an overview of BCM.

https://youtu.be/3EeMaF0ehiA

Show me how: BCM Dashboard

This video provides an overview of the dashboard that is available for users who are assigned to the Business Continuity Management profile.

https://youtu.be/Ce1ql-hTIpk

Show me how: Business Continuity Plan object

This video provides an overview of the Business Continuity Plan object and how it is used in BCM.

https://youtu.be/fb6dF9EjX3k

Show me how: Business Impact Analysis object

This video provides an overview of the Business Impact Analysis object and how it is used in BCM.

https://youtu.be/X636XWXIpGg

Show me how: Business Continuity Test Plan object

This video provides an overview of the Business Continuity Test Plan object and how it is used in BCM.

https://youtu.be/A0WgGVd3mds

OpenPages Data Privacy Management

The IBM OpenPages Data Privacy Management (DPM) solution is used by an organization to aid in complying with data privacy regulations.

Using DPM, organizations can have clear visibility of all their private or sensitive data and ensure that the data is being handled correctly. DPM assists CPOs, CDOs, CCOs, and other privacy and compliance professionals by providing visibility and enabling them to demonstrate compliance.

DPM helps organizations to:

- Support compliance with data privacy regulations
- Maintain an inventory of all private data across the organization within OpenPages by using an integration with Watson Knowledge Catalog
- Have a holistic view of all private data across their organization
- Demonstrate privacy compliance through questionnaire assessments and reporting
- Automatically kick off privacy assessments for newly loaded data assets

DPM Master profile

DPM includes the DPM Master profile.

The profile includes:

- Dashboard
- Dependent views and dependent pick lists
- Grid views and task views

Dashboard

DPM includes the DPM Master dashboard.

The DPM Master dashboard provides privacy professionals a high-level overview of the different data assets in their organization, any tasks assigned to them, and the status of privacy assessments that are being conducted in the organization.
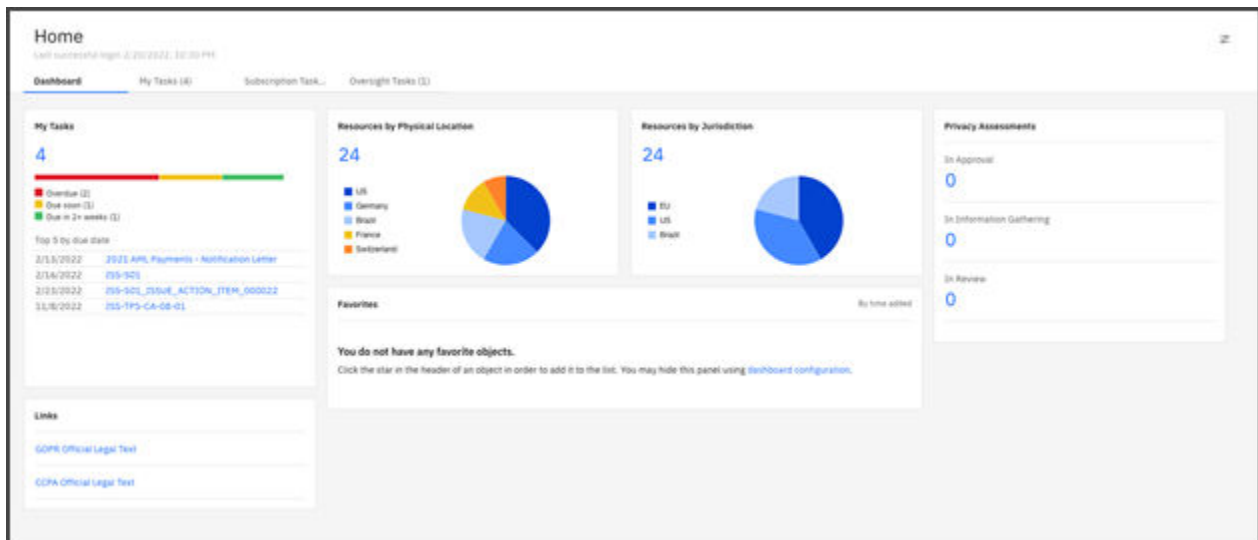
Figure 1. DPM dashboard

Sample workflows

DPM includes two sample workflows: Privacy Impact Assessment and Data Protection Impact Assessment. For more information, see "IBM OpenPages Data Privacy Management (DPM) workflows" on page 117.

OpenPages Risk Management for ESG

IBM OpenPages Risk Management for ESG helps organizations to govern and manage their ESG (environmental, social, and corporate governance) programs.

IBM OpenPages Risk Management for ESG supports the following use cases:

- Questionnaire to understand ESG priorities
- Capture and govern strategic objectives
- Link objectives to existing Processes, Risks, Controls, and Vendors
- Record a set of indicators for ESG
- Store a library of ESG regulatory requirements and disclosures
- Evidence compliance with external reporting requirements
- ESG horizon scanning
- Surface ESG ratings on Vendors (Supply Wisdom)

OpenPages Third Party Risk Management and the Supply Wisdom connector

You can use OpenPages Third Party Risk Management and Supply Wisdom along with IBM OpenPages Risk Management for ESG.

The Supply Wisdom connector enables you to import vendor details, ratings, alerts, and locations from Supply Wisdom into Vendor objects in OpenPages. You can then view the ESG ratings of your vendors in OpenPages.

To use these capabilities, you need the following components:

- IBM OpenPages Risk Management for ESG
- OpenPages Third Party Risk Management
- The Supply Wisdom connector

For information about how to configure the Supply Wisdom connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Chapter 2. What's new?

New features are available for this release of IBM OpenPages with Watson solutions.

For information about all new features for this release, see the *IBM OpenPages with Watson New Features Guide*.

New features in version 9.0.0.0

The new features in IBM OpenPages with Watson version 9.0.0.0 are described in the following sections.

Solution enhancements

Table 1. Solution enhancements	
For information about...	**See topic...**
Enhancements to IBM OpenPages Policy Management include: • A new workflow: Retire Policy Workflow • A new guide about the solution	"IBM OpenPages Policy Management (PCM) workflows " on page 123 OpenPages Policy Management Solution Document
Enhancements to IBM OpenPages Data Privacy Management include: • New profiles: **DPM Data Steward** and **DPM Privacy Officer** • New dashboards and updates to the master dashboard • New fields on the Asset object type	Chapter 8, "Profiles," on page 89
Enhancements to IBM OpenPages Financial Controls Management include: • New calculations • New reports • An updated dashboard	"Sample calculations" on page 97 "Financial Controls Management reports" on page 80
Enhancements to IBM OpenPages IT Governance include: A new object type: Threat New calculations: • Asset - Vulnerability Rating • System - Vulnerability Rating • Vulnerability - Threat Assessment New workflows: • Vulnerability Review • Threat Assessment • IT Waiver • IT Waiver Expiration Review	Chapter 3, "Object types," on page 29 "Sample calculations" on page 97 "IBM OpenPages IT Governance (ITG) workflows" on page 121

Table 1. Solution enhancements (continued)	
For information about...	**See topic...**
Enhancements to IBM OpenPages Internal Audit Management include: • The new object type: **SummaryAuditPlan** • The new calculation: Summary Audit Plan Budget and Plans • An updated dashboard	"Object type descriptions" on page 34 "Sample calculations" on page 97
Enhancements to IBM OpenPages Regulatory Compliance Management include: • The new object type: **RegulatoryEvent** • The new workflow: **Trigger Change - Regulatory**	"Object type descriptions" on page 34 "IBM OpenPages Regulatory Compliance Management (RCM) workflows" on page 124
Enhancements to IBM OpenPages Model Risk Governance include: • New fields and field groups on the Model Use Case (Register), Model, and Model Deployment (Usage) object types • New workflows: **Model Deployment**,**Model Use Case Request**, and **Model Lifecycle** • Updated views • Updated dashboards	"IBM OpenPages Model Risk Governance (MRG) workflows" on page 121
The new object types, **Subcontractor** and **VendorSubsidiary**, which can be used with OpenPages Third Party Risk Management	"Object type descriptions" on page 34
The labels of the following objects have changed: • `Register` – the label is now Model Use Case • `RiskEntity` – the label is now System • `Resource` – the label is now Asset • `ResourceLink` – the label is now Asset Link The object names have not changed.	"Object name mapping" on page 29
The super administrator (`OpenPagesAdministrator`) has access to the solutions master profiles by default.	Chapter 8, "Profiles," on page 89
The following object types are no longer included in fresh installations: • Capital Model • Capital Model Result	"Legacy object types" on page 147
The following computed fields are now URL fields: • OPSS-RA:RCSA Completion Helper • OPSS-RA:RCSA Process Alignment Helper	

Table 1. Solution enhancements (continued)	
For information about...	**See topic...**
When you do a fresh installation of solutions, sample users for the solutions are no longer created.	

New features in version 8.3.0.2

The new features in IBM OpenPages with Watson version 8.3.0.2 are described in the following sections.

Solution enhancements

Table 2. Solution enhancements	
For information about...	**See topic...**
The new solution, IBM OpenPages Risk Management for ESG, has been introduced. Added the following items: • Object types: Disclosure Statement, Product, Strategic Objective • Views • Reports • Dashboards • Profiles • Role templates • Calculations • Workflows	"Object type descriptions" on page 34 "Risk Management for ESG reports" on page 81 Chapter 8, "Profiles," on page 89 "List of role templates" on page 93 "Sample calculations" on page 97 "IBM OpenPages Risk Management for ESG workflows" on page 129
The new object type, **Requirement Version**, which can be used with IBM OpenPages Regulatory Compliance Management	"Object type descriptions" on page 34

New features in version 8.3.0.1

The new features in IBM OpenPages with Watson version 8.3.0.1 are described in the following sections.

Solution enhancements

Table 3. Solution enhancements	
For information about...	**See topic...**
Changes to IBM OpenPages Regulatory Compliance Management include: • The new object type: Ascent Supporting Information	Chapter 3, "Object types," on page 29

Table 3. Solution enhancements (continued)	
For information about...	**See topic...**
Changes to OpenPages Third Party Risk Management include: • Integration with RiskRecon to import vendors, scores, and ratings • Integration with RapidRatings to import vendors, scores, and ratings • The new object types: RiskRecon Ratings and RapidRatings Ratings • New dashboards that include panels for RapidRatings and RiskRecon • New profiles: VRM RiskRecon Master and OpenPages RapidRatings Master • New role templates: TPRM RapidRatings - All Permissions and TPRM RapidRatings - All Data - Limited Admin	"OpenPages Third Party Risk Management " on page 7 Chapter 3, "Object types," on page 29 Chapter 8, "Profiles," on page 89 Chapter 9, "Role templates," on page 93

New features in version 8.3.0

The new features in IBM OpenPages with Watson version 8.3.0 are described in the following sections.

Solution enhancements

Table 4. Solution enhancements	
For information about...	**See topic...**
Changes to IBM OpenPages Regulatory Compliance Management include: • The new object types: Compliance Theme Eval, Compliance Plan Eval, Obligation, Obligation Evaluation, and Obligation Evaluation Value • New calculations • New workflows • Support for a new object type association: Policy and Procedure object types can now have a Requirement Evaluation object as a parent. • Support for integration with RiskLens, including a new profile and a new job in the Scheduler	Chapter 3, "Object types," on page 29 Chapter 10, "GRC Calculations," on page 97 "IBM OpenPages Regulatory Compliance Management (RCM) workflows" on page 124 Chapter 8, "Profiles," on page 89

Table 4. Solution enhancements (continued)	
For information about...	**See topic...**
Changes to IBM OpenPages Model Risk Governance include: • The new object types: Model Version, Obligation • Changes to object labels: Model Scorecard is now Model Risk Scorecard, Register is now Model Entry, and Usage is now Model Deployment • The new calculation, Metric Value Update, replaces the OpenScale Update Metric Last Value Info workflow • The new calculation, Model Risk Scorecard, replaces the Model Risk Scorecard trigger • Two additional calculations: Metric Next Collection Date and Metric Value - Update from Parent Metric • New workflows • The labels of fields, field groups, and filters now use the new name for OpenScale, which is IBM Watson OpenScale	Chapter 3, "Object types," on page 29 Chapter 10, "GRC Calculations," on page 97 "IBM OpenPages Model Risk Governance (MRG) workflows" on page 121
Changes to IBM OpenPages Business Continuity Management include: • The new object types: Business Service and Business Service Eval • Additional object types that are now available to the solution: KPI, KPI Value, KRI, KRI Value, Scenario Analysis, Scenario Result • Support for new object type associations • New calculations • New workflows • New Dashboard • Integration with Supply Wisdom to provide alerts in the Business Continuity Event object and risk data within the Location object • A new profile, BCM Supply Wisdom Master	Chapter 3, "Object types," on page 29 "Sample calculations" on page 97 "IBM OpenPages Business Continuity Management (BCM) workflows" on page 112 Chapter 8, "Profiles," on page 89
Changes to IBM OpenPages Third Party Risk Management include: • The new object type, Supply Wisdom Parent Alert • New workflows • A new profile, VRM Supply Wisdom Master	Chapter 3, "Object types," on page 29 "IBM OpenPages Third Party Risk Management (TPRM) workflows" on page 134 Chapter 8, "Profiles," on page 89

Table 4. Solution enhancements (continued)	
For information about...	**See topic...**
Changes to IBM OpenPages Policy Management include: • The new object type: Obligation • The new Policy Review and Approval workflow • The new Policy Review Comment Calculation • The new PCM Owner dashboard • The default values of some settings in `Solutions/PCM` were updated to support the new Policy Review and Approval workflow	Chapter 3, "Object types," on page 29 "IBM OpenPages Policy Management (PCM) workflows " on page 123 "Sample calculations" on page 97
Changes to IBM OpenPages IT Governance include: • The new object type: Obligation • Integration with RiskLens • The new profile ITG RiskLens Master	Chapter 3, "Object types," on page 29 Chapter 8, "Profiles," on page 89
Changes to IBM OpenPages Data Privacy Management include: • New dashboard • New workflows • The new role templates	"IBM OpenPages Data Privacy Management (DPM) workflows" on page 117 "List of role templates" on page 93
Changes to IBM OpenPages Operational Risk Management include: • New dashboard • New and updated workflows, calculations, views, and field modifications to assist users in using the ORM solution out-of-the-box • Replacement of the KRI and KPI Trigger Utility with the use of calculations, workflows, and the Scheduler.	Chapter 11, "GRC Workflow," on page 105 Chapter 10, "GRC Calculations," on page 97
The name of the folder in IBM Cognos® Analytics where solution reports are stored has changed. Reports and report pages are in **Team Content** > **OpenPages Solutions Reports**. If you upgraded or migrated, your existing reports are still available in **Team Content** > **OpenPages Solutions Reports V6**.	
The solution reports have been updated: • The reports now use the new Dynamic Query Mode (DQM) framework models. • The reports now use a new stylesheet to align more closely with the OpenPages user interface. • The reports use updated JavaScript for CrossTrack links.	Chapter 6, "Reports," on page 69 See also the *IBM OpenPages with Watson Report Author's Guide*

Table 4. Solution enhancements (continued)	
For information about...	**See topic...**
New reports are now available in fresh installations: • Testing Performance and Results • Testing Detail • Consolidated Loss Event Dashboard • Loss Event Dashboard Detail – Entity • Loss Event Dashboard - Category	"Testing reports" on page 74 "Loss Event reports" on page 74
The following object types are no longer included in fresh installations: • Milestone (SOXMilestone) • Milestone Action Item (ProjectActionItem) • Questionnaire (Questionnaire) • Section (QSection) • Question (Quest)	"Legacy object types" on page 147
In fresh installations, the following fields are no longer computed fields: • `Audit: OPSS-Aud: Close Audit` – Converted to a link field • `Audit: OPSS-Aud: Plans` – Converted to a link field • `Audit: OPSS-AudEnt:Weighted Risk Score` – Converted to a text field that displays the result of a calculation • `Control Plan: OPSS-RiskEnt: Baselines` – Converted to a link field • `Resource: OPSS-Res: Resource Links` – Converted to a link field • `Plan: OPSS-Plan:Actual Hours` – Converted to a text field that displays the result of a calculation • `Plan: OPSS-Plan:Actual TE` – Converted to a text field that displays the result of a calculation • `Audit: OPSS-Aud:Actual Hours` – Converted to a text field that displays the result of a calculation • `Audit: OPSS-Aud:Actual TE` – Converted to a text field that displays the result of a calculation	"Computed fields" on page 136 Chapter 10, "GRC Calculations," on page 97
The Scenario Completion helper is no longer included in fresh installations.	

Table 4. Solution enhancements (continued)

For information about...	See topic...
For Attestation Creation Report helpers, `/OpenPages/Solutions/PCM/ Attestation/Email Sender Name` has been replaced with `/Applications/Common/ Email/Mail From Address` and `/OpenPages/ Solutions/PCM/Attestation/Email Sender Address` has been replaced with `/ Applications/Common/Email/Mail From Name`.	
For triggers that use the `from.address` attribute, if `from.address` is empty or has a value of `donotreply@openpages.com`, the value is replaced by the value in the registry setting `/Applications/Common/Email/Mail From Address`.	
The KRI and KPI Lifecycle triggers and notifications are no longer included in fresh installations. These triggers have been replaced by workflows and calculations.	"Sample workflows" on page 105

New features in version 8.2.0.3

The new features in IBM OpenPages with Watson version 8.2.0.3 are described in the following sections.

Solution enhancements

Table 5. Solution enhancements

For information about...	See topic...
The ability to import data from Supply Wisdom into IBM OpenPages Third Party Risk Management. Changes include: • Added a new object type, Supply Wisdom, as a child of the Vendor object type • Updated the Location object type to be a parent of the Vendor object type • Added new fields to the Vendor object type • Added new dashboards • Added new system views for the Vendor object type • Added a new job to the Scheduler • Added a new calculation • Added a new application permission • Updated the VRM Master and VRM Vendor Manager profiles	"OpenPages Third Party Risk Management " on page 7

Table 5. Solution enhancements (continued)	
For information about...	**See topic...**
The following IBM OpenPages Financial Controls Management profiles now include the Action Item object type: • FCM Master V2 • FCM Certification V2	"OpenPages Financial Controls Management" on page 1

New features in version 8.2.0.2

The new features in IBM OpenPages with Watson version 8.2.0.2 are described in the following sections.

Solution enhancements

Table 6. Solution enhancements	
For information about...	**See topic...**
The new solution, IBM OpenPages Data Privacy Management, has been introduced. Added the following profile: • DPM Master profile Added the following workflow: • Data Privacy Assessment Added the following dashboard: • DPM Master dashboard	"OpenPages Data Privacy Management" on page 12 Chapter 8, "Profiles," on page 89 "Sample workflows" on page 105
Changes to IBM OpenPages Financial Controls Management include new: • User profiles • Role template • Field group • Filters • Dashboards • Sample workflows • Sample calculations • Reports	"OpenPages Financial Controls Management" on page 1 "List of role templates" on page 93 "Sample workflows" on page 105 "Sample calculations" on page 97 "Financial Controls Management reports" on page 80

New features in version 8.2.0.1

The new features in IBM OpenPages with Watson version 8.2.0.1 are described in the following sections.

Solution enhancements

Table 7. Solution enhancements	
For information about...	**See topic...**
Changes to IBM OpenPages Regulatory Compliance Management include: • Ingestion of regulatory events from Reg-Track feeds • Added object types, Reg-Track Regulatory Event and Reg-Track Regulatory Event Series, for Reg-Track • Added sample workflows for Reg-Track • Added out-of-the-box rules for Reg-Track • Added notifications for Reg-Track	"OpenPages Regulatory Compliance Management" on page 8, "Object type descriptions" on page 34, and "Subcomponents" on page 50
The ability to import data from SecurityScorecard into IBM OpenPages Third Party Risk Management. Changes include: • Added new fields to the Vendor object type • Added a new dashboard, TPRM Vendor with SecurityScorecard • Added a new grid view and a new task view • Added a new job to the Scheduler • Added a new application permission • Updated the VRM Master and VRM Vendor Manager profiles	"OpenPages Third Party Risk Management " on page 7
The JSP reports for IBM OpenPages Operational Risk Management were updated.	
The Publishing Policy Report JSP for IBM OpenPages Policy Management was updated.	

New features in version 8.2.0

The new features in IBM OpenPages with Watson version 8.2.0 are described in the following sections.

Solution enhancements

Table 8. Solution enhancements	
For information about...	**See topic...**
Sample calculations are included with the new GRC Calculations feature.	"Sample calculations" on page 97

Table 8. Solution enhancements (continued)

For information about...	See topic...
The new solution, IBM OpenPages Business Continuity Management, has been introduced. Added the following object types: • BCBusinessImpactAnalysis • BCEvent • BCPlan • BCTest • BCTestResult • Location • Team Added the following profiles: • OpenPages BCM Master profile • BCM End User Added the following dashboards to the Task Focused UI: • OpenPages BCM Master dashboard • OpenPages BCM End User dashboard Added the following role templates: • Assignee • BC End User • BC Manager • BC Owner • BCP Approver • BCP Author • BCP Focal • BCP Reviewer Added the following workflows: • Workflow 1: Business Continuity Plan Review and Approval Process • Workflow 2: Business Impact Analysis to Determine Critical Processes • Workflow 3: BC Test Result Reporting Added a Cognos report on the Business Continuity Plans object. The link to it is named *Print BC Plan Details*. The link generates a Cognos report with the Business Continuity Plan object details in PDF format.	"Using OpenPages Business Continuity Management" on page 11 "Object type descriptions" on page 34 Chapter 8, "Profiles," on page 89 "List of role templates" on page 93 "Sample workflows" on page 105
IBM OpenPages Model Risk Governance (MRG) includes an out-of-the-box integration with IBM Watson OpenScale.	"OpenPages Model Risk Governance" on page 1 "Sample workflows" on page 105

Table 8. Solution enhancements (continued)

For information about...	See topic...
The following enhancements were made to IBM OpenPages Policy Management: Added the following profile: • PCM End User Added the following dashboards to the Task Focused UI: • OpenPages PCM Master dashboard • OpenPages PCM End User dashboard Added the Policy Review workflow. RegTask has the following new parents: Regulator Interaction, RI Component, and RI Sub-Component.	"OpenPages Policy Management " on page 3 Chapter 8, "Profiles," on page 89 "Sample workflows" on page 105
Changes to IBM OpenPages Regulatory Compliance Management include: • Ingestion of obligations from Ascent Reg Tech feeds • A new Compliance Review Comment object, which has the following parents: Regulator Interaction, RI Component, RI Sub-Component, RegTask, and RegChange • RI Category has a new label: RI Component • RI Request has a new label: RI Sub-Component • RegTask has the following new parents: Regulator Interaction, RI Component, and RI Sub-Component • Regulator Interaction, RI Component, and RI Sub-Component each has the following new parents: Mandate, Sub-Mandate, Requirement, Policy, Procedure, and Control	"Object type descriptions" on page 34 and "Subcomponents" on page 50
IBM OpenPages Vendor Risk Management has been renamed to IBM OpenPages Third Party Risk Management.	"OpenPages Third Party Risk Management " on page 7
Timesheet entry helpers are now available on a Reports panel on the dashboard in the Task Focused UI. Timesheet information can be viewed with the new menu item, **Audit Management** > **Timesheets**.	"Timesheet helpers" on page 62
IBM OpenPages Internal Audit Management includes a new Master dashboard.	
Added sample workflows for: • Incidents • Questionnaire Assessments	"Sample workflows" on page 105

Table 8. Solution enhancements (continued)	
For information about...	**See topic...**
Sample calculations are included with the new GRC Calculations feature.	"Sample calculations" on page 97
Several triggers are no longer enabled in fresh installations.	"Legacy triggers" on page 136
Visualizations that rendered business processes in a graphical format are no longer supported.	"Business process visualizations (legacy)" on page 135

Chapter 3. Object types

IBM OpenPages with Watson solutions consist of various object types.

The *OpenPages Object Model Details* document provides information about the relationships between object types for each solution.

Object name mapping

Default object type labels are mapped to object names.

Table 9. Object type labels and names

Object type name	Object type label	Object prefix
AscentSupportingInformation	Ascent Supporting Information	
Assertion	Assertion	AO
Attestation	Attestation	AN
AuditableEntity	Auditable Entity	AE
Auditor	Auditor	AD
AuditPhase	Audit Section	AH
AuditProgram	Audit	AU
BCBusinessImpactAnalysis	Business Impact Analysis	BI
BCEvent	Business Continuity Event	BV
BCPlan	Business Continuity Plan	BP
BCTest	Business Continuity Test Plan	BT
BCTestResult	Business Continuity Test Result	BE
BusService	Business Service	SV
BusServiceEval	Business Service Eval	SE
Campaign	Campaign	CP
Challenge	Challenge	CH
ChangeRequest	Change Request	CR
Committee	Committee	CI
CompliancePlan	Compliance Plan	CA

Object type name	Object type label	Object prefix
Table 9. Object type labels and names (continued)		
CompliancePlanEval	Compliance Plan Eval	PV
ComplianceTheme	Compliance Theme	CE
ComplianceThemeEval	Compliance Theme Eval	TV
ComplianceReviewComment	Compliance Review Comment	CR
Contract	Contract	CT
CostCenter	Cost Center	CC
CtlEval	Control Eval	CV
DisclosureStatement	Disclosure Statement	DS
Employee	Employee	EE
Engagement	Engagement	EG
Finding	Finding	FD
FIRSTLoss	FIRST Loss	FL
Incident	Incident	IN
KeyPerfIndicator	KPI	KP
KeyPerfIndicatorValue	KPI Value	KY
KeyRiskIndicator	KRI	KR
KeyRiskIndicatorValue	KRI Value	KE
Location	Location	LC
LossEvent	Loss Event	LE
LossImpact	Loss Impact	LO
LossRecovery	Loss Recovery	LR
Mandate	Mandate	MD
Metric	Metric	ME
MetricValue	Metric Value	MV
Model	Model	ML

Object type name	Object type label	Object prefix
Table 9. Object type labels and names (continued)		
ModelAttestation	Model Attestation	MK
ModelInput	Model Input	MT
ModelLink	Model Link	MN
ModelOutput	Model Output	MP
ModelScorecard	Model Risk Scorecard	MC
ModelVersion	Model Version	VN
Obligation	Obligation	OB
OblEval	Obligation Evaluation	OE
OblEvalValue	Obligation Evaluation Value	OV
Objective	Strategic Objective	OJ
ORICLoss	ORIC Loss	OR
ORXLoss	ORX Loss	OL
Plan	Plan	PN
Policy	Policy	PL
PolicyReviewComment	Policy Review Comment	RP
Preference	Preference	PF
PrefGrp	Preference Group	PG
Procedure	Procedure	PC
ProcessEval	Process Eval	PE
Product	Product	PT
Program	Program	QP
Project	Project	PJ
QuestionnaireAssessment	Questionnaire Assessment	QA
QuestionnaireTemplate	Questionnaire Template	QT
QuestionTemplate	Question Template	QQ

Object type name	Object type label	Object prefix
RAEval	Risk Assessment Eval	AV
RRRating	RapidRatings Ratings	
RegApp	Regulation Applicability	RB
RegChange	Regulatory Change	RD
RegInt	Regulator Interaction	RF
Register	Model Use Case	RJ
RegTask	Regulatory Task	RT
RegTrackRegEvent	Reg-Track Regulatory Event	
RegTrackRegSeries	Reg-Track Regulatory Event Series	
Regulator	Regulator	RE
RegulatoryEvent	Regulatory Event	
RegulatoryInitiative	Regulatory Initiative	RG
Requirement	Requirement	RQ
ReqEval	Requirement Evaluation	RY
ReqEvalValue	Requirement Evaluation Value	RZ
RequirementVersion	Requirement Version	
Resource	Asset	RU
ResourceLink	Asset Link	RL
Review	Review	RW
ReviewComment	Audit Review Comment	RC
RICat	RI Component	RH
RIReq	RI Sub-Component	RR
RiskAssessment	Risk Assessment	RA
RiskEntity	System	RN
RiskEval	Risk Eval	RV

Table 9. Object type labels and names (continued)

Table 9. Object type labels and names (continued)

Object type name	Object type label	Object prefix
RiskReconRatings	RiskRecon Ratings	
RiskSubEntity	Baseline	RS
ScenarioAnalysis	Scenario Analysis	BS
ScenarioResult	Scenario Result	BR
SectionTemplate	Section Template	QS
SOXAccount	Account	AC
SOXBusEntity	Business Entity	EN
SOXControl	Control	CN
SOXControlObjective	Control Objective	CO
SOXDocument	File	FI
SOXExternalDocument	Link	LI
SOXIssue	Issue	IS
SOXProcess	Process	PR
SOXRisk	Risk	RI
SOXSignature	Signature	SI
SOXSubaccount	Sub-Account	SU
SOXSubprocess	Sub-Process	SB
SOXTask	Action Item	AT
SOXTest	Test Plan	TE
SOXTestResult	Test Result	TR
SubContractor	Sub-Contractor	SC
Submandate	Sub-Mandate	SM
SubSectionTemplate	SubSection Template	SS
SummaryAuditPlan	Summary Audit Plan	SA
SupplyWisdom	Supply Wisdom	

Object type name	Object type label	Object prefix
SupplyWisdomParentAlert	Supply Wisdom Parent Alert	
Team	Team	TM
Threat	Threat	TH
Timesheet	Timesheet	TI
TRRIRegEvent	TRRI Regulatory Event	
TRRIRegSeries	TRRI Regulatory Event Series	
Usage	Model Deployment	US
Vendor	Vendor	VE
VendorSubsidiary	Vendor Subsidiary	VS
Vulnerability	Vulnerability	VU
Waiver	Waiver	WV
WKRegEvent	WK Regulatory Event	
Workpaper	Workpaper	WP

Table 9. Object type labels and names (continued)

Object type descriptions

IBM OpenPages with Watson solutions consist of various object types.

Account
Accounts correspond to one or more line items on a financial report. Each account is affected by recurring Processes. These Processes can introduce Risks that must be documented during the financial controls documentation project. An account is identified as significant based on factors such as size, complexity of the processes that operate on the account, or if the account is associated with new product lines within the business. The risks that might materialize and have material effect on the account are identified by consideration of the processes that operate on the account.

Ascent Supporting Information
The Ascent Supporting Information object stores supporting information that is imported from Ascent. Supporting Information is regulatory text that does not rise to the level of a legal requirement, but provides additional guidance, details, and so on to help entities to understand requirements and impact of the regulation. The Ascent Supporting Information object type has one parent, Requirement.

Assertion
The Assertion object is used to link Control objects to Account (or Sub-Account) objects. A common practice is to store the type of assertion that the Control is covering as a data field on the Assertion object.

Attestation

The Attestation object, part of the Policy Awareness capability, is used to capture an employee affirmation that they have read and understood a policy. An Attestation's primary parent is the Employee record and the secondary parent is the associated Campaign.

Asset

COBIT suggests that there are four types of IT assets, while practitioners often include more types as well. The Asset object is sub-typed using dependent fields to represent any of these types of IT assets. Assets are typically created as a pool associated to the owning or responsible IT Business Entity, then associated to the relevant operating elements (Baselines, Processes, and so on) in the IT Operating Environment, and potentially associated to relevant Business Entities for the Business as well. Although Assets can represent individual IT assets (for example, a particular Microsoft Windows server), they more often represent a group of assets (for example, a pool of Windows application servers that are used for a particular application).

Asset Link

COBIT suggests that IT assets have complicated relationships. They indicate that assets of type People, Process, Infrastructure, and Information can each be parents and can each be children of each other. In addition, assets of the same type often need to be related to each other. An Asset Link can be used to link Assets in a many-to-many fashion, but the practice (supported by the Create Resource Links helper) is to link exactly two Assets. If the names or attributes of either of the parent assets are changed, the name and attributes of the Asset Link will be out of sync with its parent Assets.

Audit

An Audit represents each execution of an audit against an Auditable Entity. For example, if an Auditable Entity is audited every two years, a separate child Audit instance must be created for each two-year period, such as 2022 and 2024. An organization might audit various processes. For example, you might audit an entity, a specific regulatory requirement, or a data center physical security.

The Audit object is configured as a self-contained object type and a folder is automatically created for each Audit instance. With this configuration, you can copy template audits and audit components from a library to the audit hierarchy without object naming conflicts.

Planning and scheduling of the Audit resources is done at the Audit level.

High-level Audit progress can be tracked by monitoring the Status values and Date values on the Audit. Key audit milestones can be tracked by adding fields that represent completion dates for each of the key milestones to track.

Use the Audit object to manage the audit process across your enterprise. The Audit identifies a holding point to capture information such as scope, objectives, timing information, review, execution, and approval roles. You can track a subset of audits that you are undertaking in a planning horizon, or all audits in the audit universe.

Audit Review Comment

The Audit Review Comment object type is used to provide feedback during the review process for an Audit and its components. It is associated as a child to the instance of the Audit, Section, Workpaper, or Finding for which feedback is being provided.

Audit Section

Audit Sections can be used to represent the phases of the Audit, work programs within the Audit, or other components of the Audit at the level of granularity you want.

Organizations might have multiple standard components for each Audit. Template audits that include sections for each standard component can be created in a library. Planned and Actual Start and End Dates for these sections are used to report progress on key milestones in the audits.

Detailed Audit progress can be tracked by including an Audit Section for each milestone. Alternatively, some organizations might add fields on the Audit that represent completion dates for each of the key milestones they want to track.

Although Audit Sections can be used for planning and scheduling Audit resources, most organizations find this method to be too detailed.

Auditable Entity

An Auditable Entity object is a child of a Business Entity and a Summary Audit Plan. An Internal Audit Business Entity hierarchy is established and all Auditable Entities are created as a child of the Internal Audit Business Entity object. Auditable Entities that are aligned with elements of the Business Entity Organizational Hierarchy are also associated to those Business Entities.

An Auditable Entity represents a single element of the Audit Universe; the collection of things in the business that might be audited. Most Auditable Entities represent business or legal entities, but they can also represent processes, long-running projects or initiatives, compliance programs, or shared IT Services.

Auditable Entities are risk ranked every year to determine the priority of performing an audit that year. A Weighted Risk Score is calculated but the score can be overridden.

Auditor

Resource planning and allocating requires key information about each individual who might perform audit work. The Auditor object is used to create a pool of Auditors who can be assigned to Audits.

Each user who is assigned to audit work is represented as an Auditor instance. Auditors are then available for resource allocation. The Auditor object includes attributes to use to evaluate and select Auditors for audit engagements, such as specialties, languages, and certifications. Auditor objects are associated with the relevant component of the Internal Audit organizational hierarchy. As a best practice, match the Name on the Auditor object with the username.

Baseline

A Baseline object type represents a template of library requirements. It is self-contained, which means folders are created for each Baseline. Baselines in the Library represent elements of the IT operating environment. They are linked to Requirements for that type of element. The Baseline object is copied from the library to the business hierarchy, an association is made to a Requirement in the library, and Risk, Control, and Test object types are created as child objects. The Risk, Control, and Test objects are populated with data from the Requirement when using the Baseline Copy Helper.

For example, a Baseline object can represent a collection of Requirement objects for a data center with Personally Identifiable Information (PII) and a Confidential Data classification. For each Requirement object, set up a best practice to define what to control (Risk object) and how to control it (Control object). You can also establish a practice for verifying the effectiveness of the Control (Test object).

Business Continuity Event

The Business Continuity Event object is used to identify an incident that negatively impacts business operation, for example, a pandemic, hurricane, tornado, or cybersecurity breach. The Business Continuity Event object type contains information such as location and type. A Business Continuity Event object can be associated with a Business Continuity Plan object to provide an easy way to relate specific occurrences to the corresponding plans.

Business Continuity Plan

A Business Continuity Plan is a proactive strategy, including policies and procedures, that describes how an organization and its critical functions will respond during and immediately following a disruption or disaster. The Business Continuity Plan addresses human resources, business processes, assets, and outsourced support services. The Business Continuity Plan object can be associated with other core business continuity objects such as Business Impact Analyses, Business Continuity Test Plans, Risk Assessments, Locations, and Teams.

Business Continuity Test Plan

Testing a business continuity plan is a valuable process used to gauge the effectiveness of the plan and assist in the identification of weaknesses or gaps. Testing can be conducted using various approaches such as table top and full simulation and can aid in the training and awareness of plan participants. The Business Continuity Test Plan object can be used to document the details of the test and can be associated with the parent Business Continuity Plan object and child objects such as the Business Continuity Test Plan Result and Issue.

Business Continuity Test Result
Business Continuity Test Result objects are child objects of a Business Continuity Test Plan. They are used to capture the results of the executed Business Continuity Test Plan. A Business Continuity Test Result can be associated with a related Business Continuity Test Plan and any accompanying Issues.

Business Entity
Business entities are abstract representations of your business structure. A business entity can contain subentities (such as departments, business units, or geographic locations). The entity structure that you create depends on your business needs. For example, you might create a parent entity for your business headquarters and a subentity for each location or department. You might also want to represent both a legal entity structure and a business entity structure.

Business entities are also used to organize library data such as risk and control libraries, or regulatory content (for example, laws, regulations, and standards).

When you set up your business entity hierarchy, work with your IBM OpenPages consultant. The structure of your business entities impacts the type and quality of information that can be extracted from the application.

In IBM OpenPages Internal Audit Management Business Entities also model the Internal Audit organizational structure, which facilitates reporting and security for the Internal Audit team. The Internal Audit organizational structure is a top-level entity to minimize the chance of accidentally granting a business user access to Internal Audit information. The elements of the Audit Universe that are owned by an Internal Audit team are associated with the team Business Entity. Another top-level Business Entity structure can be created to organize confidential Audits, providing special security to these Audits. Business Entity can also be used to organize a Library of template audit content.

Business Impact Analysis
A Business Impact Analysis (BIA) is used to evaluate the criticality of predetermined processes, their dependencies, and the effect on the business in the event of a disruption. It is used to measure the impact that events such as natural disasters, pandemics, and terrorism can have on critical business processes based on the severity of losses.

The Business Impact Analysis object type is designed to assist you with prioritizing critical impact to the business by ranking predetermined categories using numeric scoring. Numeric impact ratings can be leveraged for key data fields such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO). You can also use the calculation feature in OpenPages to translate your impact data to measurable information such Impact Scores, Impact Tiers, and Maximum Acceptable Outages (MAO).

Business Service
A Business Service is a service provided by the organization, such as withdrawing cash from and ATM or the ability to check a balance online, that can be broken down into supporting Processes. Business Services can be further classified as Important Business Services, which are services provided to external end users where a disruption would cause intolerable harm to consumers or market participants, market integrity, policyholder protection, safety and soundness, or financial stability.

A Business Service object can be a child of a Business Entity or Location object.

Business Service Eval
Business Service Eval objects are children of Business Service objects and they are used to capture values that are provided as part of the assessment of the Business Service for trending purposes. The Business Service Eval is created and populated as part of the last step of a Business Service assessment workflow.

Campaign
The Campaign object is part of the Policy Awareness capability and is used to manage the project management aspects of an awareness campaign. It is also used to define the requirements and criteria that identify which employees need to read and attest to each Policy. Campaigns are typically created in the Published Policy Hierarchy.

Challenge

The Challenge object can be used to store and evidence the presence of a Challenge to any part of the Model Inventory. A Challenge is raised and the response recorded. The Challenge object is a child of the Model and Model Deployment objects.

Change Request

The Change Request object is a child of the Model and Model Deployment objects and allows for the creation and tracking of governance activities that are related to changes in Models and their deployments. The object captures data such as Change Type, Change Description and Status. It is supported by a workflow.

Committee

The Committee object is a child of the Business Entity and allows an organization to represent governance groups/committees. These can then be aligned to Models and can also be a parent of the Employee object. It can store information such as the Terms of Reference for a committee, frequency of meetings, and detail of the Chairperson.

Compliance Plan

Compliance Plans allow for the creation of an overall plan to address regulatory requirements in a structured setting, or to structure a set of regulatory tasks. For example, a Compliance Plan might be created to track regulatory tasks, or to conduct compliance assessments against various regulatory requirements. One or multiple Compliance Themes can be grouped into an overall Compliance Plan for the organization.

Compliance Plan Eval

Compliance Plan Eval objects are children of the Compliance Plan object. Compliance Plan Eval objects are used to capture values that are provided as part of the compliance assessment that is captured on the Compliance Plan. A Compliance Plan Eval record is created and populated as the last step in the Compliance Plan BE Assessment and Compliance Plan Library Assessment workflows.

Compliance Review Comment

The Compliance Review Comment object type enables a user to add and post comments to the Regulatory Change, Regulatory Task, RI Component, RI Sub-Component, and Regulatory Interaction objects. A Compliance Review Comment can be directed to an individual or group of users for their response, and files can be uploaded onto the object to enhance collaboration among IBM OpenPages users.

Compliance Theme

Compliance Themes allow users to organize regulatory requirements into themes for assessment purposes. This allows for assessing compliance requirements beyond the typical business entity approach, by grouping regulatory requirements across themes that impact across the organization. Sample themes can include data privacy, governance, accountability, etc. This allows users to assess the impact of regulations not just within business entities, but across themes that touch on multiple areas of the organization.

Compliance Theme Eval

Compliance Theme Eval objects are children of Compliance Theme objects. Compliance Theme Eval objects are used to capture values that are provided as part of the compliance assessment that is captured on the Compliance Theme. A Compliance Theme Eval record is created and populated as the last step in the Compliance Theme BE Assessment and Compliance Theme Library Assessment workflows.

Contract

Contract objects are child objects of Vendor or Engagement objects. A Contract represents a business or legal agreement between a Business Entity and a Vendor or Engagement. A Contract contains additional, supporting information, for example, the timeframe of the contract or monetary information. Contracts are optional.

Control

Controls are policies and procedures that make sure that risk mitigation responses are performed.

After you identify the risks that occur in your practices, establish controls, such as approvals, authorizations, and verifications. These controls remove, limit, or transfer these risks.

Controls provide either prevention or detection of risks. Controls are associated with tests that ensure that a control is effective. For example, the human resources department identifies a risk in the new hire process. The process does not comply with regulations and guidelines for diversity and discrimination. Define controls to mitigate this risk, such as, establish hiring policies and procedures, and conduct mandatory training for hiring managers.

In IBM OpenPages Internal Audit Management use Controls to create a detailed model of the Controls that exist or that you want to enforce on the activities that are audited. If shared with the Business, the Controls can be rated separately by Internal Audit and by the Business.

Control Eval
Control Eval objects are similar to Risk Evaluation objects except that they are created as children of Controls. They store control assessment data. When report periods and control assessment evaluation cycles are not aligned, use Control Eval objects to capture multiple evaluation cycles within a single reporting period.

Control Objective
A Control Objective is an assessment object that defines the risk categories for a Process or Sub-Process.

Control Objectives define the COSO compliance categories that the Controls are intended to mitigate. Control Objectives can be classified into categories such as Compliance, Financial Reporting, Strategic, Operations, or Unknown.

After a Control Objective is identified, the Risks belonging to that Control Objective can then be defined. In most cases, each Control Objective has one Risk that is associated with it. However, it might have more than one Risk that is associated with it. For example, a financial services company employs traders that are aware of the required ethical standards. The HR department sets up a control objective called 'Personnel'. A risk that is associated with the Control Objective is, "Employees engage in business dealings that conflict with the company objectives for ethical and fair trading."

By default, an OpenPages Internal Audit Management Control Objective is disabled. This object is not often used, except to align with other solutions that might use it.

Cost Center
Cost Center objects are used to group loss events under a business entity. In many cases, firms want to track where loss events occur at a fine granularity, such as cost center level, but do not want to represent all of the organizational layers as business entities.

Disclosure Statement
This object type is used primarily to record text-based commentary in relation to disclosure requirements. Disclosure Statements are children of Requirements.

Employee
The Employee object is part of the Policy Awareness Capability. It is used to capture information about individual employees such as the name, title, email, region, department, or status. Information from the employee profile is then matched against the Attestation Requirements that are defined on a Campaign to determine which Employees need to attest to each Policy. Employee data is typically derived from an HR system export, loaded via Online FastMap, and resides in the reference Employee Business Entity. It is a best practice that the Employee Name field matches the user's username.

Engagement
Engagement objects are child objects of Vendor objects. An Engagement represents a single service that is provided by a Vendor. You use them to differentiate between various services and agreements you have with a Vendor. Engagements are optional. They can be subject to questionnaire assessments, risk assessments, or tiering. You can summarize and analyze risk that is associated with different Engagements. You can add a parent association to the process or sub-process that an Engagement supports.

File
The File object type is used to embed a reference to a file (such as a document, flow chart or spreadsheet) in the IBM OpenPages system, and associate it to one or more relevant objects.

Finding

Findings can be used to represent observations that are reportable to the business, to the Audit Committee, or both. Alternatively, Findings can be used to represent individual factual observations, while Issues are used to represent consolidated themes and systemic problems, which are then reported to the business, to the Audit Committee, or both.

A Finding represents anything that is uncovered in the course of an audit that needs to be accounted for and addressed by management. You can use a finding to track management's progress in addressing the underlying issue identified. The Issue object can be used in place of, or in conjunction with, the Finding object.

FIRST Loss

FIRST Loss objects can be imported from the FIRST external loss database, for use with scenario analysis, benchmarking, and reports generation, and to export loss data to analytic tools or capital allocation applications. FIRST Loss objects are often organized by loss categories, such as product lines or event types. For example, use a Business Entity to create a hierarchy for FIRST loss data. Name the root object "FIRST-data", and create category folders under the root. Link external losses to it.

Incident

An incident is an occurrence that has a potentially adverse effect on your enterprise. Create an Incident object to record information, such as the person responsible for investigating the incident and other related data. The Incident object is used by a workflow to facilitate incident analysis. Categories that apply to incidents include Regulatory Compliance, Legal Compliance, Information Security, and IT. Incidents are stored under the Business Entity or Asset where the event occurred and associated secondarily to an impacted Mandate or Policy.

Issue, Action Item

Although issues are generated in areas where internal controls are not properly implemented, use the Issue object to document a concern that is associated with any object type. For example, a Test is associated with a Control, but the Test failed the last time that it completed. This potential problem can be highlighted by capturing it in an Issue object.

An Issue is resolved through Action Items. You can use an Action Item or a series of related Action Items to form an Action Plan. Each Action Item is assigned to a user for resolution, and tracks progress. After all Action Items for an Issue are complete (when an assignee sets the value to 100%), close the Issue.

In OpenPages Internal Audit Management, Issues and Action Items can be used instead of, or with, Findings.

KPI, KPI Value

KPIs (Key Performance Indicators) are components of the risk monitoring process and are used to provide leading or lagging indicators for potential risk conditions. Each instance of a KPI within the organization can have unique target and threshold limits. The KPI Value object type records the value of a KPI object at a specific point. Create a KPI object, and then periodically (daily, weekly, monthly) create a KPI Value object so you can detect trends.

KRI, KRI Value

KRIs (Key Risk Indicators) are components of the risk monitoring process and are used to provide leading or lagging indicators for potential risk conditions. Each instance of a KRI within the organization can have unique target and threshold limits. KRI values are used to record the actual value of an indicator at a specific point in time.

Link

The Link object type is used to embed a reference to a URL in the OpenPages system, and associate it to one or more relevant objects.

Location

The Location object type is used to capture geography and location details that are needed in the contingency planning process. Location information can include, for example, the number of employees who work at a location, assets (such as computer equipment), and other location details.

Loss Event

Loss Events are used to track operational losses that occur in any part of an organization. Loss Events are typically stored under the Business Entity where the loss occurred. The Loss Event objects are used to track, assess, and manage the related internal loss data. You can add multiple impacts and recoveries for each Loss Event by using the Loss Impact and Loss Recovery objects. Loss Event, Loss Impact, and Loss Recovery objects can also be created in IBM OpenPages Loss Event Entry.

Loss Impact

A loss impact is a financial and non-financial consequence that results from a loss event. Loss Impacts track different types of impacts that are triggered by a Loss Event, such as legal liability, asset loss and damage, or business interruption. Multiple Loss Impacts can be associated with each Loss Event.

Loss Recovery

Loss Recovery objects are used to track the processes that are associated with recouping damages that result from Loss Events.

Mandate

Mandates represent external items with which organizations need to comply, such as laws, regulations, and standards. Content can be pulled from third-party providers, such as UCF, Ascent Reg Tech, or Wolters Kluwer. Mandates are represented in a Library Business Entity structure, and are not replicated throughout the system.

For example, an insurance company has a Mandate object for HIPAA and another Mandate object for GLBA. You can associate the same mandate with different groups within your organization. Privacy mandates, for example, might apply to payroll, insurance services, legal, and IT departments.

The Mandate object also supports content for regulatory compliance.

Metric, Metric Value

The Metric object records the definition of a performance measurement that the organization chooses to track. A user sets the Metric Type, Yellow, and Red Thresholds and other collection information. A Metric is a child of Model Deployment and Model objects.

The Metric Value object records the result of the metric performance measurement. It is designed to behave in a way to allow the organization to store time series results of measurement.

Model

The Model object provides representation of the Models within an organization. At a theoretical level a model as a quantitative method, system or approach that applies statistical, economic, financial or mathematical theories, techniques and assumptions to process input data into quantitative estimates. Within the Model object, key model information can be represented, including: Model Description, Model Ownership, Model Status, Development lifecycle dates, Model Type and Category, and Model Risk Assessment data. A Model object is a child of a Business Entity and parent of Model Deployment objects.

Model Attestation

Model Attestation allows an organization to request a regular sign off or *attestation* of a Model. The MRG administrator periodically creates a set of blank Model Attestations, which are assigned to the respective Model Owners. Each Model Owner answers a set of questions about the Model and submits their Model Attestation.

Model Deployment

The Model Deployment object is a child of Model. It is used as a key element of recording the deployment of one or more models.

Model Use Case

The Model Use Case object is a child of Entity and a parent of the Model object. The usage of the Model Use Case object is optional. Its primary purpose is to act as a library of Models during development.

Model Input

If an organization wants to adopt a more granular approach to model documentation, the Model Input object provides the ability to record the inputs. Fields include Input Owner, Type, Status, and

Description. A Model Input object can also be the child of a Model Output object, which allows for the creation of Model chains at a detail level if the Model Link approach is not granular enough.

Model Link

If an organization wants to adopt a less granular approach to Model documentation, use Model Link, which is a broad-type association that does not provide explicit details of the feed from one model to another. It acts as a child of multiple models to allow for the generation of Model chains.

Model Output

If an organization wants to adopt a more granular approach to Model documentation, the Model Output object provides the ability to record the Outputs of the Model. The intended purpose is to record the Description and Overview of the Output from a governance point of view.

Model Risk Scorecard

Model risk assessments are performed during the development and documentation phase of a Model. They are also typically performed periodically after a Model is in production. The Model Risk Scorecard object is used to conduct this risk assessment. The user answers a number of questions about the Model. Model Risk Scorecard triggers calculate a risk score and determine the Model tier.

Model Version

The Model Version object is a child of the Model object and a parent of Model Deployment. The Model Version object is optional. If more detail is needed when building multiple versions of a model, the Model Version object can be used as an intermediary object.

Obligation

The Obligation object type represents the normalized and harmonized "things you need to accomplish" to comply with all of the obligation's associated Mandate, Sub-Mandate, and Requirement objects.

Obligation objects accomplish two primary purposes: they translate the often difficult and wordy legal jargon of Mandates/Sub-Mandates/Requirement into plain English, and they use the commonality across multiple Mandates/Sub-Mandates/Requirements. For example, you might have many Sub-Mandates and Requirements across numerous Mandates that require the use of strong passwords. A single Obligation object can document the details for strong passwords. By complying with this single Obligation, IT can satisfy many Mandates, Sub-Mandates, and Requirements.

Typically, Obligation objects are represented in a library Business Entity structure, and are not replicated throughout the system.

Obligation Evaluation

Once users have mapped internal controls to Obligations, users can conduct an evaluation of how well they are operating in relation to the identified obligation. Users can evaluate the operating effectiveness and design effectiveness of controls within the scope of a compliance theme

Obligation Evaluation Value

Obligation Evaluation Values are used to record the actual value of an obligation at a given point in time within the scope of an Obligation Evaluation.

ORIC Loss

ORIC Loss objects can be imported from the ORIC external loss database, for use with scenario analysis, benchmarking, and reports generation, and to export loss data to analytic tools or capital allocation applications.

ORX Loss

ORX Loss objects can be imported from the ORX external loss database, for use with scenario analysis, benchmarking, and reports generation, and to export loss data to analytic tools or capital allocation applications. You can import external ORX loss data into OpenPages Operational Risk Management for use with scenario analysis.

Plan, Timesheet

A Plan object type facilitates audit resource scheduling and allocation at any level. For example, you can create a single Plan object for an entire audit, or you can create one Plan object per task for each auditor who is involved with the audit. Plan objects are used to determine the availability, skills, and experience required of the desired resource. OpenPages Audit views, reports, and so on, are aligned

with Planning at the Audit level. Plans can instead be associated to Audit Sections, in which case these components would need to be modified.

Plan objects also drive time tracking - all time is tracked against Plans. A Timesheet object type is used to record weekly actual hours and expenses that are expended against a Plan object for an Audit. Because Timesheet objects are associated with Plans, it is easy to track deviations between planned and actual time and expenses.

You typically create or modify a Plan object by using the Add or Modify Plans helper, which audit owners can access from a link on the Audit task view. You can also edit plans (but not create them) by accessing the **Audit Management** > **Plans** menu item.

You should always use the Timesheet helpers to enter, modify, and approve time and expense data. Timesheet information can be viewed by accessing the **Audit Management** > **Timesheets** menu item. You can also add the Timesheet helpers to a Reports tab on your dashboard.

Policy
Policies represent internal guidelines that are adopted by the Board of Directors or senior governance body within an organization. The text of a Policy can either be stored in standardized fields on the object or as an attachment to the object. Policies typically have a distinct lifecycle from Draft to Published to Expired, as well as a review and approval process. Draft policies typically reside in the Organizational Business Hierarchy, while Published and Expired Policies typically reside in reference Library entities. Policies are also often mapped to applicable Mandates in the Library to which they relate.

Policy Review Comment
Policy Review Comments support and facilitate the review and approval process of Policies and Procedures by Subject Matter Experts and Compliance Personnel.

Preference, Preference Group
The Preference object is a child of a Business Entity or Preference Group, and includes variable values that can drive reports, workflows, and computed fields. It has entity-specific variable values that enable different behavior for the same workflows. For example, define variable values to determine the behavior for review and approval workflows such as the appropriate users for each level of review and approval, and the thresholds for determining how many levels of review and approval are required.

The Preference Group is used to group Preference objects together. Without this grouping object, each Preference object must be associated separately with each relevant Business Entities. The Preference Group helps minimize the associated maintenance.

In the default IBM OpenPages Internal Audit Management configuration, these objects are used to hold weights for Risk Factors used in Annual Assessment Risk Ranking. Since the weights and factors can be different for each type of audit, such as financial, operational, or strategic, create a separate Preference instance for each audit type. As a child of Business Entity, this approach provides the ability to have entity-specific variable values.

In the default IBM OpenPages Model Risk Governance configuration, these objects are used to identify participants in various MRG workflows and to configure parameters in the Model Risk Scorecard configuration.

Procedure
Procedures represent the what, where, when, and how of how policies are implemented in an organization. The text of Procedures is typically stored in the fields on the object. Typically, Procedures are represented as children of a Policy and reside in the same entity structure as its parent Policy.

Process
Processes represent the major end-to-end business activities within a business entity that are subject to risk. Processes reside in areas such as financial reporting, compliance, and information security. For example, Processes in the Accounts Receivable department such as order-to-cash could be improved with controls to protect against financial reporting risks such as fraudulent behavior or financial reporting inaccuracies.

In OpenPages Internal Audit Management, Processes are also used in scoping audits. Audits can copy Processes that are created by the business entity, or create their own Processes.

Process Eval

Process Evaluation objects are children of Process objects and they are used to capture process measurement values for trending purposes.

When the reporting periods do not align with the evaluation cycles, you can use Process Eval objects to capture multiple evaluation cycles within a single reporting period.

Product

This object type is a child of the Strategic Objective object type and is used to represent Products.

Program

Program objects are used together with Questionnaire Templates to implement Questionnaire Assessments. When a business administrator launches a Program, Questionnaires Assessments are created. A Program is associated with underlying assets, Questionnaire Assessments it created, and the Questionnaire Template it is based on. The Program provides input for the workflow.

Project

A project is designed to organize regulatory tasks into an overall compliance project. For example, there may be regulatory changes that need to be addressed in the compliance framework; users can create a project to identify and assign tasks.

Questionnaire Assessment

Questionnaire Assessment objects are a means of gathering information from business users in the organization. Questionnaire Assessments are created when a Program is launched. Questionnaire Assessments are associated with underlying assets, the Program that launched it, and the Questionnaire Template it is based on. Questionnaire Assessments are used by a workflow to facilitate a review process.

Questionnaires assessments are not related to questionnaires. Information that describes questionnaire assessments, questionnaire templates, and programs does not apply to questionnaires. See "Legacy object types" on page 147.

Questionnaire Template, Section Template, SubSection Template, and Question Template

Questionnaire Template, Section Template, SubSection Template, and Question Template objects are used together with Programs to implement Questionnaire Assessments. Questionnaire Template objects are parent objects and organize Section Template objects. Section Template objects are children of Questionnaire Template objects and organize SubSection Template objects. SubSection Template objects are children of parent Section Template objects and organize Question Template objects. Question Template objects contain questions and answer choices.

RapidRatings Ratings

RapidRatings Ratings objects are used with the RapidRatings connector in IBM OpenPages Third Party Risk Management. The RapidRatings Ratings objects store financial ratings and are children of Vendor objects.

Reg-Track Regulatory Event

The Reg-Track Regulatory Event object enables the direct ingestion of regulatory event feeds from Reg-Track into IBM OpenPages Regulatory Compliance Management.

Reg-Track Regulatory Event Series

The Reg-Track Regulatory Event Series object is a collection of Reg-Track Regulatory Events that have been assigned the same Reg-Track Series ID within the Reg-Track feed. The grouping of Reg-Track Regulatory Events within the Reg-Track Regulatory Event Series allows changes to be tracked from proposed to final stage in the regulatory change evolution.

Regulation Applicability

The Regulation Applicability object resides in the organizational business hierarchy. It assesses and tracks the regulatory impact of a Mandate in the library on a Business Entity.

Regulator

The Regulator object is part of the Regulator Interaction Management capability and provides the ability for organizations to create a single inventory of all Regulators with which they interact.

Regulators are typically created in a reference Library Business Entity. The object is a child of Business Entity and can be associated to Mandates and Regulator Interactions.

Regulator Interaction

The Regulator Interaction object is part of the Regulator Interaction Management capability. The Regulator Interaction object provides the ability to manage the interactions, communication, internal work, review, and approvals that are associated with external regulators such as inquiries, submissions, filings, exams, and meetings. For complex interactions such as exams, you can use the RI Component and RI Sub-Component objects to break the interaction into smaller components or track follow-up inquiries from the regulator. Regulator Interaction can be mapped to the following parent objects: Regulator, Mandate, Sub-Mandate, Requirement, Policy, Procedure, and Control. These parent associations enable a user to link objects that might be at issue in the Regulator Interaction and to identify users who are relevant to those objects and who might need to be consulted when responding to the regulator. Individual tasks that are related to the management of and response to the regulator interaction might be assigned to users through Regulatory Task child objects.

Regulatory Change

The Regulatory Change object is part of the Regulatory Change Management capability. It supports the ability to track regulatory changes, assess the impact of a change on the organization, communicate the change internally to the appropriate people, and drive internal processes in response to the change.

Regulatory Changes typically reside in the Library Business Entity, and can be associated directly to the Regulatory Event, Mandate, Sub-Mandate, or Requirement that changed. The triaging of the Regulatory Change is performed through the assignment of child Regulatory Task objects.

For organizations that receive a Reg-Track, Thomson Reuters, or Wolters Kluwer feed of regulatory events, users can create multiple Regulatory Change objects and initiate workflows from the ingestion of a regulatory event based on rules that are created within the **Rules Engine**.

Regulatory Event

The Regulatory Event object is used with IBM OpenPages Regulatory Compliance Management (RCM). The Regulatory Event object type enables the direct ingestion of regulatory event feeds by using the REST API or IBM AppConnect into RCM. Together with the **Rules Engine**, the Regulatory Event object type supports the automated generation of workflows that assign incoming regulator events to users based on supplied data points. Documents that are impacted by regulatory change are also supported. These capabilities help to assign tasks efficiently to users to respond to, and prepare for, regulatory change efficiently. A Regulatory Event can be a child of a Business Entity, Control, Mandate, Sub-mandate, Requirement, Policy, or Procedure. Users can create Regulatory Change objects as children of Regulatory Events.

Note: If you are using a data provider such as Reg-Track, Thomson Reuters, or Wolters Kluwer, see the regulatory event object type for that feed, such as the Reg-Track Regulatory Event object type.

Regulatory Initiative

The Regulatory Initiative object is a child of the Business Entity and captures descriptive information about regulations that impact an organization. Regulatory Initiatives represent a broader grouping of regulations. For example, Anti-Money Laundering could be a Regulatory Initiative that includes several different money laundering regulations that organizations must comply with.

Regulatory Task

The Regulatory Task object is used to assign tasks to OpenPages users when the task is related to one of the following parent objects: Project, Policy, Regulatory Change, Regulator Interaction, RI Component, or RI Sub-Component. A Regulatory Task can also be associated to a Business Entity.

Requirement

The Requirement object details specific requirements, found in the related Mandate or Sub-Mandate object, that the organization needs to adhere to in order to be in compliance.

Content can be pulled from UCF, Ascent Reg Tech, or other third party providers. Typically, Requirements are represented in a Library Business Entity structure and are not replicated throughout the system.

For Ascent Reg Tech, a Requirement is created for each incoming Task.

Requirement Evaluation

Once users have mapped internal controls to requirements derived from regulations, users can conduct an evaluation of how well they are operating vis-à-vis the identified requirement. Users can evaluate the operating effectiveness and design effectiveness of controls in within the scope of a compliance theme.

Requirement Evaluation Value

Requirement Evaluation Values are used to record the actual value of requirement at a given point in time within the scope of a Requirement Evaluation.

Requirement Version

The Requirement Version object details previous and future versions of the Requirement regulatory text. The Requirement Version object is a child of Requirement. The Requirement Version object tracks the regulatory changes over time. Past versions can assist in reviewing a Requirement at a given point in time. Future versions allow the user to prepare for the future regulatory text change and to begin their impact analysis.

Review

The Review object is used to record the scheduling and outcomes of any Model Review activity. It is the child of both the Model Deployment and Model objects. The object is intended to capture the outcomes of Reviews whether they are pre-implementation, post-implementation, and performed by second or third line of defense.

RI Component

The RI Component object (formerly labeled RI Category) is part of the Regulator Interaction Management capability and is used as the middle tier of the three-tier object model (Regulator Interaction, RI Component, and RI Sub-Component). The object is used to break down a complex Regulator Interaction into smaller, more manageable records or to link a follow-up inquiry from a regulator to the parent Regulator Interaction object. Additionally, RI Component can be mapped to the following parent objects: Mandate, Sub-Mandate, Requirement, Policy, Procedure, and Control. These associations enable a user to link objects that might be at issue and to identify users relevant to those objects and who might need to be consulted when responding to the regulator. Individual tasks related to the management of and response to the regulator interaction can be assigned to users through Regulatory Task child object.

RI Sub-Component

The RI Sub-Component object (formerly labeled RI Request) is part of the Regulator Interaction Management capability and is used as the last tier of the three-tier object model (Regulator Interaction, RI Component, and RI Sub-Component). The object is used to break down a Regulator Interaction and RI Component into smaller, more manageable records. Additionally, RI Sub-Component can be mapped to the following parent objects: Mandate, Sub-Mandate, Requirement, Policy, Procedure, and Control. These associations enable a user to link objects that might be at issue and to identify users relevant to those objects and who might need to be consulted when responding to the regulator. Individual tasks related to the management of and response to the regulator interaction can be assigned to users through Regulatory Task child objects.

Risk

Risks are potential liabilities. Risks can be associated with business processes, business entities, or a compliance with a mandate. Each risk has controls that provide safeguards against the risk. The controls help lessen consequences that result from the risk. Use the Risk object to categorize risks; capture the frequency, rating, and severity of observed and computed risk data; and view reports to identify top risk items. For example, the Cash account has a process that is called Payroll. A potential risk that might occur in the payroll is a duplicate payroll disbursements or the creation of fictitious payroll disbursements. Identifying risks in processes is a key component of developing a financial controls documentation project.

In OpenPages Internal Audit Management, a Risk that is shared between an internal audit and the business can be rated separately.

Risk Assessment

Risk assessments give you the ability to evaluate and report potential liabilities for a set of business entities or processes. A Risk Assessment object contains the names of the assessor and reviewer, the assessment time frames, and the status of the assessment. Use a Risk Assessment to manage the risk self-assessment process. Associate Risk objects with a Risk Assessment to create a link between the business entity and the Risks. For example, create a Risk Assessment to assess operational risks, such as external theft and fraud, internal fraud, physical property damage, or business disruption.

Risk Assessment Eval

Risk Assessment Evaluation objects are similar to Risk Evaluation objects except that they are instantiated as children of Risk Assessments. They store risk assessment data.

Risk Eval

Risk Evaluation objects are children of Risk objects and they are used to capture risk measurement values for trending purposes. Often reporting periods do not line up with risk evaluation cycles and so Risk Eval objects can be used to capture multiple evaluation cycles within a single reporting period.

RiskRecon Ratings

RiskRecon Ratings objects are used with the RiskRecon connector in IBM OpenPages Third Party Risk Management. The RiskRecon Ratings objects store vendor ratings and scores at the category and subcategory levels. The RiskRecon Ratings objects are created under `/BusinessEntity/ Library/VRM/VRMLibrary/RiskRecon` and are children of Vendor objects.

Scenario Analysis

Scenario Analysis (SA) is an assessment technique that is used to identify and measure the potential occurrence of operational risk events or to assess operational resilience. Unlike traditional operational risk assessments, it is a forward looking "what if" analysis.

Scenario Analysis is designed to derive reasoned assessments of the likelihood and impact of plausible operational losses or to analyze operational resilience. You can use the Scenario Analysis process in OpenPages to construct Scenario Analyses and collect supporting qualitative and quantitative data. Within each Scenario Analysis, you can record a range of frequency and severity estimates in "buckets" along with supporting information for the assessment.

In IBM OpenPages Operational Risk Management (ORM), scenario analysis is often used to identify and measure events with low frequency but high severity losses, for example natural disasters, terrorism, or rogue traders. Along with its qualitative elements, scenario analysis is often used as a direct input into a firm's operational risk capital estimate. Scenario Analyses are typically created for Business Entities and assigned a Risk Category. You can also associate supporting ORM data, for example, risk assessments, relevant loss events, ORIC losses, ORX losses, and risks.

In IBM OpenPages Business Continuity Management (BCM), scenario analysis is used to identify and measure severe, but plausible scenarios, that could disrupt important business services to test the likelihood of the business service's ability to recover within established impact tolerances. Scenario Analysis objects are created as child objects of Business Service objects. The results of a scenario analysis are stored in a Scenario Result object.

Scenario Result

Scenario Result objects are children of Scenario Analysis objects and they are used to capture the results of Scenario Analysis workshops for comparison and trending purposes.

In IBM OpenPages Business Continuity Management, a Scenario Results object is created as part of the last action of the Scenario Analysis workflow.

Signature

A Signature generally indicates agreement that the object meets your approval. It has no enforcement powers, and does not prevent the item from being modified after approval has been given.

Signatures (with or without associated locks) are applied to an object from the task view of an object.

If Signature locks are configured on your system, when you sign off on an object, the object and all its associated child objects are locked and cannot be modified until you either revoke your Signature or an administrator unlocks the object.

Strategic Objective
This object type is used to represent an organization's ESG objectives. The object type includes fields for the ESG domain and goals. The Strategic Objective object type has one parent: Business Entity.

Sub-Account
A Sub-Account represents a smaller, more targeted line item that is part of a larger parent Account (or of another Sub-Account). Each Sub-Account object can be associated with parent Account or Sub-Account objects.

Sub-Mandate
Sub-Mandates represent external (or internal) sub-items with which the organization needs to comply. Content can be pulled from third-party providers, including UCF, Ascent Reg Tech, Thomson Reuters, and Wolters Kluwer. Typically, Sub-Mandates are represented in a Library Business Entity structure, and are not replicated throughout the system. Sub-Mandate is recursive, but Deloitte, UCF, Ascent Reg Tech, Thomson Reuters, and Wolters Kluwer content use exactly one level of Sub-Mandate. Sub-Mandates also support content for regulatory compliance. Sub-Mandates can be used to represent paragraphs that are derived from regulatory papers.

Sub-Process
A Sub-Process is a component of a Process. It is used to divide Processes into smaller units for assessment purposes. For example, an order-to-cash financial Process might be composed of several Sub-Processes such as accounts payable, purchasing, and general accounting. Any of these Sub-Processes might expose the Business Entity to risk and can be improved by using controls.

In OpenPages Internal Audit Management, this object is not used in audit scoping, but might be used in documenting Process details.

Sub-Contractor
Sub-Contractor objects are child objects of Vendor objects. A Sub-Contractor represents a portion of a service that is provided by a Vendor. Sub-Contractor is an optional object type. Sub-Contractors can be subject to questionnaire assessments, risk assessments, or tiering. You can summarize and analyze risk that is associated with different Sub-Contractors. You can add a parent association to the process or sub-process that a Sub-Contractor supports.

Summary Audit Plan
The Summary Audit Plan object type enables a program office to plan audits of Auditable Entities for a pre-determined period of time (annual, half year, or quarter) by scope, risk profile, forecast hours of audits, and so on.

The Summary Audit Plan object is a child of Business Entity. The children of Summary Audit Plan include: Audit and Auditable Entity.

Supply Wisdom
The Supply Wisdom object stores risk ratings of Vendors that are imported from Supply Wisdom. The Supply Wisdom object type has one parent, Vendor.

Supply Wisdom Parent Alert
The Supply Wisdom Parent Alert object stores alert data that is imported from Supply Wisdom. The import creates Business Continuity Event objects for the incoming Alert data and associates the Alerts to the corresponding Vendor and Location objects in OpenPages.

System
System is a self-contained object type, which means that folders are created for each System object. The System object groups multiple Baselines to represent elements in the operating environment that can be assessed for risk. It acts as a container for a collection of Asset objects and the related Risks, Controls, and Requirements that together perform a function or comprise an IT service. For example, a System object might represent the servers, operating systems, applications, databases, support personnel, and facilities that provide the corporate email.

Team
The Team object type allows the organization to classify groups that support the business continuity process or are impacted in the planning of business continuity. The Team object can be used to identify key members of the team, the line of business and location and can be associated with the Employee object or Business Continuity Plan object.

Test Plan

A Test Plan is a container for tests and can be associated with parent Control objects and child objects, such as Test Results and Issues. Determine the operating effectiveness of a Control by conducting detailed tests and then documenting the results. Test Plans describe the mechanisms that determine if a Control is effective. For example, a sample Control is: "Human Resources authorizes changes in employee status." A test for this control might be: "Verify HR authorization stamp on new employee records." The test verifies that the new Control is implemented and in use.

The default OpenPages Internal Audit Management configuration uses the Workpaper object in place of the Test Plan and Test Result. The Audit object needs access to these objects because they are often used to document business testing.

Test Result

A Test Result is the information that is obtained from running a test plan.

The default OpenPages Internal Audit Management configuration uses the Workpaper object in place of the Test Plan and Test Result. The Audit object needs access to these objects because they are often used to document business testing.

Threat

A Threat is any circumstance or event with the potential to adversely impact organizational operations and assets. A library of Threats can be created under the Business Entity object and associated or copied to a parent Process, System, or Asset object. Threats can also associate to Vulnerabilities to identify and assess the likelihood and impact of a Threat's exploitation of a Vulnerability, which would result in risk to an Asset, System, or Process.

TRRI Regulatory Event

The TRRI Regulatory Event object enables the direct ingestion of regulatory event feeds from Thomson Reuters into IBM OpenPages Regulatory Compliance Management.

TRRI Regulatory Event Series

The TRRI Regulatory Event Series object is a collection of TRRI Regulatory Events that have been assigned the same Series ID within the TRRI feed. The grouping of TRRI Regulatory Events within the TRRI Regulatory Event Series allows changes to be tracked from proposed to final stage in the regulatory change evolution.

Vendor

A Vendor represents a third-party company from which a firm procures goods or services. Vendors can have four types of child objects: Vendor Subsidiary, SubContractors, Engagements and Contracts. Vendors can be subject to questionnaire assessments, risk assessments, or tiering. You can summarize and analyze risk associated with different Vendors. You can add a parent association to the process or sub-process that a Vendor supports.

If you use Supply Wisdom, the Vendor object also has the Supply Wisdom object as a child object.

Vendor ratings can be imported from SecurityScorecard or Supply Wisdom by using connectors.

Vendor Subsidiary

A Vendor Subsidiary represents a subsidiary of a Vendor from which a firm procures goods or services. Vendor Subsidiary is an optional object type. Vendor Subsidiary is a child of Vendor. Vendor Subsidiary can have three types of child objects: SubContractor, Engagements and Contracts. Vendor Subsidiary can be subject to questionnaire assessments, risk assessments, or tiering. You can summarize and analyze risk associated with different Vendor Subsidiaries. You can add a parent association to the process or sub-process that a Vendor Subsidiary supports.

Vulnerability

Vulnerabilities give you the ability to track and assess security weaknesses. You assign scores to Vulnerabilities using the Vulnerabilities Common Vulnerability Scoring System (CVSS v2). The parent object for a Vulnerability can be a System, Incident, Asset, or Risk. Typically, you import Vulnerabilities from an IT security solution.

Waiver

Waivers give you the ability to document, process and manage the lifecycle of exceptions to Policies, Requirements, or Controls. Waivers can be associated to Business Entities, Policies, Procedures, Requirements, Risks, Controls, Baselines, and Assets.

WK Regulatory Event

The WK Regulatory Event object enables the direct ingestion of regulatory event feeds from Wolters Kluwer into IBM OpenPages Regulatory Compliance Management.

Workpaper

A Workpaper is any artifact or deliverable you want to track in the scope of an audit. It can represent an engagement letter, a testing matrix, interview notes, or anything else appropriate to the audit in question. The workpaper itself can be attributes that are stored on the Workpaper object, or it can be a Microsoft Word, Microsoft Excel, or other type of file that is attached to a Workpaper object. When Workpaper is used for test evidence, it documents both the test planning and the test results.

Create a Workpaper object from the task view of an Audit Section. Workpaper objects can also be copied from a library, where they represent templates of different types of workpapers that are generated by an internal audit department.

Subcomponents

IBM OpenPages with Watson solutions consist of several subcomponents.

A subcomponent is a group of objects types that supports a logical function within the solution.

The following table lists the subcomponents that are included by default.

Table 10. Subcomponents in OpenPages with Watson

Sub component	Object type label	ESG	DPM	BCM	TPR M	RCM	MRG	FCM	ORM	PCM	ITG	IAM
Organization	Business Entity	X	X	X	X	X	X	X	X	X	X	X
Preference	Preference Group, Preference	X		X	X	X	X	X	X	X	X	X
Risk Assessment	Risk Assessment, Risk Assessment Eval	X		X	X	X	X	X	X	X	X	X
Process	Process, Process Eval, Sub-Process, Control Objective	X		X	X	X	X	X	X	X	X	X
Risk	Risk, Risk Eval	X		X	X	X	X	X	X	X	X	X
Control	Control, Control Eval	X	X	X	X	X	X	X	X	X	X	X
Test	Test Plan, Test Result				X	X	X	X	X	X	X	X
Issue	Issue, Action Item	X	X	X	X	X	X	X	X	X	X	X
Questionnaire Assessment	Questionnaire Assessment, Questionnaire Template, Section Template, SubSection Template, Question Template	X	X	X	X	X	X	X	X	X	X	X

Sub component	Object type label	ESG	DPM	BCM	TPR M	RCM	MRG	FCM	ORM	PCM	ITG	IAM
Assessment Program	Program	X	X	X	X	X	X	X	X	X	X	X
Employee	Employee			X	X	X	X	X	X	X	X	X
Account	Account, Sub-Account, Assertion							X				
Scenario Analysis	Scenario Analysis, Scenario Result	X		X					X			
External Loss	ORX Loss, ORIC Loss, FIRST Loss								X			
Loss Event	Loss Event, Loss Impact, Loss Recovery, Cost Center			X					X			
KRI	KRI, KRI Value	X		X	X				X	X	X	
KPI	KPI, KPI Value	X		X					X	X	X	
Regulatory Library	Mandate, Sub-Mandate, Requirement, Obligation Ascent Supporting Information (RCM only) Requirement Version (RCM only) Disclosure Statement (ESG only)	X				X	X			X	X	
Regulatory Event	Regulatory Event TRRI Regulatory Event, TRRI Regulatory Event Series WK Regulatory Event Reg-Track Regulatory Event, Reg-Track Regulatory Event Series					X						
Incident	Incident		X	X	X					X	X	
Waiver	Waiver				X					X	X	

Table 10. Subcomponents in OpenPages with Watson (continued)

Sub component	Object type label	ESG	DPM	BCM	TPR M	RCM	MRG	FCM	ORM	PCM	ITG	IAM
Table 10. Subcomponents in OpenPages with Watson (continued)												
Policy	Policy, Procedure, Policy Review Comment			X		X	X			X		
Policy Attestation	Policy, Procedure, Attestation									X		
Campaign	Campaign, Employee, Attestation									X		
Regulator Interaction	Regulator Interaction, Regulator, RI Component, RI Sub-Component, Compliance Review Comment, Regulatory Task					X				X		
Regulatory Change	Regulatory Change, Regulation Applicability, Regulatory Task, Compliance Review Comment	X	X			X				X		
ITG Policy	Policy, Procedure										X	
System	System, Baseline		X								X	
Asset	Asset, Asset Link		X	X							X	
Annual Plan	Summary Audit Plan, Auditable Entity, Audit											X
Engagement Plan	Plan, Timesheet, Auditor											X
Findings	Finding											X
Field Work	Audit Section, Workpaper, Audit Review Comment											X
Compliance Project	Project, Compliance Plan, Compliance Plan Evaluation, Compliance Theme, Compliance Theme Evaluation, Obligation					X						

Sub component	Object type label	ESG	DPM	BCM	TPR M	RCM	MRG	FCM	ORM	PCM	ITG	IAM
Table 10. Subcomponents in OpenPages with Watson (continued)												
Requirement Evaluation	Requirement Evaluation, Requirement Evaluation Value, Obligation Evaluation, Obligation Evaluation Value	X				X						
Regulator	Regulator, Regulatory Initiative	X				X						
Model Monitoring	Metric, Metric Value						X					
Committee Structure	Committee, Employee						X					
Model Inventory and MRG triggers	Model Use Case, Model Deployment, Model, Model Version, Change Request, Model Input, Model Output, Model Link, Model Attestation, Model Risk Scorecard						X					
MRG Review and Challenge	Review, Challenge						X					
Vendor	Location, Business Continuity Event, Vendor, Engagement, Contract Supply Wisdom, Supply Wisdom Parent Alert (only if using the Supply Wisdom feed.) RiskRecon Ratings (TPRM only) RapidRatings (TPRM only) Vendor Subsidiary (TPRM only) Sub-Contractor (TPRM only)	X		X	X							

Sub component	Object type label	ESG	DPM	BCM	TPR M	RCM	MRG	FCM	ORM	PCM	ITG	IAM
Business Continuity Management	Business Service, Business Service Evaluation, Business Impact Analysis, Business Continuity Event, Business Continuity Plan, Business Continuity Test Plan, Business Continuity Test Result, Location, Team, Model			X								
Strategic Objective for ESG	Strategic Objective, Product	X										
Vulnerability	Vulnerability, Threat										X	

Table 10. Subcomponents in OpenPages with Watson (continued)

In addition to the subcomponents listed in the table, the following object types are included in each solution and can be accessed by any authorized user:

- Signature
- File
- Link

Chapter 4. Helpers

IBM OpenPages with Watson solutions include several helpers.

Troubleshooting helpers

If you encounter a problem with a helper, you can configure registry settings to create logs for the helper. Use the following registry settings to configure logging for all helpers and triggers:

- `/Solutions/ORM/Log Level/Log Level` controls the amount of logging to be produced. By default, this is set to ERROR level.
- `/Solutions/ORM/Log Level/Log Folder` defines the location of the log files in the file system. By default, this is set to `/aurora/logs/custom/`.

    The following log files are created at this location: `helpers.log` for helpers logging, and `triggers.log` and `DetectPropertyChangeToValueTrigger.log` for triggers logging.
- `/Solutions/ORM/Log Level/Log Pattern` is the output pattern you use for each log entry. This pattern conforms to the Log4j 2 formatting rules as described in the Apache documentation.

To enable troubleshooting, set the registry setting /Solutions/ORM/Log Level/Log Level to TRACE. To disable troubleshooting, reset the registry setting to ERROR.

You must restart the server if you change any of these registry settings.

Types of helpers

The following table lists the helpers that are included for each solution by default.

Table 11. Helpers in IBM OpenPages with Watson solutions

Helper	TPRM	RCM	MRG	FCM	ORM	PCM	ITG	IAM
"RCSA Completion helper" on page 56					X			
"RCSA Process Alignment helper" on page 56					X			
"RCSA Launch Utility helper" on page 57					X			
"RCSA Site Sync helper" on page 57					X			
View Policy **Note:** This helper and the Review Policy are the same helper. Each has a different function and depends upon where in the lifecycle the policy is.						X		
Review Policy **Note:** This helper and the View Policy are the same helper. Each has a different function and depends upon where in the lifecycle the policy is.						X		
"Compare Policy View helper" on page 59						X		

Helper	TPRM	RCM	MRG	FCM	ORM	PCM	ITG	IAM
"Policy Unlock helper" on page 59						X		
Publishing Batch Notifications						X		
Policy Awareness View						X		
Attestation Create Report						X		
"Get Baselines helper" on page 61							X	
"Create Resource Links helper" on page 61							X	
"Close Audit helper" on page 61								X
"Add or Modify Plans helper" on page 61								X
"Timesheet Entry Helper" on page 62								X
"Timesheet Approval Helper" on page 62								X
Launch Program helper	X	X	X	X	X	X	X	X

Table 11. Helpers in IBM OpenPages with Watson solutions (continued)

RCSA Completion helper

The RCSA Completion helper allows the RCSA Coordinator to complete the Risk Assessment and create an evaluation tree for historical referencing.

The RCSA Coordinator receives a message that asks whether to proceed. When the coordinator confirms the message, the helper completes the following actions:

1. Sets the **Risk Assessment** status field to **Approved**.
2. Creates the following linked structure for the child Evaluation record:

   • Risk Assessment Evaluation

   • Process Evaluation

   • Risk Evaluation

   • Control Evaluation

3. Copies key data to the new Evaluation records and makes secondary associations.

   You must specify which fields to copy (**Settings** menu).

RCSA Process Alignment helper

The RCSA Process Alignment helper allows the RCSA Coordinator to review the associate Processes, Risks, and Controls, and create further associations. The helper also sets the Processes, Risks, and Controls to a status of **Awaiting Assessment**.

When the RCSA coordinator wants to begin the RCSA cycle, the coordinator can start the helper from a URL link on the Risk Assessment task view.

The task-driven helper completes the following actions when it is started:

1. Adds or removes Processes, Risks, and Controls

2. Reviews Process, Risk, and Control Ownership
3. Asks if the RCSA Coordinator wants to start the Assessment
   - If the coordinator responds **Yes**, the helper continues with the following processes:
     – Sets all Risk and Controls to **Awaiting Assessment**.
     – Sets the **Submit for Approval** field on the Risk object to **No**.
     – Sets the **Approve/Reject** field on the Risk object to a blank value.
     – Sets the **Rejection Comments** field on the Risk object to a blank value.
   - If the coordinator does not want to begin the RCSA cycle, save and close the Assessment.

RCSA Launch Utility helper

The RCSA Launch Utility helper generates Risk Assessment objects for In scope entities.

The Launch Utility helper assists the administrator with starting the RCSA process in the following ways:

1. Creates a Risk Assessment under the Business Entity and associates all processes that are under that Business Entity to the Risk Assessment.
2. Asks for Risk Assessment details.

   The administrator provides values to fields on all generated Risk assessments, such as **Start Date**, **End Date**, and **Instructions / Guidance**.
3. Identifies all **In-scope** entities.
4. Generates a Risk Assessment object for all **In scope** entities.
5. Populates the Risk Assessment object with the values provided in step 1.
6. Sets the Risk Assessment status to **Not Started** and the **RCSA Administrator** field is populated with the appropriate user name.
7. Sends the RCSA coordinator an email that informs the coordinator that the RCSA cycle can start.

   The administrator can specify the content of the email through the **Settings** page. The Risk coordinator email uses information from the nearest Preference record that has the specified RCSA coordinator.

RCSA Site Sync helper

The RCSA Site Sync helper synchronizes Business instances of object data with values in a Library data structure.

When the helper starts, it identifies all changes to the Master/Library object. The helper uses a **Library reference** field as a common key and synchronizes all local instances of the object with the Master.

RCSA helpers configuration

If you are using the RCSA business process, the administrator must configure RCSA after you install the IBM OpenPages with Watson modules.

Data

The RCSA Process Alignment helper and the RCSA Site Sync helper require the use of library and staging hierarchies.

Library Hierarchy
> To have the full functionality of the RCSA helper, you must create a library hierarchy.
>
> The Library root object is a business entity and the structure contains the common business Processes, Risks, and Controls that are to be used in the RCSA process.
>
> For example: Library Entity: /RCSA Library

Staging Hierarchy

To have the full functionality of the RCSA helpers, you must create a staging hierarchy.

The Staging root object is a business entity and the structure contains a staging process and risk. The hierarchy is used to store the processes, risks, and controls that are removed from the business entity as part of the RCSA process.

An example of a staging Entity: /RCSA Staging Hierarchy

An example of a staging Process: /RCSA Staging Hierarchy/Staging Process

An example of a staging Risk: /RCSA Staging Hierarchy/Staging Risk

The library and staging hierarchy data is loaded when IBM OpenPages Operational Risk Management is installed.

Settings

The Library and Staging areas have corresponding settings that you must configure for the RCSA helpers to register the structures.

To configure these settings:

1. Log in as an administrator.
2. Click ⚙ > **System Configuration** > **Settings**.
3. Expand the options for the following entries and set the values to the staging hierarchy that you created.

   - COMMON
   - RCSA PROCESS ALIGNMENT HELPER
   - RCSA SITESYNC
   - RCSA TRIGGERS

Common

`/OpenPages/Solutions/ORM/Common/Library Path`

This value must be set to the root Library entity object, for example, /RCSA Library.

Used for the RCSA Site Sync helper and the RCSA Process Alignment helper.

RCSA Process Alignment helper

This table identifies the values used in the RCSA Process Alignment helper.

Path	Description
`/OpenPages/Solutions/ORM/ Helpers/RCSA/Alignment/ Removed Control Path`	Used by the Process Alignment helper for storing removed Controls. This value must be a path to a Risk in the system, for example, / RCSA Staging Hierarchy/Staging Risk.
`/OpenPages/Solutions/ORM/ Helpers/RCSA/Alignment/ Removed Process Path`	Used by the Process Alignment helper for storing removed Processes. This value must be a path to an Entity in the system, for example, /RCSA Staging Hierarchy.
`/OpenPages/Solutions/ORM/ Helpers/RCSA/Alignment/ Removed Risk Path`	Used by the Process Alignment helper for storing removed Risks. This value must be a path to a Process in the system, for example, / RCSA Staging Hierarchy /Staging Process.

RCSA Site Sync helper

This table identifies the values used in the RCSA Site Sync helper.

Path	Description
/OpenPages/Solutions/ORM/ Helpers/RCSA/SiteSync/Exclude object	Used by the RCSA Site Sync helper to exclude the objects that are not required to be synced.
/OpenPages/Solutions/ORM/ Helpers/RCSA/SiteSync/ Standalone offset	Used by the RCSA Site Sync helper to look back a number of days. For example, 1 is yesterday.
/OpenPages/Solutions/ORM/ Helpers/RCSA/SiteSync/ Standalone target entity	Used by the RCSA Site Sync helper as the root Organizational Hierarchy, for example, /BANK ORG.

Policy Viewers

A series of Policy Viewers facilitate the process of creating, editing, reviewing, and approving policies and procedures. It aggregates multiple sections of a policy and associated procedures into a single narrative view for editing, reviewing and approving, while allowing customers to maintain standardization on a **Policy** template.

This helper has the following views:

- **Modify Policy** - Opened from a **Policy** object, the **Modify Policy** is an editable view that allows a policy author and owner to create and edit a **Policy** object and its associated **Procedures**. The **Modify Policy** viewer is only used as part of the **Datacentric** approach to Policy Management.
- **View Policy** - Opened from a **Policy** object, the **View Policy** is a read-only view that allows users to see a policy and its procedures in a formatted, narrative view (**Datacentric** and **Hybrid** approach) or from a **Policy Attachment** link (**Docucentric** approach).
- **Review Policy** - Opened from a **Policy Review Comment** object, **Review Policy** is a role-based view that facilitates the review and approval process. In addition to displaying the **Policy** and **Procedure** objects, or the **Policy Attachment** link, it includes the **Policy Review Comment** object that allow reviewers and approvers to submit feedback by either editing the **Policy** object directly or using the **Comment** form. Reviewers are presented with either an editable or read-only view of the policy and its procedures, depending on the parameter set in IBM OpenPages with Watson on the **Settings** page. Approvers are presented with a read-only view of the policy.

Configure this component to behave according to the customer methodology using settings and application text settings.

Compare Policy View helper

The Compare Policy View helper enables users to view red-lined differences from one version of a policy to another. For example, a user can visually see the difference between a current draft of a policy and the published policy, or past expired versions.

The Compare Policy View is used with the **Datacentric** and **Hybrid** approaches.

Configure this component to behave as appropriate for the customers' methodology using settings and application text settings.

Policy Unlock helper

The Policy Unlock helper is opened from the Policy object after the policy moves into the review and approval phase. The Policy Unlock helper unlocks the Policy object and its components (**Procedures**, **Attachments**, **Policy Review Comments**) for revision.

The Policy Unlock helper supports the three policy approaches: Datacentric, Docucentric, and Hybrid.

The Policy Unlock helper supports two use cases:

1. Reopening a **Policy** object for changes within a review cycle:

   - Sets the **Approval Status** to **In Revision**.
   - Unlocks any locked objects or attachments that are needed during the revision process.
   - Updates the version number.

2. Opening a Policy for a new revision cycle:

   - Sets the **Approval Status** to In Revision.
   - Unlocks the Policy object and its components (such as **Procedures**, Attachments).
   - Resets and clears fields such as **Publishing Date**, **Publishing Status**, **Next Review Date**.
   - Updates the version number.
   - Deletes or clears **Policy Review Comment** objects.
   - Sets a flag on the corresponding published policy to signify that the draft is **In Revision**.

You can configure this component to meet your requirements by using settings and application text settings. However, do not change the display type of the Policy Author field to a Multi Valued display type. The Policy Author field must be a single User Selector field.

Publishing Batch Notification helper

The Publishing Batch Notification helper facilitates the process of promoting an approved draft policy to the published library, and moving the current published version to the expired library. It also retires a policy by moving the published policy to the published library and deleting the draft. You can use the Publishing Batch Notification Helper with the **Datacentric**, **Docucentric**, and **Hybrid** policy approaches.

The Publishing Batch Notification helper runs on a scheduled basis and performs the following tasks:

- Updates Draft Policy:
  - Sets fields on draft policy such as **Approval Status**, **Published Date**, and **Publishing Status**.
  - Updates a version number according to the significance of a policy change.
- Promotes a published **Policy** object to the expired library:
  - Renames the **Policy** object (appends `Expired – V#`).
  - Sets **Policy Location** to **Expired** and specifies the expiration date.
  - Maintains approvals and associations with objects such as **Entities** and **Mandates**.
  - Removes hybrid policy attachments.
- Promotes a draft **Policy** object to the published library:
  - Sets **Policy Location** to **Published**.
  - Maintains approvals and associations with objects such as **Entities** and **Mandates**.
  - Maintains existing object associations (**Risk Assessment**) on a published **Policy** object.
- Sends emails upon successful publishing.

Configure this component to behave as appropriate for the customer methodology by using settings and application text settings.

Policy Awareness View helper

Policy Awareness View helper is an intuitive view that allows employees (high volume, low touch users) to easily read a policy and its procedures in a narrative format. The employee attests to reading and understanding the policy.

The Policy Awareness View helper completes the following tasks:

- Displays the **Policy** and its **Procedure** objects in a single read-only, narrative form with the look and feel of a corporate policy.

- Enables employees to attest to the policy with a single click and no navigation.
- Enables employees to request an exception to the policy attestation requirement.

Configure this component to behave as appropriate for the customer methodology by using registry and application text settings.

Attestation Creation Report helper

The Attestation Creation Report helper is a scheduled notification.

This notification report supports the Policy Awareness capability. It is intended to run on a scheduled basis and completes the following tasks:

- Finds all Campaign objects with a status of **Ready to Start** associated to published policies.
- Finds all active employees that match the same attestation requirements criteria defined on the Campaign object.
- Creates an **Attestation** record for each matching employee for that policy campaign.
- Displays the **Attestation** record on the employee's dashboard.
- Sends each employee an email notification and alerts them that an attestation is due.

Get Baselines helper

Launched from a link field on the System object, this helper copies the selected Baseline from the Library to the IT operating environment, and copies, or creates and pre-populates, descendent Risks, Controls and Test Plans. The helper creates associations from the new elements back to the Library elements and writes status information to the Additional Description field on the created Baseline.

Create Resource Links helper

This helper creates an Asset Link as a child of the starting Asset, and as a child of the selected Asset. The helper pre-populates fields on the created Asset Link object.

The helper can be launched in the following ways:

- By clicking **Create Resource Link** on the **Admin** tab of the Asset task view.
- By adding the Asset Link field to the task or grid views for the Asset object. You can then launch the helper from the view.

Close Audit helper

Launched from a link field on the Audit object, the Close Audit helper facilitates automation of the Audit Close process.

The Close Audit helper provides a summary and optionally details of the readiness for close status of the audit from which this helper was launched, and all of its components. When all components are ready, the helper provides a Close Audit button which automates the actions taken when an audit is closed, such as setting and clearing field values, deleting object instances and locking objects.

Configure this component to behave as appropriate for your methodology by using the registry and application text settings.

Add or Modify Plans helper

Launched from a computed field link on the Audit object, and available only for the Audit Owner, the Add or Modify Plans helper facilitates creating and editing Audit Plans. It finds and populates Auditors to assign to the Plans.

The helper provides a summary of and the ability to modify the existing Plans for this Audit. It provides the ability to add a new Plan for this Audit. It also enables the ability to search the Auditor pool or a

selected portion of it, for Auditors who match the skills, attributes and availability requirements that are identified in the Plan. It provides the ability to view details of other Plans for each found Auditor, and to select and auto-populate the appropriate auditor from the search results.

Configure this component to behave as appropriate for the customer methodology using the registry and application text settings.

Timesheet helpers

IBM OpenPages Internal Audit Management includes timesheet helpers.

There are two timesheet helpers:

- **Timesheet Entry Helper**: This helper enables you to enter time and expenses.

  If you have the appropriate permissions, you can also use the Timesheet Entry Helper to enter time on behalf of another auditor.

- **Timesheet Approval Helper**: This helper enables you to review and approve time and expenses.

Timesheet Entry Helper

Auditors use the Timesheet Entry Helper to enter time and expenses.

The Timesheet Entry Helper has the following capabilities:

- The helper includes data entry validations, and allows auditors to delete existing timesheet entries one row at a time.
- You can configure the helper to enable members of a user group to enter time on behalf of another auditor.
- Auditors can view all rejection comments at once, and can easily jump to the timesheets that they need to update.
- Auditors can search and filter for the Audit and Plan they want when adding a new timesheet row. To help the user choose, you can configure the Audit and Plan fields that are displayed.

Click **Timesheet Entry Helper** on the Reports panel on the dashboard to open the Timesheet Entry Helper. You can also view timesheet information by using the **Audit Management** > **Timesheets** menu item.

When an auditor creates and saves timesheet entries, Timesheet objects are created and populated for any new rows, and values are saved in any existing Timesheets. T&E expenses are a single entry per row per week; they are not broken down into expense categories. T&E is always entered and displayed in Base Currency.

You can configure the helper. Click ⚙ > **System Configuration** > **Settings**, and then use the settings under **Solutions** > **IAM** > **Timesheet Entry** > **Timesheet Entry Helper**.

Timesheet Approval Helper

Time approvers for auditors, such as audit owners or plan owners, use the Timesheet Approval Helper to review and approve or reject time and expenses.

The Timesheet Approval Helper separates timesheet entry from timesheet approval. When you configure the helper, you specify who can approve or reject timesheets.

Approvers can handle all of their approvals at once, across Audits and Auditors. In addition, approvals can see the queue of timesheets that are awaiting approval.

When an approver rejects a timesheet, the auditor receives a notification email. This notification feature is optional.

Click **Timesheet Approval Helper** on the Reports panel on the dashboard to open the Timesheet Approval Helper. You can also view timesheet information using the **Audit Management** > **Timesheets** menu item.

You can configure the Timesheet Approval Helper. Click > **System Configuration** > **Settings**, and then use the settings under **Solutions** > **IAM** > **Timesheet Entry** > **Timesheet Approval Helper**.

Chapter 5. Notifications

Notifications are emails that are sent to owners of a process as a reminder to act. These notifications can occur at different stages of a process or as a final step in a trigger.

All notifications that are sent from IBM OpenPages with Watson solutions use the following sender address. Configure the email address and server settings by using the appropriate solution abbreviation:

- `/OpenPages/Solutions/ORM/Email/From Email` - the sender address that is used to send notifications.
- `/OpenPages/Solutions/ORM/Email/From Name` - configure this item to identify the email sender name that is used by notifications.
- `/OpenPages/Common/Email/Mail Server` - configure this item to identify the email server that is used to send notifications.

  This item is used by lifecycles. For emails generated by lifecycle triggers, the sender address is specified in the `trigger.xml` file. The default is donotreply@openpages.com.

For information about email settings, see the *IBM OpenPages with Watson Administrators Guide*.

OpenPages with Watson solutions consist of several notifications. The following table lists the notifications that are included for each solution by default.

Workflows that are defined in GRC Workflow can also perform notifications. You can use both notifications and workflow email notifications for the same object type but you must consider how they interact and where they conflict. For more information, see *Configuring GRC Workflow* in the *IBM OpenPages with Watson Administrator's Guide*.

Table 12. Notifications in IBM OpenPages with Watson solutions

Notification	BCM	TPRM	RCM	MRG	FCM	ORM	PCM	ITG	IAM
"Issue and Action Bulletin notification" on page 66		X	X	X	X	X	X	X	X
"Incident notification" on page 66							X	X	
"Questionnaire Assessment notification" on page 67		X	X	X	X	X	X	X	X
"Reg-Track Ingestion Error notification" on page 67			X						
"TRRI Ingestion Error notification" on page 67			X						
"WK Ingestion Error notification" on page 67			X						
"New/Amended Regulatory Library Object notification" on page 67			X						
Loss Event Entry notification						X			
Control notification		X	X	X	X	X	X	X	X
Timesheet rejection notification									X

Issue and Action Bulletin notification

During the closedown phase of the Issue Management and Remediation (IMR) process, an Issue and Action Bulletin is sent as an email notification to the users. The bulletin highlights important areas such as overdue issues and actions that are due for closure. The administrator can set the frequency of this notification by using the Issue Management and Remediation (IMR) bulletin.

When the Issue is defined, its status is set to open. The user provides the current due date. The due date is copied to a read-only field that contains the original due date. When the user creates an Issue, the Issue Owner (who might not be the same person who created the Issue) receives an email notification.

The Issue Owner identifies the actions necessary to resolve an issue. The following data is captured in an Action Item:

- Description
- Assignee
- Start Date
- Due Date
- Actual Closure date
- Status (Read Only)
- A comment to record the latest updates

The Issue Owner receives an email that summarizes the actions that require approval before the issue can be closed. The Owner can either accept or reject the closure of the issue. When actions are completed, the Issue Owner reviews the Issue and updates the status to closed. If any child actions are set to open or awaiting approval, the Issue Owner cannot close the issue.

Issues are only displayed if the lowest-level Business Entity has a child Preference object associated with it. If the Issue is generated from the lowest level Business Entity, or another object type, it is not included in this report. Define a Preference Object for every level on which to report. Other features such as the RCSA trigger use the closest parent with a Preference object. These features inherit the preference from closest parent object.

Users receive email notifications through the consolidated Issue and Action bulletins. The bulletin consolidates the following information:

- Issues that are assigned to the recipient in the past number days
- Actions that are assigned to recipient in the past number days
- Issues due for closure in the next number days
- Actions due for closure in the next number days
- Overdue issues
- Overdue actions
- Actions awaiting closure approval

Incident notification

The Incident notification sends an email to an assignee when an Incident is created and for each transition in the Incident workflow.

The Incident notification is started by the Incident workflow. The email notification contains the stage, status, and a link to the Incident.

Questionnaire Assessment notification

The Questionnaire Assessment notification sends an email to an assignee when a questionnaire assessment is created and for each transition in the workflow.

The Questionnaire Assessment notification is started by the questionnaire workflow. The email notification contains the stage, status, and a link to the Questionnaire Assessment.

Reg-Track Ingestion Error notification

The Reg-Track Ingestion Error notification sends an email to Reg-Track Administrators if the import of a Reg-Track feed fails. Reg-Track Administrators are configured when you configure the Reg-Track feed in IBM OpenPages with Watson.

TRRI Ingestion Error notification

The TRRI Ingestion Error notification sends an email to TRRI Administrators if the import of a Thomson Reuters Regulatory Intelligence (TRRI) feed fails. TRRI Administrators are configured when you configure the TRRI feed in IBM OpenPages with Watson.

WK Ingestion Error notification

The WK Ingestion Error notification sends an email to WK Administrators if the import of a Wolters Kluwer feed fails. WK Administrators are configured when you configure the WK feed in IBM OpenPages with Watson.

New/Amended Regulatory Library Object notification

The New/Amended Regulatory Library Object notification sends an email if a Mandate, Sub-Mandate, or Requirement changes as a result of an Ascent Reg Tech, Thomson Reuters Regulatory Intelligence or Wolters Kluwer import. The email is sent to the object's owner.

Chapter 6. Reports

IBM OpenPages with Watson solutions include several reports.

Additional reports are installed with OpenPages with Watson and are available to all solutions. For more information, see the *IBM OpenPages with Watson Administrator's Guide.*

The following table lists the reports that are included with each solution by default.

Report	FCM	ORM	PCM	ITG	IAM	ESG
Table 13. Reports by IBM OpenPages with Watson solution						
Risk Assessment reports						
Risk Assessment List	X	X	X	X	X	
Risk Assessment Status	X	X	X	X	X	
Risk Assessment Summary	X	X	X	X	X	
Risk Assessment Issues and Action Items	X	X	X	X	X	
Risk reports						
Risk Analysis	X	X	X	X	X	
Risk Heat Map	X	X	X	X	X	
Risk Rating by Entity	X	X	X	X	X	
Risk Rating by Category	X	X	X	X	X	
Top Risks	X	X	X	X	X	
Control reports						
Risk and Control Matrix	X	X	X	X	X	
Control Effectiveness Map	X	X	X	X	X	
Testing reports						
Testing Performance and Results	X	X	X	X	X	
Indicator reports						
KRI Dashboard		X	X	X		
KPI Dashboard		X	X	X		
Loss Event reports						
Consolidated Loss Event Dashboard		X				
Risk vs Loss		X				

Table 13. Reports by IBM OpenPages with Watson solution (continued)						
Report	**FCM**	**ORM**	**PCM**	**ITG**	**IAM**	**ESG**
Issue Management and Remediation reports						
ORM Issue Dashboard		X				
ORM Issues and Action Items		X				
Scenario Analysis reports						
Scenario Summary		X				
Regulatory Compliance reports						
Process Control Effectiveness by Mandate			X			
Regulatory Applicability Matrix			X			
IT Asset reports						
Baseline				X		
Control Plan				X		
IT Compliance reports						
IT Control Effectiveness by Mandate				X		
Requirements Library				X		
UCF Requirements Library				X		
Audit Management reports						
Audit Universe					X	
Audit Plan					X	
Auditor Plan					X	
Audit Overview					X	
Internal Audit Report					X	
Audit Deviation					X	
Auditor Deviation					X	
Auditor Timesheet Dashboard					X	
Auditor Utilization Dashboard					X	
Pending Timesheet Approvals Dashboard					X	

Report		FCM	ORM	PCM	ITG	IAM	ESG
	Timesheet Entry					X	
	Timesheet Approval Helper					X	
Questionnaire reports							
	Program Report	X	X	X	X	X	X
	Single Assessment Report	X	X	X	X	X	X
FCM reports							
	Account Scoping by Entity and Classification	X					
	Control Certification – Process Summary Report	X					
	Control Certification Status Summary Report	X					
	FCM Issues and Actions Report	X					
	FCM Process and Account Mapping	X					
	SOX Roll-up Report (FCM – Process Control Certification Report)	X					
ESG reports							
	Objective Dashboard						X
	Objective Dashboard drill-through report						X
	Objective Listing						X
	Objective KRI Dashboard						X
	ESG Compliance Dashboard						X
	Compliance by Mandate Drill-through						X
	ESG Regulation and Standard Compliance Details						X
	Vendor List - ESG Ratings Requires TPRM and Supply Wisdom						X
	ESG Vendor Drillthrough Requires TPRM and Supply Wisdom						X
	Vendor Comparison – ESG Requires TPRM and Supply Wisdom						X

Table 13. Reports by IBM OpenPages with Watson solution (continued)

Table 13. Reports by IBM OpenPages with Watson solution (continued)							
Report		FCM	ORM	PCM	ITG	IAM	ESG
	Vendor Posture - ESG Ratings Requires TPRM and Supply Wisdom						X

Risk assessment reports

Risk assessment reports provide support for management by driving better decision-making that leads to action. These reports are a part of the action stage of the Risk and Control Self-assessment (RCSA) process.

The following table describes the available risk assessment reports. Users can drill through some reports to detail information.

Table 14. Risk assessment reports		
Name	**Drill-through report**	**Description**
Risk Assessment List		Shows Risk Assessment details for a specified Business Entity and all of its descendants.
Risk Assessment Status	Risk Assessment Status Detail	Shows a stacked column chart showing the status of Risk Assessments for the specified Business Entity and its direct descendants.
Risk Assessment Summary	Risk Assessment Issues and Action Items	Shows Risk Assessment details along with all associated Risks and Controls. A drill-through report shows Issues and Action Items that are related to the Risk Assessments, Risks, or Controls.
Risk Assessment Issues and Action Items		Shows all Issues and Action Items that are related to the selected Risk Assessment and its associated Risks and controls. Parent Object shows only the Risk Assessment, Risk, and Control parents. The report prompts for two values: Business Entity and Risk Assessment. Data is filtered on the selected entity. Users can select from all Risk Assessments that are associated, whether directly or indirectly, to the selected Business Entity.

Risk reports

Risk reports are available in IBM OpenPages with Watson solutions. Users can drill through some reports to detail information.

Table 15. Risk reports		
Name	**Drill-through report**	**Description**
Risk Analysis		Shows Risks grouped by Process for a specified Business Entity.

Name	Drill-through report	Description
Table 15. Risk reports (continued)		
Name	**Drill-through report**	**Description**
Risk Heat Map	Risk Detail	Shows a table that aggregates Risks by Residual Impact and Likelihood for a specified Business Entity.
Risk Rating by Entity	Risk Rating by Entity Detail	Shows Residual Risk Rating summary information for the selected Business Entity and its descendants. A drill-through report shows Risk details.
Risk Rating by Category	Risk Rating by Category Detail	Shows Risk Category and Residual Risk Rating summary information for the selected Business Entity. A drill-through report shows Risk details.
Top Risks		Show a summary of the top Risks ranked by Residual Risk Exposure, and also shows the Inherent Risk Exposure. By default, Risk quantitative assessment fields are not included in the following solutions so this report may not be appropriate for users of these solutions: • IBM OpenPages Policy Management • IBM OpenPages Financial Controls Management • IBM OpenPages IT Governance

Control reports

Control reports are available in IBM OpenPages with Watson solutions. Users can drill through from some reports to detail information.

Name	Drill-through report	Description
Table 16. Control reports		
Name	**Drill-through report**	**Description**
Risk and Control Matrix		Shows Risk and Control data for specified Business Entity and Processes.
Control Effectiveness Map	Control Effectiveness Detail	Shows counts of Controls grouped by Processes and Operating Effectiveness. A drill-through report contains more detail.

Testing reports

Testing reports are available in IBM OpenPages with Watson solutions. Users can drill through to detail information.

Table 17. Testing reports		
Name	**Drill-through report**	**Description**
Testing Performance and Results	Testing Details	This multi-tab report shows a visual representation of test results, including test results by Testing Status and test results by Outcome over time. A drill through report lists Test Plans, results, and trends.

Indicator reports

Reporting is the final stage of the Key Risk Indicator (KRI) or Key Performance Indicator (KPI) cycle. After the owner defines the KRIs or KPIs, and captures their values, standard indicator reports are provided for summary information for the selected business entities.

The following table describes the Indicator reports available in the IBM OpenPages Operational Risk Management, IBM OpenPages Policy Management, and IBM OpenPages IT Governance solutions. Users can drill through to detail information.

Table 18. Indicator reports		
Name	**Drill-through report**	**Description**
KRI Dashboard	KRI Dashboard Detail	Displays summary KRI information for the selected Business Entity and its descendants. A drill-through report shows detail and trend information.
KPI Dashboard	KPI Dashboard Detail	Displays summary KPI information for the selected Business Entity and its descendants. A drill-through report shows detail and trend information.

Loss Event reports

Loss Event reports ensure that information about loss events is collected consistently across the organization.

The following table describes the Loss Event reports available in IBM OpenPages Operational Risk Management. Users can drill through from some reports to detail information.

Table 19. Loss Event reports		
Name	**Drill-through report**	**Description**
Consolidated Loss Event Dashboard	Loss event Dashboard Details – Entity Loss Event Dashboard Details – Category	The Loss Event Dashboard displays Loss event data. The tabs include: • Loss Events Summary • Loss Events by Entity • Loss Events by Category • Loss Event Trend • Causal Analysis Drill through reports show a list of events or categories.
Risk vs Loss		Shows the annual Net Loss of a Business Entity for a specified date compared with the current Residual Risk Exposure.

Issue Management and Remediation reports

Issues are items that are identified against the documented framework. They are deemed as negatively affecting the ability to accurately manage and report risk.

The following table describes the issue management and remediation reports available in IBM OpenPages Operational Risk Management. Users can drill through from some reports to detail information. For users of other solutions, there are two platform reports: Issues List and Issues and Action Items.

Table 20. Issue Management and Remediation reports		
Name	**Drill-through report**	**Description**
ORM Issue Dashboard	Issue Dashboard Detail	Shows a graphical representation of the number of issues by status. The report is scoped on the entity object and date range.
ORM Issues and Action Items		Variant of the Issue Dashboard Detail report. Shows summary information on the associated action items.

Scenario Analysis reports

Scenarios involve the quantification of significant events (impacts and frequencies for potential events) that can be realized for an organization. The analysis captures the what-if scenarios of losses. The scenario analysis reports support the review of existing scenarios for each Business unit.

The following table describes the scenario analysis reports available in IBM OpenPages Operational Risk Management. Users can drill through to detail information.

Table 21. Scenario Analysis reports		
Name	**Drill-through report**	**Description**
Scenario Summary	Scenario Result Detail	Shows all Scenarios by Entity. Details include ID, Description, Status, and Owner.

Regulatory Compliance reports

The following table describes the Regulatory Compliance reports available in IBM OpenPages Policy Management. Users can drill through some reports to detail information.

Table 22. Regulatory Compliance reports		
Name	**Drill-through report**	**Description**
Process Control Effectiveness by Mandate	Process Control Effectiveness by Sub-Mandate	For a selected Business Entity, the report shows associated Mandates with the % of Effective Controls associated to Processes. A drill-through report shows detail information.
Regulatory Applicability Matrix		Shows a Matrix view of the Mandates and the Business Entities for which they apply.

IT Asset reports

The following table describes the IT Asset reports available in IBM OpenPages IT Governance.

Table 23. IT Asset reports		
Name	**Drill-through report**	**Description**
Baseline		Shows key attributes of the selected Baseline, along with associated Requirements, and recommended Control Activities and Test Procedures.
Control Plan		Shows key attributes of the selected System object, along with associated Baselines, their Requirements, and recommended and implemented Control Activities and Test Procedures.

IT Compliance reports

The following table describes the IT Compliance reports available in IBM OpenPages IT Governance. Users can drill through from some reports to detail information.

Table 24. IT Compliance reports		
Name	**Drill-through report**	**Description**
IT Control Effectiveness by Mandate	IT Control Effectiveness by Sub-Mandate	For a selected Business Entity, the report shows associated Mandates with the % of Effective Controls associated to Systems. A drill-through report shows detail information. The report looks at IT operating environment Controls that are shared between Mandates and Baselines in the IT operating environment. It provides a view of Control Operating Effectiveness by Mandate. One sub-report drills through for the selected Mandate to show Control Operating Effectiveness by Sub-Mandate. The other sub-report drills through for the selected Mandate to show Test Results grouped by Asset (type=Application). This report provides a view of how compliant each application is. This report is always run from the IT operating environment (it filters out the Library Business Entity).
Requirements Library		For the selected Requirements, the report shows all applicable laws and regulations. It reports hierarchy upwards from the Requirements that fit the prompt scoping, to the Sub-Mandates and Mandates that each of those Requirements satisfy. This shows you that meeting this one Requirement satisfies many Laws. The report has one page per Requirement and associated Mandates. This report is run from the Library.
UCF Requirements Library		For the selected UCF Harmonized Controls, the report shows all applicable Authority Documents.

Audit Management reports

The following table describes the Audit Management reports available in IBM OpenPages Internal Audit Management. Users can drill through some reports to detail information.

Table 25. Audit Management reports		
Name	**Drill-through report**	**Description**
Audit Universe		For the selected audit organization, this report shows Auditable Entities, including risk ranking and previous audit results.
		Scoped by Business Entity, a user can choose sort order. If the selected Business Entity is in the Internal Audit business hierarchy, the report shows the portion of the audit universe that is owned by that internal audit team. If the Business Entity is in the organizational hierarchy, the report shows elements of the audit universe that are associated with that Business Entity or any descendent Business Entities. This report is used in the early annual planning stages to determine which elements of the audit universe to audit this year.
Audit Plan	Audit Plan Detail	For the selected audit organization and date range, this report provides a GANTT chart view of the Audit Plan.
		Scoped by business entity, status, and date range, a user can choose to display information by days, weeks, months, or quarters. Selected date range displays the current year plan, a 3 or 5-year plan, or a planning timeframe. When viewing the report, you can click **Show Details** to see the details for each scheduled audit for each Auditable Entity. Click **Hide Details** to see a roll-up of the audits for each Auditable Entity. If the Audit Scheduled Start Date and Scheduled End Date overlap with a cell, then the entire cell is highlighted. Summary cells that are shown in red indicate more than one audit is scheduled during that time for that Auditable Entity.
Auditor Plan	Auditor Plan Detail	For the selected audit organization, Auditors and date range, this report provides a GANTT chart view of Plans.
		Scoped by Business Entity, Auditor, and Date Range, you can display information by days, weeks, months, or quarters. The Auditors available are those who are associated with the selected Business Entity or its descendants. Selected date range displays the current year plan or a planning time frame. When viewing the report, you can toggle between Detail View (shows details for each Plan for each Auditor) and Summary View (shows only a roll-up of the Plans for each Auditor). If an Auditor is scheduled for more than one Plan in a given column, then the entire cell is highlighted. Summary cells that are shown in red indicate more than one Plan that is assigned during that time for that Auditor. The report does not use the Percent Allocated information on the Plan to determine whether there is a conflict.

Name	Drill-through report	Description
		Table 25. Audit Management reports (continued)
Audit Overview	• Audit Findings Detail • Audit Issues Detail • Audit Review Comments Detail	For the selected Audit, view the status of its Audit Sections and Workpapers, and view associated Findings, Issues and Audit Review Comments. Scoped by Audit, the report includes Findings, Issues, and Review Comments that are direct children of the Audit, Sections, and Workpapers. Clicking the number of Issues, Findings, or Audit Review Comments starts a detail report, which includes more details and provides links to the objects in the application.
Internal Audit Report		Complete report for the selected Audit, including an executive summary and associated Findings and Issues. Scoped by Auditable Entity and then by Audit. Includes Findings associated to Audits, Audit Sections and Workpapers, and Issues associated with the Audit.
Audit Deviation		For the selected Audit, view its Plans and Audit Sections, including schedule and budget information, with highlights for significant deviations. This report lists the plans and sections for the selected Audit. It includes schedule and budget information and highlights significant deviations. Cells shown in yellow indicate missing key information. Cells shown in red indicate an unfavorable deviation from plan of more than 20%. Scoped by Auditable Entity and then by Audit. Includes the selected Audit, and Plans and Audit Sections associated directly to the Audit.
Auditor Deviation		For the selected Auditors, view their planned and actual dates, hours and expenses. Scoped by Auditors Business Entity, Auditor and Date Range. The Auditors available are those who are associated with the selected Business Entity or its descendants. Selected date range provides the ability to view a particular timeframe. Report shows Plans for each selected Auditor including the Scheduled, Expected and Actual Start and End Dates, the number of planned hours for each, and the number of actual timesheet hours, and the amount of planned and actual T&E recorded against each Plan during each time period. Cells shown in red indicate amounts that are 20% or more larger than planned amounts. Includes all Plans where the Auditor is the selected Auditor; Plans that do not have an assigned Auditor are not included in this report. The report includes a summary row for each Auditor and for the entire report. It defaults to HTML format and is also available in Microsoft Excel format.

Table 25. Audit Management reports (continued)		
Name	**Drill-through report**	**Description**
Auditor Timesheet Dashboard		For the selected Auditors, view the status of their timesheets for a number of weeks prior to a selected date. The Lead Auditor and Audit Managers can use this dashboard to track auditors who are not submitting time and to know whether resource metrics are up-to-date. They can drill down to see the details for a week for a particular auditor.
Auditor Utilization Dashboard		For the selected Auditors and a selected year, view Auditor utilization. Audit Managers can use this dashboard to make sure that they are making good use of their auditor resources, and also to ensure that auditors are not being over worked.
Pending Timesheet Approvals Dashboard		For the selected Auditors, view the timesheets that are waiting approval for a selected number of weeks prior to a selected date. The Timesheet Approver, Lead Auditor, and Audit Manager can use this dashboard to monitor outstanding timesheet entries. They can drill down for further information.
Timesheet Entry Helper		See "Timesheet Entry Helper" on page 62.
Timesheet Approval Helper		See "Timesheet Approval Helper" on page 62.

Questionnaire reports

The following table describes the Questionnaire reports.

Table 26. Questionnaire reports		
Name	**Drill-through report**	**Description**
Program Report		For a selected Program, the report shows overall score, questionnaire progress, and response summary per section.
Single Assessment Report		For a selected questionnaire assessment, the report shows sections, questions, and answers.

Financial Controls Management reports

The following table describes the FCM reports.

Table 27. FCM reports		
Name	**Drill-through report**	**Description**
Account Scoping by Entity and Classification		Displays Account objects by Business Entity and Classification. The report includes Account Type, Balance, Annual Percentage, and In Scope field values.

Table 27. FCM reports (continued)		
Name	**Drill-through report**	**Description**
Control Certification – Process Summary Report		Shows a summary of certification status of key controls that support the process. Link found on the field on the Process view.
Control Certification Status Summary Report	Control Certification Drill-through	Shows the key control certification status filtered by Business Entity, Year, and Quarter. Found on the FCM Certification dashboard and FCM Master dashboard.
FCM Issues and Actions Report		Shows a list of issues and corresponding actions and can be filtered by Business Entity and Issue Type. Found on the FCM Certification dashboard and FCM Master dashboard.
FCM Process and Account Mapping		Users can choose the Process and or Account relationship mapping to display in the report. For example, users can view Accounts that are in scope and not associated to Processes along with Processes that are in scope and not associated to Accounts.
SOX Roll-up Report (FCM – Process Control Certification Report)		Shows a summary of the control and process certification status by quarter, filtered by Business Entity, Key Control (Y/N), and Number of Prior Certifications (Quarters). Found on the FCM Certification dashboard and FCM Master dashboard.

Risk Management for ESG reports

The following table describes the reports that are available in IBM OpenPages Risk Management for ESG. Users can drill through some reports to detail information.

Table 28. Risk Management for ESG reports		
Name	**Drill-through report**	**Description**
Objective Dashboard	Objective Dashboard drill-through report	This report is an interactive multi-tab IBM Cognos Analytics dashboard that allows an organization to review the current state of Objectives, Prioritization, and Progress versus Target. The drill-through report displays a table of Objectives.
Objective Listing		This list report displays a table of Objectives, which are filtered by Entity, Objective Status, and Progress Status. This report includes cross track links to the Task view for each Objective.

Table 28. Risk Management for ESG reports (continued)		
Name	**Drill-through report**	**Description**
Objective KRI Dashboard		This report is filtered by Objective and displays a description and trend chart for all associated Key Risk Indicators.
ESG Compliance Dashboard	Compliance by Mandate Drill-through	This report is an interactive multi-tab IBM Cognos Analytics dashboard that allows an organization to view their ESG Compliance state.
ESG Regulation and Standard Compliance Details		This report shows details about Sub-Mandates and Requirements for a selected Mandate.

If you are using IBM OpenPages Risk Management for ESG and the Supply Wisdom integration along with IBM OpenPages Risk Management for ESG, the following additional reports are available:

Table 29. Risk Management for ESG with Supply Wisdom reports		
Name	**Drill-through report**	**Description**
Vendor List - ESG Ratings	ESG Vendor Drillthrough	This detailed list report shows ESG ratings for the selected Vendors, which are filtered by Vendor Name. The drill-through report displays key Supply Wisdom ESG ratings data and includes cross track links to the Vendor.
Vendor Comparison – ESG		This report displays the Supply Wisdom ESG ratings for two vendors. The report includes a filter to select the vendors for comparison.
Vendor Posture - ESG Ratings		This report is filtered by Vendor and displays the vendor's associated Supply Wisdom ESG risks in multiple formats (Radar, Cross Tab, and Trend Line chart).

Chapter 7. Triggers

The IBM OpenPages with Watson solutions include several triggers.

IBM OpenPages with Watson has introduced the GRC Workflow and GRC Calculations features that allow an organization to update and replace their current implementations of triggers.

Triggers that currently work in your environment, continue to work. However, your organization should make a plan to transition triggers to functionality that is based on the GRC Workflow and GRC Calculations features.

For more information, see:

- "Sample calculations" on page 97
- "Sample workflows" on page 105
- *Configuring GRC Calculations* in the *IBM OpenPages with Watson Administrator's Guide*
- *Configuring GRC Workflow in the IBM OpenPages with Watson Administrator's Guide*

Triggers that have been replaced by workflows and calculations are no longer enabled by default in fresh installations of OpenPages. For more information about these triggers, see "Legacy triggers" on page 136.

The following table lists the triggers that are included and enabled with each solution by default.

Table 30. Triggers in IBM OpenPages with Watson solutions								
Trigger	**TPRM**	**RCM**	**MRG**	**FCM**	**ORM**	**PCM**	**ITG**	**IAM**
"Risk and Control Self-assessments (triggers and calculations)" on page 84	X	X		X	X	X	X	X
"Control lifecycle triggers" on page 85	X	X		X	X	X	X	X
"Policy Import trigger" on page 86						X		
"Policy Lock trigger" on page 87						X		
"Audit Risk Rating Computations trigger" on page 87								X
"Audit Close Automation trigger" on page 87								X
"Model Risk Scorecard trigger" on page 87 **Note:** This trigger is disabled by default. The Model Risk Scorecard calculation replaces the trigger.			X					
"Exchange Rate trigger" on page 88					X			

Note: These triggers are designed to work with the default configuration of OpenPages. Any changes to the configuration, such as fields, dependent picklists, and field dependencies, can impact how or whether the triggers and helpers work as designed.

Object types that contain triggers

Before you use the ObjectManager tool to load XML instance data, disable triggers on any object types for which you want to load data.

The following table lists the object types for which triggers are included by default.

Object type	TPRM	RCM	MRG	FCM	ORM	PCM	ITG	IAM
Table 31. Object types that contain triggers in IBM OpenPages with Watson solutions								
Risk	X	X	X	X	X	X	X	X
Control	X	X	X	X	X	X	X	X
File (SOXDocument)						X		
Policy						X		
Audit								X
Audit Review Comment								X
Audit Section								X
Finding								X
Plan								X
Timesheet								X
Workpaper								X
Model Risk Scorecard **Note:** This trigger is disabled by default in fresh installations.			X					

Risk and Control Self-assessments (triggers and calculations)

The Risk Assessments process is used to identify, assess, and quantify a risk profile of a business. Each Risk is assessed on either a Qualitative or Quantitative basis.

Calculations and triggers provide the process workflow for Risk Control and Self-assessment of the business.

Enable either the qualitative or quantitative method:

- If you want to assess risks using the qualitative method, enable the Qualitative Audit Risk Rating and Qualitative Risk Rating calculations and disable the Quantitative Audit Risk Rating and Quantitative Risk Rating calculations.

  When a Risk is saved, the Qualitative Risk Rating calculation figures the Qualitative Inherent Risk Rating and Qualitative Residual Risk Rating based on defined registry keys and values on preference objects.

- If you want to assess risks using the quantitative method, enable the Quantitative Audit Risk Rating and Quantitative Risk Rating calculations and disable the Qualitative Audit Risk Rating and Qualitative Risk Rating calculations.

  When a Risk is saved, the Qualitative Risk Rating calculation figures the Quantitative Inherent Risk Rating and Quantitative Residual Risk Rating based on defined registry keys and values on preference objects.

The following triggers are used for Risk and Control Self-assessments:

- Risk Assessment Create
- Risk Assessment Update

- Risk Approval Submission Create trigger

  When Submit for Approval is set to Y on a Risk object, the trigger updates the Status field on the Risk and all associated Controls from Awaiting Assessment to Awaiting Approval , sets the Process Status to Awaiting Assessment, and sends an email to the process Owner.

- Risk Approval Submission Update trigger

- Risk Control Approval Create trigger

  When Approve/Reject is set to Approve on a Risk, the trigger checks if all risks for a Process are approved. If yes, the trigger changes Process Status to Approved and sends an email to the RCSA coordinator. If no, Process Status is not changed.

- Risk Control Approval Update

The RCSA Quantitative trigger and RCSA Qualitative trigger are no longer enabled in fresh installations. For more information, see "RCSA Quantitative and RCSA Qualitative triggers (legacy)" on page 143.

Control lifecycle triggers

Triggers provide the transitions that move controls through an attestation lifecycle. Lifecycles define the stages that an object type can follow. At each stage, the system:

- Identifies a lifecycle assignee
- Defines the actions available to move to a different stage
- Automatically sends an email to the new lifecycle assignee
- Defines other attributes that are related to the current stage

The lifecycle for controls uses the following stages:

- New
- In Progress
- Attestation
- Closed

When a control is created, the system sets the lifecycle to the New stage and sends an email to the first lifecycle assignee. When the user completes the task, the trigger moves the object to the next task and the next user. A user can add a comment with every transition. Transitions take place when users open a control object in the task view and click **Action > <transition name>**. The stage determines the transition that is displayed.

The following table summarizes how the system handles controls and sets the lifecycle assignee. The Transition column contains the name of the **Lifecycle > <transition name>** in the control task view that a user clicks to trigger the transition to the next stage.

Table 32. Lifecycle process and stage owners for controls

Stage	Lifecycle assignee	Transition	Next stage	Next Status
New	Control Owner	**Start**	In Progress	In Progress
In Progress	Control Owner	**Submit for Attestation**	Attestation	Attesting
Attestation	Control Attester	**Send Back**	In Progress	Attest Rejected
Attestation	Control Attester	**Attest**	Closed	Closed
Closed	(not assigned)	**Re-Open**	In Progress	Re-Opened

Control notification

The control notification sends an email to a lifecycle assignee when a control is created and for each transition in the control lifecycle. A transition occurs when a user clicks a transition icon **Action** > **Start**, **Submit for Attestation** , **Send Back**, **Attest**, or **Re-Open**) in the control task view.

The control notification is started by the control lifecycle trigger. The email notification contains the stage, status, due date, comment, and a link to the control.

Policy Import trigger

The Policy Import trigger imports Policy and Procedure content from a structured Microsoft Word document into IBM OpenPages with Watson Policy and Procedure fields by parsing the different sections of the document. It is triggered by checking in an attachment to the Policy object.

The trigger supports the Hybrid approach to Policy Management, It also supports updating the version number in the Docucentric approach when a new policy document is checked in. As part of the import process, the trigger also performs extensive validation to ensure that the structure of the Word document adheres to the defined Policy Template.

OpenPages with Watson or the customer can configure this component to behave for the customer methodology through registry and application text settings.

The IBM OpenPages Policy Management Policy Import Trigger has the following known limitations:

- Bulleted lists only support the disc and circle bullet format.
- Numbered lists only support decimal, upper-alpha, lower-alpha, upper-roman, and lower-roman.
- Symbol fonts are not supported. You can use the **Insert Symbol** option and select a symbol using normal font (for example, the copyright symbol).
- Wingding font is not supported.
- Cannot set shading from the **Shading** menu. Workaround: Use text highlighting to achieve a similar effect. (.doc only)
- Will not display the value of a FORMDROPDOWN. (.doc only)
- Ordered lists always use a period as the separator. For example, if a list item in the Word doc looks like "1)" then it will be "1." after the import.
- For .doc, the style of the list item marker will be inferred from the text content of the list. The marker's font family and font size will match the first piece of text in the list item. The marker will be bold, italic, and/or colored if all the text in the list item has that same styling.
- Images, Word Art, and diagrams are not supported.
- Does not support importing a Table of Contents.
- All underline styles show as single solid line
- Superscript/subscripts defined by within a style are not supported (.doc only). Workaround is: Apply sub/superscript from the Font menu instead of using a style.
- Formatting overrides that conflict with custom styles. For example, if custom style includes a Strong text format and the user manually un-bolds the text within the document, the text will show up bold per the Strong style. (.doc only)
- Tabs default to 4 spaces, which is not guaranteed to match the spacing in the document since tabs are based on positioning in the document. It is better to use indent when aligning content.
- Hanging indent (that is, First Line Indents) for lists is not guaranteed to line up perfectly due to the varying width of the list item markers.
- Within lists, mixing techniques for creating bullets, lists, and indentations will often result in items not being aligned correctly and incorrect numbering of items.
- Entering several carriage returns to create spacing will not render as extra spacing.
- Unsupported features:

- Changes in Text Direction
- Double Strike Through
- Emboss, Engrave, Shadow text
- Text Effects
- Emphasis Marks
- Custom Text Spacing
- Shadowed borders
- Ascending diagonal cell borders

Policy Lock trigger

The Policy Lock trigger locks the Policy or the Policy and its components (Procedures, Attachments, Policy Review Comments) at different points in the Review and Approval Process. This trigger supports all three approaches to Policy Management: Datacentric, Hybrid, and Docucentric.

The Lock trigger supports two use cases:

- Locking Policy Attachments in support of a policy being put into a review and approval cycle to ensure that the policy content cannot be changed during approvals. (Applicable for Hybrid and Docucentric approaches.)
- Locking the entire Draft Policy hierarchy (Policy, Procedures, Attachments and Policy Review Comments) after the Policy has been given final approval and is ready for publishing. (Applicable for all three policy approaches.)

The customer can configure this component to behave as appropriate for the customer methodology using the registry and application text settings.

Audit Risk Rating Computations trigger

The Audit Risk Rating Computations trigger calculates and maintains the Audit Inherent and Residual Risk Rating field values on the Risk object.

The RCSA Quantitative trigger and the RCSA Qualitative trigger apply to the Audit Risk Rating Computations trigger.

Audit Close Automation trigger

The Audit Close Automation trigger assesses close readiness for each configured component of an audit. By default, the trigger is configured for the following object types: Audit, Audit Section, Workpaper, Finding, Audit Review Comment, Plan, and Timesheet.

When an instance of a configured object type is created or updated, the trigger evaluates all the criteria which are configured for that object type. If all the criteria have been met, then the trigger sets the Ready To Close field value to Yes. This field value is used by the Audit Close helper to determine if all of the audit components are ready to close.

Configured ready to close criteria categories include fields that are required, date fields that must be set to on or before today's date, date fields that must be set to values on or before other date field values, and user fields that cannot be set the same as other user fields.

Model Risk Scorecard trigger

The trigger on the Model Risk Scorecard object calculates scores that are used to assign a tier to a Model. Model Risk Scorecards are part of IBM OpenPages Model Risk Governance.

Note: This trigger is disabled by default. The Model Risk Scorecard calculation replaces the trigger

The trigger on the Model Risk Scorecard object is evaluated if a Model Risk Scorecard is created or if scoring input fields are updated. The trigger calculates scores and weighted scores for each input and calculates a score and a weighted score for each input category. Finally, the trigger calculates an overall score and assigns a tier to the Model based on the overall score. The trigger is configured in registry settings and uses weights and other values on Preference records whose Type is set to MRG.

Exchange Rate trigger

The Exchange Rate Trigger recalculates the specified currency field value by using the nearest exchange rate based on the configured date field, instead of the latest exchange rate loaded in the system.

For Loss Events, the Estimated Gross Loss value is updated based on the exchange rate that is closest to the Discovery Date.

For Loss Impacts, the Estimated Loss and Actual Loss values are updated based on the exchange rate that is closest to the Occurrence Date.

For Loss Recovery, the Estimated Recovery Amount and Recovery Amount values are updated based on the exchange rate that is closest to the Received Date.

The `Trigger` Run field on Loss Impacts and Loss Recoveries is disregarded by the Exchange Rate trigger. If it is set to No, the Exchange Rate trigger still runs.

You can enabled and disable the Exchange Rate Trigger. Click > **System Configuration** > **Settings**, and then edit the **Solutions** > **ORM** > **Triggers** > **Loss Events** > **FX Rate Adjuster** setting. The default is true (enabled).

Chapter 8. Profiles

IBM OpenPages with Watson solutions include one or more profiles.

Every solution has a main profile, which is called the *Master* profile. Some solutions include additional profiles. Each profile includes the following pre-configured items, which can be modified by an administrator:

- Object types
- Fields and field groups
- Views
- Dashboard
- Filters
- Reports (if available)

Some solutions include more profiles, which are subsets of the master profile.

Table 33. Profiles	
Solution	**Profiles**
IBM OpenPages Data Privacy Management	- **OpenPages DPM Master** - **DPM Data Steward**: This profile is for Data Privacy Management technical users, including data stewards, and data engineers. - **DPM Privacy Officer**: This profile is for Data Privacy Management users in roles related to privacy compliance and risk.
IBM OpenPages Business Continuity Management	- **OpenPages BCM Master** - **BCM End User**: This profile provides read-only access to employees who need to view business continuity plans within the Business Continuity Management solution. - **BCM Supply Wisdom Master***
IBM OpenPages Third Party Risk Management	- **OpenPages VRM Master** - **VRM Vendor Manager**: This profile is intended for users who are responsible for managing vendors. - **VRM Vendor**: This profile is intended for vendors. The profile gives them access to a limited set of object types such as Questionnaire. - **OpenPages RapidRatings Master*** - **VRM RiskRecon Master*** - **VRM Security Scorecard Master*** - **VRM Supply Wisdom Master*** More profiles, for example for a Process Owner, Control Tester, and other users, can be created during the implementation project.
IBM OpenPages Regulatory Compliance Management	- **OpenPages RCM Master** - **RCM Ascent Master*** - **RCM Reg-Track Master*** - **RCM TRRI Master*** - **RCM WK Master***

Table 33. Profiles (continued)	
Solution	**Profiles**
IBM OpenPages Model Risk Governance	• **OpenPages MRG Master** • **MRG Model Owner**: This profile is intended for model developers and model owners. Users assigned to this profile have access to MRG-specific task views on the shared object types Business Entity and Preference. • **MRG Model Validation**: This profile is intended for model validators and reviewers. Users assigned to this profile have access to MRG-specific task views on the shared object types Business Entity and Preference.
IBM OpenPages Financial Controls Management	• **OpenPages FCM Master** • **FCM Certification V2**: This profile is designed for users who are actively involved in the review and sub-certification process. • **FCM Master V2**: This profile is designed for users that are involved in the sub-certification or have an oversight role in the sub-certification process.

Table 33. Profiles (continued)	
Solution	**Profiles**

IBM OpenPages Operational Risk Management	• **OpenPages ORM Master**
	
	• **ORM Operational Risk Team**: This profile is intended for a power user who uses most capabilities of OpenPages but who does not need read access to library IDs and object status fields.
	
	A user of this profile can:
	
	  – Maintain processes
	  – Manage risk and control libraries
	  – Perform RCSA scoping
	  – Perform and oversee the RCSA process
	  – Administer, review, and oversee loss events
	  – Define and capture key risk indicators (KRIs)
	  – Manage issue and action closure
	  – Coordinate scenario analysis
	
	• **ORM Business User**: This profile includes the fields and configurations that are required by a risk manager to use in the operations of the business. This user is an active participant in most operational risk management activities.
	
	A user with this profile can:
	
	  – Log a loss event
	  – Perform RCSA scoping
	  – Approve risk assessments
	  – Capture KRIs
	  – Manage issue and action closure
	  – Participate in scenario workshops
	
	• **ORM Simplified User**: This profile allows a user to focus on loss events, KRI value capture, and issue management.
	
	• **OpenPages FIRST Loss**: This profile is designed to facilitate the loading of FIRST Loss data into OpenPages by using FastMap.
	
	Users of this profile can edit all fields in FIRST Loss objects so that data can be loaded. Assign this profile to users who are responsible for loading FIRST Loss data through FastMap. Give all other users read-only access to FIRST Loss objects.
	
	Note that it is not necessary to assign this profile to a user. Instead, you can configure the FastMap import spreadsheet to use the **OpenPages FIRST Loss** profile.

IBM OpenPages Policy Management	• **OpenPages PCM Master** • **PCM End User**: This profile has read-only access and is intended for employees who need to view policies and procedures. More profiles, for example for a Compliance Program Manager, Privacy Officer, and other users, can be created during the implementation project.

Table 33. Profiles (continued)	
Solution	**Profiles**
IBM OpenPages IT Governance	• **OpenPages ITG Master** Subsets of this profile that are appropriate for an IT library administrator, IT director, and other users can be created during the implementation project. • **ITG RiskLens Master***
IBM OpenPages Internal Audit Management	**OpenPages IAM Master** Subsets of this profile that are appropriate for a lead auditor, audit director, and other users can be created during the implementation project.
IBM OpenPages Risk Management for ESG	• **OpenPages ESG Master** • **OpenPages ESG Supply Wisdom Master***

* These profiles are available only if your environment includes the configuration for the related data feed.

The super administrator (OpenPagesAdministrator) has access to the following profiles by default:

- OpenPages Modules Master (already included)
- OpenPages BCM Master
- OpenPages DPM Master
- OpenPages ESG Master
- OpenPages FCM Master V2
- OpenPages IAM Master
- OpenPages ITG Master
- OpenPages MRG Master
- OpenPages ORM Master
- OpenPages PCM Master
- OpenPages RCM Master
- OpenPages VRM Master

Chapter 9. Role templates

A role template defines the privileges that a user is granted. IBM OpenPages with Watson solutions include several role templates. Role templates give application permissions and grant access to features and functions. They also give Object ACLs (RWDA).

When permission rights are assigned to a solution role template, those rights are also assigned to the **Modules Master - All Permissions** template.

By default, two role templates are included with most solutions. The template called "All Permissions" provides administrative rights and permissions to all object types that are available for the solution. The template called "All Data - Limited Admin" provides permissions to all object types that are available for the solution but does not provide administrative rights. Some solutions include additional role templates that include a subset of permissions.

For more information on permissions provided with role templates, see .

List of role templates

IBM OpenPages with Watson solutions include several role templates.

The following role templates are delivered with the solutions:

Table 34. Role templates	
Name	**Description**
Modules Master - All Permissions	Full R/W/D/A access to all enabled-by-default objects for all Solutions. Full admin rights.
Modules Master - All Data - Limited Admin	Full R/W/D/A access to all enabled-by-default objects for all Solutions. No admin rights except those associated with workflows, files and folders.
[BCM] - Assignee	R/W/A access to most default BCM objects. Participant in Business Continuity Process.
[BCM] - BC End User	Read (R) access to Business Continuity Plan objects. Employee looking to access relevant Business Continuity Plans.
[BCM] - BC Manager	R/W/D/A access to all default BCM objects. Manager on centralized Business Continuity team setting plan standards, and aggregating organization-wide plans centrally.
[BCM] - BC Owner	R/W/D/A access to most default BCM objects. Business owner of the Business Continuity Plan and it's execution.
[BCM] - BCP Approver	R/W/A access to most default BCM objects. Approver of Business Continuity Plans.
[BCM] - BCP Author	R/W/A access to most default BCM objects. Author of the relative Business Continuity Plan.
[BCM] - BCP Focal	R/A access to all default BCM objects. Business unit level executive where plan applies.
[BCM] - BCP Reviewer	R/W/A access to most default BCM objects. Reviewer of Business Continuity Plans.
DPM - All Data - Limited Admin	Full R/W/D/A access to all default DPM objects. No admin rights except those associated with workflows, files and folders.

Table 34. Role templates (continued)	
Name	**Description**
DPM - All Permissions	Full R/W/D/A access to all default DPM objects. Full admin rights.
ESG - All Data - Limited Admin	Full R/W/D/A access to all default ESG objects. Additional role permissions limited to: Files, Publishing.
ESG - All Permissions	Full R/W/D/A access to all default ESG objects. Full admin rights.
FCM - All Data - Limited Admin	Full R/W/D/A access to all default FCM objects. No admin rights except those associated with workflows, files and folders.
FCM - All Permissions	Full R/W/D/A access to all default FCM objects. Full admin rights.
FCM - Certifications	Used by roles involved in certification activities, for example, process owners or control owners. Read, write, associate, and delete access rights are granted to objects needed for FCM SOX certification, for example, Control, Control Eval, process, Process Eval, Risk, File, Issue, and some FCM objects. Most admin application permissions are not granted.
IAM - All Data - Limited Admin	Full R/W/D/A access to all default IAM objects. No admin rights except those associated with workflows, files and folders.
IAM - All Permissions	Full R/W/D/A access to all default IAM objects. Full admin rights.
ITG - All Data - Limited Admin	Full R/W/D/A access to all default ITG objects. No admin rights except those associated with workflows, files and folders.
ITG - All Permissions	Full R/W/D/A access to all default ITG objects. Full admin rights.
Loss Event Entry	Role template used by the Loss Event Entry application.
MRG - All Data - Limited Admin	Full R/W/D/A access to all default MRG objects. Limited admin rights.
MRG - All Permissions	Full R/W/D/A access to all default MRG objects. Full admin rights.
MRG - Model Developer Owner	Used by model owners and developers. This role template is similar to the Model Risk Management role template except that no write access is granted to the Review object. Most admin application permissions are not granted.
MRG - Model Risk Management	Used by model risk managers (second line of defense). Read, write, and associate access rights are granted to MRG object types. Write access is denied to the two shared object types, Preference and Business Entity. Most admin application permissions are not granted. Delete access is not granted to any object types.

Table 34. Role templates (continued)	
Name	**Description**
MRG - Model Validation	Used by model validation users. Read, write, and associate access rights are granted to a subset of MRG object types including Model, Model Use Case, Review, Change Request, and Challenge. Write access is denied to other MRG object types. Write access is denied to shared object types, Preference and Business Entity. Most admin application permissions are not granted. Delete access is not granted to any object types.
MRG - AI Factsheets - API Access	Limited role template for AI Factsheets to access the OpenPages API.
ORM - All Data - Limited Admin	Full R/W/D/A access to all default ORM objects. No admin rights except those associated with workflows, files and folders.
ORM - All Permissions	Full R/W/D/A access to all default ORM objects. Full admin rights.
[ORM] Business User	ORM role template for users who log loss events, perform RCSAs, approve risk assessments, capture KRIs, manage issue and action closure, and participate in scenario workshops.
[ORM] Operational Risk Team	ORM role template for users who maintain Process, Risk, and Control libraries, scope RCSAs, perform and oversee the RCSA process, perform loss event administration, define and capture KRIs, manage issue and action closure, and coordinate scenario workshops.
[ORM] Simplified User	ORM role template for users who need minimum access for their work on loss events, KRI value capture, and issue management.
PCM - All Data - Limited Admin	Full R/W/D/A access to all default PCM objects. No admin rights except those associated with workflows, files and folders.
PCM - All Permissions	Full R/W/D/A access to all default PCM objects. Full admin rights.
PCM End User	Read (R) access. For employees who need to view policies and procedures.
RCM - All Data - Limited Admin	Full R/W/D/A access to all default RCM objects. No admin rights except those associated with workflows, files, and folders.
RCM - All Permissions	Full R/W/D/A access to all default RCM objects. Full admin rights.
RCM - Subscriber	Read access to all default RCM objects. No admin rights except those associated with workflows, files and folders.
TPRM RapidRatings - All Permissions	Full R/W/D/A access to all default TPRM objects and RapidRatings Ratings objects. Full admin rights.
TPRM RapidRatings - All Data - Limited Admin	Full R/W/D/A access to all default TPRM objects and RapidRatings Ratings objects. No admin rights except those associated with workflows, files and folders.
VRM - All Data - Limited Admin	Full R/W/D/A access to all default TPRM objects. No admin rights except those associated with workflows, files and folders.
VRM - All Permissions	Full R/W/D/A access to all default TPRM objects. Full admin rights.

Role template permissions

Each role template defines access permissions that are enabled for each object type.

For each solution, a role template called All Permissions is provided. It includes full administrator rights. It also provides full read, write, delete, associate (RWDA) access to all object types that are included in the solution.

In addition, each solution includes a role template called All Data - Limited Admin. The template provides no administrator rights except for object types that are associated with files and folders. The templates provide full read, write, delete, associate (RWDA) access to all default object types enabled by default for the solution. For more information on access permissions that are granted to object types in role templates, see "Object type permissions assigned by role templates" on page 96.

Object type permissions assigned by role templates

A role template defines the read, write, delete, and associate access to object types enabled in each solution.

When permission rights are assigned to a role template, those rights are also assigned to the Modules Master template.

The following permissions describe the rights that are assigned to object types in role templates:

Table 35. Object type permissions

Permission	Name	Description
R	Read	Groups or users are granted the right to browse and view the details of objects.
W	Write	Groups or users are granted the right to create or modify objects within the selected folder. They cannot delete objects.
D	Delete	Groups or users are granted the right to delete objects within the folder structure.
A	Associate	Groups or users are granted the right to create associations between objects.

Chapter 10. GRC Calculations

Sample calculations are provided with OpenPages to get you started with the GRC Calculations feature.

Sample calculations

You can use the sample calculations as delivered or modify them to meet your requirements. They can also be used as templates and learning tools for your own calculations.

The sample calculations are enabled in fresh installations. Depending on the assessment method selected during the installation process, either the Quantitative Risk Rating and Quantitative Audit Risk Rating calculations or the Qualitative Risk Rating and Qualitative Audit Risk Rating calculations are enabled.

The following sample calculations are included in OpenPages:

- Loss Event

  Calculates the Net Loss, Recovery Amount, Gross Loss, and Estimated Gross Loss based on the underlying Loss Impact and Loss Recovery. If the sum of Actual Loss is 0, it uses the Estimated Gross loss.

- Qualitative Audit Risk Rating

  Automatically calculates the Qualitative Audit Inherent Risk Rating and Qualitative Audit Residual Risk Rating based on defined registry keys and preference objects.

- Qualitative Risk Rating

  Automatically calculates the Qualitative Inherent Risk Rating and Qualitative Residual Risk Rating based on defined registry keys and preference objects.

- Quantitative Audit Risk Rating

  Automatically calculates the Quantitative Audit Inherent Risk Rating and Quantitative Audit Residual Risk Rating based on defined registry keys and preference objects.

- Quantitative Risk Rating

  Automatically calculates the Quantitative Inherent Risk Rating and Quantitative Residual Risk Rating based on defined registry keys and preference objects.

- Resource CIA

  Calculates the resource criticality based on the high water mark for CIA.

- TPRM Supply Wisdom Trend

  Calculates the overall risk rating of a vendor, based on the quarterly scores from Supply Wisdom. Compares the current overall risk rating with the ratings from previous quarters to determine the trend.

KRI and KPI calculations

These KRI and KPI calculations are used by multiple solutions.

- KRIValue – Increasing, KRIValue – Decreasing

  These automatic calculations apply to KRI Values with a parent KRI in an Active status, with separate calculations applied depending on whether the parent KRI's Direction Information field is set as "Increase means greater risk" or "Decrease means greater risk." The calculation identifies the Yellow Threshold, Red Threshold, and Direction Information from the parent KRI and sets these fields on the KRI Value. The calculation sets the Breach Status on the KRI Value based on the Value field input on the KRI Value record compared against the Yellow and Red Thresholds.

- KRI Increase, KRI Decrease

These automatic calculations apply to KRIs in an Active status, with separate calculations applied depending on whether the Direction Information field is set to "Increase means greater risk" or "Decrease means greater risk." The calculation brings in the Value fields from KRI Values in a "Collected" Collection Status that are related to the KRI. The calculation sorts the values in descending order by Value Date and compares the two latest values. The calculation then sets the Indicator Trend field on the KRI by comparing the two values that are latest in time. It then sets the Value field on the KRI based on the Value from the KRI Value with the latest in time Value Date and uses this same input for determining Breach Status of the KRI by comparing the Value against the Yellow and Red Thresholds on the KRI.

- KRI Next Collection Date

This automatic calculation applies to KRIs in an Active status. The calculation sets the Next Collection Date by adding days to the KRI Next Collection Date based on the Frequency field on the KRI and the Expected Collection Date on the related KRI Values.

- KRI

This automatic calculation sets the latest Value Date from a KRI Value to the parent KRI. The calculation also sets the KRI Collection Status based on the Collection Status of the KRI Value with the most recent Value Date.

- KPI calculations

The following calculations are related to the KPI and KPI Value objects and are similar to the KRI and KRI Value calculations:

  – KPI
  – KPI – Decrease
  – KPI – Increase
  – KPI Next Collection Date
  – KPIValue – Decreasing
  – KPIValue – Increasing

IBM OpenPages Operational Risk Management (ORM) calculations

These calculations determine the next testing due date if a control test occurs on a scheduled basis and bring in the latest Test Result information to the parent Test Plan object.

- Test Plan

This automatic calculation sets the latest Performed Date from a Test Result to the parent Test Plan. The calculation also sets the Test Plan Status based on the child Test Result Status with the most recent Performed Date. The calculation sorts the Test Result values in descending order by Performed Date and compares the two latest Results. The calculation then sets the Trend field on the Test Plan by comparing the two Results that are latest in time.

- Testing Due Date

Description: This automatic calculation sets the Test Plan Due Date by adding days to the last Test Result Due Date based on the Frequency field on the Test Plan (daily, weekly, monthly, or annually) and the Expected Start Date of the Test Plan.

IBM OpenPages Business Continuity Management (BCM) calculations

Business impact analysis

- BIA Time-Based Impact

This automatic calculation does the following operations:

1. Establishes a weight for each impact assessment (Financial, Legal/Regulatory, Reputational, and Operational)

2. Converts the enum value to a numeric value (Devastating = 5; Severe = 4, Significant = 3, Moderate = 2; Minor = 1) for each time period assessed (at 24 hours, at 3 days, at 7 days, after 7 days)

3. Sets the Impact Score for each impact assessment by adding the converted enum values and multiplying by the weight provided

4. Sets an overall Impact Score by adding all impact assessment scores

5. Sets the Calculated MAO and Calculated Impact Tier based on the overall impact score.

- BIA Peak Period Quarter Scoring

This automatic calculation scores each enum selection (High = 3, Elevated = 2, Normal = 1) and sets the corresponding quarter to High, Medium, or Low based on the selection for the months within that quarter. If the combined score of the three months of the quarter is greater than or equal to 8, then High is selected; if the score is between 7 and 5, then Elevated is selected; and if 3 or 4, then Normal is selected.

- Business Continuity BIA Scoring

Determines Impact Score by using requirements, financial, and reputation impacts. Uses Impact Score to determine Impact Tier and Maximum Acceptable Outage.

This calculation is disabled by default. The BIA Time-Based Impact calculation replaces the Business Continuity BIA Scoring calculation.

- BIA – Breach Status

This automatic calculation takes into account the Breach Status of all child KPIs that are mapped to the Business Impact Analysis record. The calculation counts each such KPI Breach Status and sets the KPI Tolerance Breach Status field on the Business Impact Analysis object.

- If the calculation identifies at least one KPI Breach Status of Red, then the KPI Breach Status is set to Red.

- If the calculation identifies no related KPIs with a Breach Status of Red and at least one Yellow, the BIA's KPI Breach Status is set to Yellow.

- If the calculation identifies no related KPIs with a Breach Status of Red or Yellow and at least one KPI with a Breach Status of Green, the BIA's KPI Breach Status is set to Green.

- If a related KPI's Breach Status does not equal Red, Yellow, or Green, then the BIA KPI Breach Status field is set to "Not Applicable."

The Red and Yellow values for KPI Breach Status are displayed on the BCM Master Dashboard to identify BIAs that might require an update based on the performance that is measured by the mapped KPIs.

Pushing and comparing BIA metrics

- Process-BCM

This calculation is an automatic calculation that sets the Impact Tier, Impact Score, RTO, RPO, and MAO fields on the Process based on the most critical metrics established on a child BIA.

The calculation uses the fields that are set as part of the last stage of the Initial Business Impact Assessment and Recurring BIA Review workflows to ensure that only fields that are fully approved within the BIA are used to set fields on a related Process.

This calculation sets the Impact Tolerance Duration field from a parent Business Service that is classified as an Important Business Service onto the Process.

This calculation also sets the RTO Alignment Warning and RPO Alignment Warning field value to "Warning" on the Process object, if certain conditions are met. The RTO Alignment Warning field value of "Warning" is set when a fully approved Impact Tolerance (from a related Business Service) is less than the Recovery Time Objective or Recovery Time or when Recovery Time exceeds the Recovery Time Objective. The RPO Alignment Warning field value of "Warning" is set when the Recovery Point Objective is less than Recovery Point.

- Resource-BCM

  This automatic calculation sets and compares fields that derive from a parent Process. The calculation sets the Impact Tier, Impact Score, Process Recovery Time Objective, Process Recovery Point Objective, and MAO fields from the Process with the most critical metrics on the Asset (Resource) object. This calculation sets the RTO Alignment Warning and RPO Alignment Warning field values to "Warning" on the Asset object, if certain conditions are met. The RTO Alignment Warning field value of "Warning" is set when the Process Recovery Time Objective is less than the Resource Recovery Time Objective or Recovery Time or when Recovery Time exceeds Resource Recovery Time Objective. The RPO Alignment Warning field value of "Warning" is set when the Process Recovery Point Objective is less than the Resource Recovery Point Objective or Recovery Point or when Recovery Point exceeds Resource Recovery Point Objective.

- Vendor-BCM

  This automatic calculation sets and compares fields that derive from a parent Process. The calculation sets the Impact Tier, Impact Score, Process Recovery Time Objective, Process Recovery Point Objective, and MAO fields from the Process with the most critical metrics on the Vendor object. This calculation sets the RTO Alignment Warning and RPO Alignment Warning field values to "Warning" on the Vendor object, if certain conditions are met. The RTO Alignment Warning field value of"Warning" is set when the Process Recovery Time Objective is less than the Vendor Recovery Time Objective or Recovery Time or when Recovery Time exceeds Vendor Recovery Time Objective. The RPO Alignment Warning field value of "Warning" is set when the Process Recovery Point Objective is less than the Vendor Recovery Point Objective or Recovery Point or when Recovery Point exceeds Vendor Recovery Point Objective.

Operational resiliency

- KRI - Impact Tolerance Metric

  This automatic calculation sets the value of Impact Tolerance Metric to "Yes" for any KRI that has a parent Business Service that is classified as an Important Business Service.

- Process – Impact Tolerance Breach Status

  This automatic calculation takes into account the Breach Status of all KRIs related to the Process where Impact Tolerance Metric = "Yes." The calculation counts each such KRI Breach Status and sets the Impact Tolerance Breach Status field on the Process. If the calculation identifies at least one KRI Breach Status of Red, then the Process Impact Tolerance Breach status is set to Red. If the calculation identifies no related KRIs with a Breach Status of Red and at least one Yellow, the Process Impact Tolerance Breach Status is set to Yellow. If the calculation identifies no related KRIs with a Breach Status of Red or Yellow and at least one with a Breach Status of Green, the Process Impact Tolerance Breach Status is set to Green. If a related KRI's Breach Status does not equal Red, Yellow, or Green, or the KRI does not have a value of Impact Tolerance Metric = "Yes", then the field is set to "Not Applicable."

  The Red and Yellow values for Impact Tolerance Breach Status are used within public filters to identify potential dependencies of Business Services that might be in breach within association views on SysView-Task-BusService-5 and on the BCM Master Dashboard.

- Location – Impact Tol Breach Status

  This automatic calculation takes into account the Breach Status of all KRIs related to the Location where Impact Tolerance Metric = "Yes." The calculation counts each such KRI Breach Status and sets the Impact Tolerance Breach Status field on the Location. If the calculation identifies at least one KRI Breach Status of Red, then the Location Impact Tolerance Breach status is set to Red. If the calculation identifies no related KRIs with a Breach Status of Red and at least one Yellow, the Location Impact Tolerance Breach Status is set to Yellow. If the calculation identifies no related KRIs with a Breach Status of Red or Yellow and at least one KRI Breach Status of Green, the Location Impact Tolerance Breach Status is set to Green. If a related KRI's Breach Status does not equal Red, Yellow, or Green, or the KRI does not have a value of Impact Tolerance Metric = Yes, then the field is set to "Not Applicable."

The Red and Yellow values for Impact Tolerance Breach Status are used within public filters to identify potential dependencies of Business Services that might be in breach within association views on `SysView-Task-BusService-5` and on the BCM Master Dashboard.

- Resource – Impact Tol Breach Status

This automatic calculation takes into account the Breach Status of all KRIs related to the Asset where Impact Tolerance Metric = "Yes". The calculation counts each such KRI Breach Status and sets the Impact Tolerance Breach Status field on the Asset. If the calculation identifies at least one KRI Breach Status of Red, then the Resource Impact Tolerance Breach status is set to Red. If the calculation identifies no related KRIs with a Breach Status of Red and at least one Yellow, the Resource Impact Tolerance Breach Status is set to Yellow. If the calculation identifies no related KRIs with a Breach Status of Red or Yellow and at least one KRI with a Breach Status of Green, the Resource Impact Tolerance Breach Status is set to Green. If a related KRI's Breach Status does not equal Red, Yellow, or Green, or the KRI does not have a value of Impact Tolerance Metric = "Yes", then the field is set to "Not Applicable."

The Red and Yellow values for Impact Tolerance Breach Status are used within public filters to identify potential dependencies of Business Services that might be in breach within association views on SysView-Task-BusService-5 and on the BCM Master Dashboard.

- Vendor – Impact Tol Breach Status

This automatic calculation takes into account the Breach Status of all KRIs related to the Vendor where Impact Tolerance Metric = "Yes". The calculation counts each such KRI Breach Status and sets the Impact Tolerance Breach Status field on the Vendor. If the calculation identifies at least one KRI Breach Status of Red, then the Vendor Impact Tolerance Breach status is set to Red. If the calculation identifies no related KRIs with a Breach Status of Red and at least one Yellow, the Vendor Impact Tolerance Breach Status is set to Yellow. If the calculation identifies no related KRIs with a Breach Status of Red or Yellow and at least one KRI with a Breach Status of Green, the Vendor Impact Tolerance Breach Status is set to Green. If a related KRI's Breach Status does not equal Red, Yellow, or Green, or the KRI does not have a value of Impact Tolerance Metric = "Yes", then the field is set to "Not Applicable."

The Red and Yellow values for Impact Tolerance Breach Status are used within public filters to identify potential dependencies of Business Services that might be in breach within association views on SysView-Task-BusService-5 and the BCM Master Dashboard.

- Business Service - Breach Status

This automatic calculation takes into account the Breach Status of all KRIs related to the Business Service. The calculation counts each such KRI Breach Status and sets the Impact Tolerance Breach Status field on the Business Service. If the calculation identifies at least one KRI Breach Status of Red, then the Business Service Impact Tolerance Breach status is set to Red. If the calculation identifies no related KRIs with a Breach Status of Red and at least one Yellow, the Business Service Impact Tolerance Breach Status is set to Yellow. If the calculation identifies no related KRIs with a Breach Status of Red or Yellow and at least one KRI with a Breach Status of Green, the Business Service Impact Tolerance Breach Status is set to Green. If a related KRI's Breach Status does not equal Red, Yellow, or Green, then the field is set to "Not Applicable."

The Red and Yellow values for Impact Tolerance Breach Status are used within an Enumeration rule for `SysView-Task-BusService-5` to display a task view for a Business Service with an impact tolerance that is close to or in breach. The values are also used on the BCM Master Dashboard.

IBM OpenPages Financial Controls Management calculations

Account Scoping – Assets
When the Classification field of the Account object = Assets, this calculation:

- Calculates and sets the Annualized Value Percentage field of the Account record based on the sum of all Account object records with the same classification value and parent Business Entity.
- Sets the Account In Scope field based on a threshold percentage.

Account Scoping – Equity
When the Classification field of the Account object = Equity, this calculation:

- Calculates and sets the Annualized Value Percentage field of the Account record based on the sum of all Account object records with the same classification value and parent Business Entity.
- Sets the Account In Scope field based on a threshold percentage.

Account Scoping – Expenses
When the Classification field of the Account object = Expenses, this calculation:

- Calculates and sets the Annualized Value Percentage field of the Account record based on the sum of all Account object records with the same classification value and parent Business Entity.
- Sets the Account In Scope field based on a threshold percentage.

Account Scoping – Liabilities
When the Classification field of the Account object = Liabilities, this calculation:

- Calculates and sets the Annualized Value Percentage field of the Account record based on the sum of all Account object records with the same classification value and parent Business Entity.
- Sets the Account In Scope field based on a threshold percentage.

Account Scoping – Revenue
When the Classification field of the Account object = Liabilities, this calculation:

- Calculates and sets the Annualized Value Percentage field of the Account record based on the sum of all Account object records with the same classification value and parent Business Entity.
- Sets the Account In Scope field based on a threshold percentage.

Account Scoping – Unknown
When the Classification field of the Account object = Unknown, this calculation:

- Calculates and sets the Annualized Value Percentage field of the Account record based on the sum of all Account object records with the same classification value and parent Business Entity.
- Sets the Account In Scope field based on a threshold percentage.

BE – Account Classification Totals
Calculates fields on the Business Entity object:

- Calculates and sets the totals of the related Account object Classification field values for each of the following: Asset, Liability, Equity, Revenue, Expenses, and Unknown.
- Calculates a combined total of all Account object Classification field values.

Control Eval Certification
Supports the sub-certification process in IBM OpenPages Financial Controls Management.

Process Eval Certification
Supports the sub-certification process in IBM OpenPages Financial Controls Management.

IBM OpenPages Internal Audit Management calculations

Summary Audit Plan Budget and Plans
Calculates the following fields for the Summary Audit Plan object view: Under Over Hours, Assigned Audit Hours, Completed Hours, and Remaining Hours. The values from these fields are totaled from the related Auditable Entity and Audit objects.

IBM OpenPages IT Governance calculations

Asset - Vulnerability Rating
This calculation sets the Vulnerability Assessment Rating on the Asset based on the highest rated open Vulnerability related to the Asset.

System - Vulnerability Rating

> This calculation sets the Vulnerability Assessment Rating on the System based on the highest rated open Vulnerability related to the System or a related Asset.

Vulnerability - Threat Assessment

> This calculation sets the Overall Likelihood and Risk Rating fields based on inputs provided for threat assessment fields. The scoring is based on NIST SP 800-30 Rev. 1.

IBM OpenPages Model Risk Governance (MRG) calculations

- Metric Next Collection Date

Automatically sets Next Collection Date for active Metrics, based on the frequency of the Metric.

Note: This calculation is not applicable to IBM Watson OpenScale metrics.

- Metric Value - Update from Parent Metric

Sets the Threshold and Direction information from the parent Metric, and calculates the Breach Status of a Metric Value.

Note: This calculation is not applicable to IBM Watson OpenScale metrics.

- Metric Value - Update

Automatically updates active Metrics with data from the most recent child Metric Value. Also updates the Metric indicator trend if there is more than one collected Metric Value.

- Model Risk Scorecard

Calculates a tier for a model that can be used to assess the level of model risk. Typically, an organization will tier a model through the assessment of a number of factors. IBM OpenPages Model Risk Governance uses the following four factors: Complexity, Materiality, Operational, and Regulatory. The outcome is that each Model is assigned to Tier 1, Tier 2, or Tier 3. This calculation replaces a trigger that did the same model tiering in previous versions.

Note: This calculation is not applicable to IBM Watson OpenScale models.

IBM OpenPages Policy Management (PCM) calculations

- Policy Review Comment

Populates the Policy Review Comment (PRC) object description with the Policy Name. This information provides context to users when they view the PRC object in a list or grid view.

This calculation is optional. You can disable it, if needed.

IBM OpenPages Regulatory Compliance Management (RCM) calculations

These calculations aggregate the data from the Requirement Evaluations to Compliance Theme and Compliance Theme to Compliance Plan. These calculated metrics can help users to perform assessments.

The outputs from these calculations are stored within the corresponding Requirement Eval Value, Compliance Theme Value, and Compliance Plan Eval records for trending analysis purposes.

- Compliance Theme – Requirement Eval

This automatic calculation captures and sets fields on the Requirement Evaluation object from child Controls. The calculation counts all Controls that are mapped to the Requirement Evaluation, Controls with an Effective selection for Design Effectiveness, and Controls with an Effective selection for Operating Effectiveness. The calculation then sets the Control Count, DE Effective Count, and OE Effective Count fields on the Requirement Evaluation. The calculation also divides the count of Controls rated as Effective for Design and Operating Effectiveness from the Count of all controls and sets the Percent DE Effective and Percent OE Effective fields on the Requirement Evaluation.

- Compliance Theme – Business Entity

The calculation is applicable to Compliance Themes that are within the Business Entity hierarchy. The calculation is a roll-up of Requirement Evaluations to set the number and percent of Requirement Evaluations that were rated as Over-Target and On-Target for Design Effectiveness and Operating Effectiveness. The calculation also sets the average score for Design Effectiveness, Operating Effectiveness, and an Overall Rating for all related Requirement Evaluations that were rated as something other than "6 - Not Applicable." The average score is determined by scoring and adding each enum value from all associated Requirement Evaluations (1 – Over Target = 1; 2 – On-Target = 2; 3 – Under Target = 3; 4 – Significantly Under Target = 4; and 5 – No Relevant Control = 5) and dividing this total score by the number of Requirement Evaluations with one of the five enum values listed. A lower score indicates a higher level of compliance.

- Compliance Theme – Library

The calculation is applicable to Compliance Themes that are within the Library hierarchy. The calculation is a roll-up of Requirement Evaluations to set the number and percent of Requirement Evaluations that were rated as Over-Target and On-Target for Design Effectiveness, and Operating Effectiveness. The calculation also sets the average score for Design Effectiveness, Operating Effectiveness, and an Overall Rating for all related Requirement Evaluations that were rated as something other than "6 - Not Applicable." The average score is determined by scoring and adding each enum value from all associated Requirement Evaluations (1 – Over Target = 1; 2 – On-Target = 2; 3 – Under Target = 3; 4 – Significantly Under Target = 4; and 5 – No Relevant Control = 5) and dividing this total score by the number of Requirement Evaluations with one of the five enum values listed. A lower score indicates a higher level of compliance.

Additionally, this calculation counts the number of Requirements within the Compliance Theme under assessment and sets the Requirement Count field.

- Compliance Plan

Similar to the calculation for Compliance Themes, the Compliance Plan calculation aggregates scores provided on child Compliance Themes. The calculation is a roll-up of Compliance Themes to set the number and percent of Compliance Themes that were rated as Over-Target and On-Target for Design Effectiveness and Operating Effectiveness. The calculation also sets the average score for Design Effectiveness, Operating Effectiveness, and an Overall Rating for all related Compliance Themes that were rated as something other than "6 - Not Applicable." The average score is determined by scoring and adding each enum value from all associated Compliance Themes (1 – Over Target = 1; 2 – On-Target = 2; 3 – Under Target = 3; 4 – Significantly Under Target = 4; and 5 – No Relevant Control = 5) and dividing this total score by the number of Compliance Themes with one of the five enum values listed. A lower score indicates a higher level of compliance. The calculation also counts the number of Compliance Themes that are included in the Compliance Plan.

IBM OpenPages Risk Management for ESG calculations

Objective Priority Score

Calculates an Objective Priority Score.

Gets the values from the `Importance to Firm` and `Importance to Stakeholders` fields. The values are: Very Low = "1" , Low = "2", Medium = "3", High = "4", Very High = "5". The two values are then added together to get the Objective Priority Score, which can range from 2-10.

Objective Progress

Calculates the difference between the Objective Progress and the Objective Target. The calculation then sets the Progress Status field to **Under Achieving**, **Over Achieving**, or **On Target**.

Chapter 11. GRC Workflow

Sample workflows are provided with OpenPages to get you started with the GRC Workflow feature.

Sample workflows

You can use the sample workflows as delivered or modify them to meet your requirements. They can also be used as templates and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

Action Item Approval workflow

When an action item is created, the Action Item Approval workflow starts automatically. An email is sent to the Action Item Assignee informing them that an action item is assigned to them. The due date for the task is set to 7 days prior to the action item's Due Date. When an action item is complete, the assignee selects **Actions** > **Submit for Approval**. The workflow then does the following actions:

- Copies the value in the Issue Owner field of the parent issue to the action item's Issue Owner for Approval field.
- Sets the action item's Status field to Awaiting Approval.
- Sends an email to the Issue Owner informing them that an action item is waiting for their approval.

The Issue Owner reviews the action item, and then approves or rejects the closure of the Issue. The due date for the task is set to the action item's Due Date.

If the Issue Owner selects **Actions** > **Approve**, the workflow completes the following actions:

- Sets the Status field to Closed.
- Sets the Approve Reject field to Approve.
- Sets the Actual Completion Date to today's date.

If the Issue Owner selects **Actions** > **Reject**, the task is re-assigned to the Action Assignee. The workflow completes the following actions:

- Sets the Status field to Open.
- Sets the Approve Reject field to Reject.
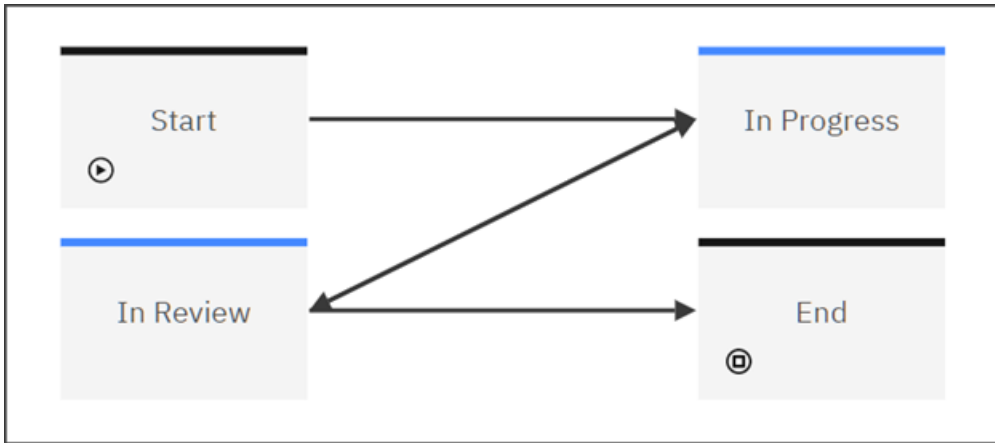
Figure 2. The Action Item example workflow

Finding workflow

The Finding workflow uses the Finding System Task view and depends upon the out-of-the-box schema for Finding and related object types.

In this workflow, note the following key elements:

- The cancellation path

   If a stage is declined, the workflow returns to the Finding Preparation stage. In your own workflow, you might choose this route or choose to go back to the immediately preceding stages. Plan the paths through the workflow in both a forward and backward direction.

- Task overrides

   The task overrides for each stage define the Key Fields that are listed. The user guidance text is from the Task View itself. With this method, the Key Fields change with each stage and are specific to a stage.

Figure 3. Finding workflow

Figure 4 — Finding Workflow: Sys-Workflow-Finding

Start – Create Workflow
Type: Auto Start
Oversight: Audit: Audit Owner
Due Date: None

Rejected
Status: Inadequate Management Response
Set Fields:
Clear - Prep Complete Date
Clear – Review Complete Date

Rejected
Status: Management Declined
Set Fields: Clear Prep Complete Date and Clear Review Complete Date, Set Mgmt Response Status= Response Provided
Condition: Mgmt response = Disagree, OR Require clarification

Rejected
Status: Rejected at Audit Review
Set Fields: Clear - Prep Complete Date
Condition: Reviewer = End user

Finding Preparation
Due Date: None
Assignee: Preparer
Subscriber: Reviewer
Task View Overrides
Key Fields
Impact, Preparer, Priority, Recommendation, Reviewer

Send for Audit Review
Email: Assignee
Condition: Preparer = end user
Validations (4):
Not Empty:
Reviewer, Recommendation, Priority, Impact
Operations (1)
Set Fields: Prep Complete Date to TODAY, Clear Mgmt Resp Stat

Review by Audit
Assignee: Reviewer
Due Date: 7 days
Task View Overrides
Key Fields
Review Comments, Reportable, Mgmt Owner

Send for Management Response
Email: Mgmt Owner
Validations: Reviewer = end user
Not Empty:
Mgmt Owner, Review Comments, Reportable
Operations Set Fields:
Review Complete Date to TODAY
Mgmt Response Status = Waiting for response

Management Response
Assignee: Mgmt Owner
Due Date: 7 days
Task View Overrides:
Key Fields
Mgmt Scheduled Completion Date, Mgmt Response, Mgmt Response Comment

Send Mgmt Response to Audit
Set Fields
Mgmt Response Status= Response Provided
Condition: Mgmt response = Agree, will create Action Plan, OR Agree, Action Plan not needed

Review Management Response
Assignee: Preparer
Due Date: 5 days

Ready to Close
Set Fields
Status = Closed

Prepared for Ready to Close

Figure 4. The specification for the Finding workflow

Incident workflow

The Incident workflow moves an incident through an investigation and approval process.

When an incident is created, the Incident workflow starts automatically. The workflow sets an owner for each stage (primary owner, approver, and reviewer). It sets the due date based on discovery date and incident criticality.

Figure 5 — Incident workflow

Start → In Progress ↔ Review ↔ Approval → Closed

Figure 5. Incident workflow

Issue review workflow

In an Issue Management and Remediation (IMR) framework, you can effectively document, monitor, remediate, and audit issues.

Issues are items that are identified against the documented framework and are deemed to negatively affect the ability to accurately manage and report risk. In its lifecycle, an issue can have one of two states: Open or Closed.

When an issue is created, the Issue Review workflow starts automatically. The workflow sets the Status of the issue to Open and the Original Due Date to the due date that was entered when the issue was created.

An email is sent to the Issue Owner, informing them that an issue is assigned to them. The due date for the task is set to 15 days prior to the issue's Due Date.

To resolve the issue, the Issue Owner establishes and records the appropriate actions.
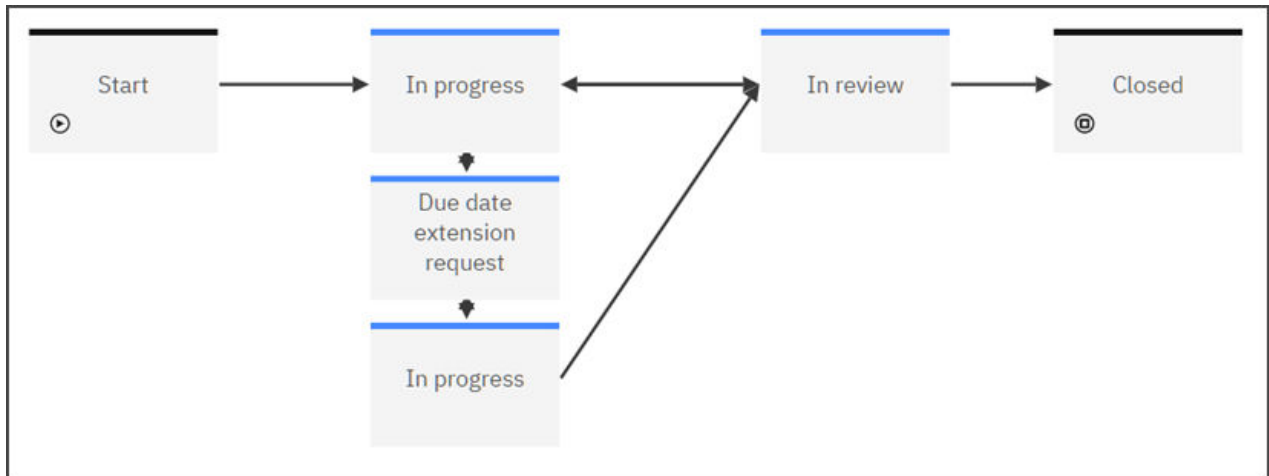
Figure 6. Issue Review workflow

The Issue Owner can request a due date extension at any time during the issue lifecycle by setting the Requested Due Date and selecting **Actions** > **Request due date change**. The Issue Approver is notified of this request via email. The approver can approve or reject the request. If approved, the issue's Due Date is set to the requested due date.

The Issue Owner can submit the issue for review by selecting **Actions** > **Submit for review**. The workflow performs the following validations:

- All action items under the issue are closed.
- The Issue Conclusion field is populated.
- The Issue Type field is populated.

If any of the validations fails, the workflow prevents the Issue Owner from submitting the issue for review. If all the validations pass, the Issue Approver is notified of the request via email. This task due date is set to the issue's Due Date. If rejected, the Issue Owner is notified of the rejection via email. The Issue Owner can make updates and then re-submit the issue for review. If the issue is approved, the issue's Status is set to Closed.

The issue can be re-opened by starting the Issue Review workflow.

KRI and KPI workflows

KRI Value Creation

This workflow creates KRI Value records and initiates workflows on the KRI Value for collection.

This workflow is set to a schedule that runs on a daily basis on KRI records. In instances when the KRI Status is "Active" and the Next Collection Date (see the KRI Next Collection Date calculation) is equal to the day the schedule is run and the KRI Value Date is not equal to the day the schedule is run, a KRI Value record is created.

In addition to creating the KRI Value record, the record is populated with values from the parent KRI, including Expected Collection Date, KRI Capturer, KRI Owner, Collection Status, Red Threshold, Yellow Threshold, and Value Date.

The KRI Value that is created by this workflow then enters the KRI Value Entry workflow.
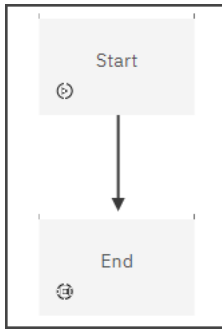
Figure 7. KRI Value Creation workflow

KRI Value Entry
This workflow assigns KRI Values to users and provides a process for KRI Value approval.

This workflow auto-starts when a KRI Value record is created and is in a Status of "Awaiting Collection." When it's created, the KRI Value is populated with data from its parent KRI, including KRI Capturer, KRI Owner, KRI Value Red and Yellow Thresholds, Description, and whether approval is required. After you enter a value, you might need to click another tab and then return to the view to see the latest KRI or KPI values.
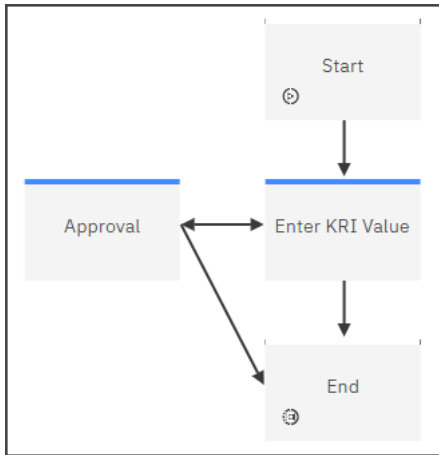
Figure 8. KRI Value Entry workflow

KPI Value Creation workflow and KPI Value Entry workflow
These workflows are similar to the KRI Value Creation and KRI Value Entry workflows

Risk and control self assessment (RCSA)

Risk & Control Self Assessment (RCSA)
This workflow can be used to establish, execute, and progress through a qualitative risk assessment. Steps include: a risk owner manually kicks off the Risk & Control Self Assessment (RCSA) workflow, performs an inherent risk assessment by identifying the inherent impact and likelihood, performs a residual risk assessment by evaluating the residual impact and likelihood, and submits the RCSA for completion.

Control Assessment
A control assessment needs to be performed before the RCSA workflow can be complete. This workflow can be used to progress through your control assessment. Steps include: a control owner manually kicks off the Control Assessment workflow, performs the control assessment by evaluating the control design and operating effectiveness, and submits for approval. The Control/Risk owner or RCSA coordinator can reject the control and send back for review, or approve and close, marking the control in "Approved" status.

Control testing workflows

The following workflows related to the Test Plan and Test Result objects are included:

- Create Test Result
- Perform Control Test
- Update & Review Test Plan

The Create Test Result workflow automatically creates a Test Result based on the schedule or frequency that is defined in the parent Test Plan. When the next due date comes for an active Test Plan, this workflow automatically creates a new Test Result, and populates it with test performer and test due date information from the parent Test Plan. With the Perform Control Test workflow, the test goes through its performance, review, documentation request (if required), and an issue is even automatically created if the test result has failed.

Loss Event Review workflow

The Loss Event Review workflow is similar to the configurable lifecycle for Loss Events.

In this workflow, take note of the following elements:

- Different paths based on an amount value

  The workflow provides different levels of approval (approval level 1 and approval level 2) based on the gross loss value of the loss event.
- Use of preference objects

  Approval level 1 and approval level 2 are retrieved from the Preference object. There are different approvers based on the division where the loss event occurred. Study this example if you want to learn more about how to implement a Preference object in workflows.
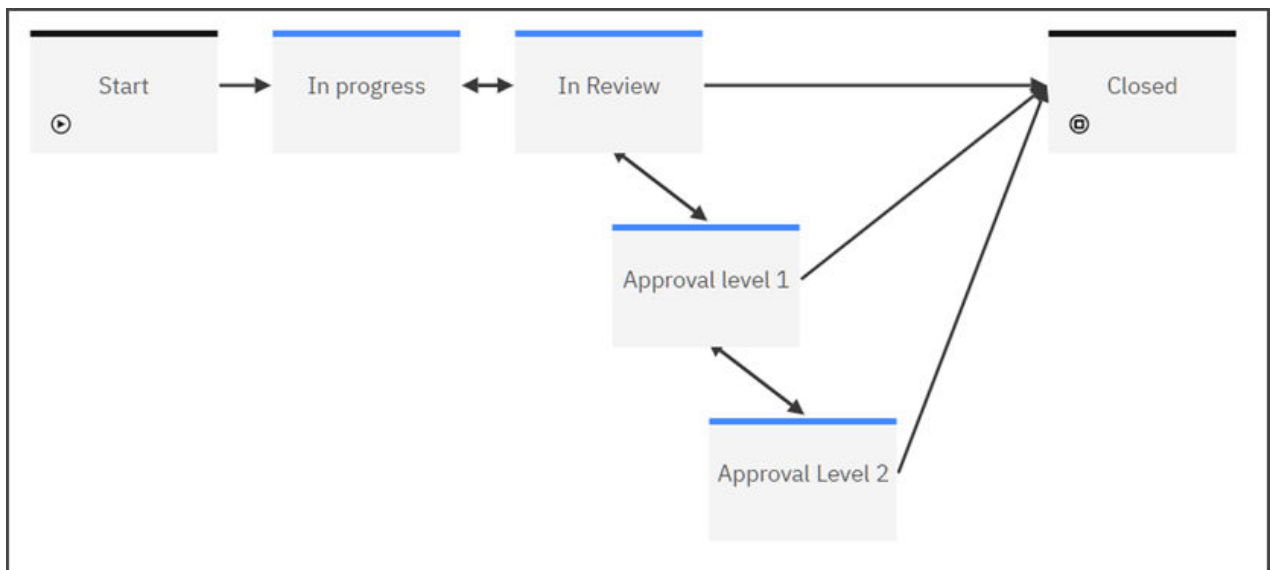
Figure 9. Loss Event Review workflow

Questionnaire Assessment workflow

The Questionnaire Assessment workflow moves a questionnaire assessment through the information gathering, review, and approval stages.
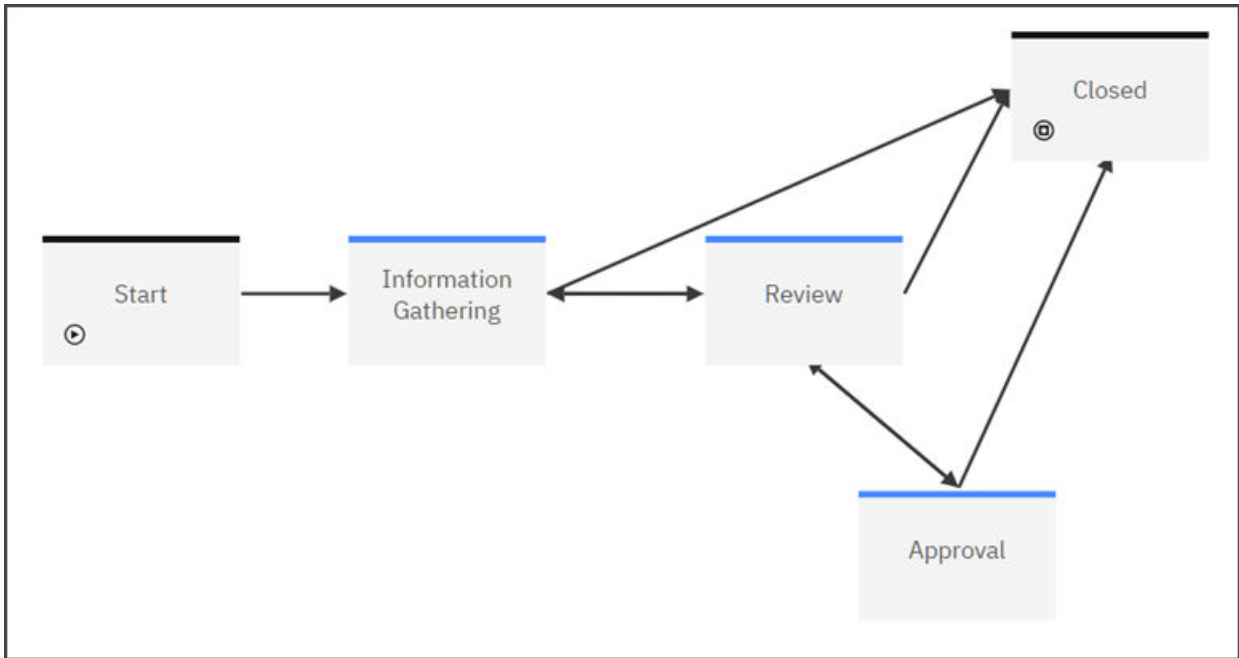
Workpaper workflow

The Workpaper workflow uses the Workpaper System Task view and depends upon the out-of-the-box schema for Workpaper and related object types.

There are multiple types of Workpapers, for example Notification Letters and Test Evidence. However, the sample workflow is high level and not defined for one specific type. In the Workpaper workflow you create, you will likely define it for a specific type of Workpaper, in which case, you can choose to have separate workflows for each type or one workflow with separate branches with conditions that specify the type.

In this workflow, take note of the following elements:

• Who can view the **Actions** button

The final two forward actions, Send for Review and Approve and Complete, are restricted to specific users, the preparer and the reviewer, respectively. These actions are displayed only to them. For all other users, there is no action on the **Actions** button. When you encounter a situation like this, you can add an explanation to the user guidance for the stage that explains why there is no option on the **Actions** button.

Figure 10. Workpaper workflow
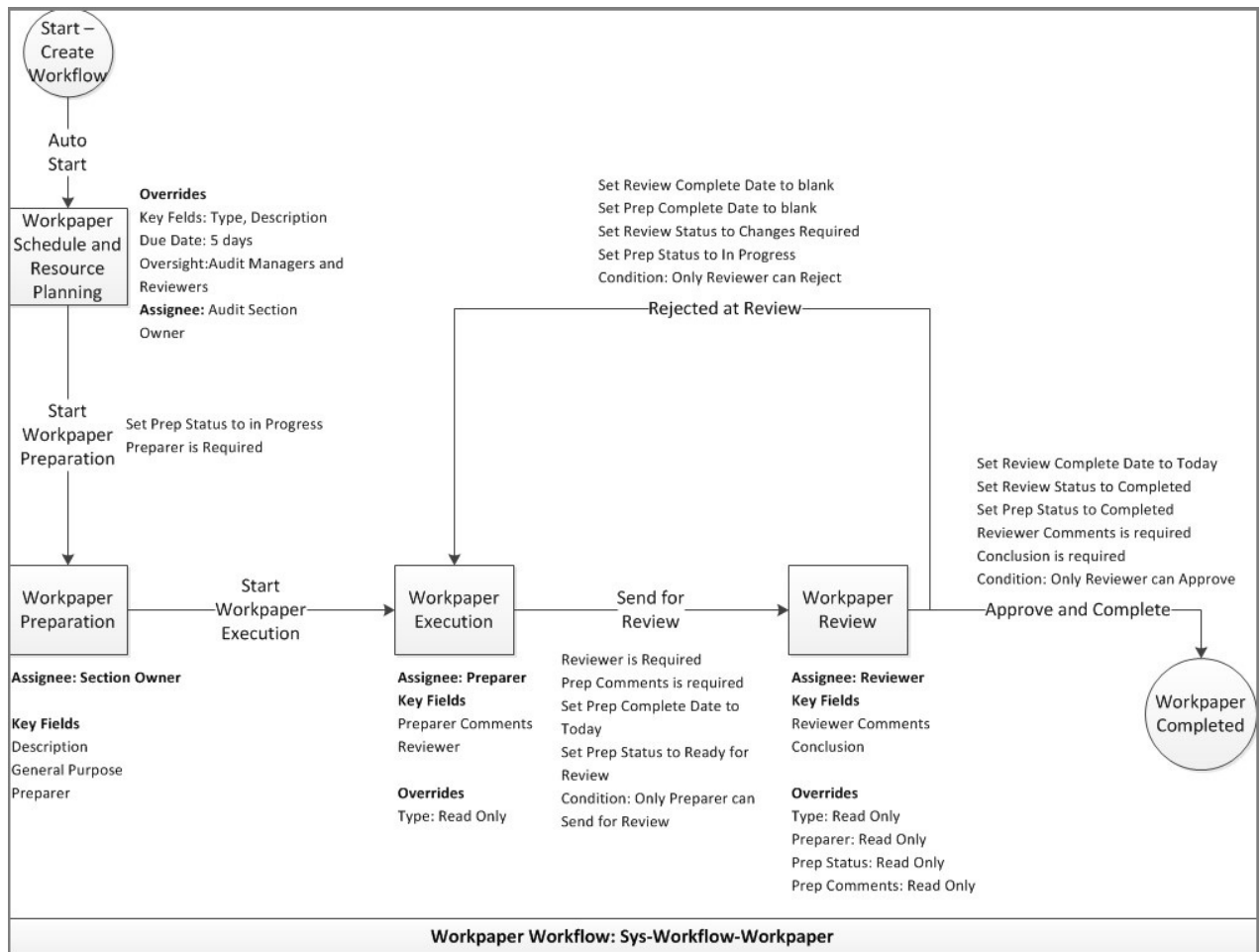
Figure 11. The specification for the Workpaper workflow

IBM OpenPages Business Continuity Management (BCM) workflows

IBM OpenPages Business Continuity Management includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as templates and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

Business Continuity Plan Review and Approval Process
> This workflow guides users through the creation of a Business Continuity Plan, continual review of the BC Plan on an annual basis, and automation for versioning of a BC Plan to ensure that a Published version of the BC Plan is always available after creation.
>
> For a new BC Plan, the workflow guides the process through the in progress, in review and approval stages. The author, reviewer, and approver are required fields to advance the workflow. Upon completion of the process, the workflow sets the next review date to 365 days and the status to published.
>
> For a published BC Plan, the user has two options:
>
> • Renew the current BC Plan without making changes to the published version
>
> > If this option is selected, a comment is required by the reviewer and the workflow sets the next review date to 365 days. The workflow advances the process to require only an approval.
>
> • Revise the published BC Plan

If this option is selected, the workflow "locks" the current BC Plan, makes a copy of the plan, and sets the status of the copied plan to draft.

The copied draft version of the plan moves through the review and approval process of the workflow. Upon completion, the workflow sets the plan status to "published", increments the version number, and sets the next review date to 365 days. The status of the previously published plan is set to archived.

Note: The following child associations that were present on the previous ("locked") BC Plan also appear on the new version of the BC Plan: BCTest Plan, Teams, and Business Impact Analysis (BIA). All parent associations, with the exception of BC Events, are preserved for the new BC Plan.
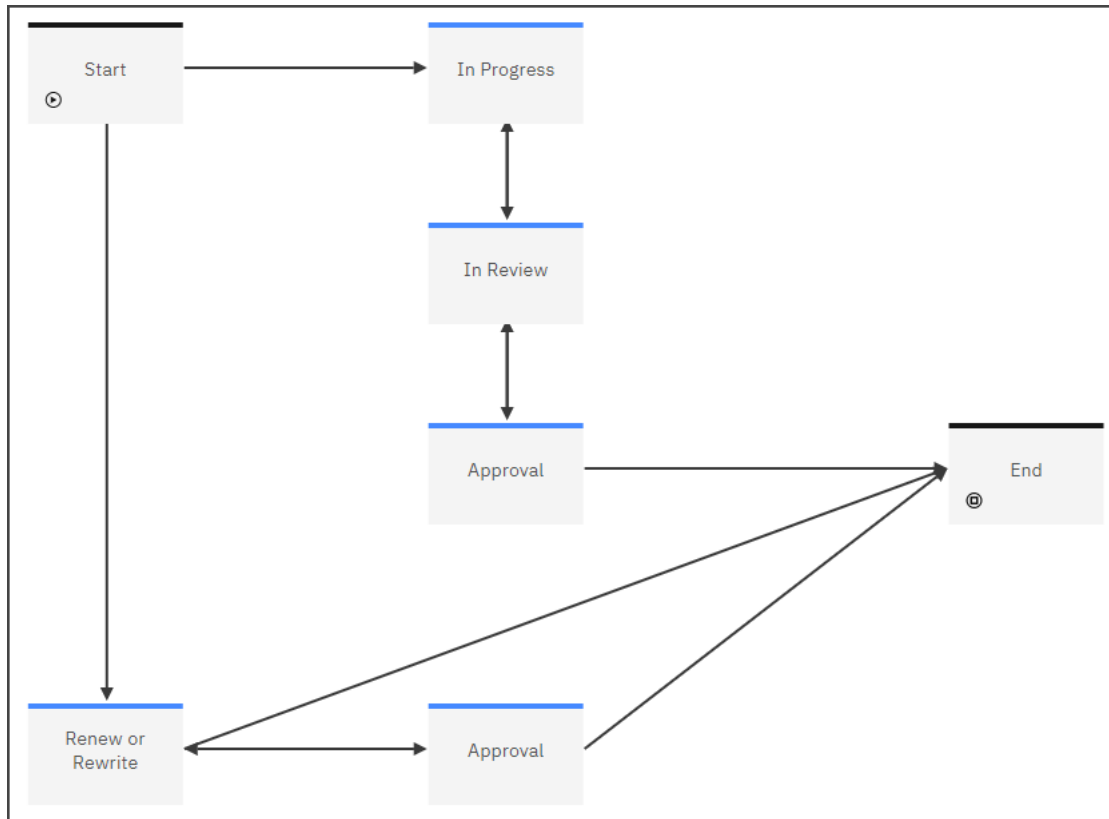
Figure 12. Business Continuity Plan Review and Approval Process workflow

Initial Business Impact Assessment

This workflow assists users through the creation of the Business Impact Assessment.

This workflow starts when a new Business Impact Analysis (BIAs) is created.
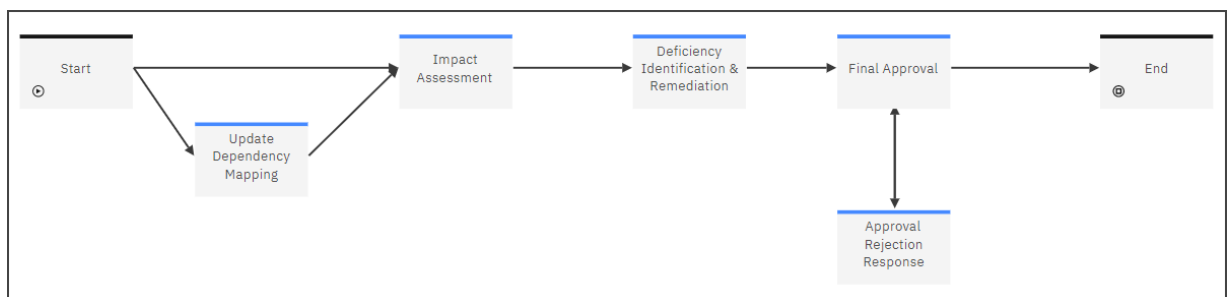
Figure 13. Initial Business Impact Assessment workflow

Recurring BIA Review

This workflow ensures that BIAs are reviewed at least on an annual basis by scheduling a recurring BIA review or permitting an ad hoc review by the owner.

This manual workflow can be started by the Owner of the BIA or when the Next Scheduled Review Date exceeds the date the weekly schedule is run.

Figure 14. Recurring BIA Review workflow

BC Test Plan Creation

This workflow provides users with a process for creating business continuity test plans.

This auto-start workflow starts when a BC Test Plan record is created.
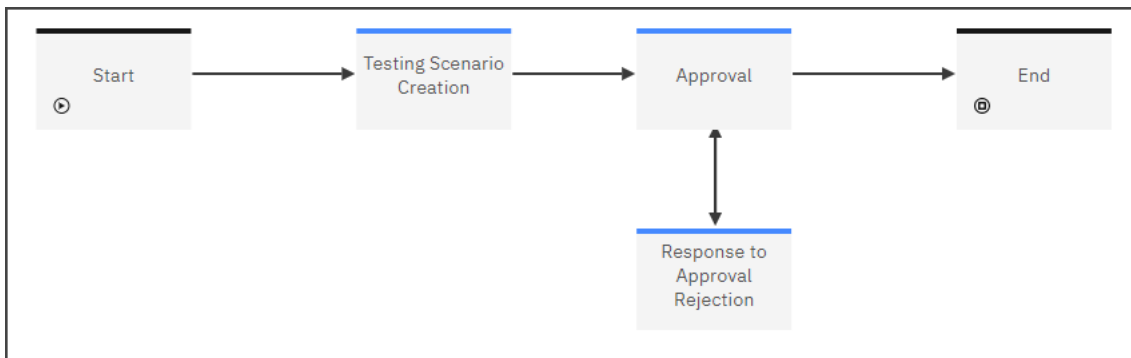
Figure 15. BC Test Plan Creation

BC Test Plan Execution

This workflow provides users with a process for executing a BC Test Plan and for recording observations from the testing of the BC Test Plan.

This manual workflow can be started manually by the Owner or it can be started automatically based on a schedule
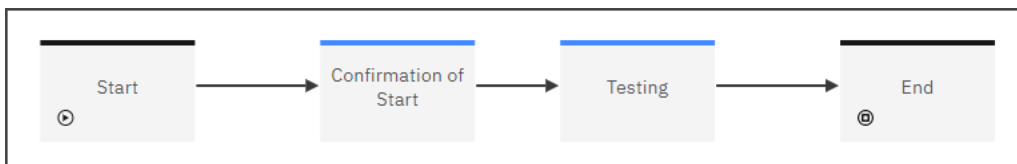
Figure 16. BC Test Plan Execution

BC Test Result Documentation

This workflow provides users with a process for documenting results for executed BC Test Plans and for remediating issues identified during testing.
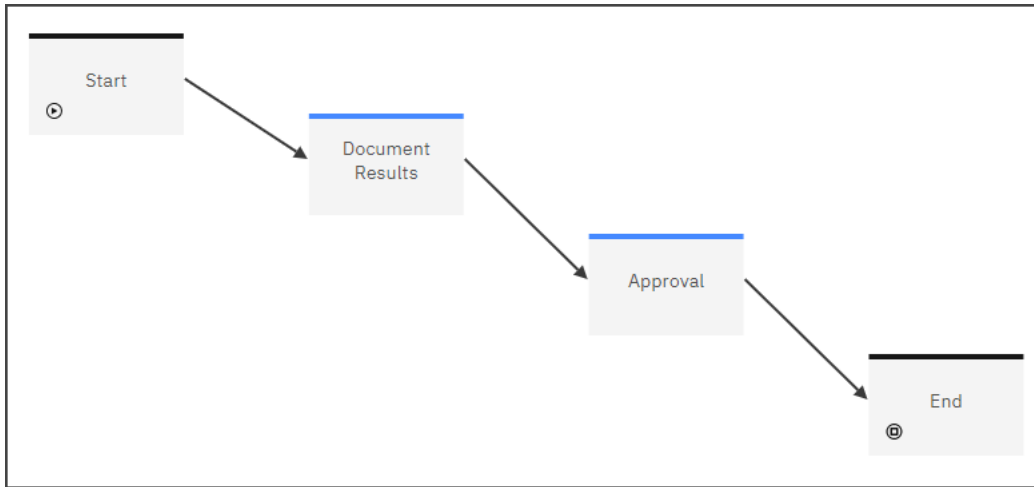
Figure 17. BC Test Result Documentation workflow

Dependency Review Workflow

Operational resilience requirements mandate that dependency mappings of Important Business Services are updated at least on an annual basis. This workflow reminds Process Owners of the need to update Process dependencies on the Process object.

This manual start workflow can be started by the Process Owner when the Process is mapped to an Important Business Service, or when the Dependency Mapping Review Date is empty or more than 365 days from the date of the execution of the schedule.
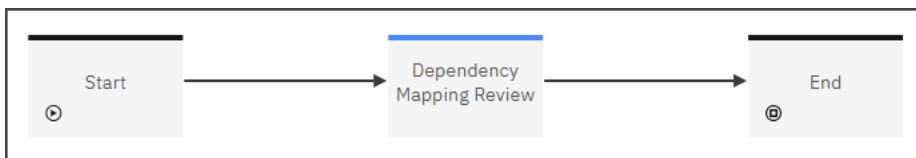
Figure 18. Dependency Review workflow

Business Service Initial Assessment

This workflow provides users with a way to catalog all business services and document the decision-making process for classifying business services as Important Business Services. For Important Business Services, users map the business service to related Processes and Locations, map to new or existing metrics related to measuring disruption to and performance of the Important Business Service, and set impact tolerances that identify the point in time when intolerable harm would result from a disruption of service.

The workflow starts when a Business Service record is created.
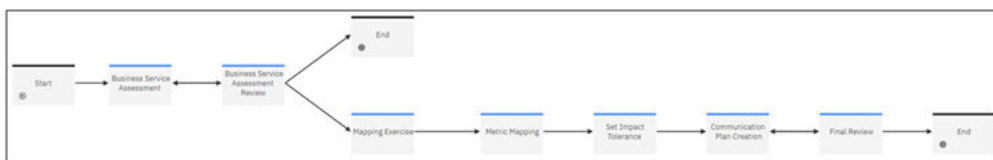
Figure 19. Business Service Initial Assessment

Business Service Periodic Assessment

A review of the Important Business Service Classification and the Impact Tolerance setting is required at least on an annual basis. This workflow ensures that a review occurs on an annual basis.

This workflow can be started by the Owner of the Business Service for a record in "Complete" status or when the execution of the daily schedule matches the Next Scheduled Review Date field. The workflow branches based on whether the Business Service is classified as an Important Business Service or a Regular Business Service.
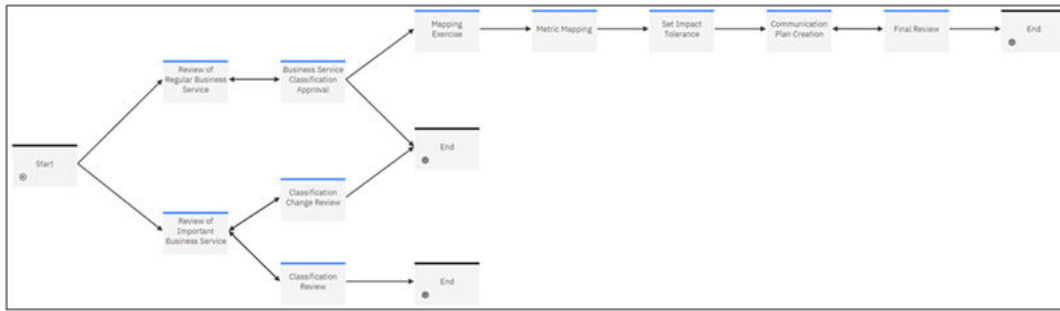
Figure 20. Business Service Periodic Assessment

Business Service Scenario Mapping
This workflow maps Scenario Analyses to a Business Service in a Status of "Complete".

The Owner of the Business Service can manually start this workflow to map Scenarios to the Business Service.
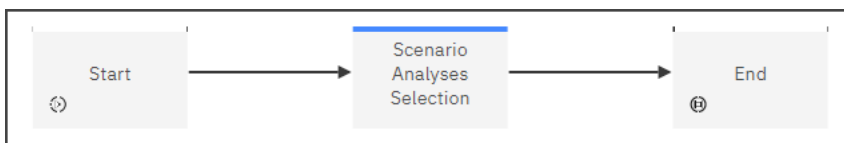
Figure 21. Business Service Scenario Mapping

Scenario Development and Testing
This workflow provides a process for creating scenarios for testing the Business Service impact tolerance, performing the testing, and recording the results of the testing.

This workflow starts for any Scenarios that have not already undergone testing and are categorized as Scenario Scope = Resilience.
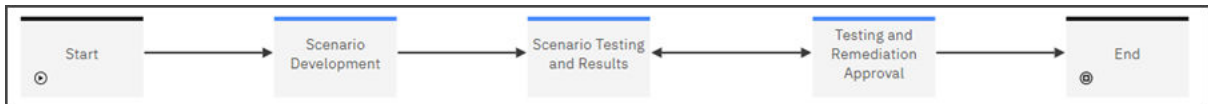
Figure 22. Scenario Development and Testing

Business Service Scenario Testing
This workflow provides a process for the scheduled testing of Scenarios against Business Service Impact Tolerances.

This workflow starts from a schedule for Scenarios that are categorized with Scenario Scope = Resilience in a Status of Analysis Complete that have a Next Review Date greater or equal to the date the schedule is run. Alternatively, the Scenario Analysis Owner can manually start the workflow for a Scenario categorized with Scenario Scope = Resilience.
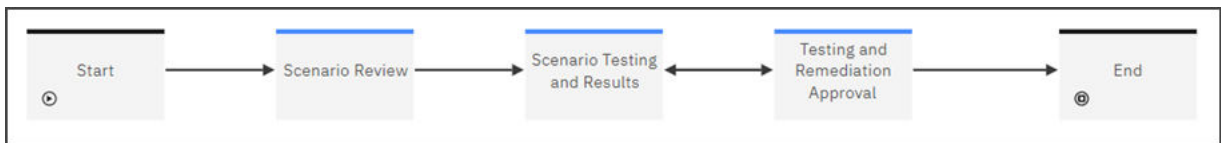
Figure 23. Business Service Scenario Mapping

Imp Bus Service – Breach Remediation
This workflow provides a process for sending notifications and for remediating breaches and near breaches to Business Service Impact Tolerances.

This workflow starts when the Business Service Impact Tolerance Breach Status is in a Red or Yellow state.
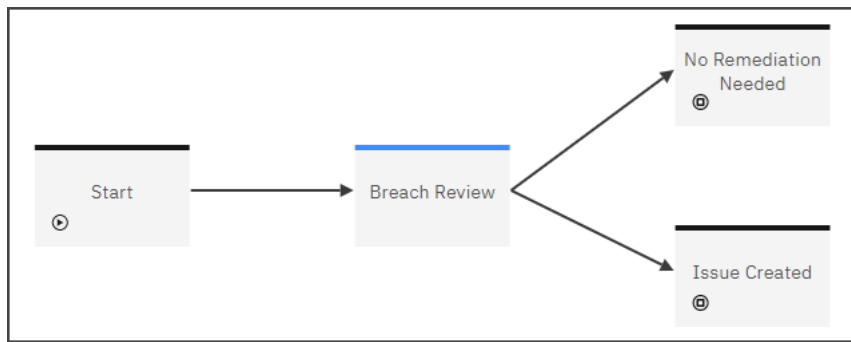
Figure 24. Imp Bus Service – Breach Remediation

IBM OpenPages Data Privacy Management (DPM) workflows

IBM OpenPages Data Privacy Management includes two sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as a template and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

Privacy Impact Assessment

When a new data asset (resource) is imported into Watson Knowledge Catalog, the Privacy Impact Assessment workflow starts automatically. The first stage is Data Asset Review, where a privacy officer (business owner) must determine whether a privacy assessment is needed or not. If the privacy officer needs more information, the officer can request more information from the data steward (primary owner) by selecting **Actions** > **Request Additional Information**. The data asset owner would then need to provide the requested information and select **Actions** > **Submit for Data Asset Review**.

If the privacy officer determines that a privacy assessment is not needed, the officer selects **Actions** > **Privacy Assessment Not Needed**. This action sets the PIA Status field on the resource to Not Needed, and then the workflow ends.

If the privacy officer determines that a privacy assessment is needed, the officer selects **Actions** > **Privacy Assessment Needed**. This action sets the PIA Status field on the resource to Needed and creates a Questionnaire Assessment, which is assigned to the data steward (primary owner) of the resource.

The privacy officer then selects a questionnaire template for the assessment, and the data steward completes the questionnaire. When the questionnaire is complete, the data steward selects **Actions** > **Submit for Approval**.

The privacy officer now reviews the privacy assessment and can either **Approve PIA** or **Reject PIA**. If rejected, the assessment is returned to the data steward for remediation. If the assessment is approved, the workflow ends.
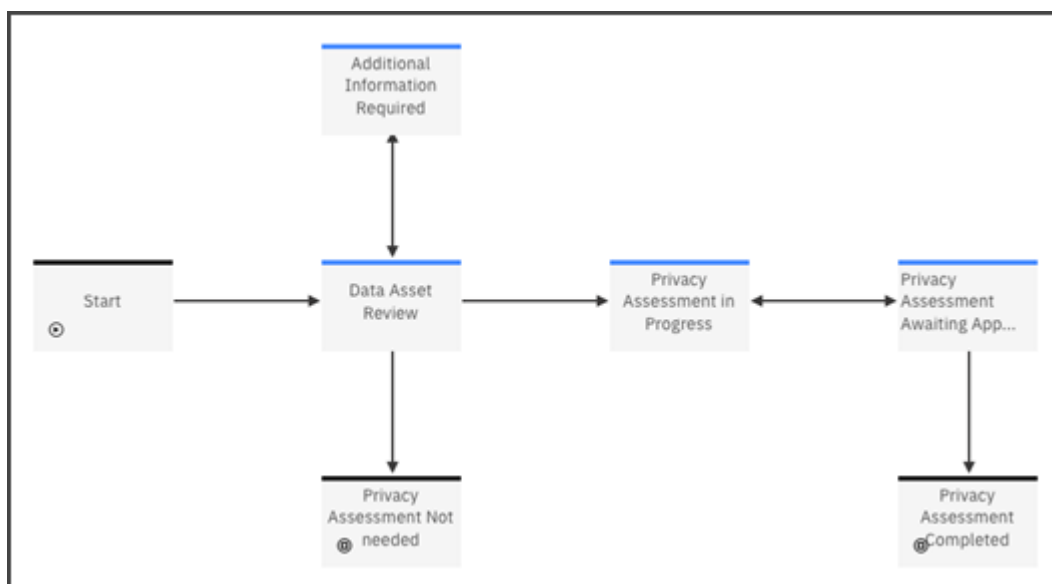
Figure 25. Privacy Impact Assessment workflow

Data Protection Impact Assessment

After a privacy impact assessment (PIA) on a data asset is completed or if a PIA is not needed, the Data Protection Impact Assessment workflow starts automatically. When it starts, the workflow sets the DPIA Status field on the resource to Needed and creates a Questionnaire Assessment that is assigned to the privacy officer (business owner) of the resource.

At the first stage of the workflow, DPIA Started, a data steward (primary owner) has the option to override and cancel the DPIA, if it is determined that the DPIA is not needed. In this case, the data steward selects **Actions** > **Override – DPIA not needed** .

If the data steward does not override the DPIA, then the data steward completes the questionnaire assessment and selects **Actions** > **DPIA Completed**.

At the next stage of the workflow, DPIA Awaiting Approval, the privacy officer (business owner) reviews the DPIA questionnaire assessment, and has the option to reject it by selecting **Actions** > **Reject PIA**, which sends it back to the data steward for remediation, or approve it by selecting **Actions** > **Approve PIA**, which ends the workflow.
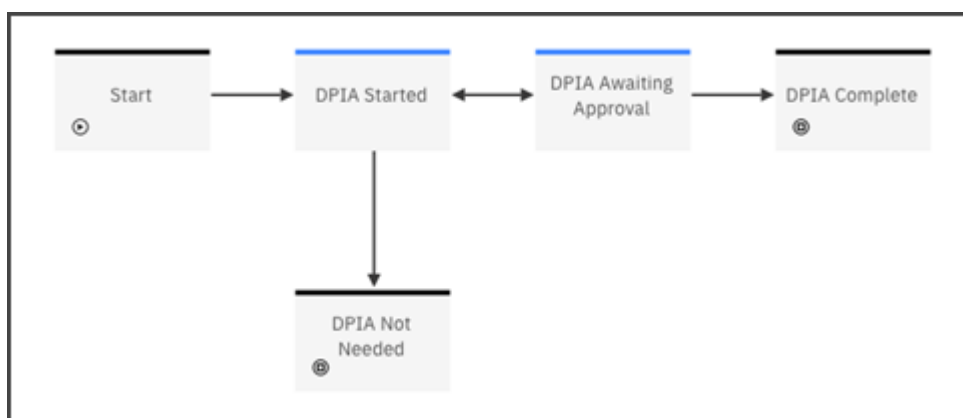
Figure 26. Data Protection Impact Assessment workflow

IBM OpenPages Financial Controls Management (FCM) workflows

IBM OpenPages Financial Controls Management includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as templates and learning tools for your own workflows.

FCM includes the following sample workflows:

- FCM Certification – Business Level
- FCM Certification – Control Eval
- FCM Certification – Process Eval
- FCM Certification – Control
- FCM Certification – Process

The workflows support the internal sub-certification framework at the Control and Process levels. Two distinct workflow paths, Control sub-certification and Process sub-certification, facilitate this and run simultaneously starting at the Business Entity Level.

Depending on the organization's internal sub-certification framework, you can choose to:

- Enable only one of these workflow paths.

  For example, the Control workflow may be disabled if the sub-certification at the Process level is all that is needed to meet your organization's requirements.

- Disable the FCM Certification – Business Level workflow if the business entity is not categorized as in-scope for SOX.

  If the FCM Certification – Business Level workflow is disabled, operations performed in this workflow must be reviewed, such as re-setting the Certification Status field to "Not Reviewed" to determine the impacts to the overall sub-certification process and remaining workflows.

FCM Certification – Business Entity Level workflow

- The sub-certification process begins at the Business Entity level.
- The workflow is activated for all business entities that are in scope for SOX.
- The Business Level workflow has two stages, start and end.
- The out-of-the-box workflow is started by using the Scheduler, which is set to start each calendar quarter and may be adjusted to the organization's needs.
- This workflow triggers the start of the following workflows:
  – FCM Certification - Control (field "classification" = key controls, workflow applicability = key controls), and
  – FCM Certification - Process (field "in scope" = SOX, workflow applicability = in scope for SOX)

Workflow Path at the Control level

The objectives of the FCM Certification – Control Workflow are to:

- Start automatically from the Business Level workflow for all Controls that are classified as "key" controls.
- Create a new Control Eval object for each key Control.
- Automatically start the FCM Certification – Control Eval workflow.

The objectives of the FCM Certification – Control Eval Workflow are to:

- Provide a mechanism for the user to certify the control data for each key Control on a quarterly basis.
- Create a read only record of the certification (the Control Eval object) with the relevant data points mapped from the Control object on a specific date

The user has the option to complete the workflow with the following action: Certify or Certify with Exception.

The user can perform the following actions:

- Certify – the Exception Description field must be blank
- Certify with Exception - the Exception Description field must be populated with the exception description.
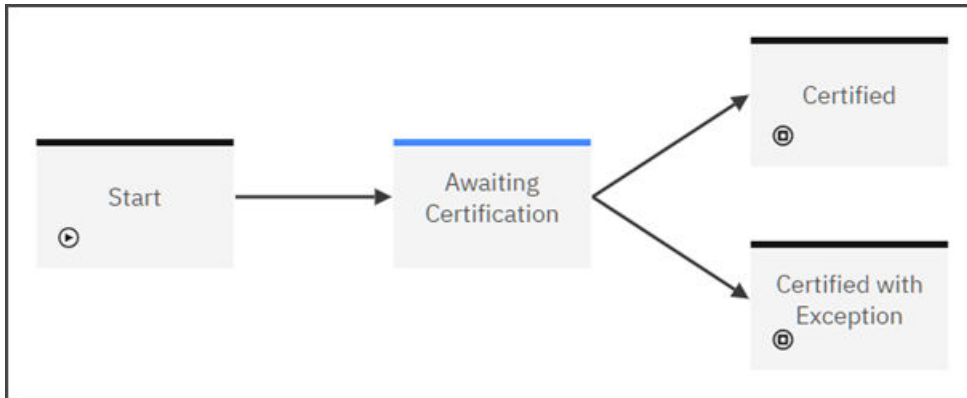- After certification is complete, the Control Eval object is locked to maintain the integrity of the data.

Figure 27. FCM Certification - Control Eval

Workflow Path at the Process level

The objectives of the FCM Certification – Process Workflow are to:

- Start automatically from the Business Level workflow for all Processes that are "in scope for SOX".
- Create a new Process Eval object for each in-scope process.
- Automatically start the FCM Certification – Process Eval workflow.

The objectives of the FCM Certification – Process Eval Workflow are to:

- Provide a mechanism for the user to certify the process data for each "in scope" process on a quarterly basis.
- Create a read only record of the certification (the Process Eval object) with the relevant data points mapped from the Process object on a specific date

The user has the option to complete the workflow with the following actions: Certify or Certify with Exception.

The user can perform the following actions:

- Certify – the Exception Description field must be blank
- Certify with Exception - the Exception Description field must be populated with the exception description.
- After the sub-certification is complete, the Process Eval object is locked to maintain the integrity of the data.
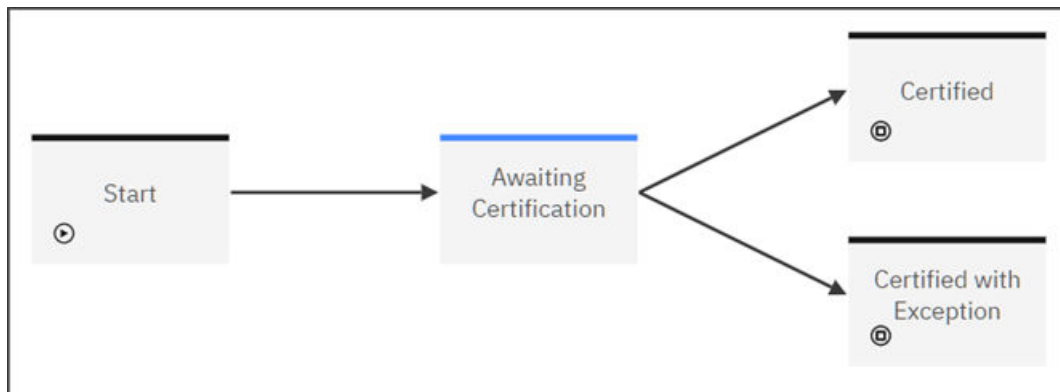
Figure 28. FCM Certification - Process Eval

IBM OpenPages IT Governance (ITG) workflows

IBM OpenPages IT Governance includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as a template and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

Vulnerability Review
> This automatic workflow tracks the progress of assessing the severity of an identified vulnerability and provides an option for the user to launch the Threat Assessment workflow.

Threat Assessment
> This manual workflow can be launched from the Vulnerability Review workflow.
>
> The Threat Assessment workflow tracks the progress of identifying any Threats that might exploit a Vulnerability and assessing the likelihood and impact of the exploitation of the Vulnerability by the identified Threat(s).

IT Waiver
> This automatic workflow tracks the request and response for obtaining a waiver whenever the Waiver is categorized as InfoSec Policy, IT Policy, IT Requirement, or IT Control in the Type field. If the request is approved, the Assignee must provide an expiration date for the Waiver. Otherwise an expiration date of one year from the date of approval is assigned.

IT Waiver Expiration Review
> This automatic workflow is launched on a schedule for any Waiver approved from the IT Waiver workflow when the expiration date is less than 30 days from the date the schedule is run. The user that requested approval in the IT Waiver workflow will make a determination whether an extension of the Waiver is needed. If an extension is needed, the Waiver will progress to the Waiver Extension Review Stage where it will either be approved and a new Expiration Date granted or it will be rejected.

IBM OpenPages Model Risk Governance (MRG) workflows

IBM OpenPages Model Risk Governance includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as templates and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

Model Candidate workflow

> This workflow allows a user to add a Model object to the inventory as a candidate. The Model candidate is submitted for Approval as either a Model or a Non Model. The approver can override the candidate proposal. After a model candidate is confirmed as a Model, the Model Development and Documentation process can begin.

Model Risk Assessment workflow

This workflow performs a model risk assessment on the model, the results of which are used to assign a tier to the model. The Model Risk Scorecard calculation then uses the values in Preference records to compute risk scores and tier. At the end of the workflow, the scores and tier are copied to the parent Model.

Model Validation workflow

This workflow is performed at the completion of the model development and documentation workflow. The Review Planning team that is identified on a Preference object is responsible for completing this review. This workflow is also used for conducting reviews after the model is in production.

Model Attestation workflow

This workflow is typically started by an MRG administrator and records a model owner's response to a request for attestation.

Challenges workflow

This workflow is started against a Model, one of its Model Deployments, or a Review. The result can be no action or changes to a Model or Model Deployment.

Model Change Request workflow

This workflow provides governance for changes to Models. A workflow can be based on changes in the business or to the data and other inputs to a Model. Users can accept, approve, or reject the change and decide whether it is material or not.

Metric Value workflow

This workflow automates the Breach Status calculation and facilitates performance monitoring of deployed models. This process is critical to the ability to proactively decide to change the model or its usages or to remove a model from production. Typically, an MRG administrator creates Metric Value objects, a Metric Capturer provides the latest data for the Metric, and the Metric Owner reviews and approves it. The workflow calculates breach status for the Metric and copies the most recent Metric Value information to the Metric.

Metric Value Creation workflow

When the next collection date comes due for an active metric, this workflow automatically creates a new metric value, and populates it with owner, capturer, and threshold information from the parent metric. The collector can then populate the metric value information and submit it for review.

Note: This workflow is not applicable to IBM Watson OpenScale metrics.

Model Decommission workflow

This workflow is used to remove a Model from production and retire it.

Model Lifecycle
This workflow takes an AI model from the completion of the candidate process through to approval for deployment. It includes multiple stages and sub-workflows that involve various stakeholders.

Model Use Case Request
The Model Use Case Request workflow is used to assess risk and obtain business approval for a model use case. Once a model use case is approved, model development can begin.

Model Deployment
The Model Deployment workflow is used to govern the process of model deployment once development is complete. If the model is being deployed in production, there is an additional step to productionize the model before deployment is complete.

IBM OpenPages Policy Management (PCM) workflows

IBM OpenPages Policy Management includes a sample workflow. You can use it as-is or modify it to meet your requirements. The sample workflow can also be used as a template and learning tools for your own workflows.

The sample workflow is enabled in fresh installations.

Policy Review and Approval workflow

The Policy Review and Approval workflow enables organizations to manage the policy review and approval process through automation. The workflow addresses the following use cases:

- Creation of a new policy
- Annual policy review process
- Ad hoc or off-cycle reviews

The following table shows the Applicability Rule conditions that trigger the workflow for each use case:

Table 36. Applicability rule conditions that trigger the workflow to start

Use Case	Applicability Rule	Example Trigger Events
New Policy	• Version field is empty	• Reg Change • Internal Events
Annual Review Process	• Next Review Date field = today • Status field = draft	• Annual Review
Off Cycle	• Revision Type field = Off-Cycle Review	• Reg Change • Internal Events

Example users of this workflow include:

- Review / Triage stage: Policy Owner, Policy Manager
- Edit / Author stage: Policy Author, Policy Editors
- SME Reviewer / Approver: SME, Manager
- Executive / Approvers: Supervisors, Managers, Compliance, Executives

The features used in this workflow include:

- Applicability rules (see Table 36 on page 123)
- Scheduler – a job is set by default for daily reviews
- Guidance is provided at each stage for the specific activity and user
- Views at each workflow stage are adjusted to the user's role
- A Policy Review Comment (PRC) object is created at the Review and Approval stages (SME / Executive) to document the approval, comments, and relevant fields
- A calculation populates the Policy Name on the Policy Review Comment object description field

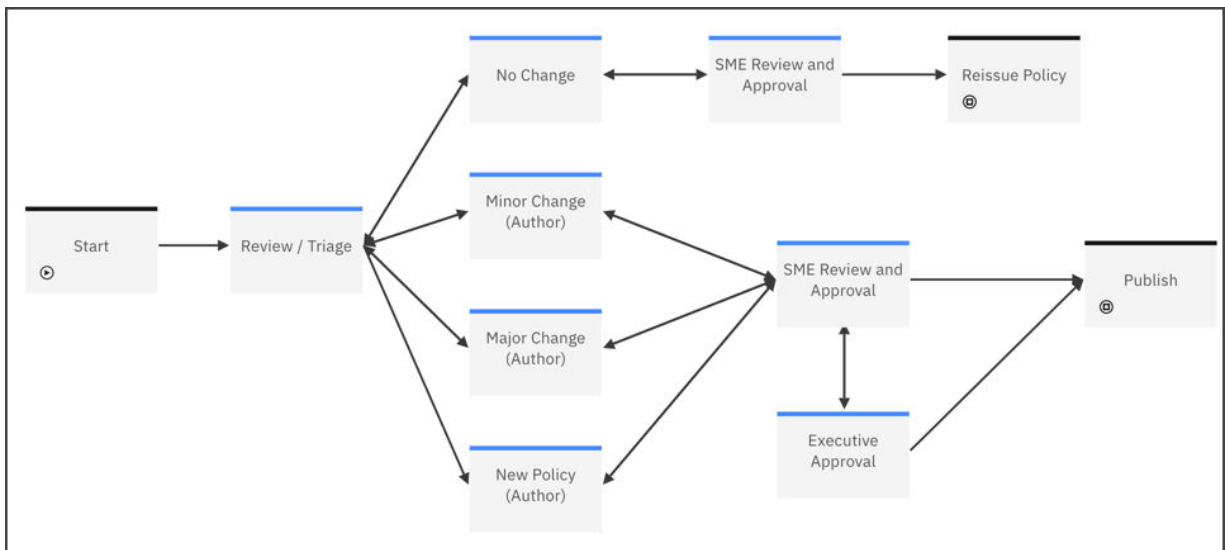**Note:** You can add stages to the workflow for additional approvers.

Figure 29. Policy Review and Approval workflow

Retire Policy workflow

This workflow is triggered when the Publishing Status = Ready to Retire.

The workflow takes the user through a review and approval process for retiring the policy. At each of these stages, a Policy Review Comment (PRC) object is generated to document the SME Approval stage and the Executive Approval stage.

The Publishing helper needs to be triggered at the end of the process to complete the retiring of the policy. The Publishing Helper will delete the draft policy and move the published version of the policy to the expired policy library folder.
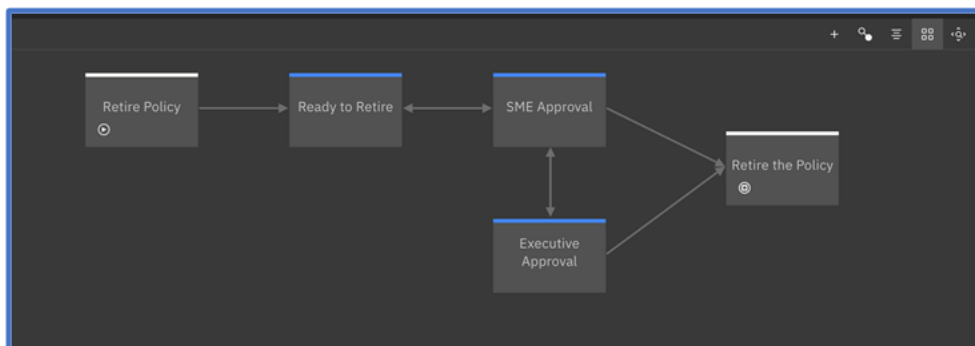
Figure 30. Retire Policy workflow

IBM OpenPages Regulatory Compliance Management (RCM) workflows

IBM OpenPages Regulatory Compliance Management includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as templates and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

OpenPages includes sample workflows for processing Regulatory Events. The workflows can be modified without the need for development resources or coding. Workflows can be tailored to match your organization's methodology for processing alerts published by regulatory agencies.

Regulatory Change Review Workflow

When a Regulatory Change record is created, this workflow starts. The user determines the applicability of the Regulatory Change record and determines the impact of the Regulatory Event. The user can also create and assign Regulatory Tasks to users within RCM for actions that need to be taken to respond to the Regulatory Event. When Regulatory Tasks are assigned to users, this workflow cannot close until all related Regulatory Tasks have been completed.

Regulatory Task Workflow

When a Regulatory Task record is created, this workflow starts. The workflow alerts the owner of the Regulatory Task that a record has been created and assigned to them. After the user completes the assignment that is provided in the Regulatory Task record and clicks **Task Completed**, the workflow changes the status field to **Completed** and populates the date that the task was completed.

Regulator Interaction Workflow

This workflow guides the user through preparing for, and responding to, a regulator interaction, such as a meeting request, inquiry, or examination. A user creates a Regulator Interaction record and then can add documents to the record prior to manually initiating the workflow. The workflow is assigned to the user listed as Primary Internal Contact of the primary parent Regulator record associated to the Regulator Interaction, otherwise the Owner field must be input for the workflow to initiate. The user then proceeds through identifying other users for collaboration, preparing a plan to respond to the regulator interaction, executing the plan, and awaiting the outcome of the interaction prior to closing the workflow. The fields provided for each view within the workflow are tailored for the user based on the type of regulator interaction and the stage of the workflow.

RI Component Workflow

This workflow automatically initiates upon the creation of an RI Component record. Similar to the Regulator Interaction Workflow, the user proceeds through stages for preparing a plan to respond to the regulator, executing the plan, and awaiting the final outcome of the interaction with the regulator. The fields that are provided in each view within the workflow are tailored for the user based on the type of regulator interaction and the stage of the workflow.

RI Sub-Component Workflow

This workflow automatically initiates upon the creation of an RI Sub-Component record. Similar to the Regulator Interaction Workflow, the user proceeds through stages for preparing a plan to respond to the regulator, executing the plan, and awaiting the final outcome of the interaction with the regulator. The fields that are provided in each view within the workflow are tailored for the user based on the type of regulator interaction and the stage of the workflow.

Compliance Review Comment Workflow

This workflow automatically initiates upon the creation of a Compliance Review Comment record when a Reviewer has been identified by the creator of the record. A workflow stage is assigned to the Reviewer to review the comment provided by the creator of the record. After inputting information in the Comment Response field, the Reviewer can submit the response for the record creator's review. The creator of the record can then close the workflow or request a follow-up review from the Reviewer.

Compliance Theme Library Creation

This workflow assists users in the construction of Compliance Themes that can be deployed to Business Entities for assessment. The workflow starts automatically when users create a new Compliance Theme library object.

Compliance Theme Library Update

This workflow assists users in updating Compliance Themes, which can later be deployed to Business Entities for assessment. This workflow is started manually.

Requirement Evaluation

This workflow assists users in evaluating the effectiveness of Controls for managing the compliance risk of mapped Requirements. This workflow is started manually.

After you launch the Compliance Theme Deployer but before you start the Requirement Evaluation workflow, assign a user as the Owner of the Requirement Evaluation.

Compliance Theme BE Assessment

This workflow assists users in evaluating the effectiveness of Controls for managing the compliance risk of mapped Requirements within a Theme.

This workflow is scheduled to run daily. The workflow is initiated for a Compliance Theme when all of its child Requirement Evaluations are in a Review Status of "Completed."

Compliance Plan BE Assessment

This workflow assists users in evaluating the effectiveness of Controls for managing the compliance risk of all Requirements within a business unit.

This workflow is scheduled to run daily. The workflow is initiated when all child Compliance Themes within a Business Entity hierarchy are in a Review Status of "Completed."

Requirement Assessment

This workflow assists users in evaluating the effectiveness of Controls for managing the compliance risk of mapped Requirements. This assessment is performed at the Requirement level for a review of all child Requirement Evaluations.

This workflow is scheduled to run weekly. The workflow is initiated for a Requirement when all child Requirement Evaluations are in a Review Status of "Completed."

Compliance Theme Library Assessment

This workflow assists users in evaluating the effectiveness of Controls for managing the compliance risk of mapped Requirements within a Theme Library.

This workflow is scheduled to run daily. The workflow is initiated when all child Requirements have an Overall Requirement Score defined.

Compliance Plan Library Assessment

This workflow assists users in evaluating the effectiveness of Controls for managing the compliance risk of all mapped Requirements within the enterprise.

This workflow is scheduled to run daily. The workflow is initiated when all child Compliance Themes within the Library are in a Review Status of "Completed."

Compliance Assessment Reset

The workflow is invoked from the Compliance Plan object. The workflow initiates a waterfall of other two-stage workflows to reset values when a new compliance assessment cycle is necessary. Run this workflow from ⚙ > **Solution Configuration** > **Workflows** to ensure that all Compliance Plans are reset.

Compliance Theme - Library Reset

This workflow is launched by the Compliance Assessment Reset workflow. The Compliance Theme - Library Reset workflow resets values on Library Compliance Themes.

Compliance Theme - BE Reset

This workflow is launched by the Compliance Assessment Reset workflow. The Compliance Theme - BE Reset workflow resets values on Compliance Themes that are located within a Business Entity hierarchy.

Requirement Eval Reset

This workflow is launched by the Compliance Theme – BE Reset Workflow. The Requirement Eval Reset workflow resets values on Requirement Evaluations that are mapped to a Compliance Theme.

Trigger Change - Regulatory

This workflow creates a Regulatory Change record and associates the record to a Regulatory Event when the conditions of a rule from the **Rules Engine** are met that indicate the Regulatory Event addresses a regulatory change, such as a proposed or final rule published in the Federal Register. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Regulatory Change**. This workflow enables the association of multiple Regulatory Change records to a Regulatory Event so that multiple users can analyze the impact of the Regulatory Event on their particular areas of responsibility within the organization.

Workflows for the Reg-Track connector

The following workflows are available with the Reg-Track connector:

Trigger Change - Regulatory

This workflow creates a Regulatory Change record and associates the record to a Reg-Track Regulatory Event when the conditions of a rule from the Rules Engine are met that indicate the Reg-Track Regulatory Event addresses a regulatory change, such as a proposed or final rule published in the Federal Register. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Regulatory Change**. This workflow enables the association of multiple Regulatory Change records to a Reg-Track Regulatory Event so that multiple users can analyze the impact of the Reg-Track Regulatory Event on their particular areas of responsibility within the organization.

Trigger Change - Horizon Scanning

This workflow creates a Regulatory Change record and associates the record to a Reg-Track Regulatory Event when the conditions of a rule from the Rules Engine are met that indicate the Reg-Track Regulatory Event addresses an issue other than a regulatory change, such as a speech or enforcement action published by a regulator. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Horizon Scanning**. This workflow enables the association of multiple Regulatory Change records to a Reg-Track Regulatory Event so that multiple users can analyze the impact of the Reg-Track Regulatory Event on their particular areas of responsibility within the organization.

Reg-Track Regulatory Change Review Workflow

When a Regulatory Change record is created, this workflow starts. The workflow guides the user through the processing of a Reg-Track Regulatory Event. The user determines the applicability of the Reg-Track Regulatory Event that is associated with the Regulatory Change record and determines the impact of the Reg-Track Regulatory Event. The user can also create and assign Regulatory Tasks to users within RCM for actions that need to be taken to respond to the Reg-Track Regulatory Event. When Regulatory Tasks are assigned to users, this workflow cannot be closed until all related Regulatory Tasks have been completed.

Send Email Notification

This workflow can be used to send mail notifications to users who are named within a rule that is created in the Rules Engine.

Workflows for the Thomson Reuters connector

The following workflows are available with the Thomson Reuters connector:

Trigger Change - Regulatory

This workflow creates a Regulatory Change record and associates the record to a TRRI Regulatory Event when the conditions of a rule from the Rules Engine are met that indicate the TRRI Regulatory Event addresses a regulatory change, such as a proposed or final rule published in the Federal Register. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Regulatory Change**. This workflow enables the association of multiple Regulatory Change records to a TRRI Regulatory Event so that multiple users can analyze the impact of the TRRI Regulatory Event on their particular areas of responsibility within the organization.

Trigger Change - Horizon Scanning

This workflow creates a Regulatory Change record and associates the record to a TRRI Regulatory Event when the conditions of a rule from the Rules Engine are met that indicate the TRRI Regulatory Event addresses an issue other than a regulatory change, such as a speech or enforcement action published by a regulator. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Horizon Scanning**. This workflow enables the association of multiple Regulatory Change records to a TRRI Regulatory Event so that multiple users can analyze the impact of the TRRI Regulatory Event on their particular areas of responsibility within the organization.

TRRI Regulatory Change Review Workflow

When a Regulatory Change record is created, this workflow starts. The workflow guides the user through the processing of a TRRI Regulatory Event. The user determines the applicability of the TRRI Regulatory Event that is associated with the Regulatory Change record and determines the impact of the TRRI Regulatory Event. The user can also create and assign Regulatory Tasks to users within RCM for actions that need to be taken to respond to the TRRI Regulatory Event. When Regulatory Tasks are assigned to users, this workflow cannot be closed until all related Regulatory Tasks have been completed.

Send Email Notification

This workflow can be used to send mail notifications to users who are named within a rule that is created in the Rules Engine.

Workflows for the Wolters Kluwer connector

The following workflows are available with the Wolters Kluwer connector:

Trigger Change - Regulatory

This workflow creates a Regulatory Change record and associates the record to a WK Regulatory Event when the conditions of a rule from the Rules Engine are met that indicate the WK Regulatory Event addresses a regulatory change, such as a proposed or final rule published in the Federal Register. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Regulatory Change.** This workflow enables the association of multiple Regulatory Change records to a WK Regulatory Event so that multiple users can analyze the impact of the WK Regulatory Event on their particular areas of responsibility within the organization.

Trigger Change - Horizon Scanning

This workflow creates a Regulatory Change record and associates the record to a WK Regulatory Event when the conditions of a rule from the Rules Engine are met that indicate the WK Regulatory Event addresses an issue other than a regulatory change, such as a speech or enforcement action published by a regulator. The workflow also populates certain fields on the created Regulatory Change record, including categorizing the Regulatory Change record as **Horizon Scanning**. This workflow enables the association of multiple Regulatory Change records to a WK Regulatory Event so that multiple users can analyze the impact of the WK Regulatory Event on their particular areas of responsibility within the organization.

WK Regulatory Change Review Workflow

When a Regulatory Change record is created from a WK Regulatory Event, this workflow starts. The workflow guides the user through the processing of a WK Regulatory Event. The user determines the applicability of the WK Regulatory Event that is associated with the Regulatory Change record and determines the impact of the Regulatory Event. The user can also create and assign Regulatory Tasks to users within RCM for actions that need to be taken to respond to the Regulatory Event. When Regulatory Tasks are assigned to users, this workflow cannot be closed until all related Regulatory Tasks have been completed.

Send Email Notification

This workflow can be used to send mail notifications to users who are named within a rule that is created in the Rules Engine.

IBM OpenPages Risk Management for ESG workflows

IBM OpenPages Risk Management for ESG includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as templates and learning tools for your own workflows.

ESG includes workflows for the following use cases:

- Objective management
- ESG compliance applicability
- ESG compliance assessment

The workflows for objective management are:

Objective creation workflow
When an Objective is created, this workflow allows the user to populate key fields related to the description, ownership, categorization, and prioritization of the objective.
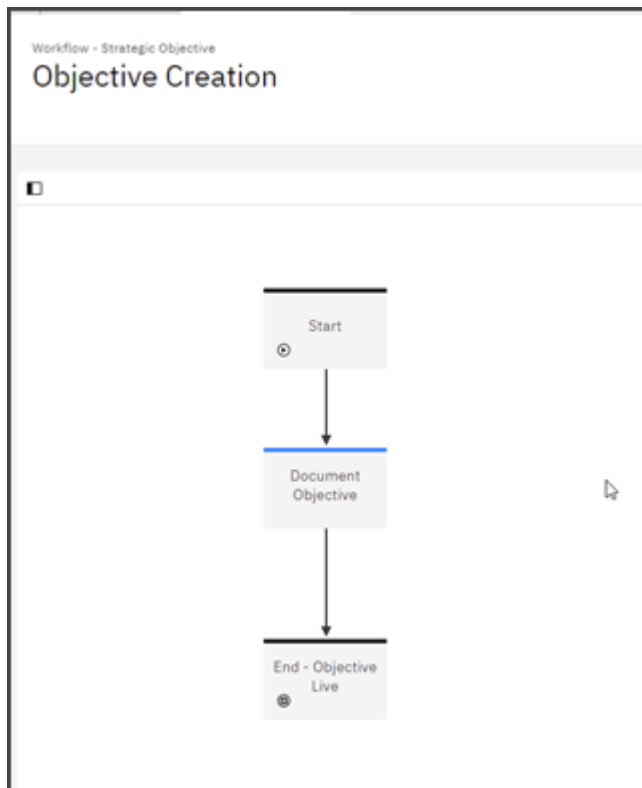
Figure 31. Objective creation workflow

Objective update workflow
This workflow is used to update an objective or mark it as Complete.
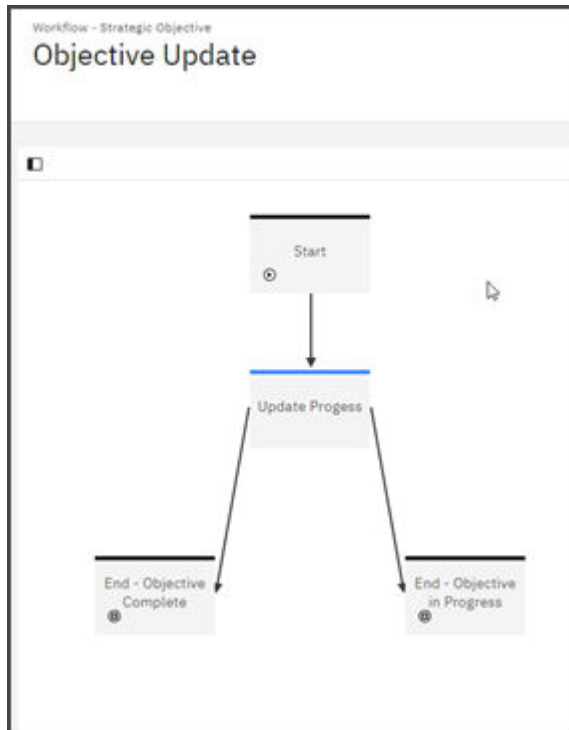
Figure 32. Objective update workflow

The workflows for compliance applicability are:

ESG applicability - Mandate workflow
This workflow creates applicability assessments. No user action is required. This workflow launches the "ESG Applicability - SubMandate" workflow for all associated SubMandates.
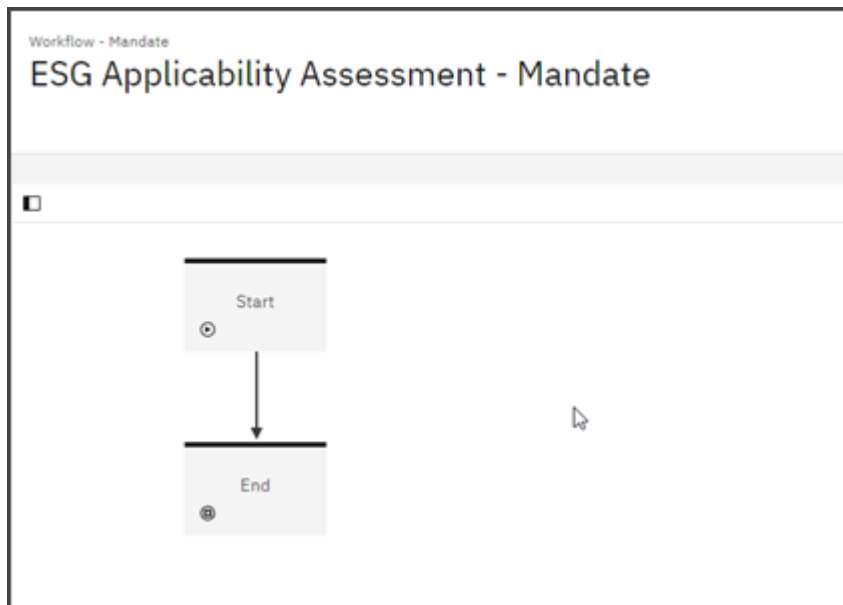

Figure 33. ESG applicability - Mandate workflow

ESG applicability - SubMandate workflow

This workflow is launched from the parent Mandate. The workflows prompts the Mandate owner to assess applicability for ESG on each SubMandate. Upon submission, the workflow launches the "ESG Applicability – Requirement" workflow for the associated requirements.
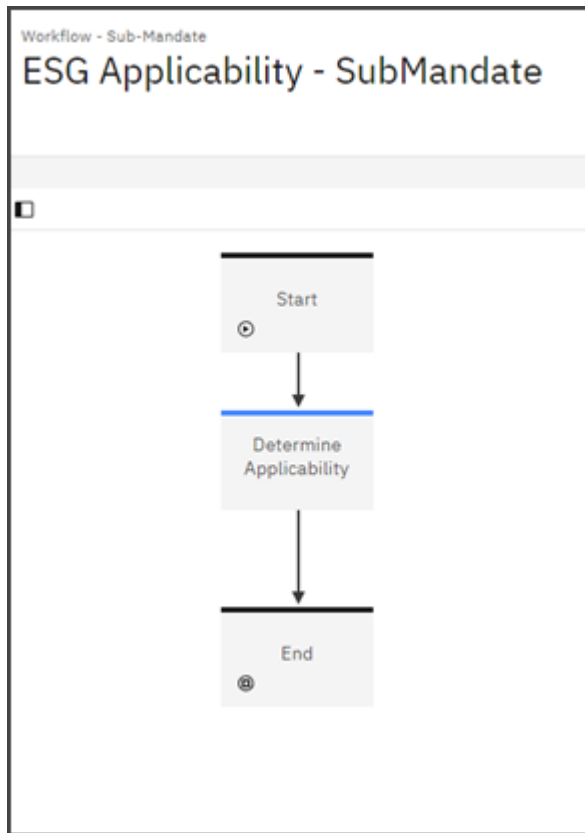
Figure 34. ESG applicability - SubMandate workflow

ESG Applicability – Requirement

This workflow allows the Mandate owner to record if the requirement is applicable and reportable for ESG. The user also records the assessment type for the Requirement: Measured (use of KRIs) or Disclosure Statement.
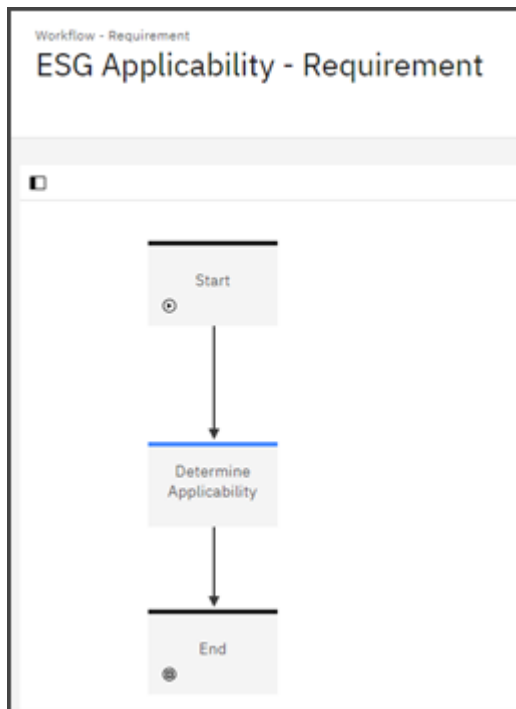
Figure 35. ESG applicability - Requirement workflow

The workflows for compliance assessment are:

ESG Compliance Assessment – Launch workflow
This workflow has no user tasks. The workflow launches the "ESG Compliance Assessment - Requirement" workflow for all descendant (Mandate, SubMandate, and Requirement) Requirements that are marked as Applicable for ESG.
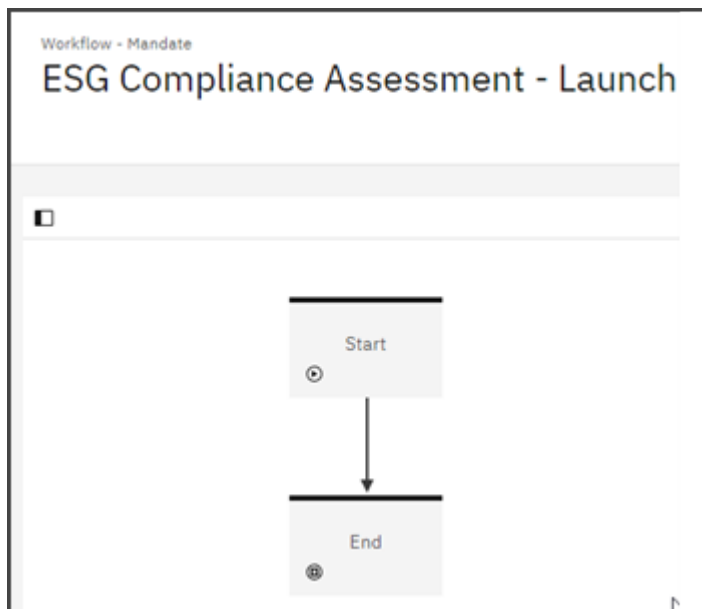
Figure 36. ESG Compliance Assessment – Launch workflow

ESG Compliance Assessment – Requirement workflow
This is a two-stage assessment and approval workflow for Requirements that are applicable for ESG.
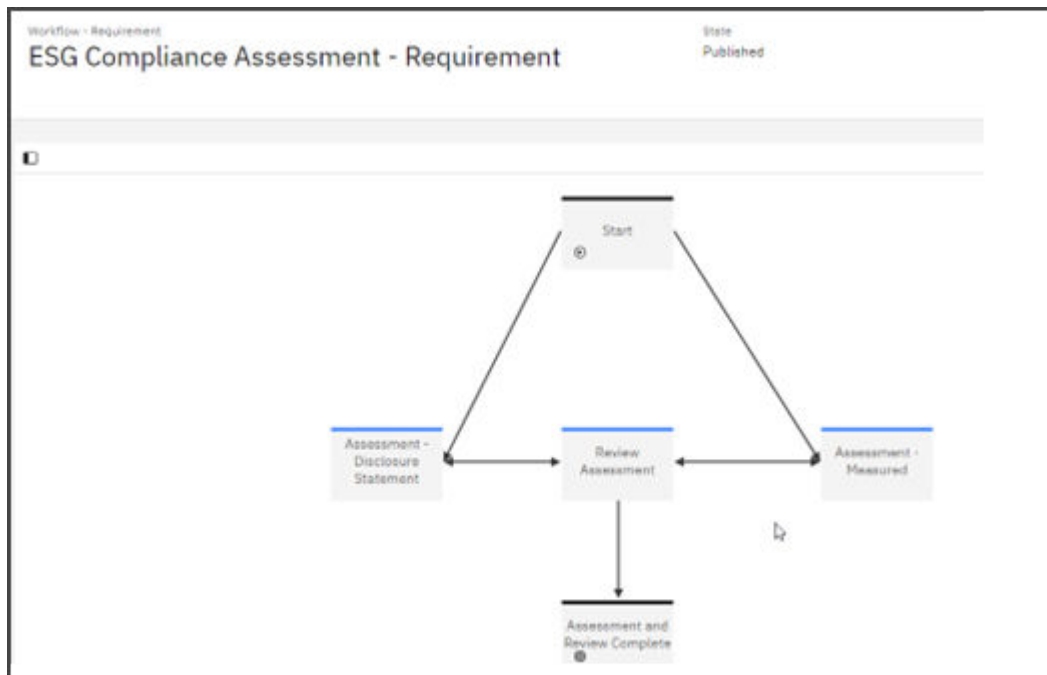
Figure 37. ESG Compliance Assessment - Requirement workflow

Disclosure Statement and Review workflow

This is a two-stage assessment and approval workflow for Disclosure Statements.
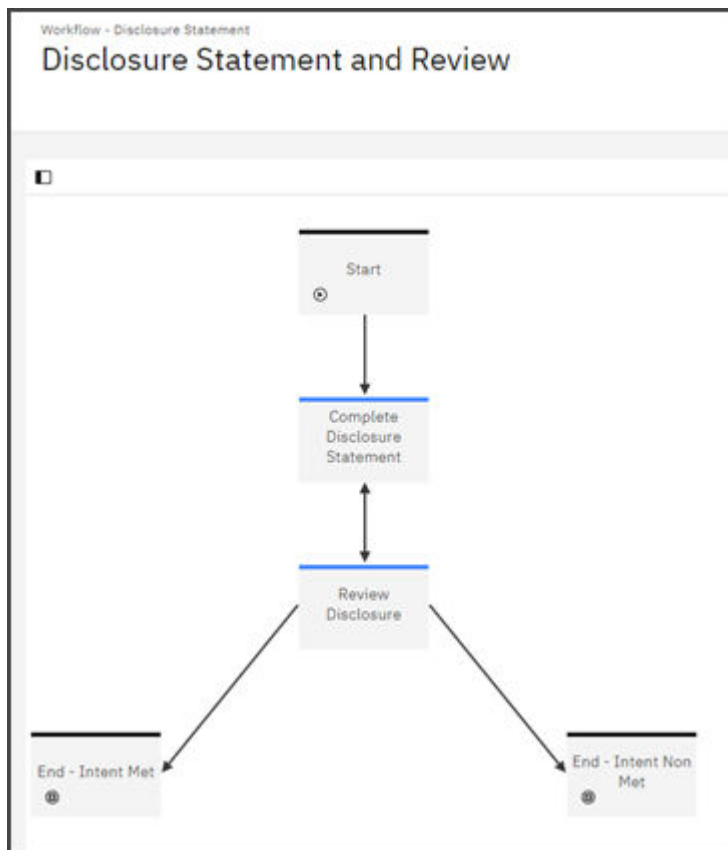
Figure 38. Disclosure Statement and Review workflow

IBM OpenPages Third Party Risk Management (TPRM) workflows

IBM OpenPages Third Party Risk Management includes sample workflows. You can use them as-is or modify them to meet your requirements. The sample workflows can also be used as templates and learning tools for your own workflows.

The sample workflows are enabled in fresh installations.

Vendor Selection

This workflow is used when selecting vendors. This workflow can be used by Procurement or a Business Entity in their process. The first step is to identify the vendor responsibilities to be added as part of the client's RFI process. Once determined, the RFI will be created and a list of vendors to participate is determined. The client then uses their own RFI process and tracks the outcomes. The end user will then use the Due Diligence workflow prior to final selection. At the completion of the Vendor Selection workflow, the user can launch the Vendor Onboarding workflow.

Vendor Due Diligence

This workflow is for conducting due diligence on a potential third party. A questionnaire or checklist (based on internal processes) can be added to document the due diligence process. The workflow begins with identifying the vendor, assigning a user to the due diligence task. Once the fact gathering is complete, the workflow documents the approval steps to either accept or reject a vendor.

Vendor Onboarding

This workflow is used for onboarding a third party. A questionnaire or checklist (based on internal processes) can be added to document the onboarding process. The workflow begins after a Vendor has been through the due diligence and selection workflows and the initial contract is signed. A user will review and input relevant information, assign the vendor's criticality, and will assign controls and KRIs. The final step will be to schedule the next assessment period for the vendor.

Vendor Contract Negotiations

This workflow allows a user to track the progress of contract negotiations. The workflow begins with the Business defining the contractual terms and providing them to Legal for drafting and editing. Once the draft contract is prepared, the contract is delivered to the Vendor with steps for redlining and final approval.

Vendor Termination

This workflow allows a user to complete the termination process of a vendor. Steps include identifying the vendor, finding a replacement vendor (if needed), completing a termination checklist, termination notice, and final confirmation.

Vendor Assessment

The user will use this workflow when conducting a vendor risk assessment. Steps include Questionnaire identification, Questionnaire preparation, conducting assessment, review, accept/reject, and creation of issues.

Vendor Identified Global Issue

This workflow can be used when a global issue is identified across your vendors. A global issue is likely created due to a failure of the end user's policy, procedure, and/or control that a vendor has adopted. Steps include: identifying a global (enterprise-wide) issue that has been discovered; identifying the deficiencies that raised the issue; reviewing the internal policies, procedures, and controls; updating needed documentation; and sending notice to all vendors of the updates made.

Vendor Issue Remediation

This workflow can be used when an issue with a vendor has been identified to work through the remediation process. Steps include: identifying an issue with a vendor, identification of the deficiencies that raised the issue, creating an action plan, completing the mitigation tasks, documenting an exception and/or termination.

Appendix A. Legacy features

The following features have been deprecated or removed from IBM OpenPages with Watson.

Business process visualizations (legacy)

Visualizations that rendered business processes in a graphical format are no longer supported in IBM OpenPages with Watson.

The infrastructure, for example, the object types and triggers, that supported business process visualizations can exist in your system if you are using an older version of OpenPages.

Visualizations of business processes supported the risk management process and data analysis by providing graphical views of process, subprocesses, activities, risks, and controls. They included Business Entity organization charts and process diagrams.

Object types

Visualizations included the following object types:

- Data Input and Data Output objects

  The Data Input Object and Data Output Object are child objects of the Process and can have associations only to existing Risks. They represent elements of a flow to depict an Input into the Business Flow or an Output from various activities within a process, such as running a report or updating a CRM system or getting an external data source feed.

- Process Diagram objects

  A Process Diagram is a child object of the Process and can have many diagrams per process. It is used to store the sequence of subprocesses or activities within a process with associated Risks and Controls along with any annotations such as decision nodes. All attributes of the Business Process visualization are stored in the Process Diagram object.

Computed field

Visualizations included one computed field, `OPSS-ProcDiag.ProDiaLnk`, on the Process Diagram object type.

Report

Visualizations included the Process Analysis report and the following drill-through reports:

- Business Process Flow
- Business Entity Hierarchy diagram
- Risk Heat Map

The report shows Risks and Controls in the context of a process diagram. It provides an aggregated view of Risk and Controls with risk rating and control effectiveness at the Process and Business Entity level.

Triggers

Visualizations included triggers that were based on the Data Input and Data Output objects. The Visualization triggers prevent a user from adding new Risks as children of the Data Input and Data Output object types. The Data Input and Data Output objects are children of the Process and can have associations only to existing Risks. The data input object represents elements of a flow to depict an input into the Business Flow. The data output object depicts an output from activities within a process, such as running a report or updating a CRM system.

System file type

Visualizations used the VizConfig system file type for visualization configuration files.

Tasks in the Standard UI

Users accessed visualizations by using the following tasks in the Standard UI:

• **Organization** > **Business Entities** > **Business Entity Chart field** > **Hierarchy Diagram link**
• **Organization** > **Processes** > **Associations** > **Process Diagrams**

Computed fields

The following table lists legacy computed fields. These fields are replaced by URL fields. A computed field is a read-only field whose value is derived from the values of other fields. Computed fields can contain data types such as Boolean, date, decimal, integer, and simple strings.

Table 37. Computed fields in OpenPages with Watson solutions

Object type label Field group Field name	Description	RCM	ORM	PCM	ITG	IAM
Risk Assessment OPSS-RA RCSA Completion Helper	Creates a link that launches the RCSA Completion helper. This helper allows the RCSA Coordinator to complete the Risk Assessment and create an evaluation tree for historical referencing.		X			
Risk Assessment OPSS-RA RCSA Process Alignment Helper	Creates a link that launches the RCSA Process Alignment helper. This helper allows the RCSA Coordinator to review the associate Processes, Risks, and Controls, and create further associations. The helper also sets the Processes, Risks, and Controls to a status of Awaiting Assessment.		X			

Legacy triggers

The IBM OpenPages with Watson solutions include several triggers that are not enabled in fresh installations.

These triggers have been replaced by functionality that is available in the GRC Workflow and GRC Calculations features.

The following table lists the triggers that are no longer enabled.

Table 38. Triggers that are not enabled in fresh installations

Trigger	TPRM	RCM	MRG	FCM	ORM	PCM	ITG	IAM
"Loss Event Lifecycle triggers (legacy)" on page 139					X			
"Questionnaire Assessment Lifecycle triggers (legacy)" on page 140	X	X	X	X	X	X	X	X

Table 38. Triggers that are not enabled in fresh installations (continued)								
Trigger	TPRM	RCM	MRG	FCM	ORM	PCM	ITG	IAM
"Incident Lifecycle triggers (legacy)" on page 141						X	X	
"KRI and KPI Lifecycle triggers (legacy)" on page 146					X	X	X	
"Model Risk Scorecard trigger" on page 87 **Note:** This trigger is disabled by default but it's still available in fresh installations.			X					
"RCSA Quantitative and RCSA Qualitative triggers (legacy)" on page 143					X			
Triggers for the Scenario Analysis object type: Scenario Completion Update and Scenario Completion Create					X			
"Business process visualizations (legacy)" on page 135 triggers (triggers for the Data Input and Data Output object types).								

Loss Event lifecycle triggers (version 7.2.0.1 and later) (legacy)

Triggers provide the transitions that move loss events through an investigation lifecycle. Lifecycles define the stages that an object type can follow

These triggers are not enabled in fresh installations.

At each stage, the system:

- Identifies a lifecycle assignee
- Defines the actions available to move to a different stage
- Automatically sends an email to the new lifecycle assignee
- Defines other attributes that are related to the current stage

The lifecycle for loss events uses the following stages:

- New
- Open
- Awaiting Approval
- Awaiting Approval L1
- Awaiting Approval L2
- Closed

When a loss event is created, the system sets the lifecycle to the New stage and sends an email to the first lifecycle assignee. When the user completes the task, the trigger moves the object to the next task and the next user. A user can add a comment with every transition. Transitions take place when users open a loss event object in the detail view and click Lifecycle > *<transition icon>*. The stage determines the transition icon that is displayed.

> ⚠️ **Attention:** Before OpenPages Version 7.2.0.1, a trigger existed for Loss Event objects to verify the date fields and to populate the approver fields on the loss event at the time the user set the **OPSS-LossEv:Submit** field to **Yes**. As of OpenPages Version 7.2.0.1 and later, this trigger

now fires on the lifecycle transition from Open to Submit, so the trigger now fires on the field **OPLC-Std:LCTransition** with a value of **Submit**. The **OPSS-LossEv:Submit** field on the loss event is now redundant.

A second trigger existed to lock the loss event and its children upon closure. Before OpenPages Version 7.2.0.1, this trigger was fired on the field **OPLC-LossEv:Status** with a value of **Approved**. As of OpenPages Version 7.2.0.1 and later, this trigger now fires on the **OPLC-Std:LCStage** field with a value of **Closed**.

The following table summarizes how the system handles loss events and sets the lifecycle assignee. The Transition icon column contains the name of the Lifecycle ><transition icon> in the issue detail view that a user clicks to trigger the transition to the next stage.

Table 39. Lifecycle process and stage owners for loss events

Stage	Lifecycle assignee	Transition icon	Next stage	Next Status
New	Owner	**Start**	Open	Open
Open	Owner	**Submit**	Closed	Closed
Open	Owner	**Submit**	Awaiting Approval	Awaiting Approval
Open	Owner	**Submit**	Awaiting Approval L1	Awaiting Approval L1
Awaiting Approval	Approver	**Reject Approval**	Open	Approval Rejected
Awaiting Approval	Approver	**1 Stage Close**	Closed	Approved 1 level
Awaiting Approval L1	Approver	**Send For L2 Approval**	Escalation Review	Escalation Review
Awaiting Approval L1	Approver	**Reject L1 Approval**	Open	Approval L1 Rejected
Awaiting Approval L2	Approver L2	**2 Stage Close**	Closed	Approved 2 levels
Awaiting Approval L2	Approver L2	**Send Back to L1 Approval**	Awaiting Approval L1	Sent Back to L1
Awaiting Approval L2	Approver L2	**Reject L2 Approval**	Open	Approval L2 Rejected

When a **Submit** transition is made, the trigger compares the Gross Loss with the threshold values provided in the Preference record associated with the nearest Business Entity to the loss event. For a Gross Loss less than threshold 1, the loss event transitions to the Closed stage. (This is a Loss Event 0 Stage lifecycle.)

For loss events that have a Gross Loss greater than threshold 1 and less than threshold 2, the **Approver** field is copied from the Preference record to the loss event. The loss event transitions to the Awaiting Approval stage. (This is a Loss Event 1 Stage lifecycle.) By default, the trigger sets the Due Date to be 14 days from the date of submission.

For loss events that have a Gross Loss greater than threshold 2, both the **Approver** and **Approver L2** fields are copied from the Preference record to the loss event. The loss event is transitioned to the Awaiting Approval L1 stage. (This is a Loss Event 2 Stage lifecycle.) By default, the trigger sets the Due Date to be 14 days from the date of submission.

If the loss event is transitioned back to the Open stage, then the trigger runs again on **Submit** and, if the Gross Loss has changed, might alter the lifecycle. When the loss event is transitioned to the Closed stage, a trigger closes and locks all of the child impacts and recoveries. The trigger then locks the loss event.

Loss event notification

The loss event notification sends an email to a lifecycle assignee when a loss event is created and for each transition in the loss event lifecycle. A transition occurs when a user clicks a transition icon (Lifecycle > **Start**, **Submit**, **Reject Approval** , **1 Stage Close**, **Send For L2 Approval**, **Reject L1 Approval** , **2 Stage Close**, **Send Back to L1 Approval** , or **Reject L2 Approval**) in the loss event detail view.

The loss event notification is started by the loss event lifecycle trigger. The email notification contains the stage, status, due date, comment, and a link to the loss event.

Loss events and GRC Workflow

You can use both configurable lifecycles and workflows for Loss Events but you must consider how they interact and where they conflict. For more information, see *Configuring GRC Workflow* in the *IBM OpenPages with Watson Administrator's Guide*.

Conditions that control the Lifecycle button

When an object that uses lifecycles is opened in a detail or activity view, the **Lifecycle** > **<transition icon>** button is displayed or hidden based on the current user and lifecycle information on the object.

It is displayed if all of the following conditions are met:

- The reporting period is the current reporting period
- The following fields are defined on the object type: LCStage, LCTransition, LCAssignee, LCComment, and LCAppData
- LCStage has a non-empty value
- One or more transitions are mapped to the current LCStage value with a picklist dependency
- The current user is set in LCAssignee, is a member of a group set in LCAssignee, or has explicit write permission to the object

It is hidden if any of the conditions are not met.

The Lifecycle button is hidden if changes are made that interfere with a lifecycle process. If you add fields to an object type after object instances exist, default values are not assigned to the new fields. Fields such as LCStage and LCAssignee do not likely have valid values on the existing instances. The Lifecycle button is then hidden, which ensures that new lifecycles do not interrupt previous lifecycles for existing object instances.

If an object type has both a workflow and a configurable lifecycle, the workflow **Actions** button in Task Views in the Task Focused UI takes priority over the lifecycle **Actions** button. For more information, see *Configuring GRC Workflow* in the *IBM OpenPages with Watson Administrator's Guide*.

Loss Event Lifecycle triggers (legacy)

The Loss Event Lifecycle triggers calculate and maintain three fields on the Loss Event object, when related fields are created or changed on any descendant Loss Impact and Loss Recovery objects.

These triggers are not enabled in fresh installations.

The triggers automate the approval process and remediation performance of Loss Event as described in the triggers for Loss Event Approval Submission and Loss Event Approval.

The loss event lifecycle process consists of three triggers.

Loss Event Computation trigger

The Loss Event Computation trigger computes summary values in system base currency on a Loss Event that is based on associated Loss Impact and Recoveries.

Loss Event Approval Submission trigger

The Loss Event Approval Submission trigger changes a Loss Event from an Open event to the Approval stage of its lifecycle. The trigger validates data.

The trigger occurs when the user transitions the Loss Event Lifecycle from **Open** to **Submit**.

The trigger sets the LC Due Date to 14 days from the submission date

Loss Event Approval trigger

The trigger locks the Loss Event and any Child Impact and Recoveries.

The trigger occurs when the user transitions the Loss Event Lifecycle from **Open** or **Awaiting Approval** to **Closed**.

Questionnaire Assessment Lifecycle triggers (legacy)

These triggers are not enabled in fresh installations.

Questionnaires assessments are a means of gathering information from business users in the organization. Triggers provide the transitions that move questionnaire assessments through a lifecycle. Lifecycles define the stages that an object type can follow. At each stage, the system:

- Identifies a lifecycle assignee
- Defines the actions available to move to a different stage
- Automatically sends an email to the new lifecycle assignee
- Defines other attributes that are related to the current stage

The lifecycle is selected on the program. It can be:

- Two-stages: information gathering to closed
- Three-stages: information gathering to review to closed
- Four-stages: information gathering to review to approval to closed

When a program is launched, the system creates one questionnaire assessment object per employee, resource, process, subprocess, vendor, or engagement in the program. It sets the lifecycle to the information gathering stage and sends an email to the first lifecycle assignee. When the user completes the task, the trigger moves the object to the next task and the next user. A user can add a comment with every transition. Transitions take place when users work with questionnaire assessments in the questionnaire UI. Emails are sent at each transition except if the assignee remains the same. By default, emails are not sent when questionnaire assessments move to the closed stage.

The following table summarizes the lifecycles for questionnaire assessments. The **Transition icon** column contains the name of the icon in the questionnaire UI that a user clicks to trigger the transition to the next stage.

Table 40. Lifecycle process for questionnaire assessments

Lifecycle	Stage	Transition icon	Next stage	Next Status
Two-stages	Information gathering	**Submit and Close**	Closed	Complete
Three-stages	Information gathering	**Submit**	Review	In Review
	Review	**Action** > **Reject**	Information gathering	Rejected
		Action > **Approve and Close**	Closed	Complete

Table 40. Lifecycle process for questionnaire assessments (continued)				
Lifecycle	Stage	Transition icon	Next stage	Next Status
Four-stages	Information gathering	**Submit**	Review	In Review
	Review	**Action** > **Reject**	Information gathering	Rejected
		Action > **Submit for Approval**	Approval	In Approval
	Approval	**Action** > **Reject**	Review	Approval Rejected
		Action > **Approve**	Closed	Approved

For questionnaire assessments, the underlying assets determine how the system sets the lifecycle assignees. The following table summarizes how lifecycle assignees are determined.

Table 41. Lifecycle assignees for questionnaire assessments						
Lifecycle	Stage	Resource	Process/ Subprocess	Employee	Vendor	Engagement
Two-stages	Information gathering	Primary owner	Owner	Employee account	Vendor owner	Engagement owner
	Closed	-	-	-	-	-
Three-stages	Information gathering	Primary owner	Owner	Employee account	Vendor owner	Engagement owner
	Review	Program owner	Program owner	Employee manager	Vendor - Business Unit Owner	Vendor - Business Unit Owner
	Closed	-	-	-	-	-
Four-stages	Information gathering	Primary owner	Owner	Employee account	Vendor owner	Engagement owner
	Review	Business owner	Business owner	Employee manager	Vendor - Business Unit Owner	Vendor - Business Unit Owner
	Approval	Program owner	Program owner	Program owner	Program owner	Program owner
	Closed	-	-	-	-	-

Incident Lifecycle triggers (legacy)

These triggers are not enabled in fresh installations.

Triggers provide the transitions that move incidents through an investigation lifecycle. Lifecycles define the stages that an object type can follow. At each stage, the system:

- Identifies a lifecycle assignee
- Defines the actions available to move to a different stage
- Automatically sends an email to the new lifecycle assignee
- Defines other attributes that are related to the current stage

The lifecycle for incidents uses the following stages:

- New

- In progress
- Review
- Escalation
- Escalation review
- Closed

When an incident is created, the system sets the lifecycle to the New stage and sends an email to the first lifecycle assignee. When the user completes the task, the trigger moves the object to the next task and the next user. A user can add a comment with every transition. Transitions take place when users open an incident object in the detail view and click **Lifecycle** > **<transition icon>**. The stage determines the transition icon that is displayed.

The following table summarizes how the system handles incidents and sets the lifecycle assignee. The **Transition icon** column contains the name of the transition icon that displays in the incident detail view.

Table 42. Lifecycle process and stage owners for incidents				
Stage	**Lifecycle assignee**	**Transition icon**	**Next stage**	**Next Status**
New	Primary owner	**Start**	In Progress	In Progress
In Progress	Primary owner	**Send for Review**	Review	In Review
		Escalate	Escalation	Escalated
Review	Reviewer	**Review Reject**	In Progress	Review Rejected
		Review Close	Closed	Closed
Escalation	Business owner	**Send for Escalation Review**	Escalation Review	Escalation Review
		De-escalate	In Progress	De-escalated
Escalation Review	Reviewer	**Escalation Review Close**	Closed	Escalated and Closed
		Escalation Review Reject	Escalation	Escalation Review Rejected
Closed	None	**Re-open**	In Progress	Reopened

Lifecycle triggers added in version 7.2.0.1 (legacy)

Following enablement of the 7.2 lifecycle feature in OpenPages, any object that uses the new lifecycle and has a preexisting lifecycle must be modified to use the new lifecycle field groups and fields.

These triggers are not enabled in fresh installations.

Triggers provide the transitions that move issues through an investigation lifecycle. Lifecycles define the stages that an object type can follow.

OpenPages Version 7.2.0.1 introduces three new lifecycles; controls, issues, and loss events. In 8.1.0 the issue triggers were deprecated and functionality moved to GRC Workflow.

For more information about control triggers, see "Control lifecycle triggers" on page 85.

Loss events had existing triggers to assist with the existing lifecycle of the objects, and these triggers are updated to use the new lifecycle fields. If you are using these triggers in versions earlier than OpenPages Version 7.2.0.1, you must modify the appropriate fields that were previously used for the loss event triggers in the openpages-solutions.xml file.

Before OpenPages Version 7.2.0.1, a trigger existed for Loss Event objects to verify the date fields and to populate the approver fields on the loss event at the time the user set the **OPSS-LossEv:Submit** field to **Yes**. As of OpenPages Version 7.2.0.1 and later, this trigger now fires on the lifecycle transition from

Open to Submit, so the trigger now fires on the field **OPLC-Std:LCTransition** with a value of **Submit**. The **OPSS-LossEv:Submit** field on the loss event is now redundant.

A second trigger existed to lock the loss event and its children upon closure. Before OpenPages Version 7.2.0.1, this trigger was fired on the field **OPLC-LossEv:Status** with a value of **Approved**. As of OpenPages Version 7.2.0.1 and later, this trigger now fires on the **OPLC-Std:LCStage** field with a value of **Closed**.

For more information, see "Loss Event lifecycle triggers (version 7.2.0.1 and later) (legacy)" on page 137.

Existing custom client solutions that have triggers, field dependencies, pick lists, or reports that use fields that are connected to the existing lifecycle of the objects must be reviewed and updated. Where necessary, fields to be replaced on the object (such as the **Status** or **Assignee** fields) must be updated in the configuration for the existing solution.

Lifecycle configuration (legacy)

In IBM OpenPages with Watson, lifecycles can be configured to reduce the need to implement business logic through custom triggers.

Lifecycle can be configured to set field values during a transition on fields other than the LC fields. These fields can be short or long text, single and multiple enumerated, Boolean, integer, decimal, date, user, and user group field types. Depending upon the field type, the field values can be set in the following ways:

- as an absolute or relative value
- as an addition to an existing value in the field
- populated based upon a value in another field

For example, this could be used to copy the lifecycle Status field value to the "normal" status field, so that existing views, reports and helpers can continue to use that status field value.

Lifecycle can also be configured with conditional logic to gate transitions. You can use Boolean logic using field values on the object and on immediate child and parent objects. The logic can include values from text, single and multiple enumerated, Boolean, integer, decimal, and date field types. For example, this could be used to prohibit submitting a Loss Event for approval if it does not have a recognition Date value. If the conditions are not met, then the transition processing is stopped and an error is displayed in the user interface, and recorded in the log.

For more information on how to configure lifecycles, see the *Trigger Developer Guide*.

RCSA Quantitative and RCSA Qualitative triggers (legacy)

The Risk Assessments process is used to identify, assess, and quantify a risk profile of a business. Each Risk is assessed on either a Qualitative or Quantitative basis.

Note: The RCSA Quantitative and RCSA Qualitative triggers are not enabled in fresh installations. They have been replaced by functionality that is available in the GRC Workflow and GRC Calculations features. See "Risk and Control Self-assessments (triggers and calculations)" on page 84.

RCSA Quantitative trigger

The Risk and Control Self-assessments (RCSA) Quantitative trigger sets the Risk Rating and establishes impact, likelihood, and exposure for risks that are entered with the Quantitative method. The trigger occurs only if the values for the **Impact** or **Likelihood** fields for **Risk** were modified.

Important: Determine if you want to assess risks using a quantitative or qualitative approach. This trigger does not apply if you use the qualitative approach. The option for quantitative or qualitative is set during the installation of IBM OpenPages with Watson solutions.

When a Risk object is updated, associated, or disassociated, the trigger completes the following actions:

- Obtains the parent Preference object.

The trigger attempts to find the Preference object associated with the Business Entity. The trigger traverses up the parent Entity hierarchy until a Preference object that is associated with a Business Entity is found. The preference object contains the settings for required parameters as described in the Severity table.

- Determines the Impact fields of the Risk object.

The Impact is calculated by identifying the threshold range in which the Severity Value falls. If any Severity value is null, the previous value is managed as the MAX Severity.

Table 43. Impact value based on severity value	
Severity value	**Impact value**
>= 0 and <= Severity 1	1
> Severity 1 and <= Severity 2	2
> Severity 2 and <= Severity 3	3
> Severity 3 and <= to Severity 4	4
> Severity 4 and <= Severity 5	5
> Severity 5 and <= Severity 6	6
> Severity 6 and <= Severity 7	7
> Severity 7 and<= Severity 8	8
> Severity 8 and <= Severity 9	9
> Severity 9	10

- Determines the **Likelihood** fields on the Risk object.

The Likelihood field is calculated by identifying the threshold range in which the Frequency value falls. If any Frequency value is null, the previous value is managed as the MAX frequency.

Table 44. Likelihood value based on frequency value	
Frequency value	**Likelihood value**
>= 0 and <= Frequency 1	1
> Frequency 1 and <= Frequency 2	2
> Frequency 2 and <= Frequency 3	3
> Frequency 3 and <= Frequency 4	4
> Frequency 4 and <= Frequency 5	5
> Frequency 5 and <= Frequency 6	6
> Frequency 6 and <= Frequency 7	7
> Frequency 7 and <= Frequency 8	8

Table 44. Likelihood value based on frequency value (continued)	
Frequency value	**Likelihood value**
> Frequency 8 and <= Frequency 9	9
> Frequency 9	10

- Calculates the Exposure by multiplying Severity by Frequency
- Where the Impact value is *X* and the Likelihood value is *Y*:

  The XMAX value is the maximum value for impact. The YMAX value is the maximum value for likelihood.

  The XMAX and YMAX settings are available at `/OpenPages/Application/GRCM/ORM/Triggers/RCSA/XMAX` and `/OpenPages/Application/GRCM/ORM/Triggers/RCSA/YMAX`.

  The XMAX and YMAX values are defined during installation. Do not change these values. If these values are changed, the RCSA Qualitative and Quantitative triggers might not correctly compute the risk rating.

  The trigger computes the Risk Rating by using the following formula:

  `((X x X) + (Y x Y)) / ((Xmax x Xmax) + (Ymax x Ymax))`

  The rating value is `0 - 1` and expressed as a percentage.

Table 45. Risk ratings based on rating values	
Rating value	**Risk rating**
0 - 25 %	LOW (green)
26-50 %	MEDIUM (yellow)
51-75 %	HIGH (orange)
76-100 %	VERY HIGH (red)

RCSA Qualitative trigger

The Risk and Control Self-assessments (RCSA) Qualitative trigger sets the Risk Rating and establishes severity, frequency, and exposure for risks that are entered with the Qualitative method.

Important: Determine the method to use to assess risks: quantitative or qualitative. If you chose quantitative, this trigger does not apply. The option for quantitative or qualitative is set during the installation of IBM OpenPages with Watson solutions.

Add the Assessment Method field to Task Views for Risk. The value in this field determines whether the Qualitative or Quantitative method is triggered.

When a **Risk** object is updated, associated, or disassociated, the trigger completes the following actions:

- Evaluates the Preference record for the entity, or its parent entity if no Preference record exists.

  The trigger attempts to find the Preference object associated with the business entity. The trigger traverses up the parent Entity hierarchy until a Preference object that is associated with a business entity is found. The preference object contains the settings for required parameters as described in the Severity table.

- Evaluates the **Severity** fields of the Risk object.

  Severity is determined by the Impact Value mappings that are specified in the Risk object. For example, if the Risk object impact value is 1, the Risk is 1. If the impact value is 2, the Severity is 2, and so on. The maximum impact value for a Risk object is 10, for which the Severity is 10.

- Based on the Likelihood, evaluates the Frequency fields of the Risk object.

The Frequency is determined by the Likelihood Value mappings that are specified in the Risk object. For example, if the Risk object likelihood value is 1, the Frequency is 1. If the likelihood value is 2, the Frequency is 2, and so on. The maximum likelihood value for a Risk object is 10, for which the Frequency is 10.

- Calculates the Exposure as Severity multiplied by Frequency.
- Where the Impact value is *X*, Likelihood value is *Y*:

The XMAX value is the maximum value for impact. The YMAX value is the maximum value for likelihood.

The XMAX and YMAX settings are available at `/OpenPages/Application/GRCM/ORM/Triggers/ RCSA/XMAX` and `/OpenPages/Application/GRCM/ORM/Triggers/RCSA/YMAX`.

The XMAX and YMAX values are defined during installation. Do not change these values. If these values are changed, the RCSA Qualitative and Quantitative triggers might not correctly compute the risk rating.

The trigger computes the Risk Rating using the following formula:

`((X x X) + (Y x Y)) / ((Xmax x Xmax) + (Ymax x Ymax))`

The rating value is `0  -  1` and expressed as a percentage.

Table 46. Risk ratings based on rating values	
Rating value	**Risk rating**
0 - 25 %	LOW (green)
26-50 %	MEDIUM (yellow)
51-75 %	HIGH (orange)
76-100 %	VERY HIGH (red)

KRI and KPI Lifecycle triggers (legacy)

The KRI and KPI Lifecycle triggers calculate and maintain field values on the KRI/KPI and KRI/KPI Value object types.

Note: If you're using the KRI and KPI Lifecycle triggers, consider using the KRI and KPI workflows instead. For more information, see "Sample workflows" on page 105.

The KRI or KPI Lifecycle trigger runs only if the **Collection Status** of the KRI or KPI value is set to **Collected**, and the **Value** and **Value Date** fields are not blank.

When a KRI or KPI Value object is updated, associated, or disassociated, the trigger completes the following steps:

1. Determines whether KRI or KPI is set for approval.

   - If the status is **Yes**, the trigger updates the status to **Awaiting Approval** and proceeds with steps 2, 3, 4, and 6.
   - If the status is **No**, the trigger updates the status from **Awaiting Collection** to **Collected** and proceeds with steps 2, 3, 4, and 5.

2. Copies the current threshold information from the KRI or KPI to the child KRI or KPI Value.

3. Evaluates the Breach status.

4. Copies the KRI or KPI **Value**, **Value Date**, **Collection**, and **Breach** status to the parent KRI or KPI.

5. If the status of the KRI or KPI **Breach** field changed from **Green** or **Amber** to **Red**, the trigger sends an email notification to the Risk Owner to inform the owner of the breach.

6. If the status is set to **Awaiting Approval**, the KRI or KPI Value is displayed on the dashboard of the KRI or KPI Owner. The KRI or KPI Owner can approve or reject the value:

- If the KRI or KPI Owner saves the record with a **Reject** status, the KRI or KPI **Value**, **Value Date**, and the **Approve / Reject** field are changed to a blank and the KRI or KPI Value status is set to **Awaiting Collection**.
- If the KRI or KPI Owner saves the record with an **Approved** status, the **Collection** status changes to **Collected** on the **Value** field and on the KRI or KPI.

Note: When the KRI or KPI owner defines the KRI or KPI, the owner can specify the details regarding its approval.

Legacy object types

The IBM OpenPages with Watson solutions include several object types that are not enabled in fresh installations.

Capital Model
The Capital Model object is used to store operational risk capital modeling results derived by using the advanced measurement approach (AMA).

Capital Model Result (ModelResult)
The Capital Model Result object is the resulting operational risk capital estimate or the aggregate loss distribution that results from the simulation of the selected best fit frequency and severity distributions. Each Capital Model Result is associated to a Capital Model object. For Single Models (Scenario Model, Internal Loss Model, FIRST Loss Model) Individual Value at Risk (VaR) capital is displayed at varying percentiles (the number and value of percentiles can be configured). For Independent and Correlated Models, capital is displayed for Individual VaR, Additive ESF (Expected Shortfall), and Additive VaR at varying percentiles (the number and value of percentiles can be configured).

Questionnaire, Section, Question
Questionnaire, Section, and Question objects are used together to implement questionnaires. Questionnaires are created as templates in a library and gather information from respondents. Section objects are children of parent Questionnaire objects and organize sets of related questions. Question objects are children of Section objects and capture respondent data. Business administrators use the Questionnaire Set Up Activity View to configure questionnaire templates. Questionnaire templates are then copied to parent Business Entity, Process, Sub-Process, or Employee object types.

Questionnaires are not related to questionnaire assessments. Information that describes questionnaires does not apply to questionnaire assessments.

Milestone, Milestone Action Item
A Milestone represents a significant point in the development of your project. You can tie Milestones to specific dates, or use them to signify the completion of a portion of the entire project. Milestones can contain other Milestones or Milestone Action Items. You cannot associate a Milestone with other objects in the object hierarchy.

A Milestone Action Item is a specific objective that must be completed to reach a Milestone. In general, all Milestone Action Items that are associated with a Milestone must be completed to reach a Milestone. When you are assigned a Milestone Action Item object, it is displayed (if configured) in the My Milestone Action Items section of your My Work tab.

Legacy reports and helpers

The reports that are available in IBM OpenPages with Watson solutions have changed.

KRI Value Creation utility
This helper has been replaced by calculations and workflows.

KRI Value Creation utility
This helper has been replaced by calculations and workflows.

Scenario Completion helper
This helper has been replaced by calculations and workflows.

Testing reports

- The Testing Dashboard report has been replaced by the Testing Performance and Results report
- The Testing Dashboard Details report has been replaced by the Testing Details report

For more information, see "Testing reports" on page 74.

Loss Event reports

The following reports have been replaced by the Consolidated Loss Event Dashboard and its detail reports:

- Loss Event Dashboard
- Loss Event Dashboard Detail
- Loss Event Summary
- Loss Event Detail
- Loss Event Trend
- Loss Event Trend Detail

For more information, see "Loss Event reports" on page 74.

Capital Modeling reports

The following reports have been removed:

- Capital Contributions by Business Entity
- Capital Contributions by Risk Category
- Model Results Fragment

Legacy workflows and calculations

The IBM OpenPages with Watson solutions include several workflows and calculations that are not enabled in fresh installations.

OpenScale Update Metric Last Value Info workflow

The OpenScale Update Metric Last Value Info workflow supports the integration of MRG with IBM Watson OpenScale. It updates the Metric Last Value Information fields on Metric objects for IBM Watson OpenScale models with values from the most recent Metric Value object that IBM Watson OpenScale sent to OpenPages. The workflow updates the following four fields on the Metric object:

- Breach Status
- Collection Status
- Value
- Value Date

The Metric Value Update calculation replaces the OpenScale Update Metric Last Value Info workflow.

Business Impact Analysis to Determine Critical Processes

This workflow moves the Business Impact Analysis (BIA) through a review and approval process. A calculation on the BIA object is required to move it to the approval phase. After approval, two of the resulting values of the calculation, Impact Tier and Maximum Acceptable Outage, are saved on the Process parent of the BIA object.

This workflow is disabled in fresh installations. A set of BIA workflows replaces the Business Impact Analysis to Determine Critical Processes workflow.

Policy Review workflow (PCM)

This workflow is designed to advance a Policy object through a policy review and approval process. A Policy Review Comment (PRC) object is created by each action prior to the review stages (SME, executive, and final) and associated with the Policy in review. The PRC captures the comments and approvals for each reviewer. The executive review is optional, depending on whether the policy changes are substantive.

This workflow is replaced by the Policy Review and Approval Workflow.

Model Development and Documentation workflow

This workflow takes a model from the completion of the candidate process through to approval for deployment. It consists of four stages and multiple sub-workflows that involve various stakeholders:

- Definition and planning (model owner)
- Development and documentation (model developer)
- Pre-implementation review (model validation)
- Approval (head of model development)

This workflow is replaced by the Model Lifecycle workflow.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Location Code IE9
Tower 3
900 Chelmsford Street

Lowell, MA 01851-5114
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Copyright

Trademarks

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

S

supply chain [13](#)
sustainability [13](#)

T

third-party risk [13](#)
TPRM
    workflows [134](#)
triggers
    control lifecycle [85](#)
    Incidents [141](#)
    KRI Lifecycle [146](#)
    loss event lifecycle [137](#)
    Questionnaire assessments [140](#)
    updating lifecycle [142](#)

U

updating lifecycle triggers [142](#)

W

what's new [15](#)