metricstream

Arno Release | SPRING '21

IT and Cyber Risk Management

User Guide

Copyright Notices

Written and designed at MetricStream, Inc., 6201 America Center Drive, Suite 240, San Jose, CA 95002, U.S.A.

Printed in the U.S.A.

Contents

Overview

The IT-Risk Management product Guide gives you a simple overview of the navigation within the **IT-Risk Management product**, the most common functionalities and some reference guidelines which you can use while working on the product.

This guide is intended for IT-Risk Managers, IT-Risk Analysts and IT - Risk Assessors who can use this as a reference document while working on the product.

The product provides a configurable framework that enables Information Security Groups to adopt a business-driven approach to manage information security and information technology risks. It also, helps in identifying, assessing, and treating information security risks on business critical processes, information technology assets and applications.

The product provides capability to document the Risks, defining and managing mitigating controls, performing multi-dimensional risk assessments, identifying issues, and implementing recommendations and remediation plans along with powerful analytics, dashboards and reporting.

Sections:

- Key Components
- Module-level User Guide

Key Components

The following figure illustrates the key components of the IT-Risk Management product.

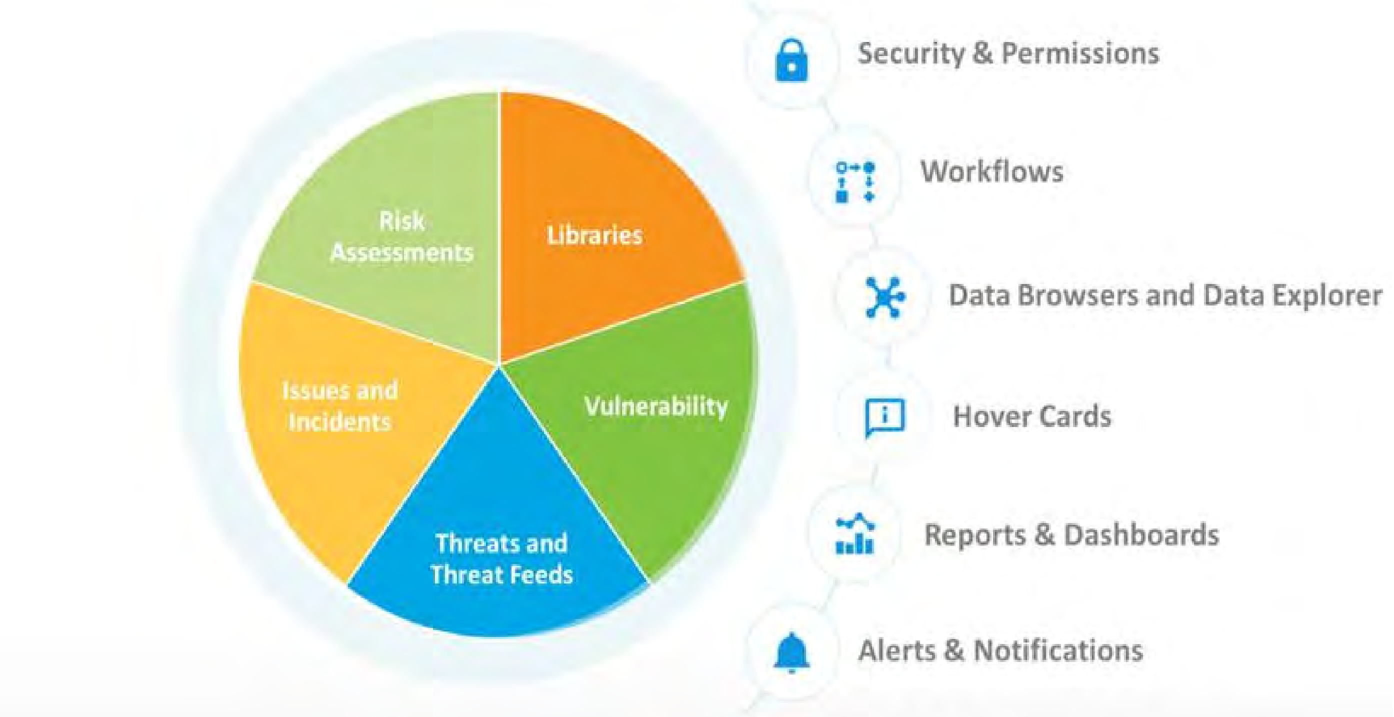


Figure 1 IT-Risk Management Key Components

The key components help organizations identify, record, manage, and assess risks as well as to take appropriate actions to keep risk under control. The following table describes the key components of the IT-Risk Management product

Key Component	Description
Issues	Logs findings/issues that are raised during Risk assessments and implements relevant actions to remediate the possible issues.
Libraries	Hosts the library contents such as Risks, Controls, Assets, Asset Classes, and Processes related to IT- Risk. With Libraries, you can manage all framework library contents that are required for managing the IT-Risk .
Risk Assessments	Provides a centralized risk framework to document, manage, and assess IT-risks faced by an organization. With Risk Assessments, you can keep your organizations up-to-date with business changes and provide mechanisms to evaluate the changes against the evolving threat landscape, emerging trends, and new technologies. It also provides valuable information to help organizations to decide, whether additional controls are necessary to protect sensitive data and other important business assets.
Threat and Threat Feeds	Gains the insight into the list of threats. Ability to capture adhoc threat alert details, threats and their actors. Also, configure channels, subscriptions, remediation templates and remediation rules.
Vulnerability	Gains the insight into the list of vulnerabilities. Ability to capture vulnerability details to identify the severity and their exposure level.

Module-level User Guide

Click the respective links in the following table to open the component-level user guides.

Guide	Read this guide to...
Governance, Risk, and Compliance Foundation User Guide	Know about the list of GRC library types, general approval workflow of the GRC library items, form-level details of each library type, and the GRC library-related reports.
Risk Assessment User Guide	Understand the risk assessment approach, approval workflow (Plan and assessment), risk assessment setup (Including form level details for perspective, quantitative factors, qualitative factors, scoring algorithm, risk assessment profile), details on how to create risk assessment plans, how to perform risk assessments, various assessment methods, heat maps, reports, and charts.
Issues User Guide	Learn the issues workflow, know the details on initiating and managing issues, implementing action plans, monitoring and closing issues, reopening and updating issues, bulk reassignment, data upload, reports, and charts.
Threat and Vulnerabilities User Guide	Learn the threat and vulnerability security model with the roles and privileges. Details on how to manage threats (capturing, editing and reviewing threat actor details and threat details). Also, details on managing the connectors dashboard (pulling in vulnerability assessments form external scanning tools).
GRC Intelligence User Guide	Understand the details on GRC intelligence process flow, channel, ad hoc alerts, channel group, channel subscription, subscribed content access, log issues, reports, and charts.
IT and Cyber Risk User Guide	Learn the quantifiable risk assessments, know the details on assessing IT risks against threats, vulnerabilities, and how to specify the scope of the assessment.
Surveys User Guide	Know about the questionnaire approval workflow, setting up, working on, and approving questionnaire, setting up tabular response templates, uploading questionnaire, creating survey/score card/ certification, reassigning surveys, survey responses and approvals, scoring logic, reports, and charts.
IT and Cyber Risk Management Reports Guide	Know about the list of all the IT-Risk reports with their filters and columns described.

Note: If the preceding links are not accessible on browser, download and open this PDF guide in Adobe Acrobat.

Security Model

The **IT-Risk Management** product operates based on the access rights of users.

The security model structure is defined when you:

- Create roles and assign infocenters and activities to the roles, as required
- Create organization structure and organization-role pair
- Assign users to organization-role pair

Note: Contact your system administrator to perform the above mentioned actions.

Roles, Privileges, and Infocenters

The following table lists the different roles, privileges and related infocenters in the **IT-Risk Management** product.

Role	Privilege	Infocenter/Page
IT - Risk Manager	Review and approve: • Library contents • Risk Assessment plans • Risk assessments • Issues	• Overview • Qualitative Assessments • Threats • Vulnerabilities • Libraries • Issues • Setup
IT - Risk Analyst	Create, view, Review, and edit: • Library contents • Risk Assessment plans • Risk assessments • Issues	• Overview • Qualitative Assessments • Threats • Vulnerabilities • Libraries • Issues • Setup
IT - Risk Assessor	Perform and work on: • Risk assessments • Issue remediation	• Qualitative Assessments • Issues
ITGRC Administrator	Configure API users to create GRCF Libraries	• ITGRC Apps Administration o Setup
ITR LOB-Head	Review and approve: • Library contents • Risk Assessment plans • Risk assessments • Issues	• Overview • Qualitative Assessments • Threats • Vulnerabilities • Libraries • Issues

Role	Privilege	Infocenter/Page
ITR Cyber Risk Manager	Configure Parameter Categories GRC Approve GRC Object GRC Edit All GRC Objects GRC Edit Control Objective of Level 1 and Below GRC View All GRC Objects GRC View GRC Object GRCI Create GRC Libraries GRCI Create Log Issue GRCI Create Adhoc Alert GRCI Create Notify User GRCI Edit Channel GRCI Edit Notify User GRCI Edit Relate GRC Library GRCI View Channel GRCI View Subscription GRCI View Notify User GRCI View Relate GRC Library GRCI Create Subscription GRCI Content Access ICR Approve Risk Assessment ICR Approve Schedule ICR Assess Risks ICR Edit Assessment Type ICR Edit Profile ICR Edit Question API setup ICR Edit Risk Assessment Schedule by Initiator Org ICR Edit Risk Assessment Schedule by Assessor Org ICR Edit Risk Assessment Schedule by Approver Org ICR Edit Risk Assessment Schedule by Scoped Org ICR Edit Scope API setup ICR Initiate Assessment ICR View Question API setup ICR View Risk Assessment Schedule Initiator Org ICR View Risk Assessment Schedule by Assessor Org ICR View Risk Assessment Schedule Approver Org ICR View Risk Assessment Schedule by Scoped Org ICR View Risk Assessment by Approver Org ICR View Risk Assessment by Assessor Org	• Overview • Quantitative Assessments • Threats • Vulnerabilities • Libraries • Issues • Setup

Role	Privilege	Infocenter/Page
	ICR View Risk Assessment by Initiator Org ICR View Risk Assessment by Scoped Org ICR View Scope API setup ISM Approve Action ISM Approve Issue ISM Create Issue ISM Implement Action ISM Issue Owner ISM Reopen Closed Actions ISM Reopen Closed Issues ISM Review Action ISM Review Issue ISM Update Closed Actions ISM Update Closed Issues ISM View Issue By Issue Owner Organization ISM View Issue By Issue Approver Organization ISM View Issue By Related To Organization ITGRC Rest Service Call GRCI View Alters GRCI Create Channel GRCI Create Channel Group Manage Data Import Export QSM Approve Questionnaire QSM Manage Questionnaires QSM Setup Questionnaire QSM View Questionnaire TVM Configure Connectors TVM Edit Remediation Rules TVM Edit Remediation Templates TVM Approve Threat TVM Approve Threat Actor TVM Approve Vulnerability TVM Edit All Threat TVM Edit All Threat Actor TVM Edit All Vulnerability TVM View All Threat TVM View All Threat Actor TVM View All Vulnerability TVM View Threat TVM View Vulnerability	

Role	Privilege	Infocenter/Page
ITR Cyber Risk Analyst	Configure Parameter Categories GRC Edit Control Objective of Level 1 and Below GRC Edit GRC Object GRC View GRC Object GRCI Create GRC Libraries GRCI Create Log Issue GRCI Create Adhoc Alert GRCI Create Notify User GRCI Edit Channel GRCI Edit Notify User GRCI Edit Relate GRC Library GRCI View Channel GRCI View Subscription GRCI View Notify User GRCI View Relate GRC Library GRCI Create Subscription GRCI Content Access ICR Approve Risk Assessment ICR Assess Risks ICR Edit Assessment Type ICR Edit Profile ICR Edit Question API setup ICR Edit Risk Assessment Schedule by Initiator Org ICR Edit Risk Assessment Schedule by Assessor Org ICR Edit Risk Assessment Schedule by Approver Org ICR Edit Risk Assessment Schedule by Scoped Org ICR Edit Scope API setup ICR Initiate Assessment ICR View Question API setup ICR View Risk Assessment Schedule Initiator Org ICR View Risk Assessment Schedule by Assessor Org ICR View Risk Assessment Schedule Approver Org ICR View Risk Assessment Schedule by Scoped Org ICR View Risk Assessment by Approver Org ICR View Risk Assessment by Assessor Org ICR View Risk Assessment by Initiator Org	• Overview • Quantitative Assessments • Threats • Vulnerabilities • Libraries • Issues • Setup

Role	Privilege	Infocenter/Page
	ICR View Risk Assessment by Scoped Org ICR View Scope API setup ISM Approve Action ISM Approve Issue ISM Approver Comments ISM Create Issue ISM Implement Action ISM Issue Owner ISM Reopen Closed Actions ISM Reopen Closed Issues ISM Review Action ISM Review Issue ISM Update Closed Actions ISM Update Closed Issues ISM View Issue By Issue Owner Organization ISM View Issue By Issue Approver Organization ISM View Issue By Related To Organization ITGRC Rest Service Call GRCI View Alters GRCI Create Channel GRCI Create Channel Group Manage Data Import Export QSM Manage Questionnaires QSM Setup Questionnaire QSM View Questionnaire TVM Edit Remediation Rules TVM Edit Remediation Templates TVM Edit Threat TVM Edit Threat Actor TVM Edit Vulnerability TVM View Threat TVM View Threat Actor TVM View Vulnerability	

Role	Privilege	Infocenter/Page
ITR Cyber Risk Assessor	Configure Parameter Categories GRC View GRC Object ICR Assess Risks ICR View Profile ICR View Risk Assessment by Approver Org ICR View Risk Assessment by Assessor Org ICR View Risk Assessment by Initiator Org ICR View Risk Assessment by Scoped Org ISM Create Issue ISM Implement Action ISM Issue Owner ISM Review Action ISM Review Issue ISM View Issue By Issue Owner Organization ISM View Issue By Issue Approver Organization ISM View Issue By Related To Organization ITGRC Rest Service Call QSM View Questionnaire TVM View Threat	• Quantitative Assessments • Issues
ITR Cyber Risk Admin	Configure Parameter Categories GRC Edit GRC Object ICR Edit Assessment Type ICR Edit Profile ICR Edit Question API setup ICR Edit Scope API setup ICR View Question API setup ICR View Scope API setup ITGRC Rest Service Call ITGRC Configure GRC Libraries API Users Manage Data Import Export QSM Manage All Questionnaires QSM Setup Questionnaire QSM View All Questionnaire TVM Configure Connectors	• Setup

Role	Privilege	Infocenter/Page
ITR LOB Head	Configure Parameter Categories GRCI View Notify User GRCI View Relate GRC Library GRCI Content Access ICR Approve Risk Assessment ICR Approve Schedule ICR View All Risk Assessment Schedule ICR View Risk Assessment by Approver Org ICR View Risk Assessment by Assessor Org ICR View Risk Assessment by Initiator Org ICR View Risk Assessment by Scoped Org ISM View Issue By Issue Owner Organization ISM View Issue By Issue Approver Organization ISM View Issue By Related To Organization ITGRC Rest Service Call GRCI View Alters TVM View All Threat TVM View All Threat Actor TVM View All Vulnerability	• Overview • Quantitative Assessments • Threats • Vulnerabilities • Libraries • Issues

Note: The infocenter is referred to as 'page' throughout the document.

Infocenters

This chapter provides detailed information on landing pages and the components available in the landing pages of the **IT-Risk Management** product.

Sections:

- Product Home Page
- Overview
- Qualitative Assessments
- Quantitative Assessments
- Threats
- Vulnerabilities
- Libraries
- Issues
- Setup (ITGRC Apps Administrator)
- Setup (for other users)
- Setup (Quantitative Assessment)

Product Home Page

Product home page is a structured, user focused, default page that appears when you log on to the product. The home page can consist of metric cards, reports, and charts which give a quick overview on the tasks that you can perform.

The default components of the home page vary according to the role. You can customize your home page according to your requirement.

For information on customizing the home page, refer to the MetricStream Arno Release Spring ‘21 - Platform - User Guide.

The following page is a sample home page available to an **IT Risk Analyst**:

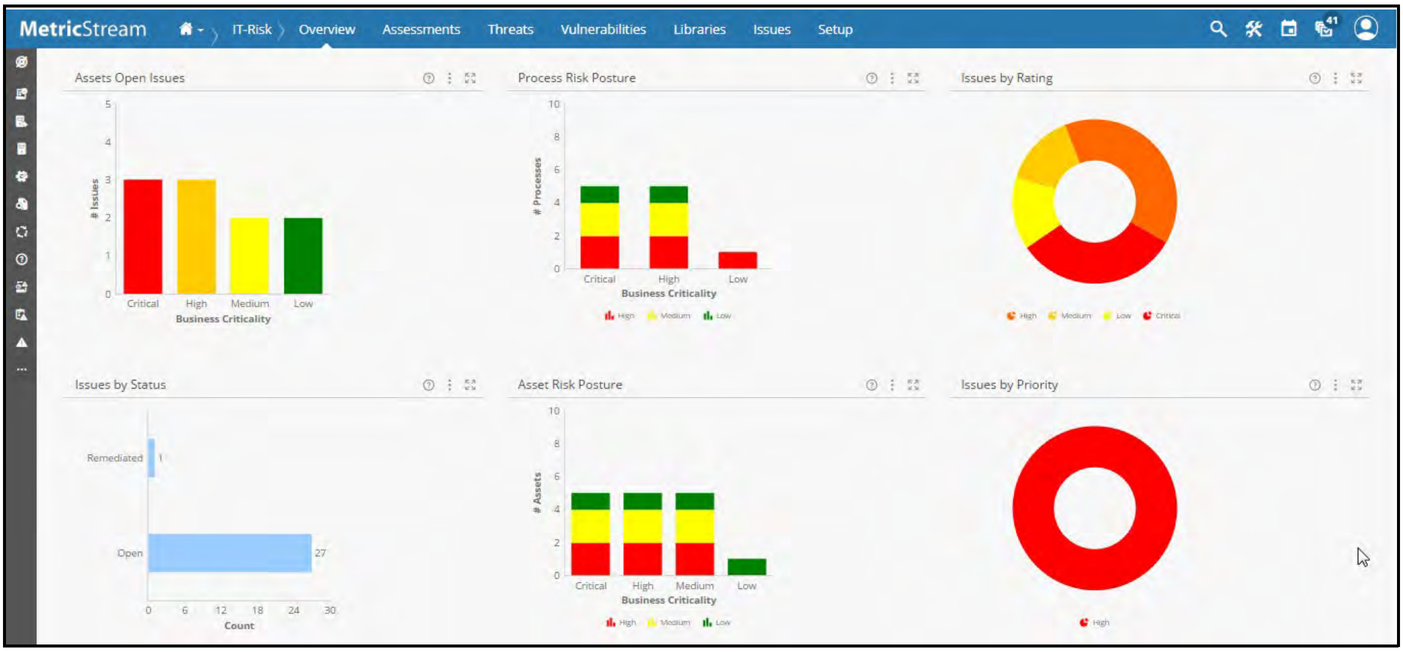


Figure 2 Product Home Page

Overview

The **Overview** page (infocenter) allows you to access reports that provide valuable risk insights and aggregated IT- Risk information on IT- Assets, IT - Processes, IT-Asset Classes, and Organizations. It also provides the enterprise-wide visibility into the IT-Risk management related details. The details in this page helps in identifying the potential opportunities for improvements.

The following **Overview** page is available for an IT - Risk Analyst. For more information on the role-infocenter/ privilege mapping, see Roles, Privileges, and Infocenters.

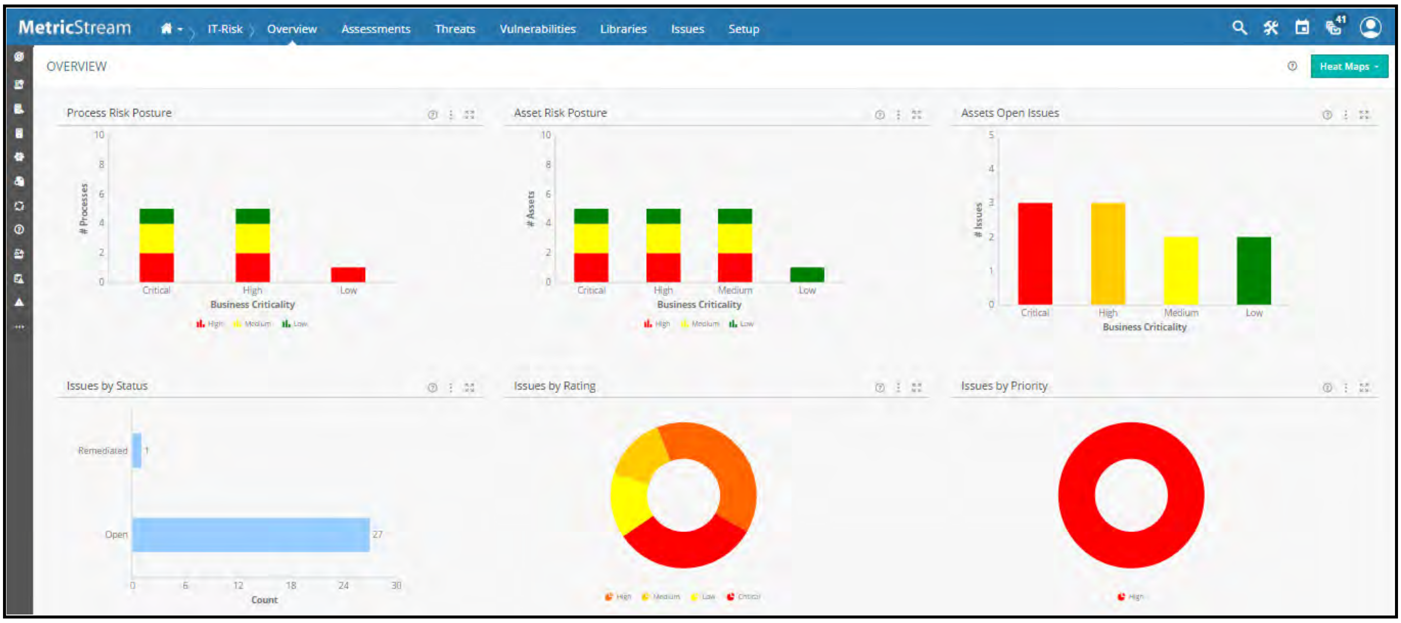


Figure 3 Overview Page

Heat Maps

Use the links within the **Heat Maps** drop-down list to access the heat map charts available in **IT- Risk Management** product, as shown in the following figure.

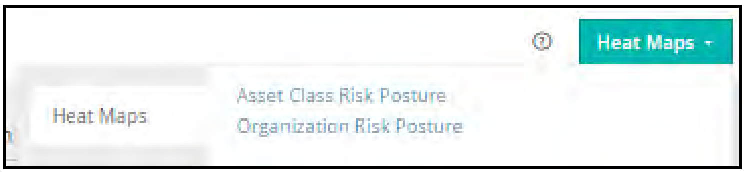


Figure 4 Heat Maps of Overview

You can access the following heat map reports:

- **Asset Class Risk Exposure**: Opens the **Asset Class Risk Posture Heat Map**. For more information on heat map, see Asset Class Risk Posture Heat Map.
- **Organization Risk Exposure**: Opens the **Organization Risk Posture Heat Map**. For more information on heat map, see Organization Risk Posture Heat Map.

Process Risk Posture Chart

The **Process Risk Posture** chart displays the summary of processes in the system that are risk assessed.

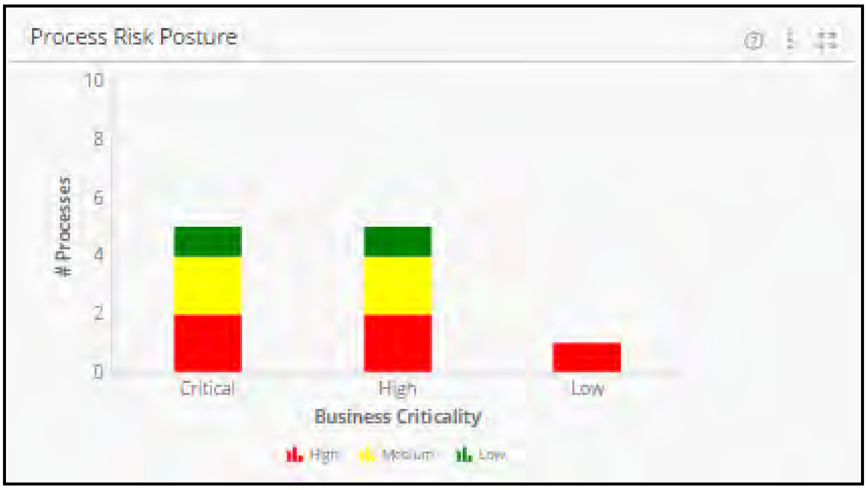


Figure 5 Process Risk Posture Chart

The hover number on a colored stack indicates the number of processes for that risk rating under the corresponding Business Criticality.

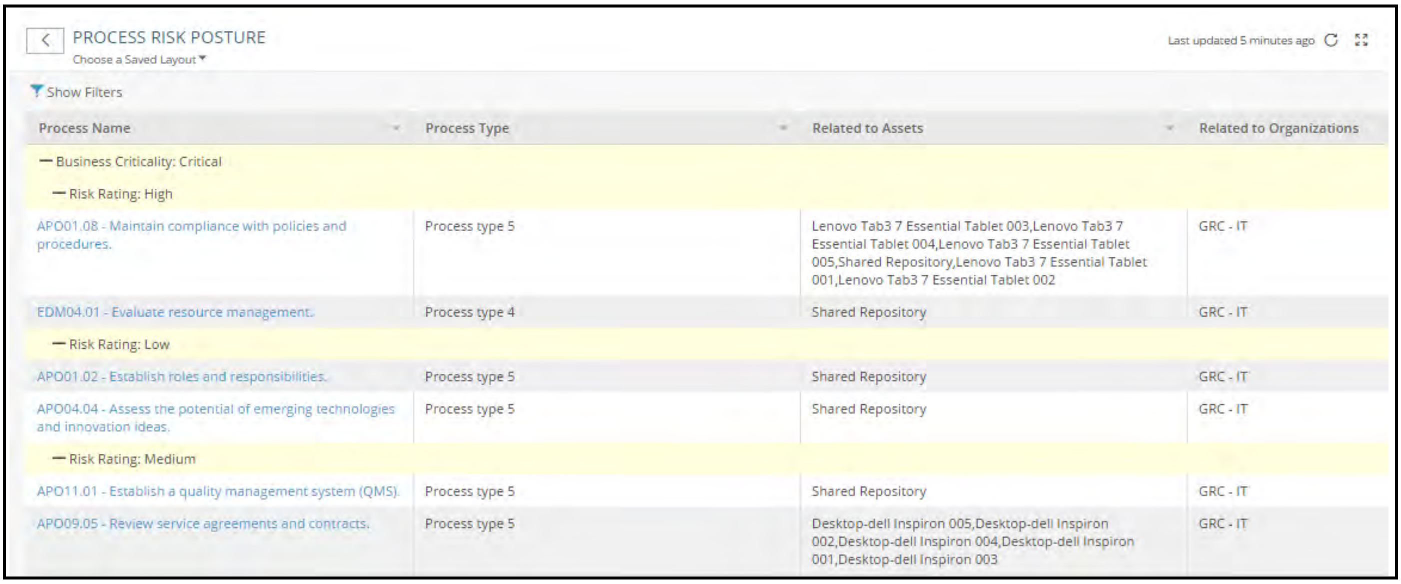
For example, when you hover over the red stack in **Critical** business criticality bar and it shows 2, then the number of processes with High risk rating is **2**. Similarly, when you hover on yellow and it shows 3, then the number of processes with Medium risk rating is **3**.

When you click any one of the colored stacks, the drill down Process Risk Posture Report opens. It displays a combined list of processes having different risk ratings and same Business Criticality.

Description	Drill Down
The bar chart illustrates the following: • X-axis: Represents the Business criticality of Process • Y-axis: Represents the count of processes The following are the stack details: • High: Number of processes rated high for a process criticality • Medium: Number of processes rated medium for a process criticality • Low: Number of processes rated low for a process criticality	Process Risk Posture Report

Process Risk Posture Report

The **Process Risk Posture** report is a drill down of the **Process Risk Posture** chart. This report displays the combined view of Business Criticality of a process and it's Risk Rating that allows you to identify the risky Processes. For example: A Process with Business Criticality = Low and Risk Rating = High is not as risky as a Process with Business Criticality = Critical and Risk Rating = High.



Process Name	Process Type	Related to Assets	Related to Organizations
— Business Criticality: Critical			
— Risk Rating: High			
APO01.08 - Maintain compliance with policies and procedures.	Process type 5	Lenovo Tab3 7 Essential Tablet 003,Lenovo Tab3 7 Essential Tablet 004,Lenovo Tab3 7 Essential Tablet 005,Shared Repository,Lenovo Tab3 7 Essential Tablet 001,Lenovo Tab3 7 Essential Tablet 002	GRC - IT
EDM04.01 - Evaluate resource management.	Process type 4	Shared Repository	GRC - IT
— Risk Rating: Low			
APO01.02 - Establish roles and responsibilities.	Process type 5	Shared Repository	GRC - IT
APO04.04 - Assess the potential of emerging technologies and innovation ideas.	Process type 5	Shared Repository	GRC - IT
— Risk Rating: Medium			
APO11.01 - Establish a quality management system (QMS).	Process type 5	Shared Repository	GRC - IT
APO09.05 - Review service agreements and contracts.	Process type 5	Desktop-dell Inspiron 005,Desktop-dell Inspiron 002,Desktop-dell Inspiron 004,Desktop-dell Inspiron 001,Desktop-dell Inspiron 003	GRC - IT

Figure 6 Process Risk Posture Report

Key Columns:

- **Process Name:** Displays the name of the process that is risk assessed.
  - Place the pointer on the name of the Process to view the hover card. Click the process name to view the details of the process.
  - You can also view the related processes and organization to which the process is mapped. Click Reports icon in the hover card and scroll down, to view all the related reports.
- **Related to Assets:** Displays the asset to which the risk assessed process is associated.
- **Related to Organizations:** Displays the organization to which the risk assessed process is associated.

Asset Risk Posture Chart

The **Asset Risk Posture** chart displays the summary of assets in the system that are risk assessed. The assets are identified based on the on the total number of assets within an asset class.

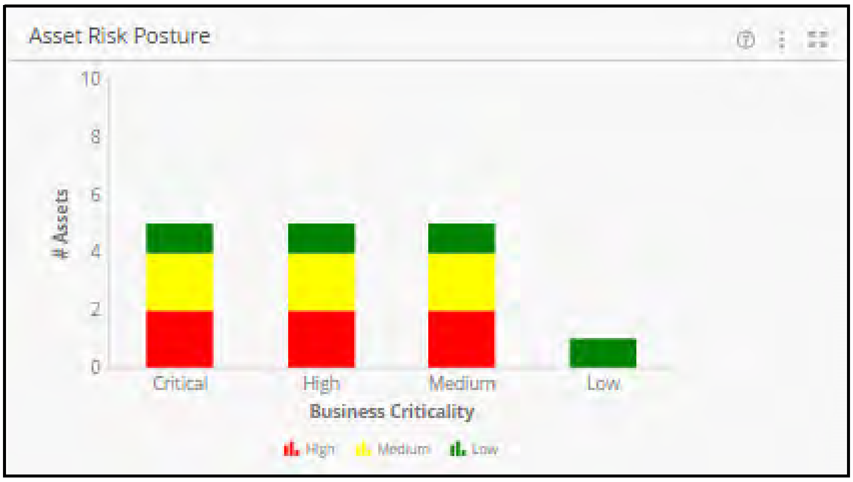


Figure 7 Asset Risk Posture Chart

The hover number on a colored stack indicates the number of assets for that risk rating under the corresponding Business Criticality.

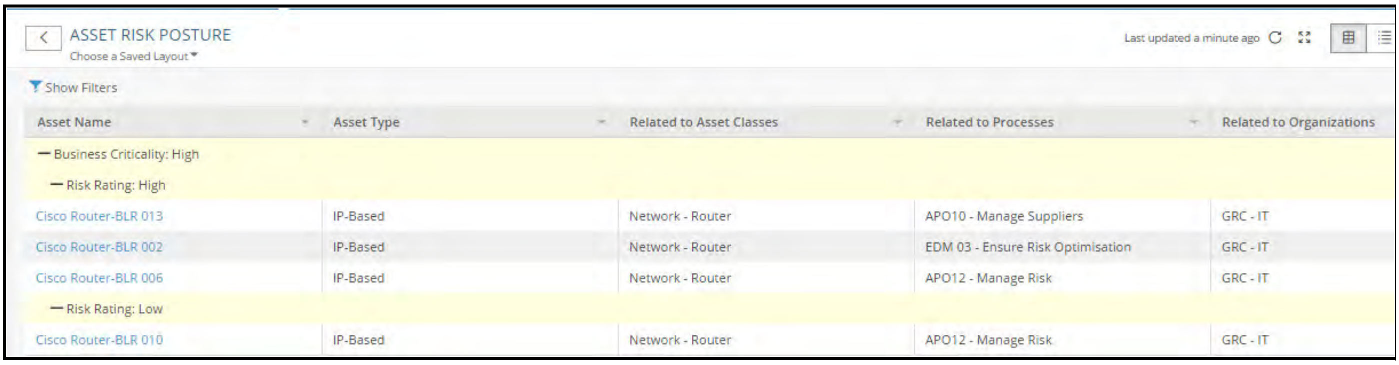
For example, when you hover over the red stack in **Critical** business criticality bar and it shows 2, then the number of assets with High risk rating is **2**. Similarly, when you hover on yellow and it shows 3, then the number of assets with Medium risk rating is **3**.

When you click any one of the colored stacks, the drill down Asset Risk Posture Report opens. It displays a combined list of assets having different risk ratings and same Business Criticality.

Description	Drill Down
The bar chart illustrates the following: • X-axis: Represents the Business criticality of asset • Y-axis: Represents the count of assets The following are the stack details: • High: Number of assets rated high for a business criticality • Medium: Number of assets rated medium for a business criticality • Low: Number of assets rated low for a business criticality	Asset Risk Posture Report

Asset Risk Posture Report

The **Asset Risk Posture** report is a drill down of the **Asset Risk Posture** chart. This report displays the combined view of Business Criticality of an Asset and its Risk Rating that allows you to identify the risky assets. For example, an Asset with Business Criticality = Low and Risk Rating = High is not as risky as an Asset with Business Criticality = Critical and Risk Rating = High.



ASSET RISK POSTURE

Choose a Saved Layout

Last updated a minute ago

Show Filters

Asset Name	Asset Type	Related to Asset Classes	Related to Processes	Related to Organizations
— Business Criticality: High				
— Risk Rating: High				
Cisco Router-BLR 013	IP-Based	Network - Router	APO10 - Manage Suppliers	GRC - IT
Cisco Router-BLR 002	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
Cisco Router-BLR 006	IP-Based	Network - Router	APO12 - Manage Risk	GRC - IT
— Risk Rating: Low				
Cisco Router-BLR 010	IP-Based	Network - Router	APO12 - Manage Risk	GRC - IT

Figure 8 Asset Risk Posture Report

Key Columns:

- **Asset Name:** Displays the name of the asset that is risk assessed.
  - Place the pointer on the name of the asset to view the hover card. Click the asset name to view the details of the asset.
  - You can also can view the related asset class and organization to which the asset belongs. Click 📄 in the hover card and scroll down, to view all the related reports.
- **Related to Asset Classes:** Displays the asset classes to which the risk assessed asset is associated.
- **Related to Organizations:** Displays the organization to which the risk assessed asset is associated.

Assets Open Issues Chart

The **Assets Open Issues** chart displays the summary of open issues against the assets in the system.

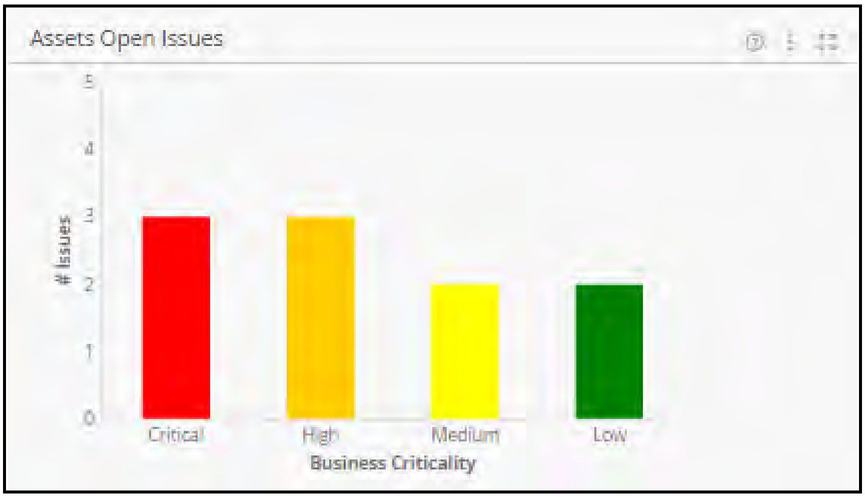
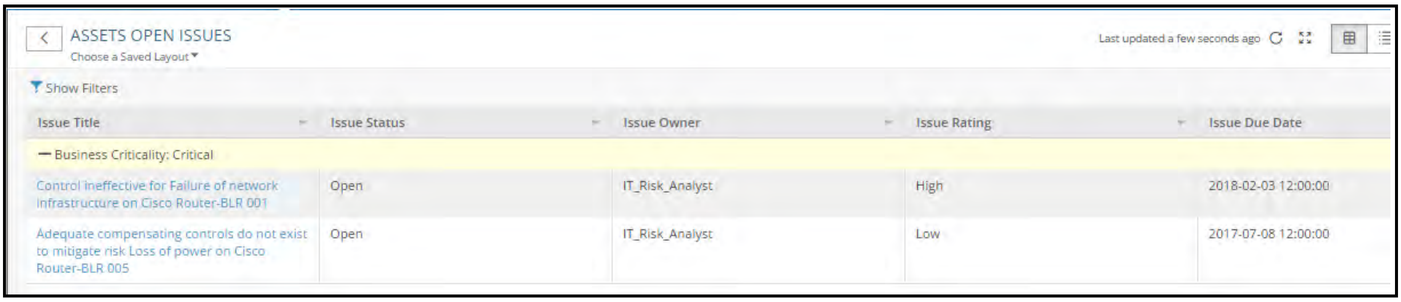


Figure 9 Assets Open Issues Chart

Description	Drill Down
The bar chart illustrates the following: • X-axis: Represents the Asset Business criticality • Y-axis: Represents the count of Issues The following are the stack details: • High: Number of issues open for an Asset business criticality which is rated high • Medium: Number of issues open for an Asset business criticality which is rated medium • Low: Number of issues open for an Asset business criticality which is rated low	Assets Open Issues Report

Assets Open Issues Report

The **Assets Open Issues** report is a drill down of the **Assets Open Issues** chart. This report displays the details of open issues against the asset.



Issue Title	Issue Status	Issue Owner	Issue Rating	Issue Due Date
— Business Criticality: Critical				
Control ineffective for Failure of network infrastructure on Cisco Router-BLR 001	Open	IT_Risk_Analyst	High	2018-02-03 12:00:00
Adequate compensating controls do not exist to mitigate risk Loss of power on Cisco Router-BLR 005	Open	IT_Risk_Analyst	Low	2017-07-08 12:00:00

Figure 10 Assets Open Issues Report

Key Columns:

- **Issue Title:** Displays the name of the issue. Place the pointer on the name of the Issue to view the hover card. Click the Issue Title to view the details of the Issue. Also, you can view the related Asset to which the issue is related.
  - Drill Down: **Issue** form.
- **Issue Due Date:** Displays the date by which the issue remediation is due.
- **Assets:** Displays the asset to which the issue is open.

Issues by Status Chart

The **Issues by Status** chart displays the number of issues in the system which are in different statuses.

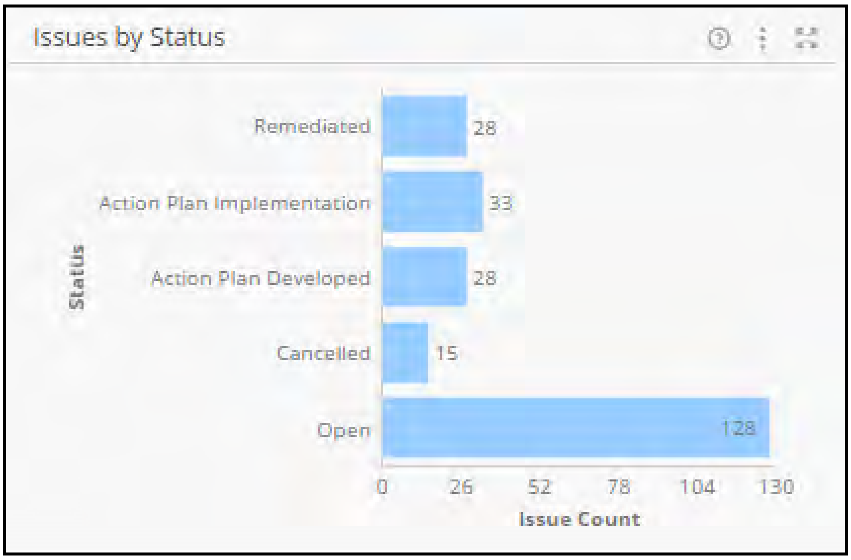


Figure 11 Issues by Status Chart

Description	Drill Down
The bar chart illustrates the following: • X-axis: Represents the status of the issue • Y-axis: Represents the number of issues	Issues Report For details, refer to the MetricStream Issues User Guide Release 7.0 SP1.

Issues by Rating Chart

The **Issues by Rating** chart displays the number of issues based on the issue rating.

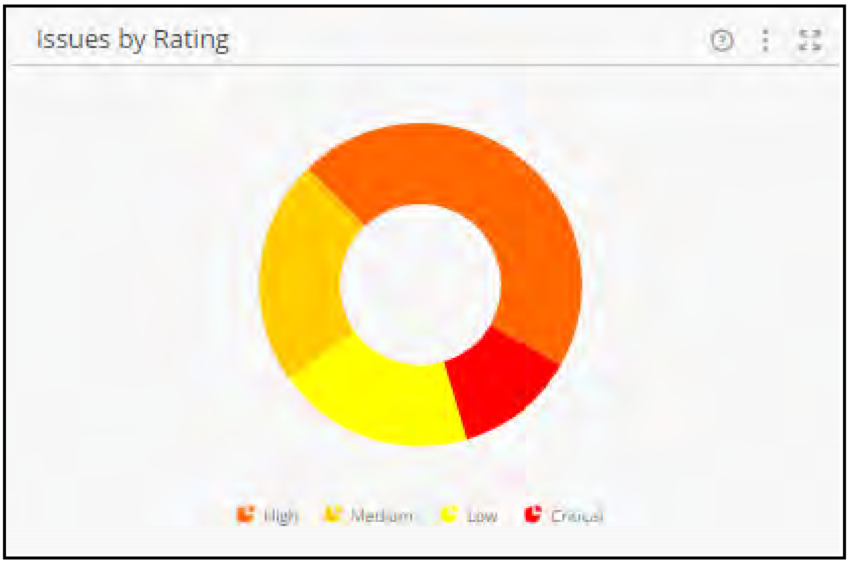


Figure 12 Issues by Rating Chart

Description	Drill Down
The pie chart illustrates the following: • High: Represents the number of issues rated high • Medium: Represents the number of issues rated medium • Low: Represents the number of issues rated low • Critical: Represents the number of issues rated critical **Notes:** - This chart displays all the issues that have passed through the manage issue stage. - The rating is considered for issues that are in the **Open** status. The status of the issue is termed as **Open** when it is any of the workflow stages other than **Closed** or **Canceled**.	Issues Report For details, refer to the MetricStream Issues User Guide Release 7.0 SP1.

Issues by Priority Chart

The **Issues by Priority** chart displays the number of open issues based on priority.

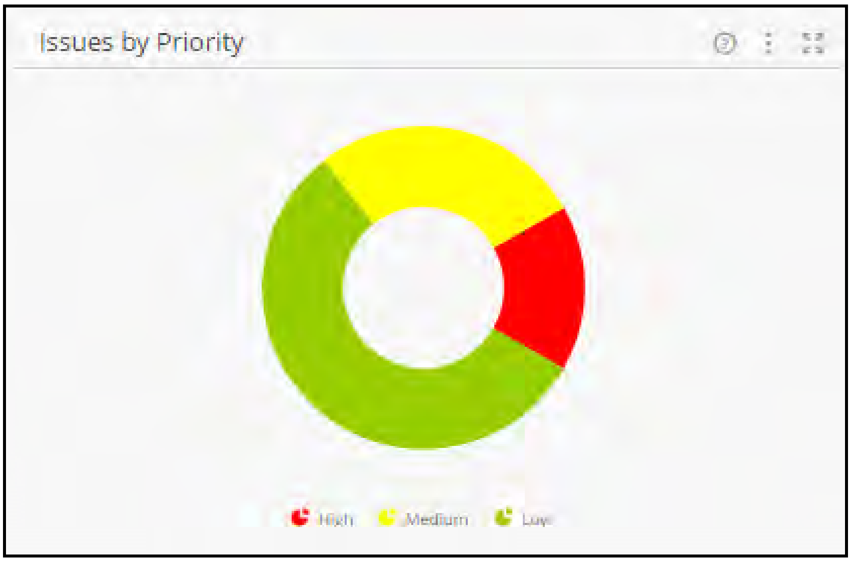
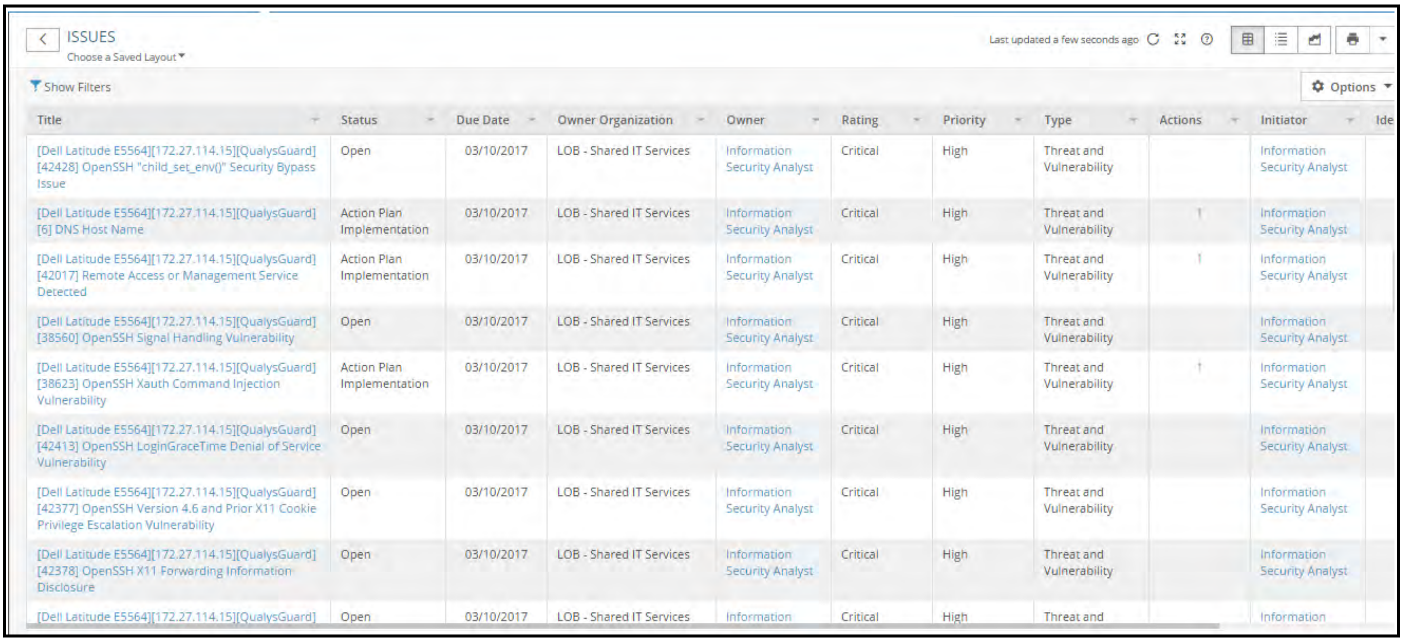


Figure 13 Issues by Priority Chart

Description	Drill Down
The pie chart illustrates the following: • High: Represents the number of open issues which are of high priority • Medium: Represents the number of open issues which are of medium priority • Low: Represents the number of open issues which are of low priority	Issues Report **Note:** For details, refer to the MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Issues Report

The **Issues** report displays the details of issues triggered in the system.



ISSUES

Choose a Saved Layout

Last updated a few seconds ago

Show Filters

Options

Title	Status	Due Date	Owner Organization	Owner	Rating	Priority	Type	Actions	Initiator	Ide
[Dell Latitude E5564][172.27.114.15][QualysGuard] [42428] OpenSSH "child_set_env()" Security Bypass Issue	Open	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability		Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [6] DNS Host Name	Action Plan Implementation	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability	1	Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [42017] Remote Access or Management Service Detected	Action Plan Implementation	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability	1	Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [38560] OpenSSH Signal Handling Vulnerability	Open	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability		Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [38623] OpenSSH Xauth Command Injection Vulnerability	Action Plan Implementation	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability	1	Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [42413] OpenSSH LoginGraceTime Denial of Service Vulnerability	Open	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability		Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [42377] OpenSSH Version 4.6 and Prior X11 Cookie Privilege Escalation Vulnerability	Open	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability		Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard] [42378] OpenSSH X11 Forwarding Information Disclosure	Open	03/10/2017	LOB - Shared IT Services	Information Security Analyst	Critical	High	Threat and Vulnerability		Information Security Analyst	
[Dell Latitude E5564][172.27.114.15][QualysGuard]	Open	03/10/2017	LOB - Shared IT Services	Information	Critical	High	Threat and		Information	

Figure 14 Issues Report

Key Columns:

- **Title:** Displays the title of the issue.
  - Drill Down: **Issue** form
- **Status:** Displays the status of the issue.
- **Owner:** Displays the name of the issue owner. Move the mouse pointer over this field to view the hover card.

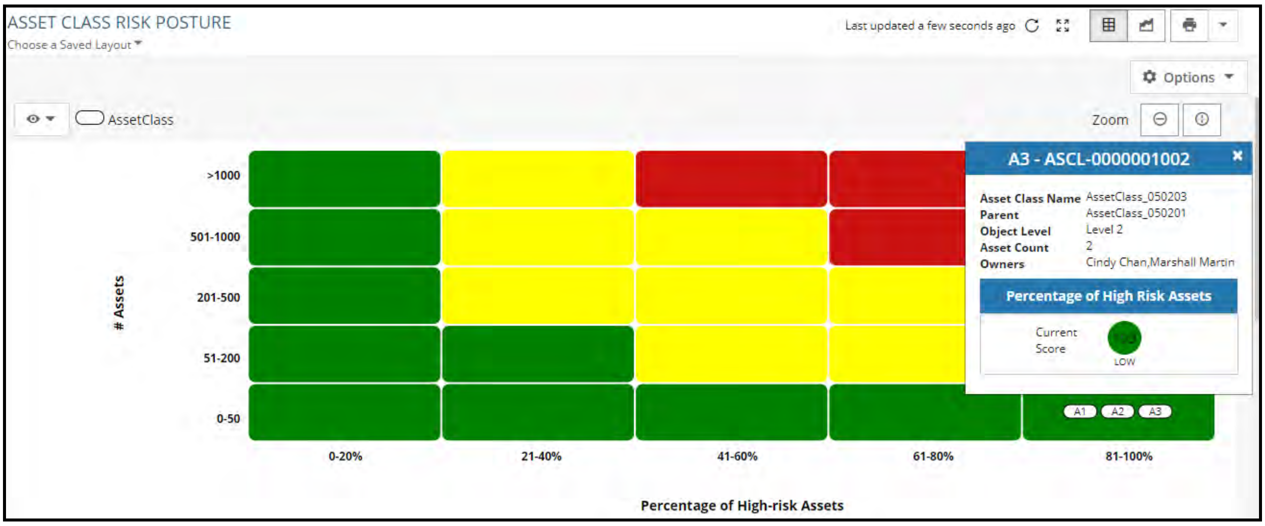
Note: For details, refer to the MetricStream Arno Release Spring ‘21 - GRC Foundation - User Guide.

- **No. of Actions:** Displays the number of actions associated with the issue.
  - Drill Down: **Actions** report

Note: For more details, refer to the MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Asset Class Risk Posture Heat Map

The **Asset Class Risk Posture Heat Map** chart displays risky asset classes which needs attention to mitigate the associated risks. The chart plots the asset classes based on the total number of assets within an asset class as well as the % of assets which has the same risk rating. For example, if an asset class contains 1% of its Assets in High Risk and this 1% is equal 1,000 Assets, then the IT Risk manager should pay attention to this type of risk and prioritize to mitigate the risk.



A3 - ASCL-0000001002

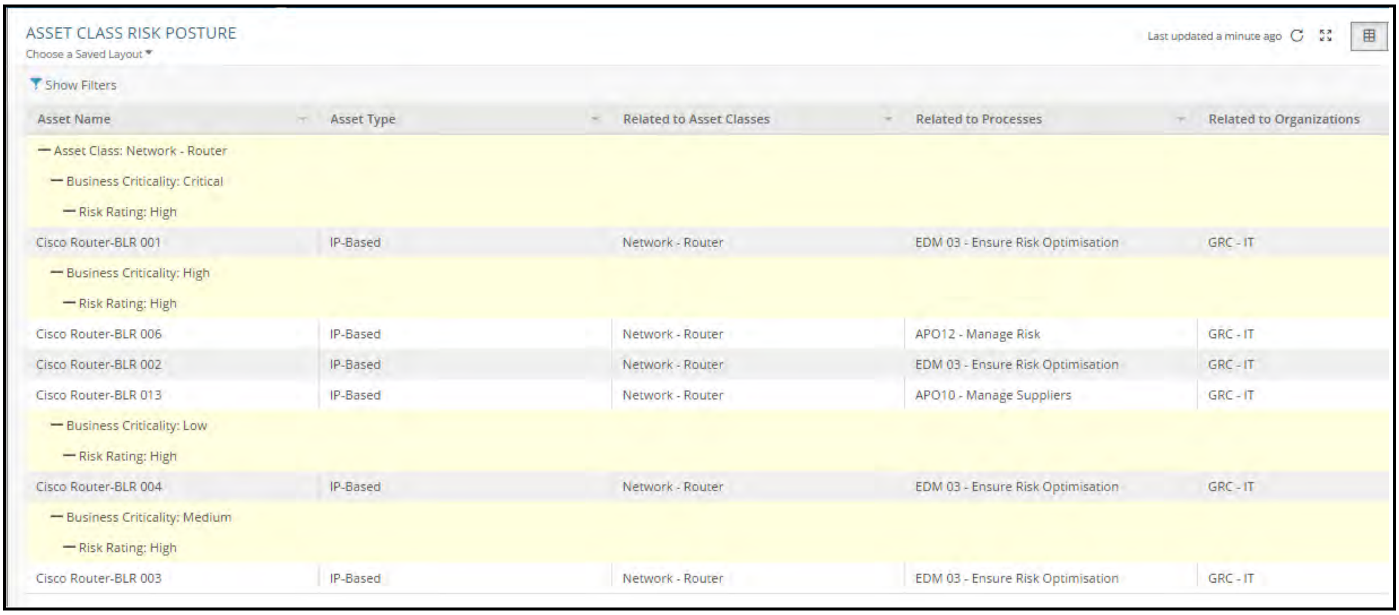
Asset Class Name AssetClass_050203
Parent AssetClass_050201
Object Level Level 2
Asset Count 2
Owners Cindy Chan,Marshall Martin

Figure 15 Asset Class Risk Posture Heat Map

Description	Drill Down
The heat map illustrates the following: • X-axis: Percentage of high risk assets • Y-axis: Count of assets	Asset Class Risk Posture Report

Asset Class Risk Posture Report

The **Asset Class Risk Posture** report is a drill down report of **Asset Class Risk Posture Heat Map** chart. This report displays the details of risky Asset classes by using the total number of Assets within an Asset class.



ASSET CLASS RISK POSTURE

Choose a Saved Layout

Last updated a minute ago

Show Filters

Asset Name	Asset Type	Related to Asset Classes	Related to Processes	Related to Organizations
— Asset Class: Network - Router				
— Business Criticality: Critical				
— Risk Rating: High				
Cisco Router-BLR 001	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
— Business Criticality: High				
— Risk Rating: High				
Cisco Router-BLR 006	IP-Based	Network - Router	APO12 - Manage Risk	GRC - IT
Cisco Router-BLR 002	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
Cisco Router-BLR 013	IP-Based	Network - Router	APO10 - Manage Suppliers	GRC - IT
— Business Criticality: Low				
— Risk Rating: High				
Cisco Router-BLR 004	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
— Business Criticality: Medium				
— Risk Rating: High				
Cisco Router-BLR 003	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT

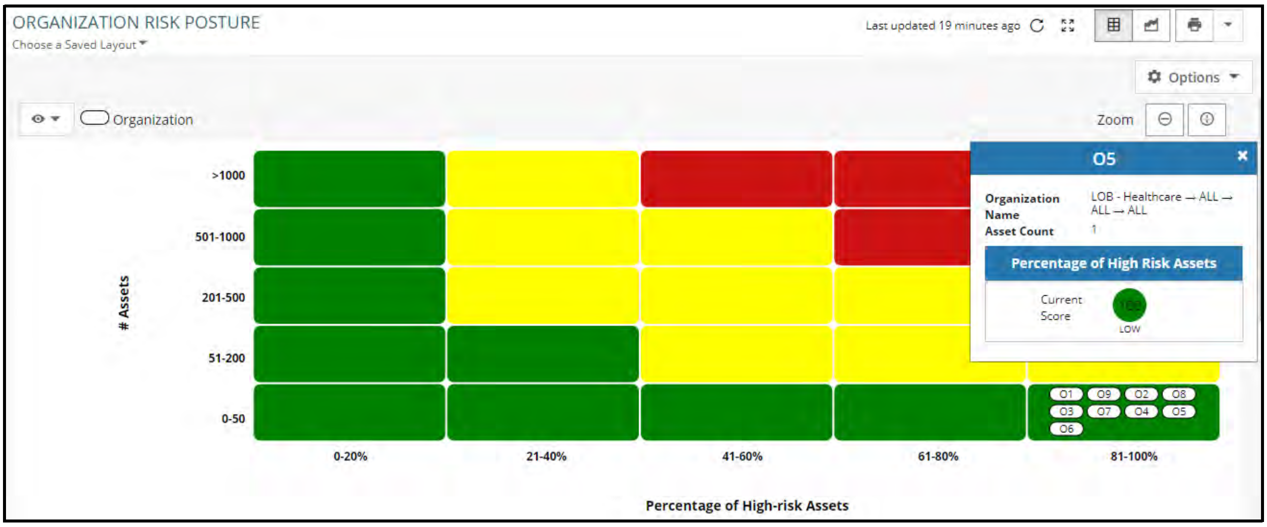
Figure 16 Asset Class Risk Posture Report

Key Columns:

- **Asset Name:** Displays the name of the asset which is risk assessed.
- **Related to Asset Classes:** Displays the asset classes to which the risk assessed asset is associated.
- **Related to Organizations:** Displays the organization to which the risk assessed asset is associated.

Organization Risk Posture Heat Map

The **Organization Risk Posture Heat Map** chart displays risky organizations which needs attention to mitigate the associated risks. The chart plots the organizations based on the total number of organizations related to an asset which has the same risk rating. For example, if an organization contains 1% of its Assets in High Risk and this 1% is equal 1,000 Assets, then the IT Risk manager should pay attention to this type of risk and prioritize to mitigate the risk.



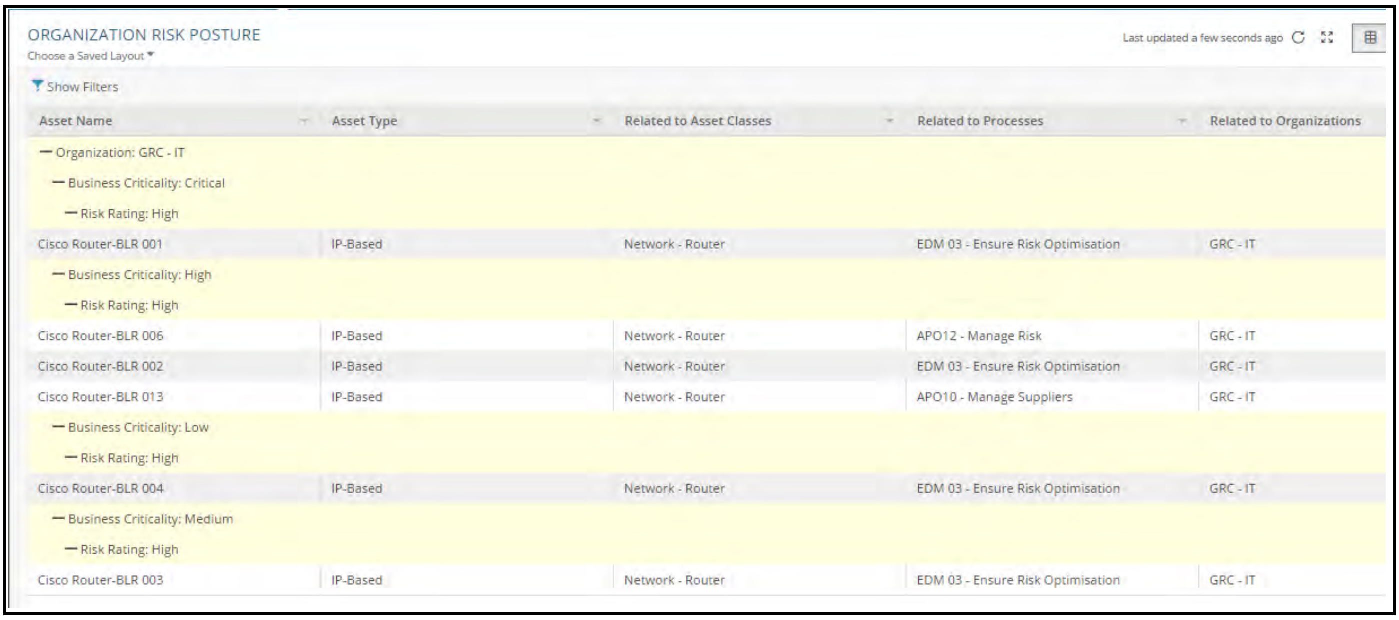
Organization Name: LOB - Healthcare → ALL → ALL → ALL
Asset Count: 1

Figure 17 Organization Risk Posture Heat Map

Description	Drill Down
The heat map illustrates the following: • X-axis: Percentage of high risk assets • Y-axis: Count of assets	Organization Risk Posture Report

Organization Risk Posture Report

The **Organization Risk Posture** report is a drill down report of **Organization Risk Exposure Heat Map** chart. This report displays the details of risky organizations by using the total number of Assets related to an organization.



ORGANIZATION RISK POSTURE

Asset Name	Asset Type	Related to Asset Classes	Related to Processes	Related to Organizations
— Organization: GRC - IT				
— Business Criticality: Critical				
— Risk Rating: High				
Cisco Router-BLR 001	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
— Business Criticality: High				
— Risk Rating: High				
Cisco Router-BLR 006	IP-Based	Network - Router	APO12 - Manage Risk	GRC - IT
Cisco Router-BLR 002	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
Cisco Router-BLR 013	IP-Based	Network - Router	APO10 - Manage Suppliers	GRC - IT
— Business Criticality: Low				
— Risk Rating: High				
Cisco Router-BLR 004	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT
— Business Criticality: Medium				
— Risk Rating: High				
Cisco Router-BLR 003	IP-Based	Network - Router	EDM 03 - Ensure Risk Optimisation	GRC - IT

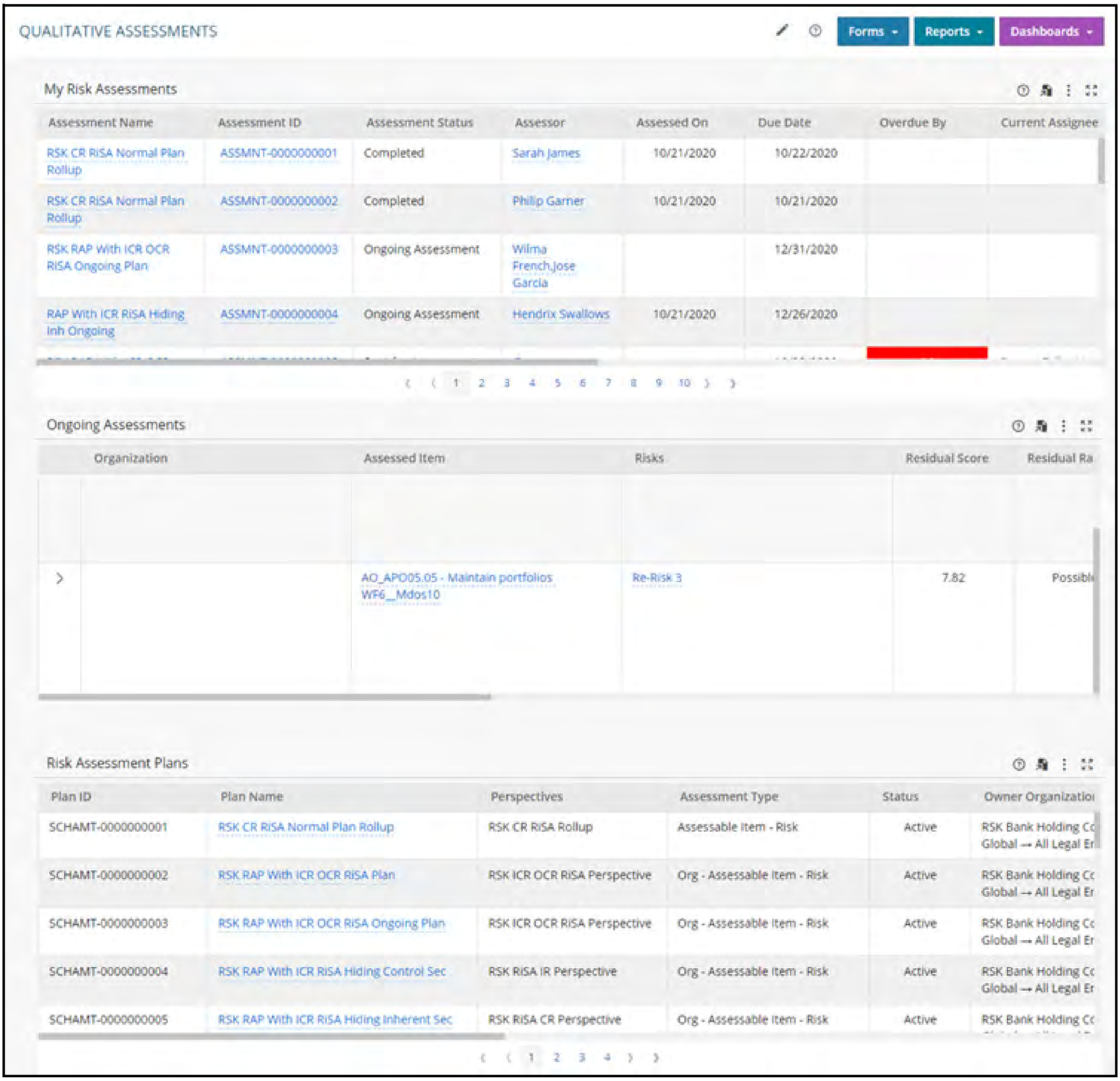
Figure 18 Organization Risk Posture Report

Key Columns:

- **Asset Name:** Displays the name of the asset which is risk assessed.
- **Related to Asset Classes:** Displays the asset classes to which the risk assessed asset is associated.
- **Related to Organizations:** Displays the organization to which the risk assessed asset is associated.

Qualitative Assessments

Use the **Qualitative Assessments** page to schedule risk assessments, assess risks and controls, log findings and issues, and reassess risks. The following **Qualitative Assessments** page is available for IT- Risk Manager and IT-Risk Analyst. For more information on the role-infocenter/privilege mapping, see Roles, Privileges, and Infocenters.



My Risk Assessments

Assessment Name	Assessment ID	Assessment Status	Assessor	Assessed On	Due Date	Overdue By	Current Assignee
RSK CR RISA Normal Plan Rollup	ASSMNT-0000000001	Completed	Sarah James	10/21/2020	10/22/2020		
RSK CR RISA Normal Plan Rollup	ASSMNT-0000000002	Completed	Philip Garner	10/21/2020	10/21/2020		
RSK RAP With ICR OCR RISA Ongoing Plan	ASSMNT-0000000003	Ongoing Assessment	Wilma French,Jose Garcia		12/31/2020		
RAP With ICR RISA Hiding Inh Ongoing	ASSMNT-0000000004	Ongoing Assessment	Hendrix Swallows	10/21/2020	12/26/2020		

Ongoing Assessments

	Organization	Assessed Item	Risks	Residual Score	Residual Ra
>		AO_APO05.05 - Maintain portfolios WF6__Mdos10	Re-Risk 3	7.82	Possibl

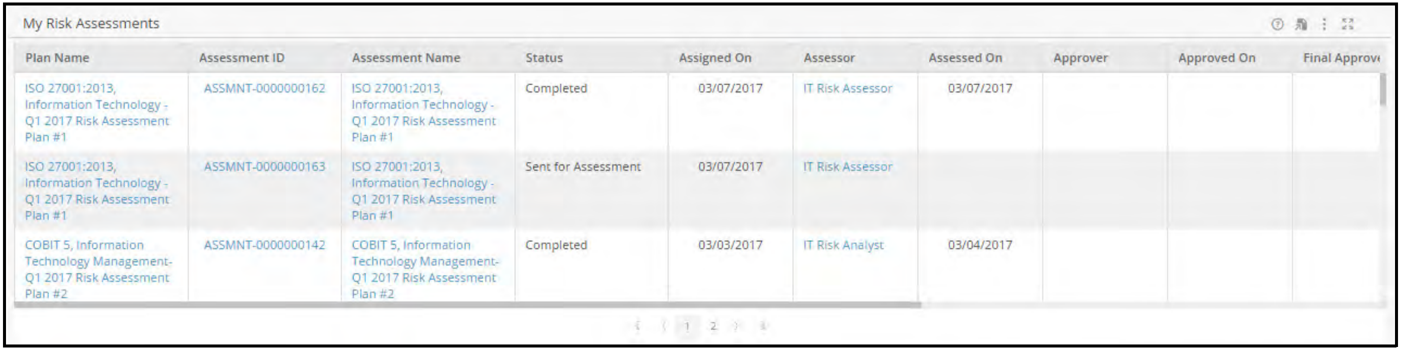
Risk Assessment Plans

Plan ID	Plan Name	Perspectives	Assessment Type	Status	Owner Organizatio
SCHAMT-0000000001	RSK CR RISA Normal Plan Rollup	RSK CR RISA Rollup	Assessable Item - Risk	Active	RSK Bank Holding Co Global → All Legal En
SCHAMT-0000000002	RSK RAP With ICR OCR RISA Plan	RSK ICR OCR RISA Perspective	Org - Assessable Item - Risk	Active	RSK Bank Holding Co Global → All Legal En
SCHAMT-0000000003	RSK RAP With ICR OCR RISA Ongoing Plan	RSK ICR OCR RISA Perspective	Org - Assessable Item - Risk	Active	RSK Bank Holding Co Global → All Legal En
SCHAMT-0000000004	RSK RAP With ICR RISA Hiding Control Sec	RSK RISA IR Perspective	Org - Assessable Item - Risk	Active	RSK Bank Holding Co Global → All Legal En
SCHAMT-0000000005	RSK RAP With ICR RISA Hiding Inherent Sec	RSK RISA CR Perspective	Org - Assessable Item - Risk	Active	RSK Bank Holding Co

Figure 19 Qualitative Assessments Page

My Risk Assessments Report

Use the **My Risk Assessments** report to view and work on the risk assessments assigned to you.



My Risk Assessments

Plan Name	Assessment ID	Assessment Name	Status	Assigned On	Assessor	Assessed On	Approver	Approved On	Final Approv
ISO 27001:2013, Information Technology - Q1 2017 Risk Assessment Plan #1	ASSMNT-0000000162	ISO 27001:2013, Information Technology - Q1 2017 Risk Assessment Plan #1	Completed	03/07/2017	IT Risk Assessor	03/07/2017			
ISO 27001:2013, Information Technology - Q1 2017 Risk Assessment Plan #1	ASSMNT-0000000163	ISO 27001:2013, Information Technology - Q1 2017 Risk Assessment Plan #1	Sent for Assessment	03/07/2017	IT Risk Assessor				
COBIT 5, Information Technology Management- Q1 2017 Risk Assessment Plan #2	ASSMNT-0000000142	COBIT 5, Information Technology Management- Q1 2017 Risk Assessment Plan #2	Completed	03/03/2017	IT Risk Analyst	03/04/2017			

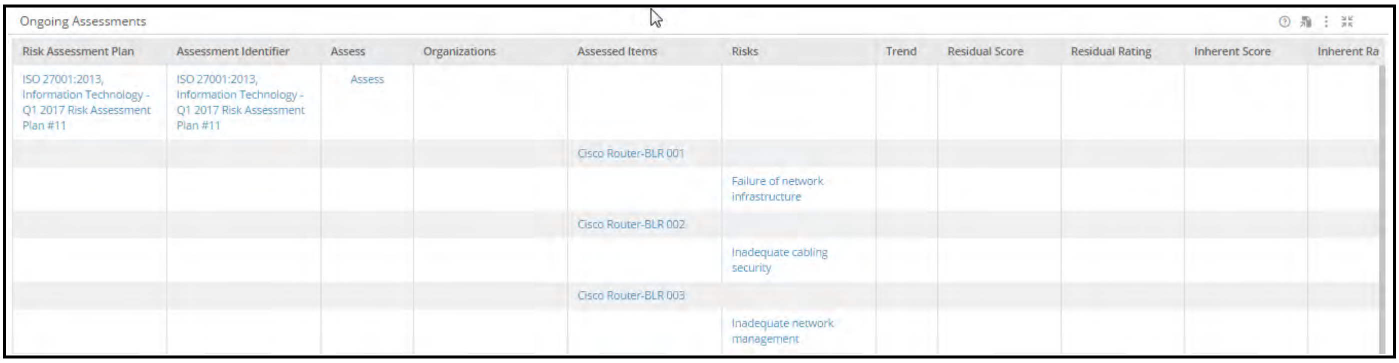
Figure 20 My Risk Assessments Report

Key Columns:

- **Plan Name:** Displays the name of the risk assessment plan which you need to assess.
- **Assessment ID:** Displays the identification number of the risk assessment plan.
    - o Drill Down: **Risk Assessment** form

Ongoing Assessments Report

Use the **Ongoing Assessments** report to view and work on the ongoing risk assessments.



Ongoing Assessments

Risk Assessment Plan	Assessment Identifier	Assess	Organizations	Assessed Items	Risks	Trend	Residual Score	Residual Rating	Inherent Score	Inherent Ra
ISO 27001:2013, Information Technology - Q1 2017 Risk Assessment Plan #11	ISO 27001:2013, Information Technology - Q1 2017 Risk Assessment Plan #11	Assess								
				Cisco Router-BLR 001						
					Failure of network infrastructure					
				Cisco Router-BLR 002						
					Inadequate cabling security					
				Cisco Router-BLR 003						
					Inadequate network management					

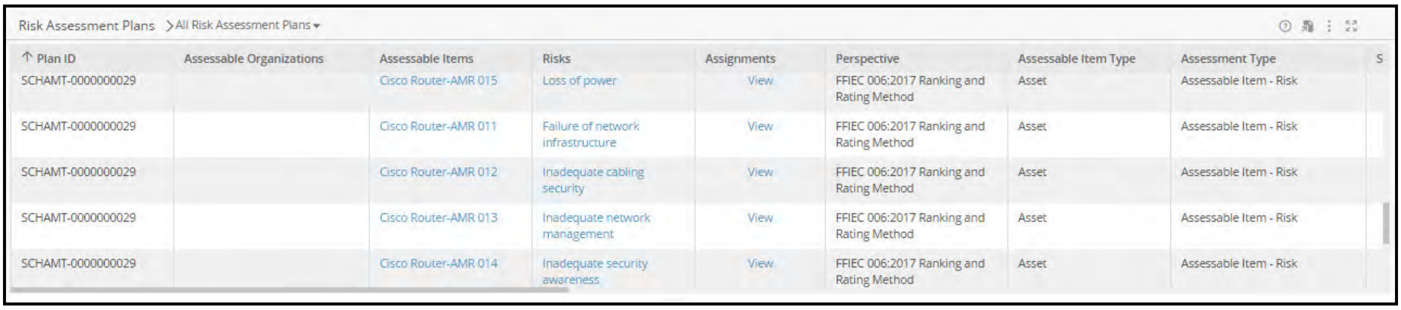
Figure 21 Ongoing Assessments Report

Key Columns:

- **Risk Assessment Plan:** Displays the name of the risk assessment plan which needs to be assessed.
- **Trend:** Displays the trend based on the rating.
- **Assess:** Displays the 'Assess' link.
    - o Drill Down: **Risk Assessment** form

Risk Assessment Plans Report

Use the **Risk Assessment Plans** report to view all the risk assessment plans in the system.



Risk Assessment Plans > All Risk Assessment Plans

Plan ID	Assessable Organizations	Assessable Items	Risks	Assignments	Perspective	Assessable Item Type	Assessment Type	S
SCHAMT-0000000029		Cisco Router-AMR 015	Loss of power	View	FFIEC 006:2017 Ranking and Rating Method	Asset	Assessable Item - Risk	
SCHAMT-0000000029		Cisco Router-AMR 011	Failure of network infrastructure	View	FFIEC 006:2017 Ranking and Rating Method	Asset	Assessable Item - Risk	
SCHAMT-0000000029		Cisco Router-AMR 012	Inadequate cabling security	View	FFIEC 006:2017 Ranking and Rating Method	Asset	Assessable Item - Risk	
SCHAMT-0000000029		Cisco Router-AMR 013	Inadequate network management	View	FFIEC 006:2017 Ranking and Rating Method	Asset	Assessable Item - Risk	
SCHAMT-0000000029		Cisco Router-AMR 014	Inadequate security awareness	View	FFIEC 006:2017 Ranking and Rating Method	Asset	Assessable Item - Risk	

Figure 22 Risk Assessment Plans Report

Key Columns:

- **Plan Name:** Displays the name of the risk assessment plan which needs to be assessed.
- **Assessment Type:** Displays the type of assessment applicable for a specific assessment plan.
- **Risks:** Displays the name of the risk against which the assessment needs to be done.

Forms

A risk assessment is required to identify, assess, and mitigate risks. A risk assessment plan involves identifying scope of assessment, specifying the frequency of assessments, risk assessors, and approvers. You can also create tasks for the plans to meet the immediate requirements. Use the links within the **Forms** drop-down list, as shown in the following figure, to manage risk assessments.

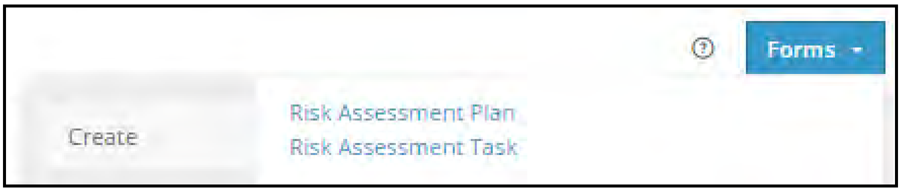


Figure 23 Forms of Assessments

You can create the following risk assessments/tasks:

- **Risk Assessment Plan:** Opens the **Risk Assessment Plan** form, where you can set up the risk assessment plan.
- **Risk Assessment Task:** Opens the **Risk Assessment Task** form, where you can create risk assessment tasks for the existing risk assessment plans.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Risk Assessments - User Guide.

Reports

Use the links within the **Reports** drop-down list to access the reports available in the **IT- Risk Management** product, as shown in the following figure.

Figure 24 Reports of Assessments

The **Reports** button has two links within it:

- Risk Assessments Link
- Other Reports Link

Risk Assessments Link

Within **Risk Assessments** link, you can access the following key reports:

- **Risk Aggregation Report**: Opens the **Risk Aggregation Report** report, which displays the aggregated score and ratings for different dimensions in business hierarchies to analyze the impact of risk based on multiple dimensions such as functions, business unit or location.
- **Risk Assessment Status Details Report:** Opens the **Risk Assessment Status Details** report, which provides the number of days for which you want to view the plan and risk assessment task details. This report displays the current status of all the risk assessments that are assigned to the assessors along with its risk assessment workflow status. By default, the report displays the data of assessments assigned in the past one month.
- **Risk Control Assessments Report:** Opens the **Risk Control Assessments** report, which displays the details of control rating done as part of the risk assessments performed within a chosen perspective.
- **Risks Identified During Assessments Report:** Opens the **Risk Identified During Assessments** report, which displays the list of Risks added during the risk assessment.

Other Reports Link

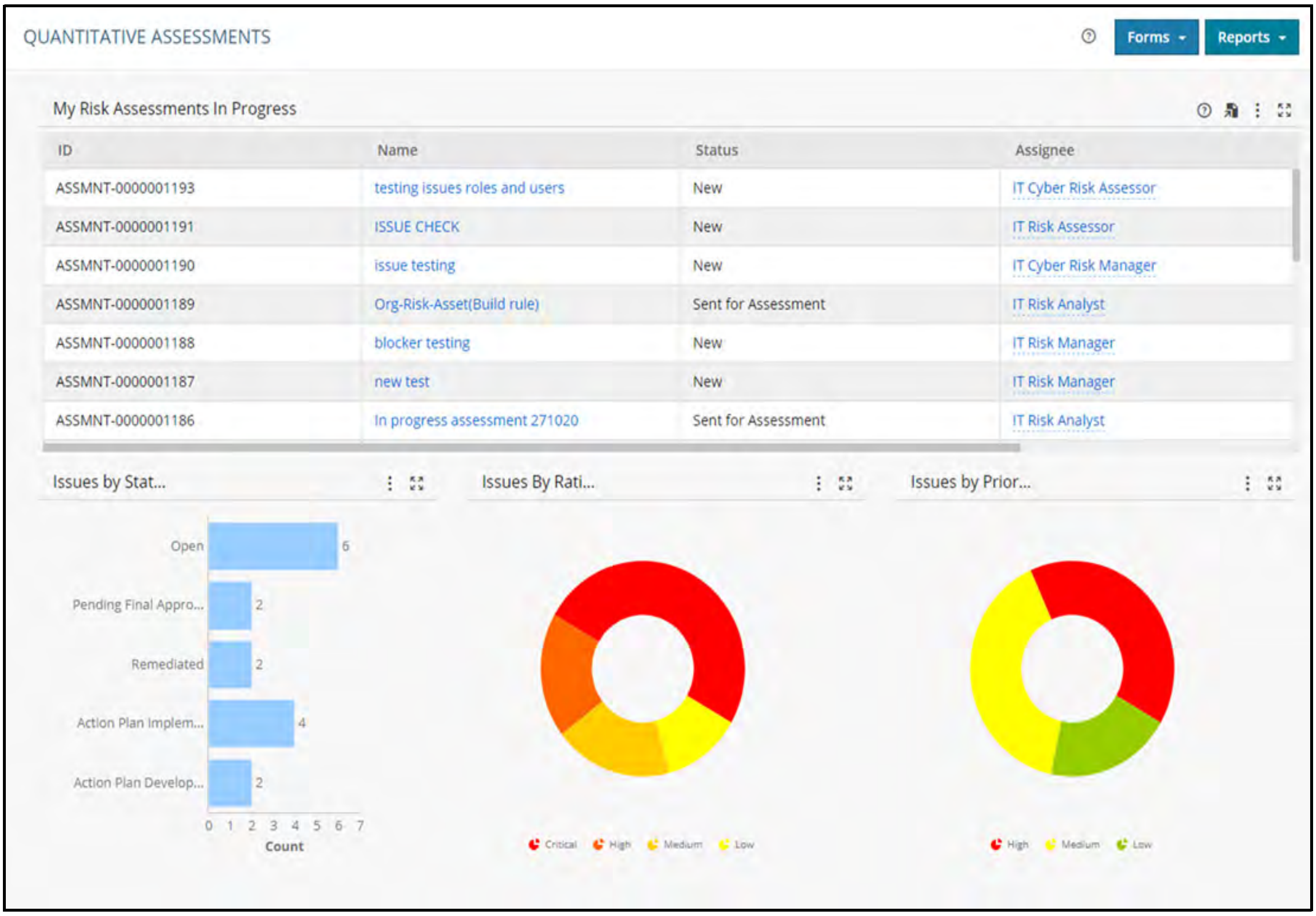
Within **Other Reports** link, you can access the following key reports:

- **Inherent Risks Breakdown by Category:** Opens the **Inherent Risks Breakdown by Category** report, which provides the Perspective value to view the required details. This report provides information on the Inherent Risk ratings of different risk categories that are assessed for the specified Perspective.
- **Residual Risks Breakdown by Category:** Opens the **Residual Risks Breakdown by Category** report, which provides the Perspective value to view the required details. This report provides information on the Residual Risk ratings of different risk categories that are assessed for the specified Perspective.
- **Risk Register:** Opens the **Risk Register** report, which provides end-to-end assessment details of the latest assessments performed. This report also provides details on the organizations, assessable entities, risks and factors that were assessed, and their contribution to the overall assessments.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Risk Assessments - User Guide.

Quantitative Assessments

Use the **Quantitative Assessments** page to create quantifiable risk assessments, assess IT risks against threats, vulnerabilities, and specify the scope of the assessment.

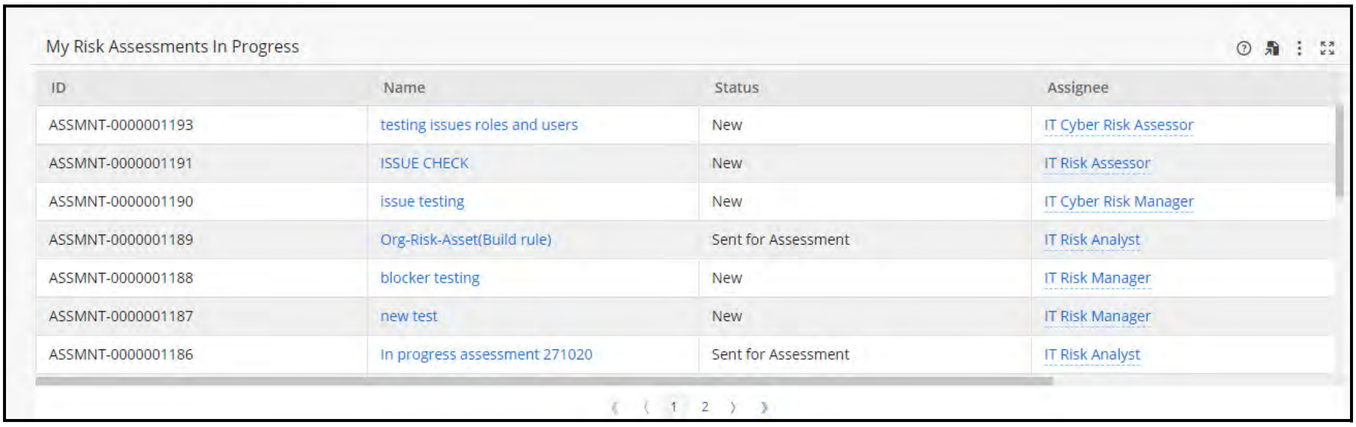


ID	Name	Status	Assignee
ASSMNT-0000001193	testing issues roles and users	New	IT Cyber Risk Assessor
ASSMNT-0000001191	ISSUE CHECK	New	IT Risk Assessor
ASSMNT-0000001190	issue testing	New	IT Cyber Risk Manager
ASSMNT-0000001189	Org-Risk-Asset(Build rule)	Sent for Assessment	IT Risk Analyst
ASSMNT-0000001188	blocker testing	New	IT Risk Manager
ASSMNT-0000001187	new test	New	IT Risk Manager
ASSMNT-0000001186	In progress assessment 271020	Sent for Assessment	IT Risk Analyst

Figure 25 Quantitative Assessments Page

My Risk Assessments In Progress Report

Use the **My Risk Assessments In Progress** report to view and work on your ongoing IT risk assessments.



ID	Name	Status	Assignee
ASSMNT-0000001193	testing issues roles and users	New	IT Cyber Risk Assessor
ASSMNT-0000001191	ISSUE CHECK	New	IT Risk Assessor
ASSMNT-0000001190	issue testing	New	IT Cyber Risk Manager
ASSMNT-0000001189	Org-Risk-Asset(Build rule)	Sent for Assessment	IT Risk Analyst
ASSMNT-0000001188	blocker testing	New	IT Risk Manager
ASSMNT-0000001187	new test	New	IT Risk Manager
ASSMNT-0000001186	In progress assessment 271020	Sent for Assessment	IT Risk Analyst

Figure 26 My Risk Assessments In Progress Report

Key Columns:

- **ID:** Displays the assessment ID.
- **Name:** Displays the assessments that are not closed. When you click on it, the corresponding assessment form is launched.
- **Status**: Displays the status of the assessment.

Issues by Status Chart

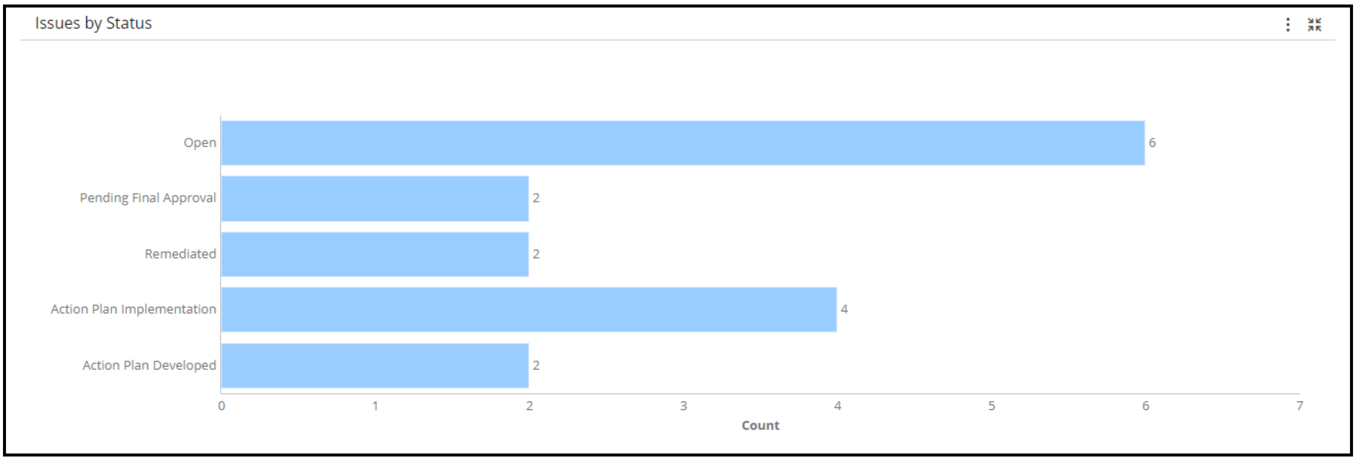


Figure 27 Issues by Status Chart

Description

This bar chart displays the issues based on status. It displays only the issues that are triggered by Source Type as IT and Cyber Risk. This charts displays the issue details which are logged using IT Risk Assessment form.

Drill down:

Issues Report

Issues by Rating Chart

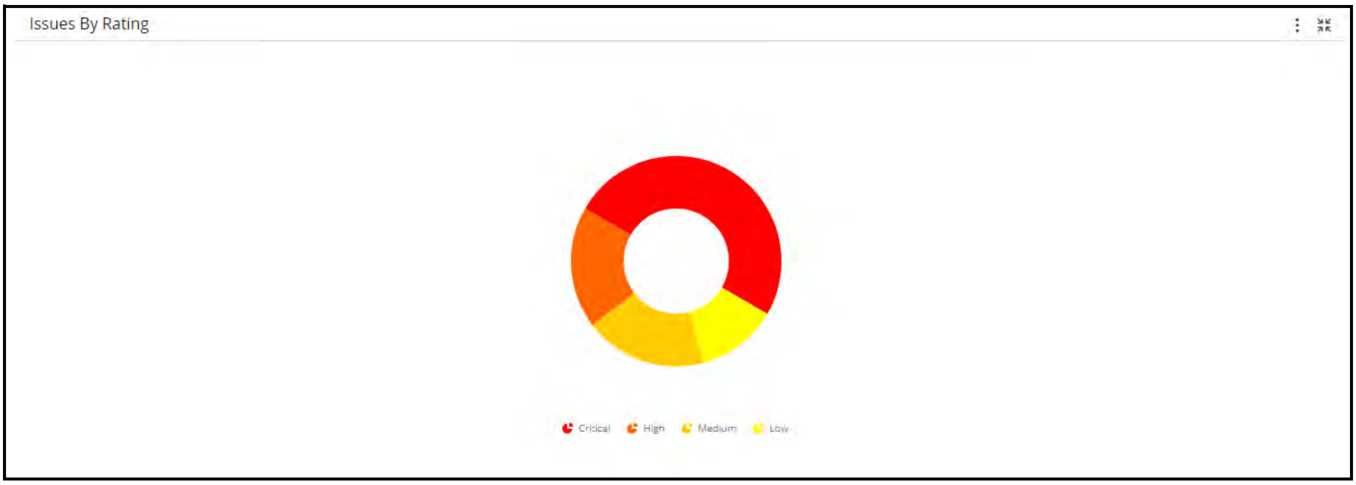


Figure 28 Issues by Rating Chart

Description

This pie chart displays the issues based on rating. It displays only the issues that are triggered by Source Type as IT and Cyber Risk. This charts displays the issue details which are logged using IT Risk Assessment form.

Drill down:

Issues Report

Issues by Priority Chart

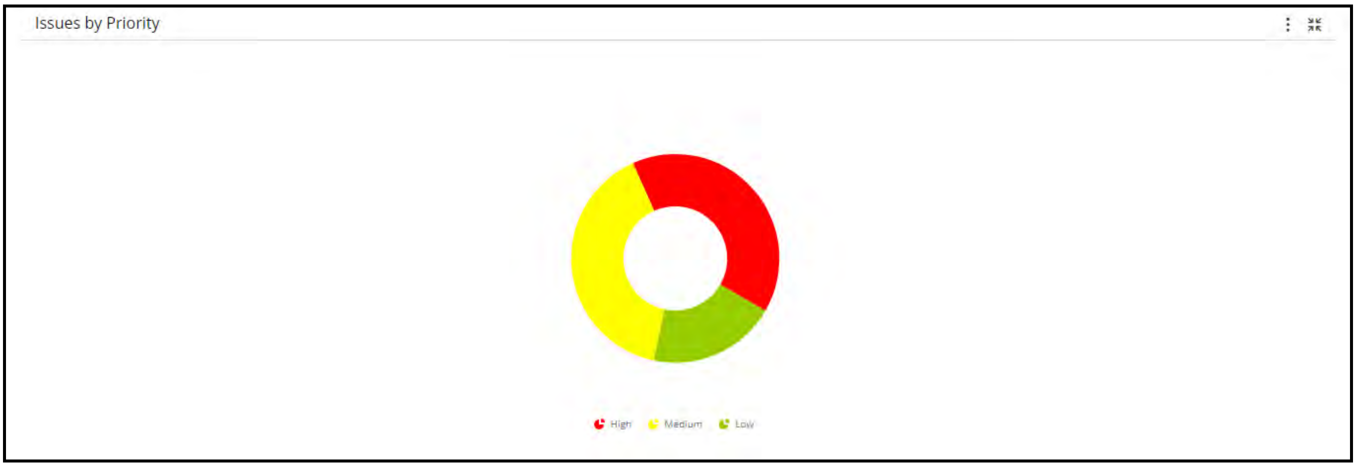


Figure 29 Issues by Priority Chart

Description

This pie chart displays the issues based on priority. It displays only the issues that are triggered by Source Type as IT and Cyber Risk. This charts displays the issue details which are logged using IT Risk Assessment form.

Drill down:

Issues Report

Forms

Use the link within the **Forms** drop-down list, as shown in the following figure, to manage risk assessments.

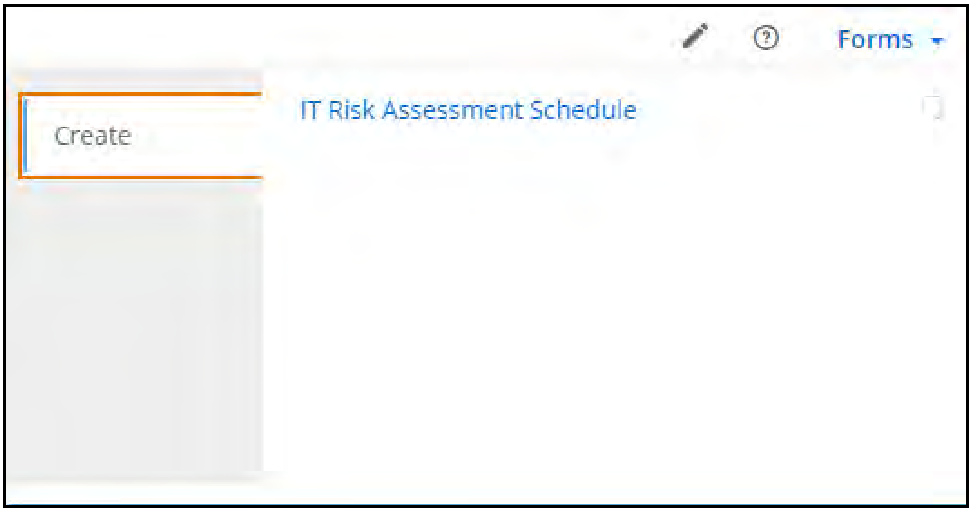


Figure 30 Form of IT Risk Assessment Schedule

You can access the following form:

- **IT Risk Assessment Schedule** - Opens the IT Risk Assessment Schedule form, where you can setup the risk assessment to occur at specific frequency.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - IT and Cyber Risk - User Guide.

Reports

Use the links within the **Reports** list to access the IT- Risk Assessment reports, as shown in the following figure.

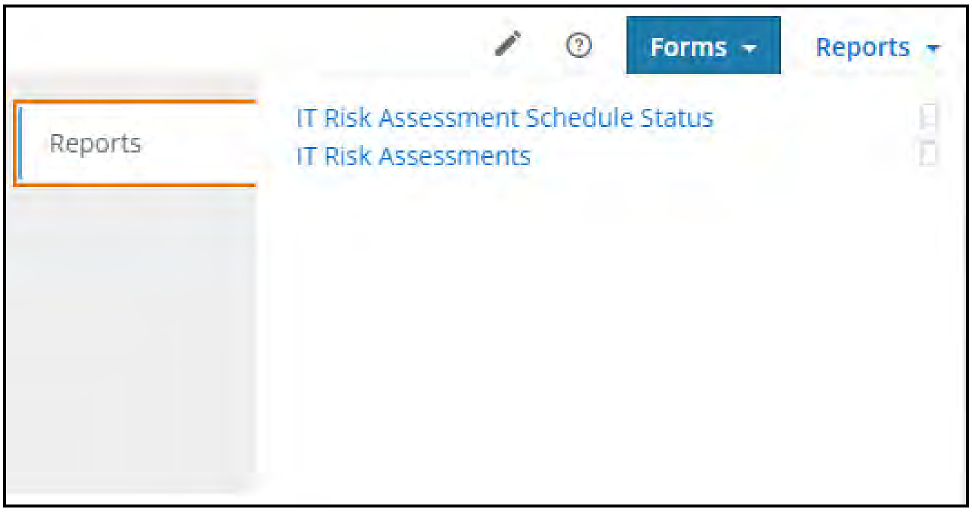


Figure 31 Report of IT Risk Assessments

You can access the following key reports:

- **IT Risk Assessment Schedule Status** - Opens the IT Risk Assessment Schedule Status report, which provides the status of the schedule created for the IT risk assessments.

- **IT Risk Assessments** - Opens the IT Risk Assessments report, which provides the view of completed IT risk assessment available in the system. Only the completed and canceled assessments are visible in this report.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - IT and Cyber Risk - User Guide.

Threats

Use the **Threats** page to gain insight into the list of threats through the threats by threat strength chart and threats by likelihood of initiation chart. You can capture ad hoc threat alert details, the details of different threats, and threat actors to identify the strength of the threat and possibility of the threat being carried out. You can also view reports related to threats and threat actors.

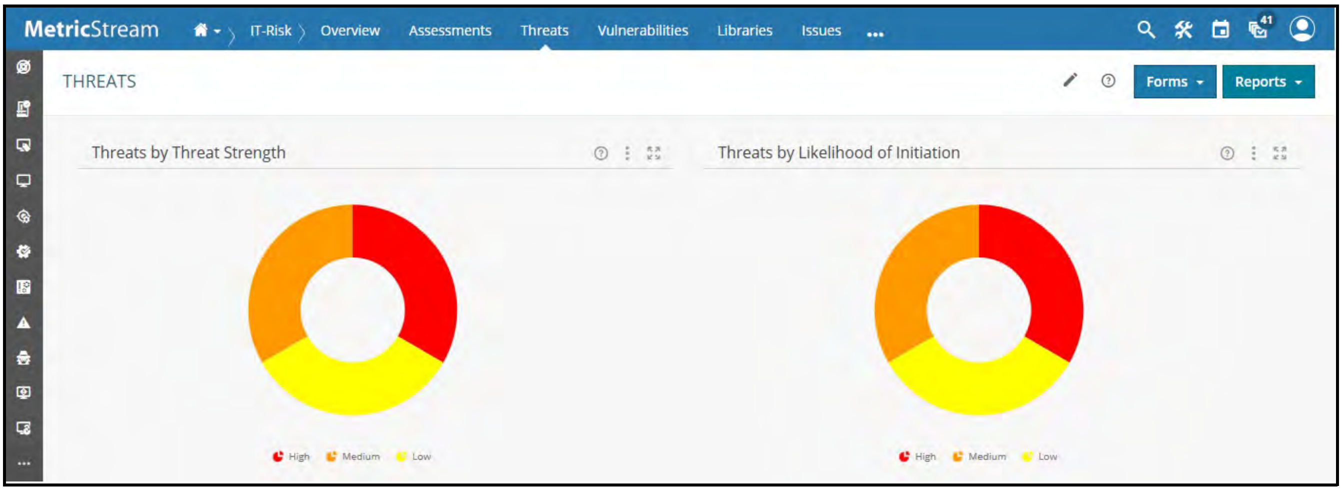


Figure 32 Threats

Threats by Threat Strength Chart

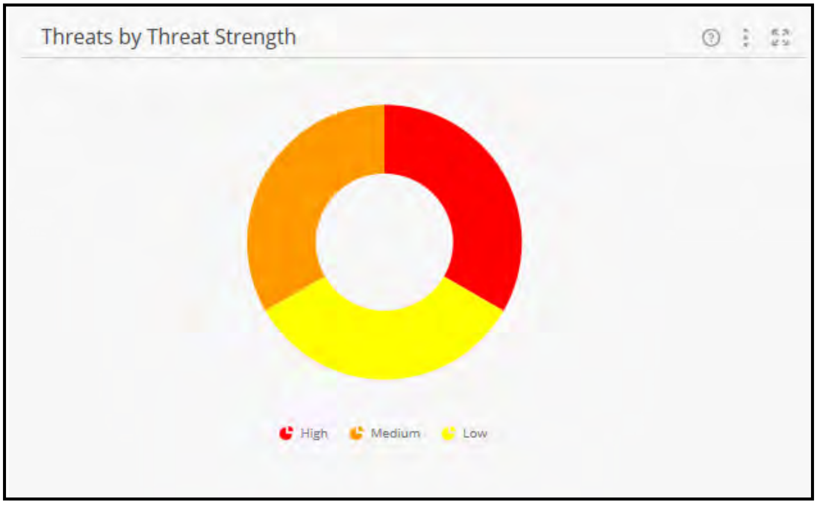


Figure 33 Threats by Threat Strength Chart

Description

This pie chart displays the number of threat records based on their strength, such as High, Medium, and Low.

Drill down:

Threats report

Threats by Likelihood of Initiation Chart

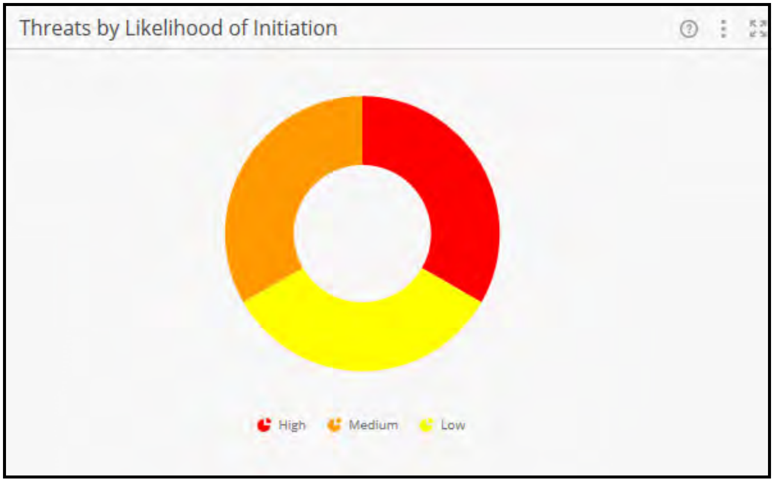


Figure 34 Threats by Likelihood of Initiation Chart

Description

This pie chart displays the number of threat records based on their likelihood of initiation, such as High, Medium, and Low.

Drill down:

Threats report

Forms

Click **Forms** and use the appropriate forms to capture the details of ad hoc alerts, different threats, and threat actors. Use links within the **Forms** button to access the available key forms, as displayed in the following figure.

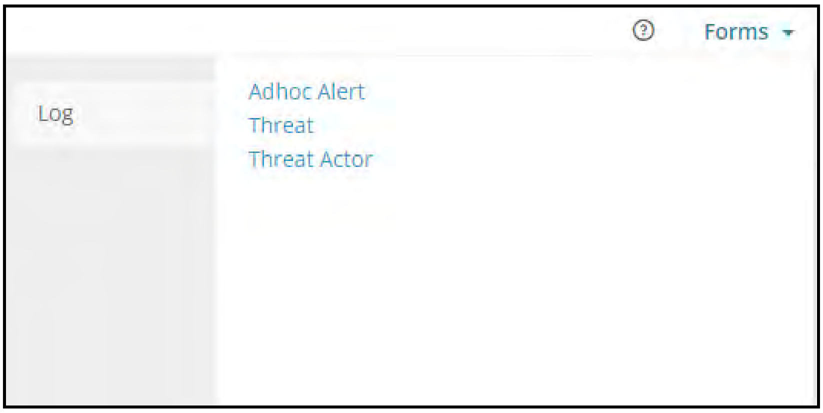


Figure 35 Threats Forms

Forms	Description
Adhoc Alert	Use this form to capture ad hoc alert details.
Threat	Use this form to capture the details of different threats, assess the threats, and identify its strength and possibility of the threat being carried out.
Threat Actor	Use this form to capture the details of different threat actors and assess their motives.

Note: For more information on capturing details of ad hoc alerts, threats, and threat actors, refer to MetricStream Arno Release Spring '21 - Threat and Vulnerability Management - User Guide.

Reports

Click **Reports** and view the required reports related to threats.

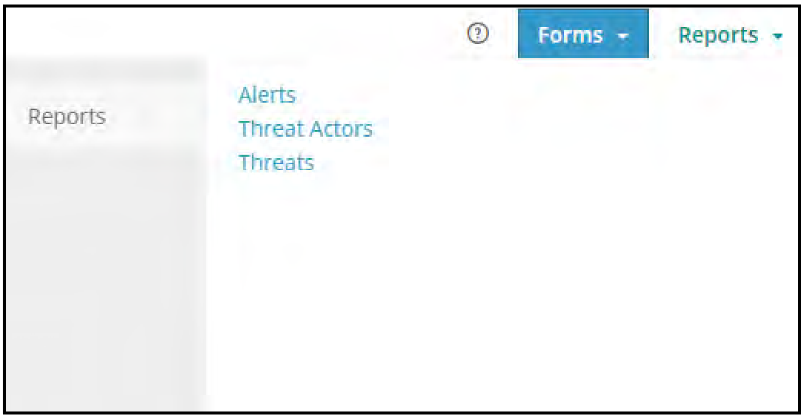


Figure 36 Threats Reports

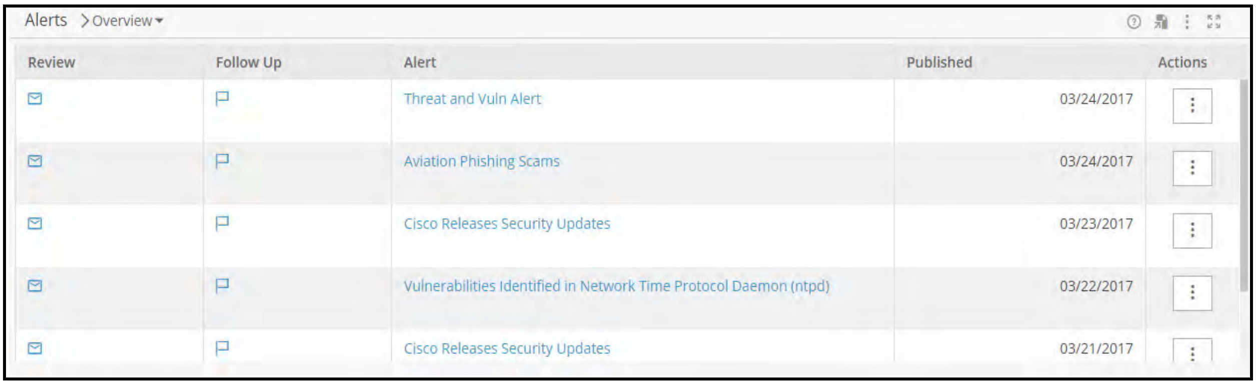
The following table provides the list of the threat related reports.

Reports	Drill-down Reports
Alerts	
Threat Actors	- Motive Details - Capability Details
Threats	- Threat Actors - Related Assets - Related Asset Classes

Alerts

The Alerts report provides the list of threat alert channels from various subscriptions along with the detailed threat information.

Information Security Analyst can view and analyze the list of Alerts subscribed from RSS or Email based threat alert Channels. Trigger threat remediation workflow for prioritized threats and log findings or issues to respective issue owners to track the applicability response.



Review	Follow Up	Alert	Published	Actions
✉	⚐	Threat and Vuln Alert	03/24/2017	⋮
✉	⚐	Aviation Phishing Scams	03/24/2017	⋮
✉	⚐	Cisco Releases Security Updates	03/23/2017	⋮
✉	⚐	Vulnerabilities Identified in Network Time Protocol Daemon (ntpd)	03/22/2017	⋮
✉	⚐	Cisco Releases Security Updates	03/21/2017	⋮

Figure 37 Alerts Report

For more information, refer to the MetricStream Arno Release Spring ‘21 - GRC Intelligence - User Guide.

Threat Actors

Use this report to:

View the details of all the available threat actor details.

Key Columns

Column	Description
Name	Displays the name of the threat actor. Drill Down: **Threat Actor** form
Motives	Displays the number of motive details associated with the threat actor to carry out the threat. Drill Down: Motive Details
Confidentiality	Displays the assessed confidentiality level for the motives of the threat actor.
Integrity	Displays the assessed integrity level for the motives of the threat actor.
Availability	Displays the assessed availability level for the motives of the threat actor.
Capabilities	Displays the number of capability details associated with the threat actor. Drill Down: Capability Details.
Type	Displays the type of threat actor.
Sponsors	Displays the sponsors for the threat actor.
Region of Operation	Displays the region of operation of the threat actor.

Threats

Use this report to:

View the details of all the available threat details.

Key Columns

Column	Description
Name	Displays the name of the threat. Drill Down: **Threat** form
Likelihood of Initiation	Displays the assessed level for the likelihood of initiation of the threat.
Threat Strength	Displays the assessed level of the threat strength.
Threat Vector	Displays the path through which the threat can be initiated.
Threat Actors	Displays the number of threat actors associated with the threat. Drill Down: Threat Actors
Confidentiality	Displays the assessed confidentiality level for the threat actor details associated with the threat.

Column	Description
Integrity	Displays the assessed integrity level for the threat actor details associated with the threat.
Availability	Displays the assessed availability level for the threat actor details associated with the threat.
Trend	Displays the trend of the threat whether upward or downward.
Threat Type	Displays the type of threat.
Issues	Displays the number of internal issues captured for threat.
Related to Assets	Displays the number of assets associated with the threat. Drill Down: Related Assets.
Related to Asset Classes	Displays the number of asset classes associated with the threat. Drill Down: Related Asset Classes.

Motive Details

Use this report to:

This is a drill down report from the Threat Actors report. You can view the details of all the motives associated with the selected threat actor.

Key Columns

Column	Description
Motive	Displays the name of the motive associated with the threat actor.
Confidentiality	Displays the confidentiality level of the motive.
Integrity	Displays the integrity level of the motive.
Availability	Displays the availability level of the motive.

Capability Details

Use this report to:

This is a drill down report from the Threat Actors report. You can view the details of all the capabilities associated with the selected threat actor.

Key Columns

Column	Description
Skill	Displays the name of the skill associated with the threat actor.
Skill Level	Displays the skill level of the skill associated with the threat actor.
Resource Level	Displays the availability level of the resource for the threat actor to carry out the threat.
Likelihood of Initiation	Displays the likelihood of initiation level of threat by the threat actor.

Threat Actors

Use this report to:
This is a drill down report from the **Threats** report. You can view the details of all the threat actors associated with the selected threat.

Key Columns

Column	Description
Actor Name	Displays the name of the threat actor.
Skill	Displays the name of the skill associated with the threat actor.
Skill Level	Displays the skill level for the skill associated with the threat actor.
Resource Level	Displays the availability level of the resource for the threat actor to carry out the threat.
Likelihood of Initiation	Displays the level of likelihood of initiation of threat by the threat actor.
Confidentiality	Displays the assessed confidentiality level for the motives of the threat actor.
Integrity	Displays the assessed integrity level for the motives of the threat actor.
Availability	Displays the assessed availability level for the motives of the threat actor.

Vulnerabilities

Use the **Vulnerabilities** page to gain insight into the list of vulnerabilities through vulnerabilities by severity chart and vulnerabilities by exposure charts. You can capture vulnerability details to identify the severity and exposure level of the vulnerability. You can also view reports of these vulnerabilities.

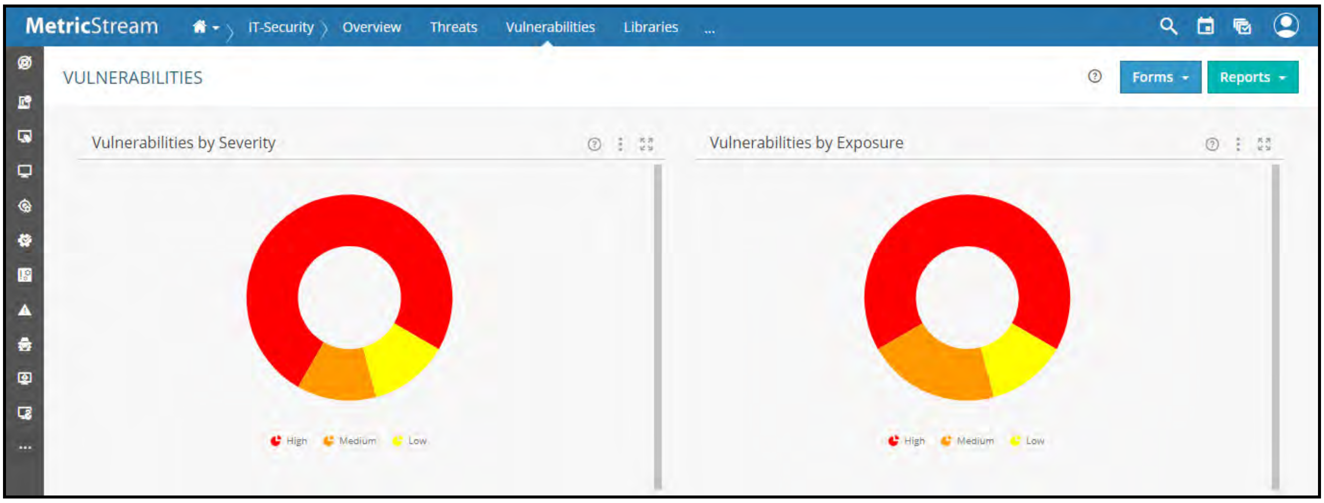


Figure 38 Vulnerabilities

Vulnerabilities Metric Cards

The **Metric Cards** summarizes the key metrics and displays the information in a nugget. The cards, when clicked upon, provides access to drill down reports, which analyses the key metric further. The cards are configurable based on your organization's requirements. The following cards are available currently:

- The **Unassigned Vulnerabilities** metric card displays the aggregated count of identified vulnerabilities as per their combined risk rating. The count of identified vulnerabilities with top 2 combined risk ratings is also displayed. The Unassigned Vulnerabilities metric card summarizes any Asset – Vulnerability pair that does not have an associated Issue (That is, it did not match a Rule and it simply went to the default rule for computing a CRR – note that the Issue was not created either via. the Rule or via. the manual route). You can drill down to Unassigned Vulnerabilities report for details when required. Within the Unassigned Vulnerabilities, **Vulnerability Summary** is made a hyper-link. On click of the link, you can see the additional details of the vulnerability.
- The **Remediation Issues** metric card displays the aggregated count of issues auto triggered for identified vulnerabilities based on remediation rules. The count of remediation issues with top 2 combined risk ratings is also displayed. The count in these top 2 ratings (for example, **Critical** and **High**), is a subset of the aggregated count. When you click on any of these links, it drills down to Remediation Issues report. This report displays the details of the remediation issues, their combined risk rating details and the issue types.
- The **Remediation Incidents** metric card displays the aggregated count of incidents auto triggered for identified vulnerabilities based on remediation rules. The count of remediation incidents with top 2 combined risk ratings is also displayed. The count in these top 2 ratings (for example, **Critical** and **High**), is a subset of the aggregated count. When you click on any of these links, it drills down to Remediation Incidents report. This report displays the details of the remediation incidents, their combined risk rating details and the incident types.

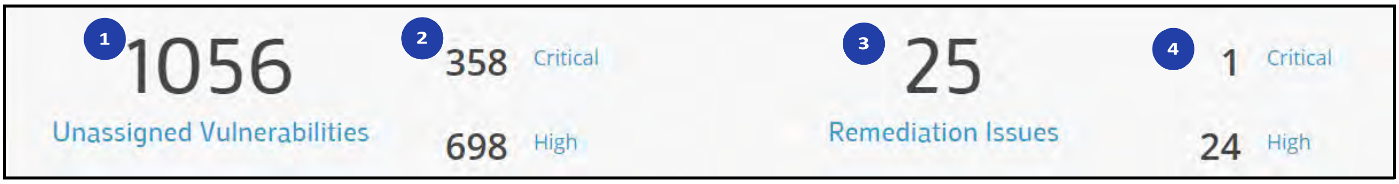


Figure 39 Metric Cards of Overview (Issues)

The numbered callouts identify the following:

1. Aggregated count of unassigned vulnerabilities of the top 2 combined risk ratings is displayed.

   Example: Total number of unassigned vulnerabilities comprising the top 2 ratings is 1056, as per the above image.

2. The count of unassigned vulnerabilities classified based on top 2 combined risk ratings is displayed.

   Example: Number of unassigned vulnerabilities having critical combined risk rating is 358, and number having high combined risk rating is 698.

3. Aggregated count of remediation issues of the top 2 combined risk ratings is displayed.

   Example: Total number of remediation issues comprising the top 2 ratings is 25, as per the above image.

4. The count of remediation issues classified based on top 2 combined risk ratings is displayed.

   Example: Number of remediation issues rated as critical is 1 and number rated as high is 24.

5. Aggregated count of remediation incidents of the top 2 combined risk ratings is displayed.

   Example: Total number of remediation incidents comprising the top 2 ratings is 25, as per the above image.

6. The count of remediation incidents classified based on top 2 combined risk ratings is displayed.

   Example: Number of remediation incidents rated as critical is 1 and number rated as high is 24.

Unassigned Vulnerabilities

This report displays the list of Asset-Vulnerability pairs that does not have an associated Issue or Incident. The report classifies the asset-vulnerability pairs based on their combined risk ratings. You can search within the list by using filters.

Remediation Issues

This report displays the list of auto triggered issues for identified vulnerabilities. The report classifies the issues based on their combined risk ratings. You can search within the list by using filters.

Remediation Incidents

This report displays the list of auto triggered incidents for identified vulnerabilities. The report classifies the incidents based on their combined risk ratings. You can search within the list by using filters.

Remediation Incidents

Remediation Incidents by Status

Remediation Incidents by Status is a bar chart. Use this chart to view the Incidents report filtered by the status of the incidents.

Notes:

- Users mapped to role **ITR LOB-Head** can view all three metric cards.
- Users mapped to role **IT-Risk Manager** can view only Unassigned Vulnerabilities and Remediation Issues metric cards.
- Users mapped to role **IT-Risk Analyst** can view only Unassigned Vulnerabilities and Remediation Incidents metric cards.

Dashboards

Use links within the **Dashboards** button to access the available charts, as displayed in the following figure.

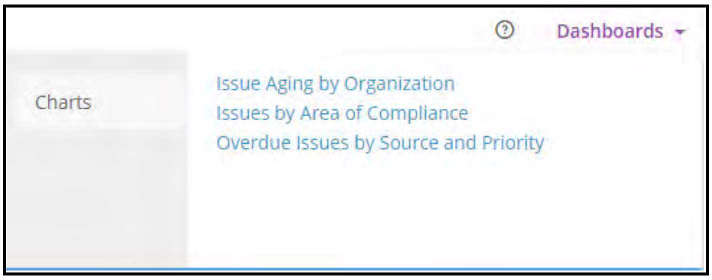

Dashboards
Charts
Issue Aging by Organization
Issues by Area of Compliance
Overdue Issues by Source and Priority

Figure 40 Dashboards of Overview (Issues)

You can access the following charts:

- **Issue Aging by Organization**: This chart provides an overview of all remediation issues based on owner organizations and the due dates. It displays the issues that are:
  - Not Due Yet
  - Passed due date in 1-30 days
  - Passed due date in 31-90 days
  - Passed due date above 90 days
- **Issues by Area of Compliance**: This chart displays the issues classified by related area of compliance. It displays the count of issues that are:
  - Overdue for more than predefined number of days
  - Overdue for more than or equal to predefined number of days
  - Ongoing
- **Overdue Issues by Source and Priority**: This chart displays the overdue issues that are triggered by various sources - for example, IT-Security.

Vulnerabilities by Severity

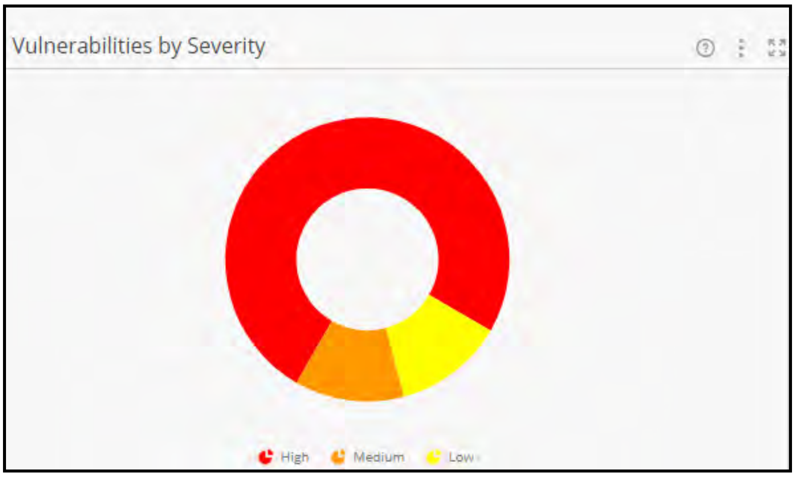


Figure 41 Vulnerabilities by Severity Chart

Description

This pie chart displays the number of vulnerability records based on their severity levels, such as High, Medium, and Low.

Drill down:

Vulnerabilities report

Vulnerability by Exposure Chart

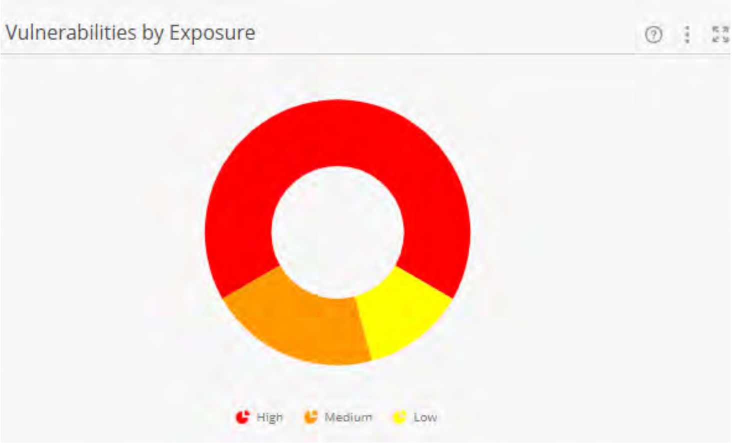


Figure 42 Vulnerabilities by Exposure Chart

Description

This pie chart displays the number of vulnerability records based on their exposure levels, such as High, Medium, and Low.

Drill down:

Vulnerabilities report

Remediation Issues by Status Chart

Remediation Issues by Status is a bar chart. Use this chart to view the remediation issues based on their status.

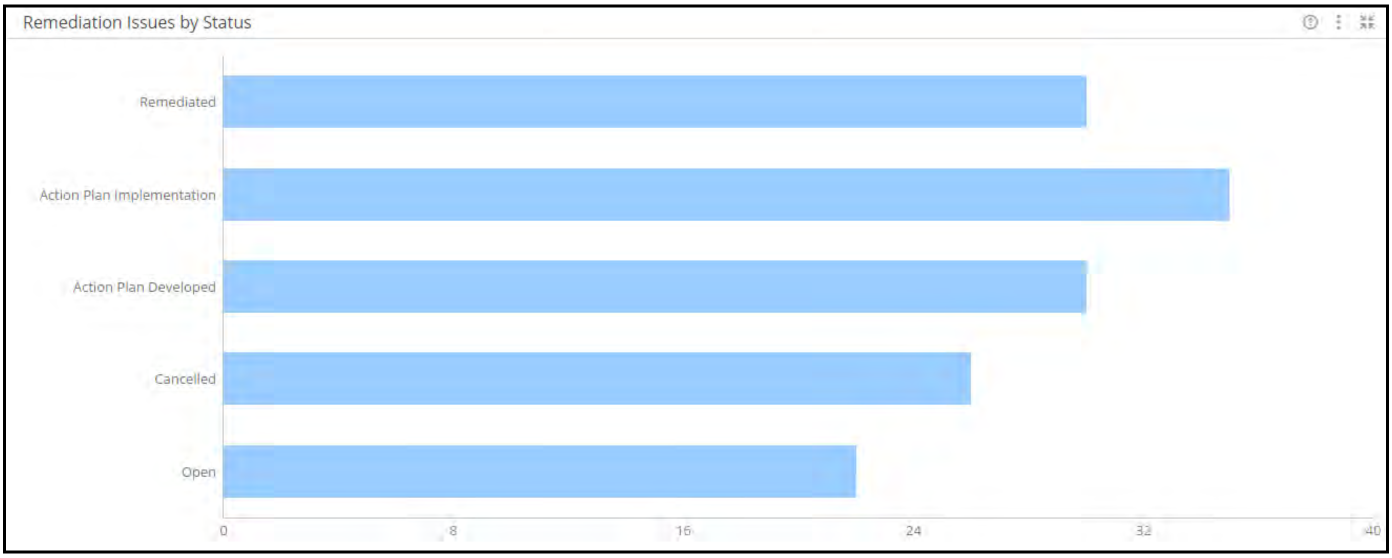


Figure 43 Remediation Issues by Status Chart

Description	Drill Down
The bar chart illustrates the following: • **X-axis**: Shows the count of issues. • **Y-axis**: Shows the different status of an issue (Example, Open, Action Plan Implementation, Action Plan Developed).	Remediation Issues report For more information, see MetricStream Arno Release Spring '21 - Issues - User Guide.

Remediation Issues by Rating Chart

Remediation Issues by Rating is a pie chart. Use this chart to view the remediation issues based on their rating.

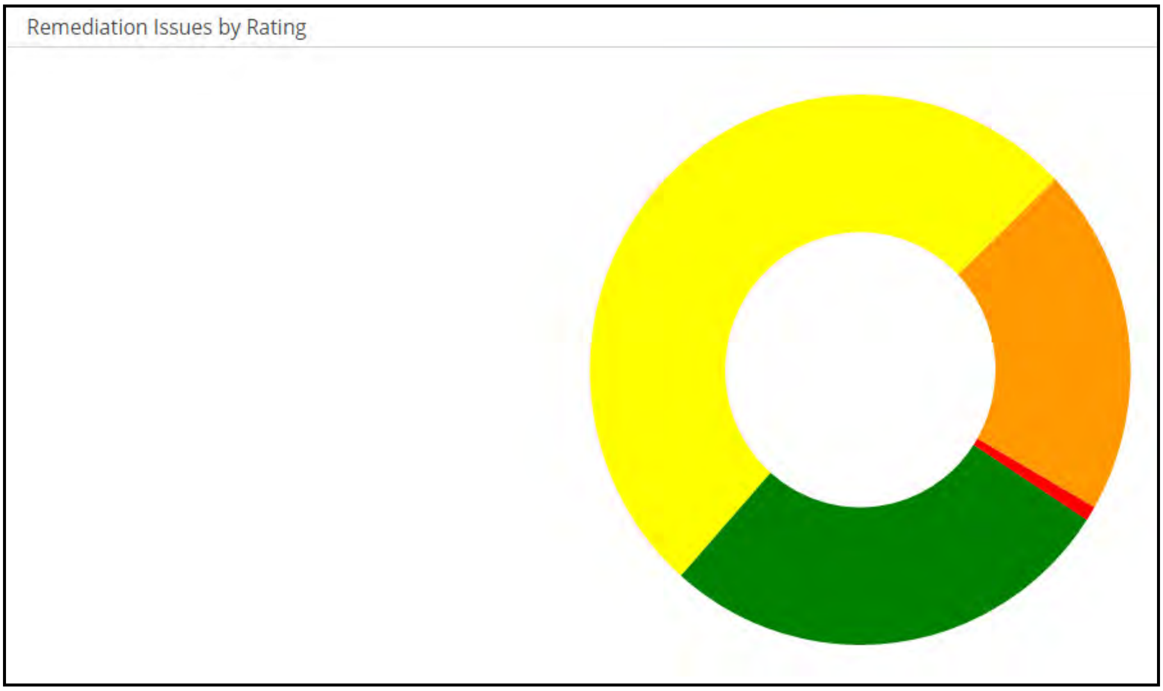


Figure 44 Remediation Issues by Rating Chart

Description	Drill Down
The pie chart displays the remediation issues of the following ratings: • Critical • High • Medium • Low	Remediation Issues report For more information, see MetricStream Arno Release Spring '21 - Issues - User Guide.

Remediation Issues by Priority Chart

Remediation Issues by Priority is a bar chart. Use this chart to view the remediation issues based on their priority.

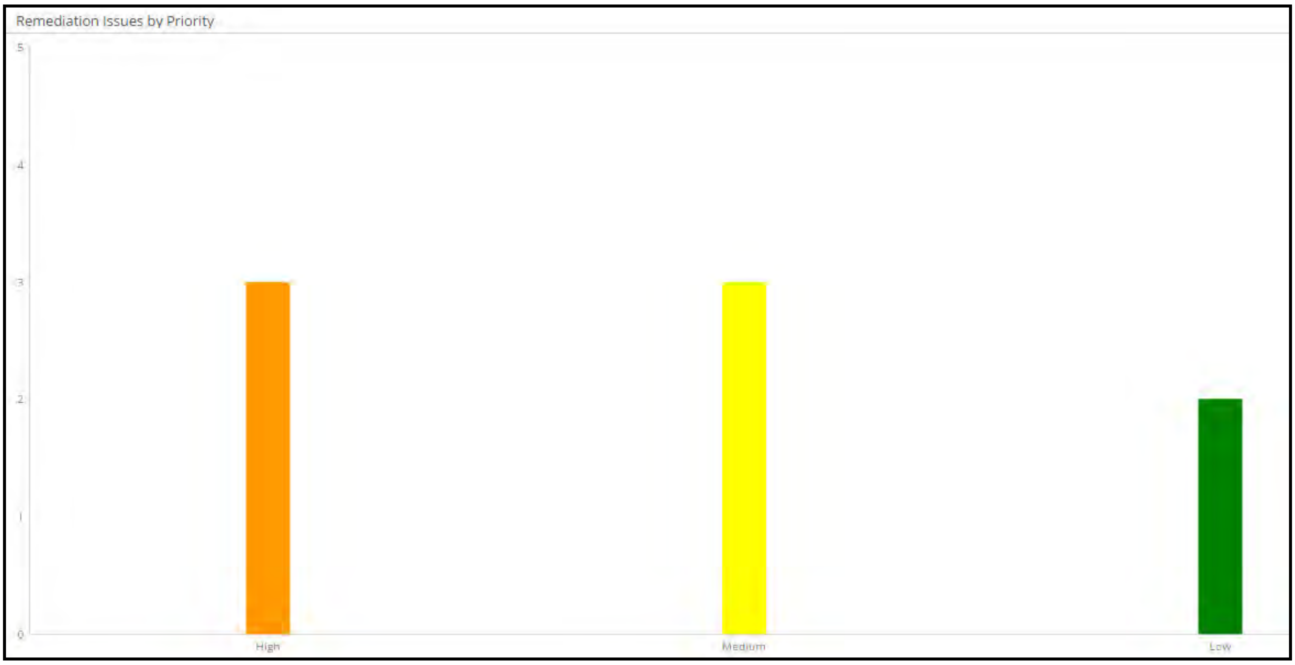


Figure 45 Remediation Issues by Priority chart

Description	Drill Down
The bar chart illustrates the following: • **X-axis**: Represents the following Priority levels of the issues: o High o Medium o Low • **Y-axis**: Represents the number of issues for each level	Remediation Issues report **Note:** For more information, see MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Remediation Incidents by Status

Remediation Incidents by Status is a bar chart. Use this chart to view the Incidents report filtered by the status of the incidents.

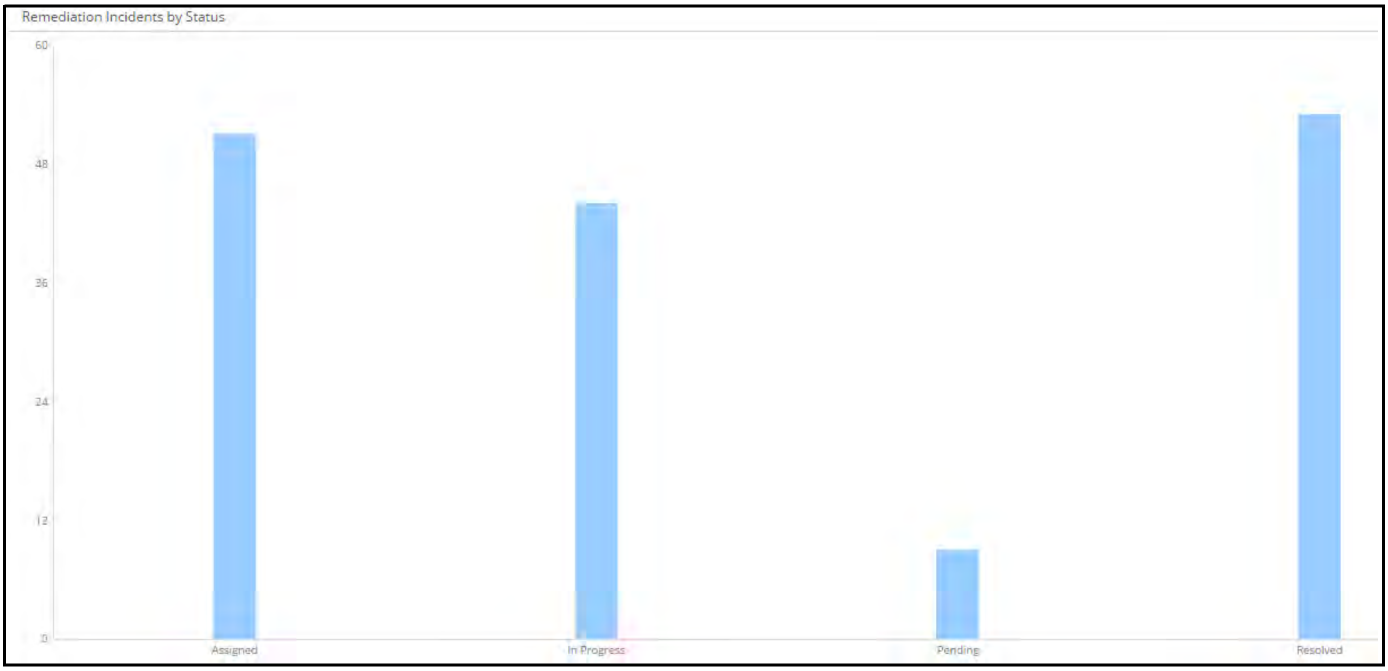


Figure 46 Remediation Incidents by Status Chart

Description	Drill Down
The bar chart illustrates the following: • **X-axis**: Shows the status of incidents. • **Y-axis**: Shows the count of incidents.	Remediation Incidents report For more information, see MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Remediation Incidents by Impact

Remediation Incidents by Impact is a pie chart. Use this chart to view the Incidents report filtered by the impact values of the incidents.

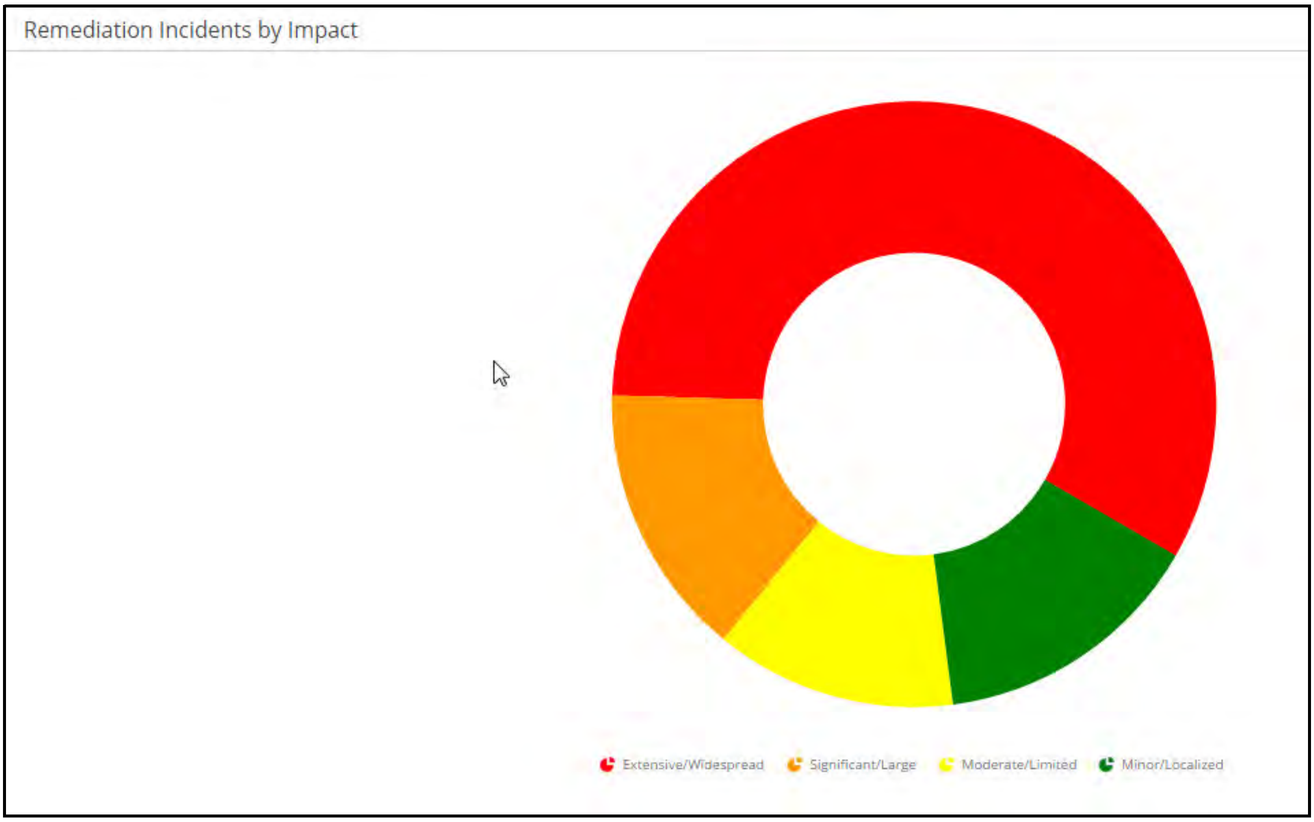


Figure 47 Remediation Incidents by Impact Chart

Description	Drill Down
The pie chart displays the remediation issues of the following impact values: • Extensive/Widespread • Significant/Large • Moderate/Limited • Minor/Localized	Remediation Incidents report For more information, see MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Remediation Incidents by Urgency

Remediation Incidents by Urgency is a bar chart. Use this chart to view the Incidents report filtered by the levels of urgency of the incidents.

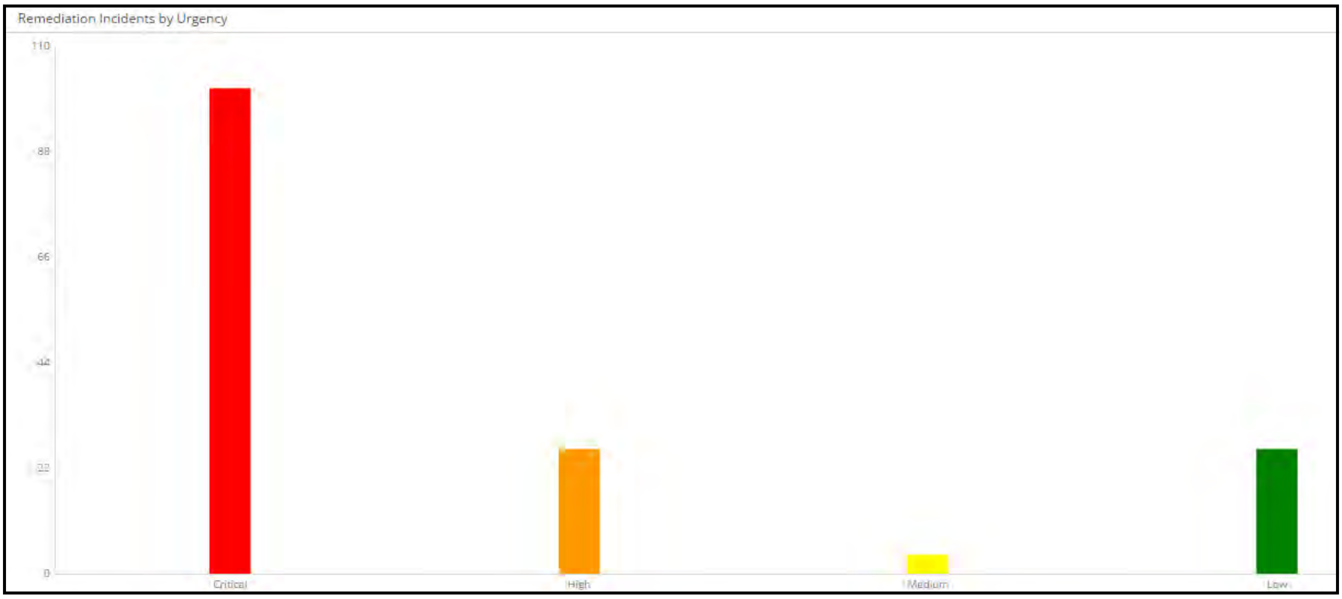


Figure 48 Remediation Incidents by Urgency Chart

Description	Drill Down
The bar chart illustrates the following: • **X-axis**: Shows the levels of urgency of incidents. • **Y-axis**: Shows the count of incidents.	Remediation Incidents report For more information, see MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Forms

Click **Forms** and then click **Vulnerability** to capture the details of vulnerabilities.

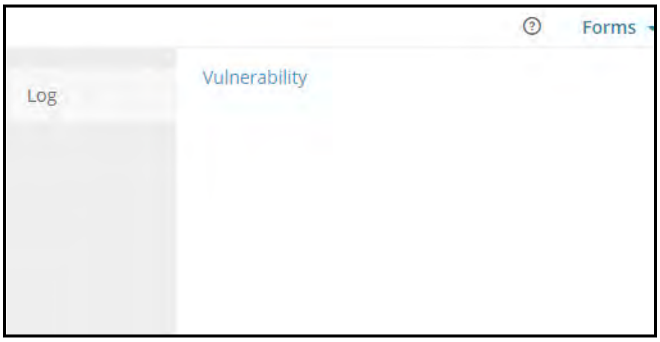


Figure 49 Vulnerability Forms

Forms	Description
Vulnerability	Use this form to capture the details of different vulnerabilities and assess their severity.

Note: For more information on capturing details of vulnerability, refer to in MetricStream Arno Release Spring ‘21 - Threat and Vulnerability Management - User Guide.

Note: .

Reports

Click **Reports** and view the required reports related to vulnerabilities.

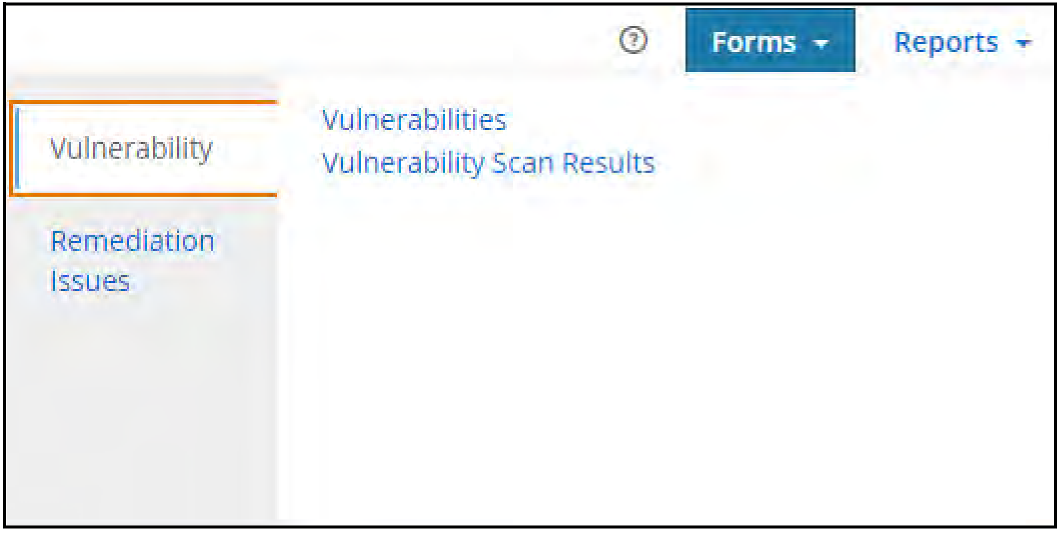


Figure 50 Vulnerabilities Reports

The following table provides the list of the vulnerabilities related reports.

The following table provides the list of the reports.

Navigation	Reports	Drill-down Reports
From **Vulnerabilities** infocenter, go to **Reports** and click **Vulnerability**	Vulnerabilities	• Related Assets • Related Asset Classes
	Vulnerability Scan Results	Vulnerability Summary
From **Vulnerabilities** infocenter, go to **Reports** and click **Remediation Issues**	Remediation Issues **Note:** Remediation Issues report is displayed to the users with IT_Risk_Manger role.	
From **Vulnerabilities** infocenter, go to **Reports** and click **Remediation Incidents**	Remediation Incidents **Note:** Remediation Incident report is displayed to the users with IT_Risk_Analyst role.	

Note: Users with IT_LOB_Head role can view Vulnerabilities, Vulnerability Scan Results, Remediation Issues and Remediation Incidents reports.

Remediation Issues

This is a key report and includes a list of all the remediation issues (both automated and manually triggered) in the system for the following combined risk ratings:

- Critical
- High
- Medium
- Low

Remediation Incidents

This is a key report that displays the list of auto triggered incidents for identified vulnerabilities. The report classifies the incidents based on their combined risk ratings.:

- Critical
- High
- Medium
- Low

Vulnerabilities

Use this report to:

View the details of all the available vulnerabilities that are captured manually by the user.

Key Columns

Column	Description
Name	Displays the name of the vulnerability. Drill Down: **Vulnerability** form
CVSS Base Score	Displays the base score of vulnerability based on Common Vulnerability Scoring System (CVSS).
CVSS Temporal	Displays the temporal score of the vulnerability based on Common Vulnerability Scoring System (CVSS).
Type	Displays the type of vulnerability.
Category	Displays the category of vulnerability.
Severity	Displays the severity level of the vulnerability.
Exposure	Displays the exposure level of the vulnerability.
Source	Displays the source of the vulnerability.
Issues	Displays the number of internal issues captured for vulnerability.
Related to Assets	Displays the number of assets associated with the vulnerability. Drill Down: Related Assets
Related to Asset Classes	Displays the number of asset classes associated with the vulnerability. Drill Down: Related Asset Classes.

Vulnerability Scan Results

Use this report to:

View the details all the vulnerabilities that are identified through scanner and shows the issues that are triggered based on the remediation rules and the default rules. The report also displays the status for each Issue ID/Incident ID. The vulnerabilities are classified in four types of combined risk ratings. They are:

- Critical
- High
- Medium
- Low.

Note: Click on **Log Issue** / **Create Issue** if you want to manually trigger an Issue/Incident. Manual triggering of issues/incidents is based on configuration parameter.

Mandatory Filters

Filter	Description
Combined Risk Rating	Select the combined risk rating of vulnerability.
Source	Select the connectors from which the vulnerability is captured.
Issue/Incident Created?	Select whether issue/incident for the vulnerability were created or not.

Key Columns

Column	Description
Combined Risk Rating	Displays the risk rating of the vulnerability.
Asset Name	Displays the name of the asset associated with the vulnerability. Move the mouse pointer over this column to view the Hover Card.
Source	Displays the connector from which the vulnerability is captured.
Vulnerability Summary	Displays the type of vulnerability. Drill Down: Vulnerability Summary
Type	Displays the type of vulnerability.
Category	Displays the category of vulnerability.
CVSS Base Score	Displays the base score of vulnerability based on Common Vulnerability Scoring System (CVSS).
Issue/Incident ID	• If issue/incident is created, then Issue/Incident ID is displayed. • If issue/incident is not created, then the Log Incident link is displayed to log an issue or incident.
Issue/Incident Status	Displays the status of the created issue/incident.

Vulnerability Summary

Use this report to:

View the summary of the selected vulnerability scan result.

Key Columns

Column	Description
Displays	Displays the description of the vulnerability.
Consequence	Displays the consequence details that may occur due to the vulnerability.
Solution	Displays the details of the solution taken to rectify the vulnerability.
CVE IDS	Displays the CVE ID of the vulnerability.
Severity	Displays the severity of vulnerability.

Related Assets

Use this report to:

This is a drill down report from the **Threats** report and the **Vulnerabilities** report. You can view the name of all the assets associated with the selected threat/vulnerability.

Key Columns

Column	Description
Name	Displays the name of the assets associated with the threat/vulnerability.

Related Asset Classes

Use this report to:

This is a drill down report from the **Threats** report and the **Vulnerabilities** report. You can view the name of all the asset classes associated with the selected threat/vulnerability.

Key Columns

Column	Description
Name	Displays the name of the asset classes associated with the threat/vulnerability.

Related Vulnerabilities

Use this report to:
This is a drill down report from the **Threats** report and the **Vulnerabilities** report. You can view the name of all the vulnerabilities associated with the selected threat/vulnerability.

Key Columns

Column	Description
Name	Displays the name of the vulnerabilities associated with the threat/vulnerability.

Related Controls

Use this report to:
This is a drill down report from the **Threats** report and the **Vulnerabilities** report. You can view the name of all the controls associated with the selected threat/vulnerability.

Key Columns

Column	Description
Name	Displays the name of the controls associated with the threat/vulnerability.

Related Risks

Use this report to:
This is a drill down report from the **Threats** report and the **Vulnerabilities** report. You can view the name of all the risks associated with the selected threat/vulnerability.

Key Columns

Column	Description
Name	Displays the name of the risks associated with the threat/vulnerability.

Related Threat

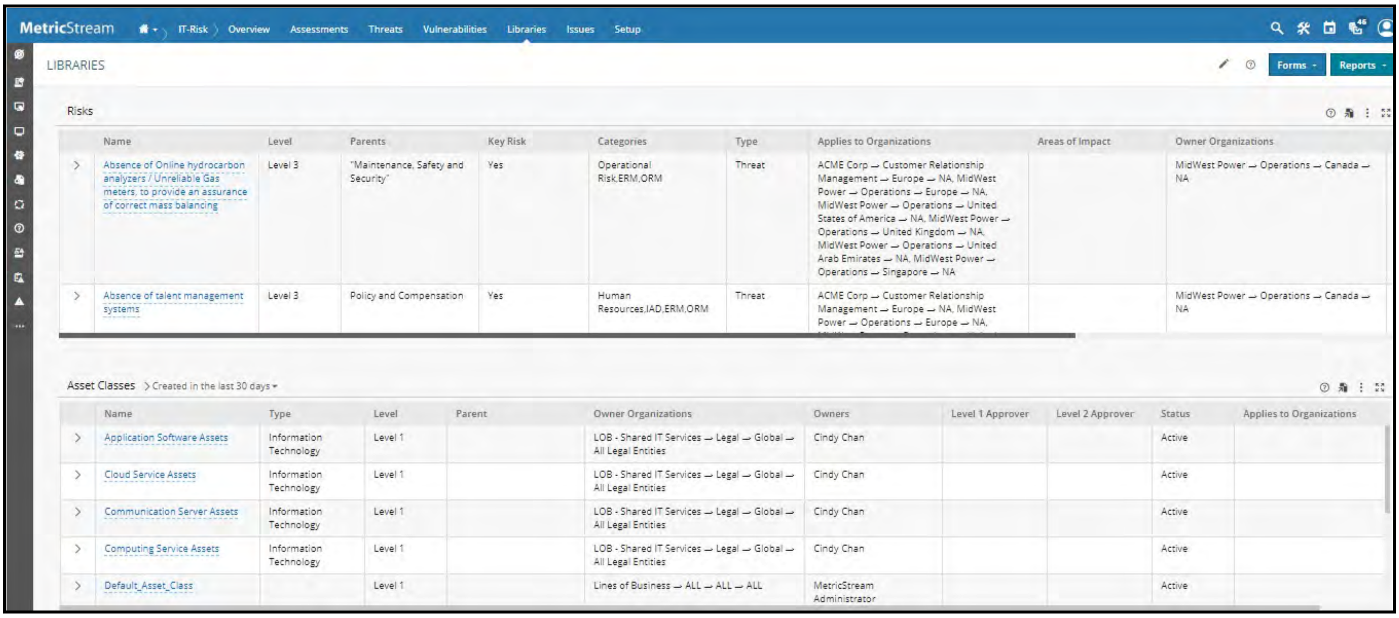
Use this report to:
This is a drill down report from the **Threats** report and the **Vulnerabilities** report. You can view the name of all the threat associated with the selected threat/vulnerability.

Key Columns

Column	Description
Name	Displays the name of the threat associated with the threat/vulnerability.

Libraries

Use the **Libraries** page to manage libraries such as risks, asset, asset classes, processes related to IT- Risk Management. Also, able to structure the IT - Risk Assessment my mapping the Risks to related asset, asset classes and processes as required. View reports related to libraries and modify them. The following **Libraries** page is available for IT - Risk Manager and IT - Risk Analyst. For more information on the role-infocenter/privilege mapping, see Roles, Privileges, and Infocenters.



LIBRARIES

Risks

	Name	Level	Parents	Key Risk	Categories	Type	Applies to Organizations	Areas of Impact	Owner Organizations
>	Absence of Online hydrocarbon analyzers / Unreliable Gas meters, to provide an assurance of correct mass balancing	Level 3	"Maintenance, Safety and Security"	Yes	Operational Risk,ERM,ORM	Threat	ACME Corp → Customer Relationship Management → Europe → NA, MidWest Power → Operations → Europe → NA, MidWest Power → Operations → United States of America → NA, MidWest Power → Operations → United Kingdom → NA, MidWest Power → Operations → United Arab Emirates → NA, MidWest Power → Operations → Singapore → NA		MidWest Power → Operations → Canada → NA
>	Absence of talent management systems	Level 3	Policy and Compensation	Yes	Human Resources,IAD,ERM,ORM	Threat	ACME Corp → Customer Relationship Management → Europe → NA, MidWest Power → Operations → Europe → NA,		MidWest Power → Operations → Canada → NA

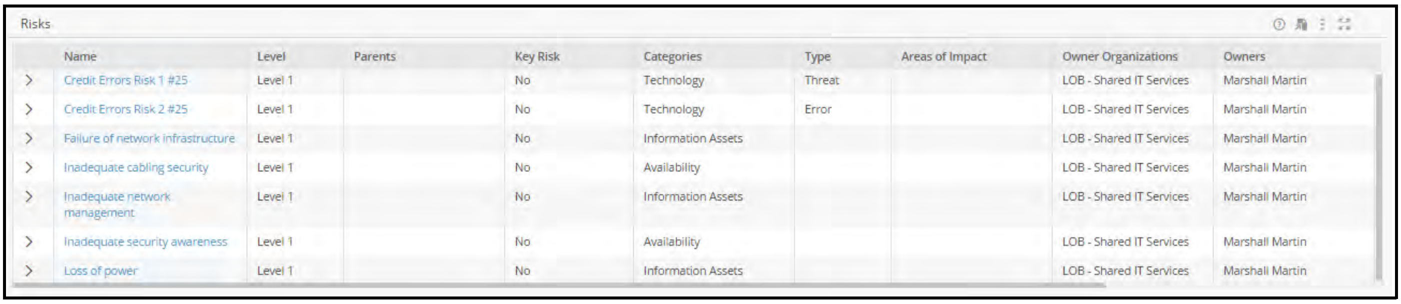
Asset Classes > Created in the last 30 days

	Name	Type	Level	Parent	Owner Organizations	Owners	Level 1 Approver	Level 2 Approver	Status	Applies to Organizations
>	Application Software Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan			Active	
>	Cloud Service Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan			Active	
>	Communication Server Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan			Active	
>	Computing Service Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan			Active	
>	Default_Asset_Class		Level 1		Lines of Business → ALL → ALL → ALL	MetricStream Administrator			Active	

Figure 51 Libraries Page

Risks Report

Use the **Risks** report to view the details of all the Risks in the system and manage them.



Risks

	Name	Level	Parents	Key Risk	Categories	Type	Areas of Impact	Owner Organizations	Owners
>	Credit Errors Risk 1 #25	Level 1		No	Technology	Threat		LOB - Shared IT Services	Marshall Martin
>	Credit Errors Risk 2 #25	Level 1		No	Technology	Error		LOB - Shared IT Services	Marshall Martin
>	Failure of network infrastructure	Level 1		No	Information Assets			LOB - Shared IT Services	Marshall Martin
>	Inadequate cabling security	Level 1		No	Availability			LOB - Shared IT Services	Marshall Martin
>	Inadequate network management	Level 1		No	Information Assets			LOB - Shared IT Services	Marshall Martin
>	Inadequate security awareness	Level 1		No	Availability			LOB - Shared IT Services	Marshall Martin
>	Loss of power	Level 1		No	Information Assets			LOB - Shared IT Services	Marshall Martin

Figure 52 Risks Report

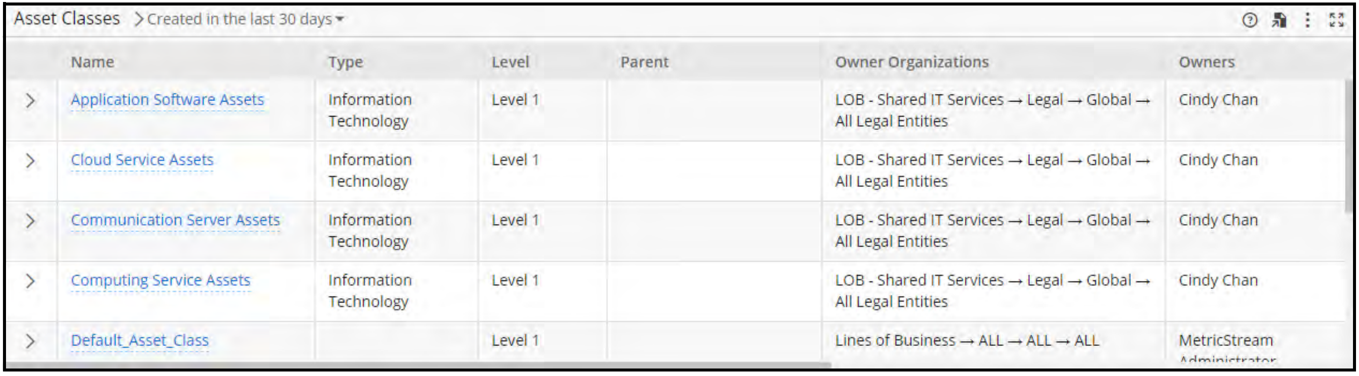
Key Columns:

- **Name:** Displays the name of the Risk.
  - Drill Down: **Risk** form
- **Categories:** Displays the category of the Risk.
- **Parents:** Displays the parent risk.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Governance, Risk and Compliance Foundation - User Guide.

Asset Classes

Use Asset Classes report to view details of the active and inactive Asset Classes in the library.



Asset Classes > Created in the last 30 days

	Name	Type	Level	Parent	Owner Organizations	Owners
>	Application Software Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan
>	Cloud Service Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan
>	Communication Server Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan
>	Computing Service Assets	Information Technology	Level 1		LOB - Shared IT Services → Legal → Global → All Legal Entities	Cindy Chan
>	Default_Asset_Class		Level 1		Lines of Business → ALL → ALL → ALL	MetricStream Administrator

Key Columns:

- **Name**: Displays the Asset Class name. When you move the pointer over the name, the Hover Card appears.
  - o Drilled-down: **Asset Class** form.
- **Level**: Displays the level of the Asset Class.
- **Parent**: Displays the name of the parent Asset Class. This column remains blank if the hierarchical level of the Asset Class is level 1.
- **Status**: Displays the status of the Asset Class.

Forms

Use the links within the **Forms** drop-down list to create the library contents such as Asset, Asset class, Process and so on that are required for conducting the IT - Risk assessments as shown in the following figure.

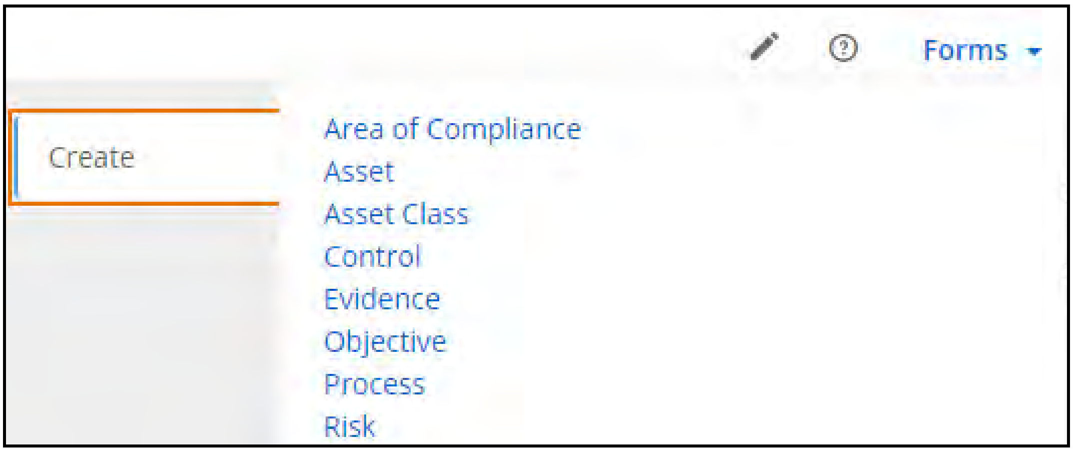


Figure 53 Forms of Libraries

You can create:

- **Area of Compliance:** Opens the **Area of Compliance** form. Use this form to document the area of compliances related to IT - Risk such 12 CFR Part 205, Electronic Fund Transfers, COBIT 5, 17 CFR Part 240.15d-15, and so on.
- **Asset:** Opens the **Asset** form. Use this form to document the assets related to IT.
- **Asset Class:** Opens the **Asset Class** form. This categorizes the assets based on their features and operational capabilities. It models the business and technical categorization of assets. An asset can belong to one or more asset classes and an asset class can have one or more assets.
- **Control:** Opens the **Control** form. Define methods, procedures, processes, systems, or software artifacts designed to enforce and reflect the policies, procedures, practices, and organizational structures, which are

required to ensure that the business objectives are achieved, and undesirable events are detected and corrected.

- **Evidence:** Opens the **Evidence** form. This servers as a single centralized repository for all the documents which can be used during the IT-Risk related activities.
- **Objective**: Opens the **Objective** form. Use the form to define and create a new objective and also send it for approval.
- **Process:** Opens the **Process** form. Use this form to document all the processes related to IT asset management.
- **Risk:** Opens the **Risk** form. Use this form to document the Risk related to IT such as Asset Management Risk, Access Control, Abuse of user right permission and so on.

Note: For details, refer to the MetricStream Arno Release Spring '21 - Governance, Risk and Compliance Foundation - User Guide.

Reports

Use the links within the **Reports** drop-down list to view and modify the library contents such as Asset, Asset class, Process and so on that are required for conducting the IT - Risk assessments as shown in the following figure.

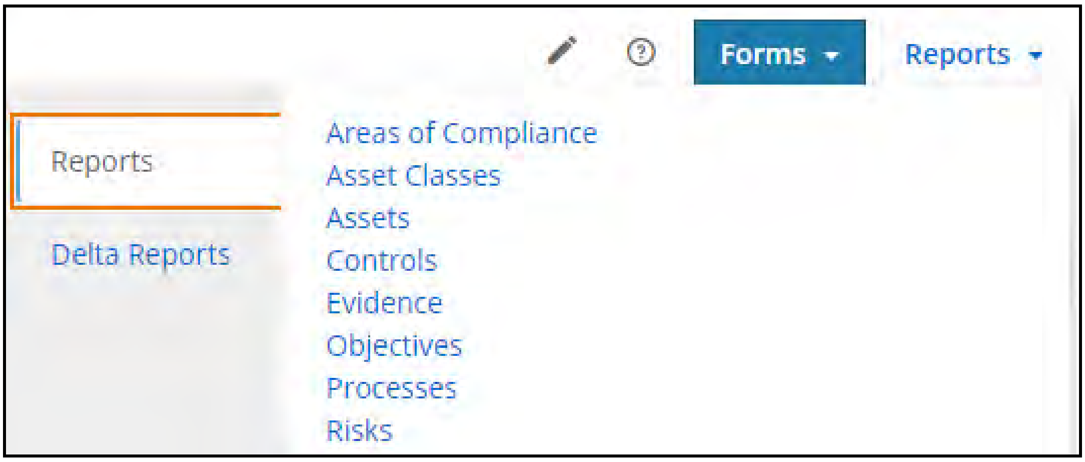


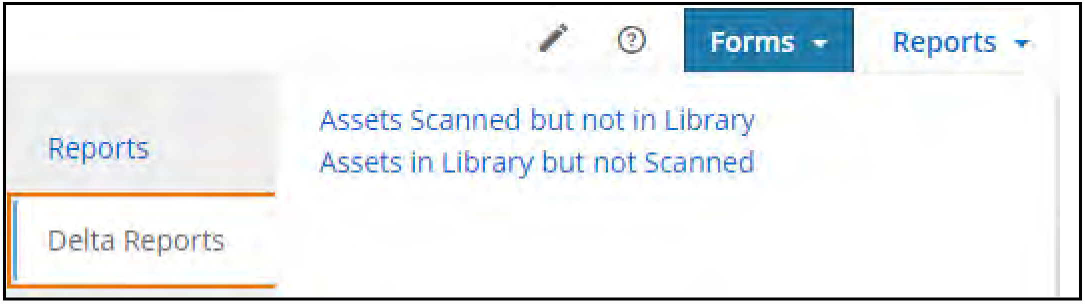
Figure 54 Reports of Libraries

You can access the following key reports:

- **Areas of Compliance:** Opens the **Areas of Compliance** report, which displays all the areas of compliance in the application.
- **Asset Classes:** Opens the **Asset Classes** report, which displays all the asset classes available in the application.
- **Assets:** Opens the **Assets** report, which displays all the assets available in the application.
- **Controls:** Opens the **Controls** report, which displays all the controls available in the application.
- **Evidence:** Opens the **Evidence** report, which displays all the evidences available in the application.
- **Objectives**: Opens the **Objectives** report, which displays all the objectives available in the application.
- **Processes:** Opens the **Processes** report, which displays all the processes available in the application.
- **Risks:** Opens the **Risks** report, which displays all the risks available in the application.

Note: For details, refer to the MetricStream Arno Release Spring '21 - Governance, Risk and Compliance Foundation - User Guide.

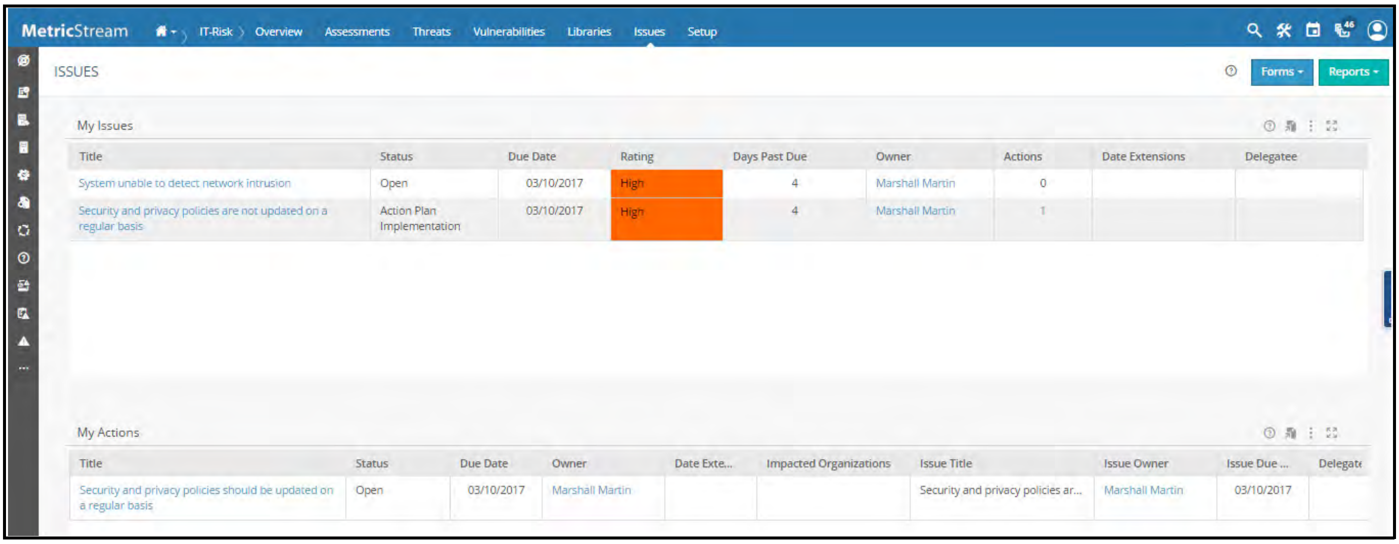
You can also Access delta reports:


Forms
Reports
Reports
Delta Reports
Assets Scanned but not in Library
Assets in Library but not Scanned

- **Assets Scanned but not in Library**: This report provides a list of assets scanned by either of the network vulnerability scanners QualysGuard or Nessus or both. These assets are not created in GRC Libraries.
- **Assets in Library but not Scanned:** This report provides a list of available assets in GRC Libraries. These assets are not scanned by either of the network vulnerability scanners - QualysGuard or Nessus or both.

Issues

Use the **Issues** page to report an issue, initiate an action to resolve the issue, view different issue/action details. The following **Issues** page is available for IT - Risk Manager, IT - Risk Analyst and It - Risk Assessor. For more information on the role-infocenter/privilege mapping, see Roles, Privileges, and Infocenters.



ISSUES

My Issues

Title	Status	Due Date	Rating	Days Past Due	Owner	Actions	Date Extensions	Delegatee
System unable to detect network intrusion	Open	03/10/2017	High	4	Marshall Martin	0		
Security and privacy policies are not updated on a regular basis	Action Plan Implementation	03/10/2017	High	4	Marshall Martin	1		

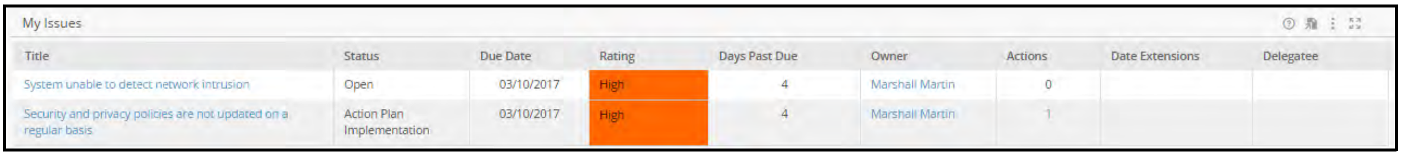
My Actions

Title	Status	Due Date	Owner	Date Exte...	Impacted Organizations	Issue Title	Issue Owner	Issue Due ...	Delegate
Security and privacy policies should be updated on a regular basis	Open	03/10/2017	Marshall Martin			Security and privacy policies ar...	Marshall Martin	03/10/2017	

Figure 55 Issues Page

My Issues Report

Use the **My Issues** report to view the details of all the issues that you need to manage and monitor. Using this report, you can initiate actions, delegate and so on based on the workflow stage of the issue.



My Issues

Title	Status	Due Date	Rating	Days Past Due	Owner	Actions	Date Extensions	Delegatee
System unable to detect network intrusion	Open	03/10/2017	High	4	Marshall Martin	0		
Security and privacy policies are not updated on a regular basis	Action Plan Implementation	03/10/2017	High	4	Marshall Martin	1		

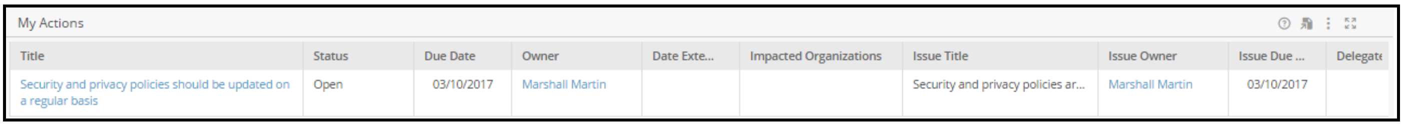
Figure 56 My Issues Report

Key Columns:

- **Title:** Displays the title of the issue.
  - Drill Down: **Issue** form
- **Due Date:** Displays the date by when issue needs to be remediated.

My Actions Report

Use the **My Actions** report to view the list of actions that you need to work on to remediate the issue.



My Actions

Title	Status	Due Date	Owner	Date Exte...	Impacted Organizations	Issue Title	Issue Owner	Issue Due ...	Delegate
Security and privacy policies should be updated on a regular basis	Open	03/10/2017	Marshall Martin			Security and privacy policies ar...	Marshall Martin	03/10/2017	

Figure 57 My Actions Report

Key Columns:

- **Title:** Displays the title of the issue.
  - o Drill Down: **Issue** form
- **Due Date:** Displays the date by when issue needs to be remediated.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Forms

Use the links within the **Forms** drop-down list to log an issue, initiate an action, and auto delegate an issue as shown in the following figure.

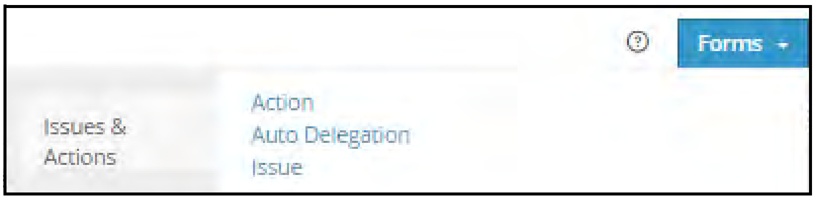


Figure 58 Forms of Issues & actions

You can access the following forms:

- **Action:** Opens the **Action** form. Use this form to initiate an action to resolve the issue.
- **Auto Delegation:** Opens the **Auto Delegation** form. Use this form to delegate the action to a different user.
- **Issue:** Opens the **Issue** form. Use this form to report an issue.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Reports

Use the links within the **Reports** drop-down list to view and assign issues, as shown in the following figure.

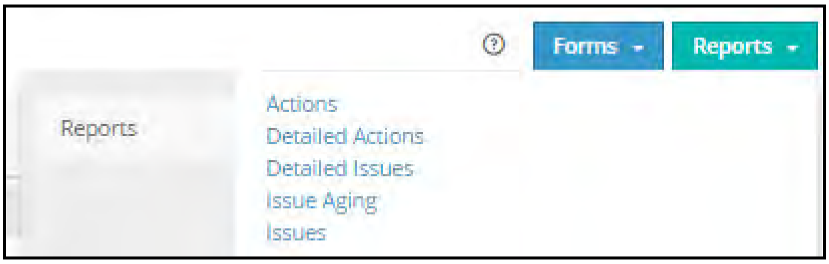


Figure 59 Reports of Issues

You can access the following reports:

- **Actions**: Use the **Actions** report to view the details (such as percentage of action completed and date on which the action was closed) of all the action items triggered in the system.
- **Detailed Actions**: Use the **Detailed Actions** report to view the details (such as status and owner of the action) about all the actions created in the system along with the issue associated with it.
- **Detailed Issues**: Use the **Detailed Issues** report to view the detailed information (such as status and rating of the issue) about all the issues triggered in the system.
- **Issue Aging**: Use the **Issue Aging** report to view the aggregated count of issues by the time period. The split by the time period helps the user to identify issues that need immediate attention (issues already overdue) and plan activities for issues that will become overdue soon. This report displays the following:
  - Issues that have become overdue in the last 1 month, 1-3 months, beyond 3 months and so on.
  - Issues that will become overdue in the next 1 month, 1-3 months, and beyond 3 months.
- **Issues**: Use the **Issues** report to view the details (such as due date and action associated) of all the issues triggered in the system.

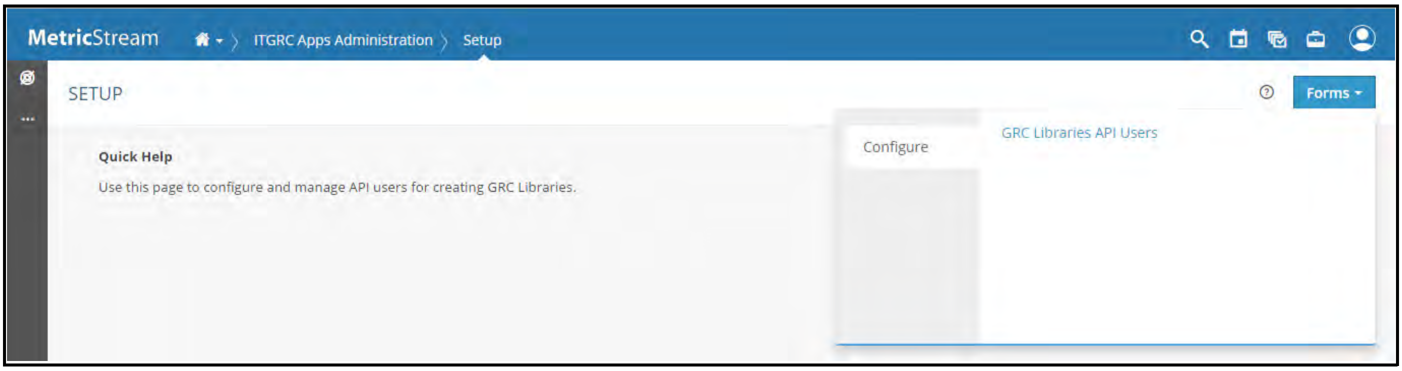
Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Issues - User Guide.

Setup (ITGRC Apps Administrator)

You need to configure this before you can start the setup of IT-Risk Management Framework. Use the Setup page to configure and manage the API users who can create the GRC Libraries - Areas of Compliance, Asset Classes, and Assets.

Note: **ITGRC_Configure_GRC_Libraries_API_Users** activity should be mapped to ITGRC Apps Administrator.

The following Setup page is only available for ITGRC Apps Administrator. For more information on the role-infocenter/privilege mapping, see Roles, Privileges, and Infocenters.



Quick Help

Use this page to configure and manage API users for creating GRC Libraries.

Figure 60 Setup Page for ITGRC Apps Administrator

Forms

Use the link within the **Forms** button to access the forms, as illustrated next.

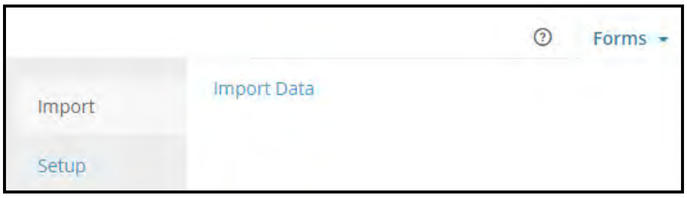


Figure 61 Forms of Setup

Forms	Description
Import	
Import Data	Opens the **Import Data** form to upload the library content, Threat Actor, Threat, and Vulnerability details. For more information, refer Uploading Data.
Setup	
GRC Libraries API Users	Opens **GRC Libraries API Users** form. Use this form to configure and manage API users. For more information, refer GRC Libraries API Users Form.
GRC Libraries Relationship Configuration	Opens **GRC Libraries Relationship Configuration** form. Use this form to configure relationships with GRC library. For more information, refer to the MetricStream Arno Release Spring ‘21 - GRC Intelligence - User Guide.

Forms	Description
IT-GRC Apps Configuration	Opens **IT-GRC Apps Configuration** form. Use this form to configure motives of the threat actor, and scale to be used in the **Threat** form. For more information, refer IT-GRC Apps Configuration Form. You can also capture issue types and asset business criticality. For more information, refer to MetricStream Arno Release Spring ‘21 - IT-Compliance Management - User Guide.

Uploading Data

You can upload the data directly to the Threat actor, Threat, and Vulnerability forms by downloading an export Excel template, enter the details, and then upload them back.

To upload data:

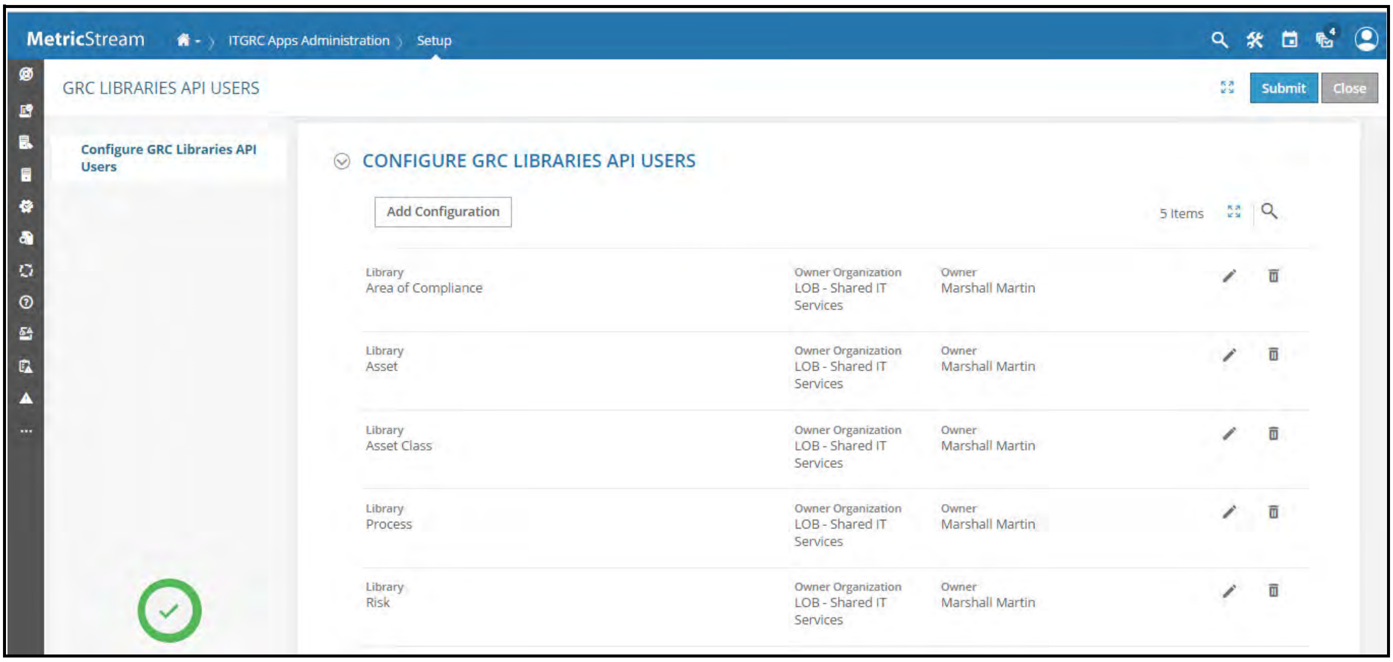
1. Open the **Data Import Excel Template** report.
2. In the **Template File** column, click the required link (for example, MS_ITS_THREAT_ACTOR.xls) to download the Excel template.
3. Open the template, fill the details, and then save the file.
4. From **Forms**, click **Import** and click **Import Data**.
   The **Import Data** form appears.
5. From the **Entity** list, select the required (Threat, Threat Actor, or Vulnerability) entity.
6. From the **Profile** list, select the required profile.
7. In the **File to import** field, click ■ to browse and import the updated file.
8. Click **Submit**.

Note: Use the Import Status report to view the details about the recently uploaded data.

GRC Libraries API Users Form

You can add new configurations to the list and edit or delete existing configurations with this form. You can configure 5 library options:

- Area of Compliance
- Asset
- Asset Class
- Process
- Risk


MetricStream
ITGRC Apps Administration
Setup
GRC LIBRARIES API USERS
Submit
Close
Configure GRC Libraries API Users
CONFIGURE GRC LIBRARIES API USERS
Add Configuration
5 Items

Library	Owner Organization	Owner
Area of Compliance	LOB - Shared IT Services	Marshall Martin
Asset	LOB - Shared IT Services	Marshall Martin
Asset Class	LOB - Shared IT Services	Marshall Martin
Process	LOB - Shared IT Services	Marshall Martin
Risk	LOB - Shared IT Services	Marshall Martin

Figure 62 Configuring GRC Libraries API Users

Adding a configuration

To add a new configuration:

1. Click **Add Configuration**.
   The **Configuration** window appears.
2. Provide information in the required fields as described in the following table.

Field	Description
Library	From the drop-down list, select the required library option. For example, Asset.

Field	Description
Owner Organization	The organization that is responsible for managing the selected library option. To select one or more organizations: **1.** Click Add icon associated with the field. The **Owner Organization** window appears displaying the defined organization structure. **2.** Select the required organization structure, and then click **Add**. a. If you want to add more organization structures in the **Owner Organization** window, select the **Add Another** check box. b. Select the organization structure that needs to be added, and then click **Add to List**. After you added all the required organizations, click **Done** to close the Owner Organization window.
Owner	The users of the selected owner organization, who are responsible for managing the selected library option. The list of users available for selection is based on the selected organization structure.

3. Click **Done** to confirm the selection.

Note: Click **Cancel** to discard the changes.

Editing a configuration

To edit an existing configuration:

Step 1 Click Edit icon. The **Configuration** window appears.

Step 2 Refer to steps 2 through 7 of Adding a configuration.

Deleting a configuration

To delete an existing configuration:

Click Delete icon to delete a configuration.

Note: Click Undo icon to undo the deletion.

After completing the changes, click **Submit** to confirm the configuration changes.

IT-GRC Apps Configuration Form

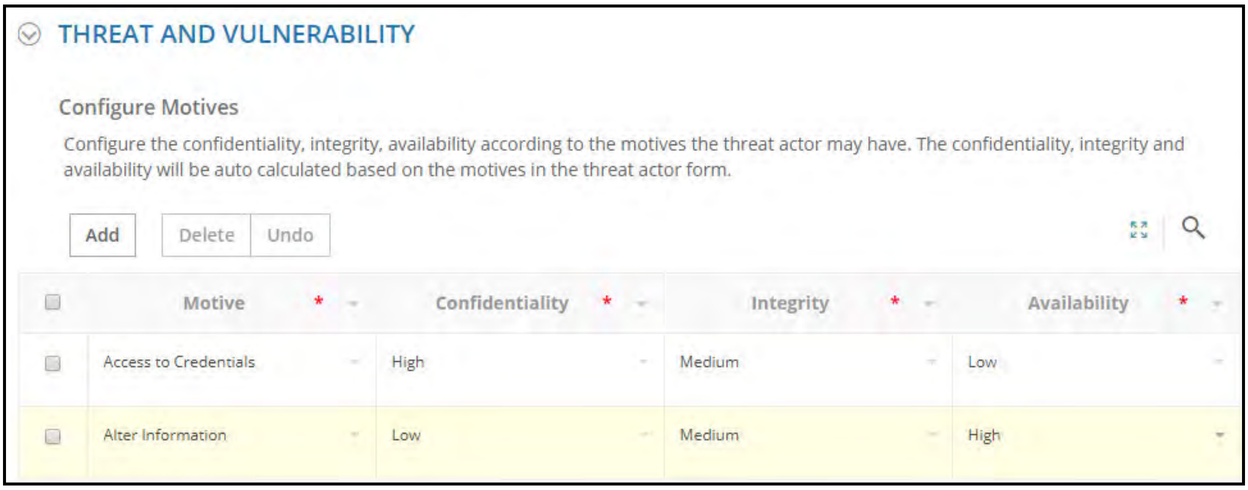
The **IT-GRC Apps Configuration** form allows you to configure the details related to IT-Compliance and Threat and Vulnerability.

The **IT-GRC Apps Configuration** form comprises the following sections:

HEADER	Displays the action buttons to take action on the form.
IT-COMPLIANCE	Helps you to configure issue types and business criticality rate for assets. For more information, refer to IMetricStream Arno Release Spring ‘21 - IT-Compliance Management - User Guide..
THREAT AND VULNERABILITY	Helps you to configure motives of the threat actor and scale to be used in the **Threat** form.

To configure details related to Threat and Vulnerability:

1. From **Setup** and click **IT-GRC Apps Configuration**.
   The **IT-GRC Apps Configuration** form opens.
2. In the **Threat and Vulnerability** section, proceed to configure motives of the threat actor and scale of measurement of threat actor skills.
   a. In the **Configure Motives** subsection, click **Add** to add motives of the threat actor.
   A row appears.



THREAT AND VULNERABILITY

Configure Motives

Configure the confidentiality, integrity, availability according to the motives the threat actor may have. The confidentiality, integrity and availability will be auto calculated based on the motives in the threat actor form.

☐	Motive *	Confidentiality *	Integrity *	Availability *
☐	Access to Credentials	High	Medium	Low
☐	Alter Information	Low	Medium	High

Figure 63 Configure Motives subsection

b. Provide required information in the columns as described in the following table.

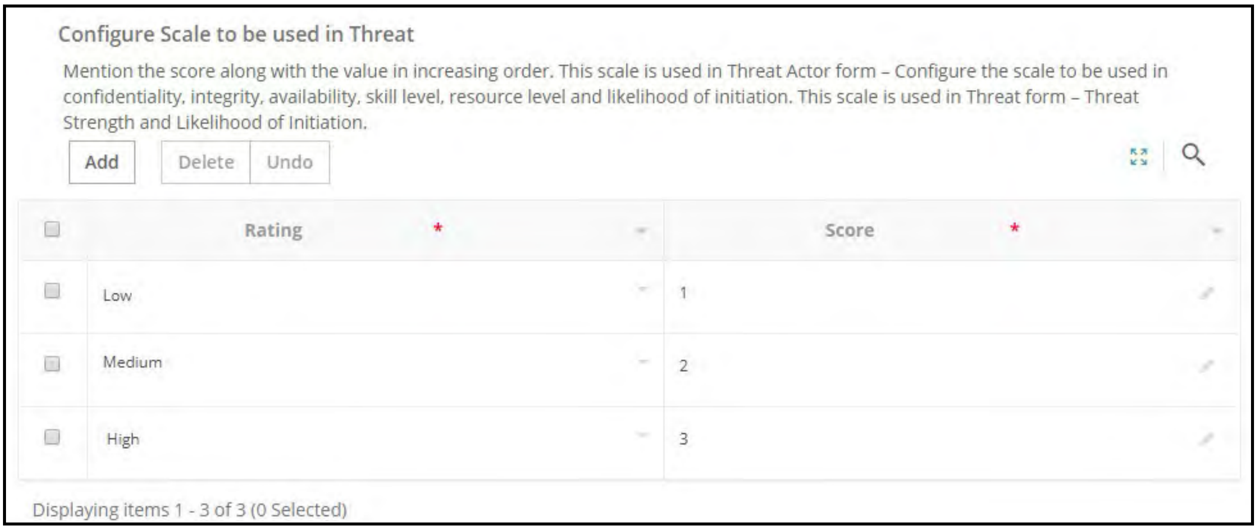
Column	Description
Motive	The motives of the threat actors.
Confidentiality	The confidentiality level corresponding to the motive.
Integrity	The integrity level corresponding to the motive.
Availability	The availability level corresponding to the motive.

Notes:

- To delete any added motives, select them, and then click **Delete**.
- To retrieve the last deleted motives, click **Undo**.

- The motives configured here is available in the **Motives** field in the **Threat Actor** form. For more information, refer to MetricStream Arno Release Spring ‘21 - Threat and Vulnerabilities - User Guide.

c. In the **Configure Scale to be used in the Threat** section, click **Add**.
A row appears.



Configure Scale to be used in Threat

Mention the score along with the value in increasing order. This scale is used in Threat Actor form – Configure the scale to be used in confidentiality, integrity, availability, skill level, resource level and likelihood of initiation. This scale is used in Threat form – Threat Strength and Likelihood of Initiation.

□	Rating *	Score *
□	Low	1
□	Medium	2
□	High	3

Displaying items 1 - 3 of 3 (0 Selected)

Figure 64 Configure Scale to be used in Threat subsection

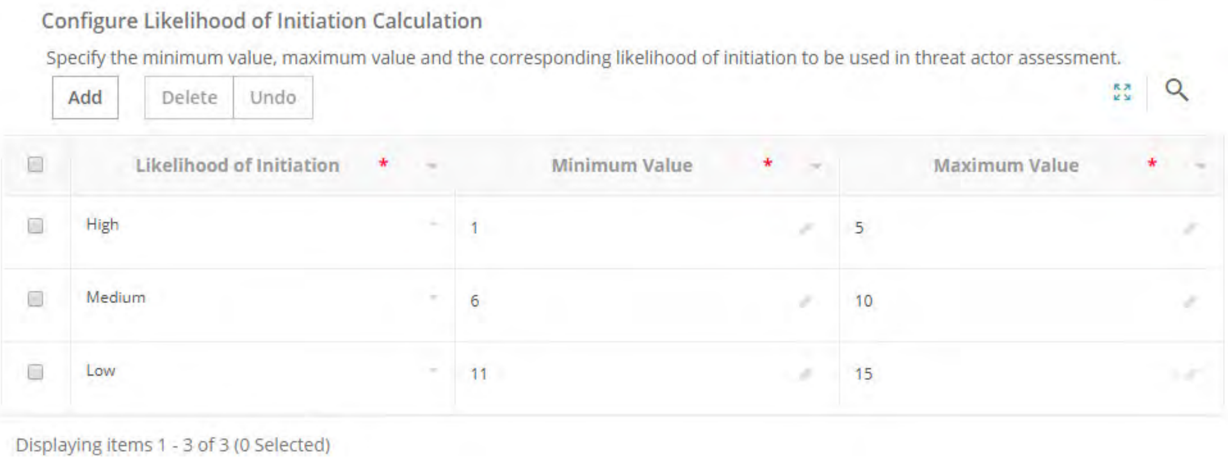
d. Provide required information in the columns as described in the following table.

Column	Description
Rating	The rating for the skill and resource level associated with the threat actor.
Score	The score corresponding to the skill and resource level rating.

Notes:

- To delete any added scale, select them, and then click **Delete**.
- To retrieve the last deleted scale, click **Undo**.
- The measurement scale configured for the confidentiality, integrity, availability, skill, and resource levels for the motives is used in the **Threat Actor** form.
- The configured measurement scale is used for calculating the **Likelihood of Initiation** is used in the **Threat Actor** form. For more information, refer to MetricStream Arno Release Spring ‘21 - Threat and Vulnerabilities - User Guide.
- The configured measurement scale is used in the calculation of **T**hreat Strength is used in the **Threat** form. For more information, refer MetricStream Arno Release Spring ‘21 - Threat and Vulnerabilities - User Guide.

e. In the **Likelihood of Initiation Calculation** subsection, click **Add**.
   A row appears.



Configure Likelihood of Initiation Calculation

Specify the minimum value, maximum value and the corresponding likelihood of initiation to be used in threat actor assessment.

□	Likelihood of Initiation *	Minimum Value *	Maximum Value *
□	High	1	5
□	Medium	6	10
□	Low	11	15

Displaying items 1 - 3 of 3 (0 Selected)

Figure 65 Configure Likelihood of Initiation Calculation subsection

f. Provide required information in the columns as described in the following table.

Column	Description
Likelihood of Initiation	The level of likelihood of initiation used in threat actor assessment.
Minimum Value	The minimum value corresponding to the likelihood of initiation.
Maximum Value	The maximum value corresponding to the likelihood of initiation.

Notes:

- To delete any added Likelihood of Initiation, select them, and then click **Delete**.
- To retrieve the last deleted Likelihood of Initiation, click **Undo**.
- Based on the configured measurement scale and likelihood of initiation, the **Likelihood of Initiation** of a **Capability** is calculated. For example, if the selected rating is High and Medium with a score of 1 and 2 respectively, then the Likelihood of Initiation is 1 x 2 = 2 and as 2 is in the range of 1 to 5, the **Likelihood of Initiation** is calculated as **High**.

3. Click **Submit** to save the changes made to the IT-GRC Configuration form.

Note: Click **Close** to close the form without saving changes.

Editing IT-GRC Apps Configuration

You can edit an existing IT-GRC Apps Configuration, if you have the required privilege.

1. Open the IT-GRC Apps Configuration form from a relevant report.
2. Click **Edit Configuration**.
   The IT-GRC Apps Configuration form is opened in the edit mode. For more information, refer IT-GRC Apps Configuration Form.
3. Make the necessary changes, and then perform the required action.

Reports

Use links within the **Reports** button to access the IT-GRC Apps Configuration report, as displayed in the following figure.

GRC Libraries API Users Configuration

Use this report to:
View the GRC libraries API users configuration and edit the configuration, if required. For more information on editing the GRC libraries API users Configuration, refer Editing a configuration.

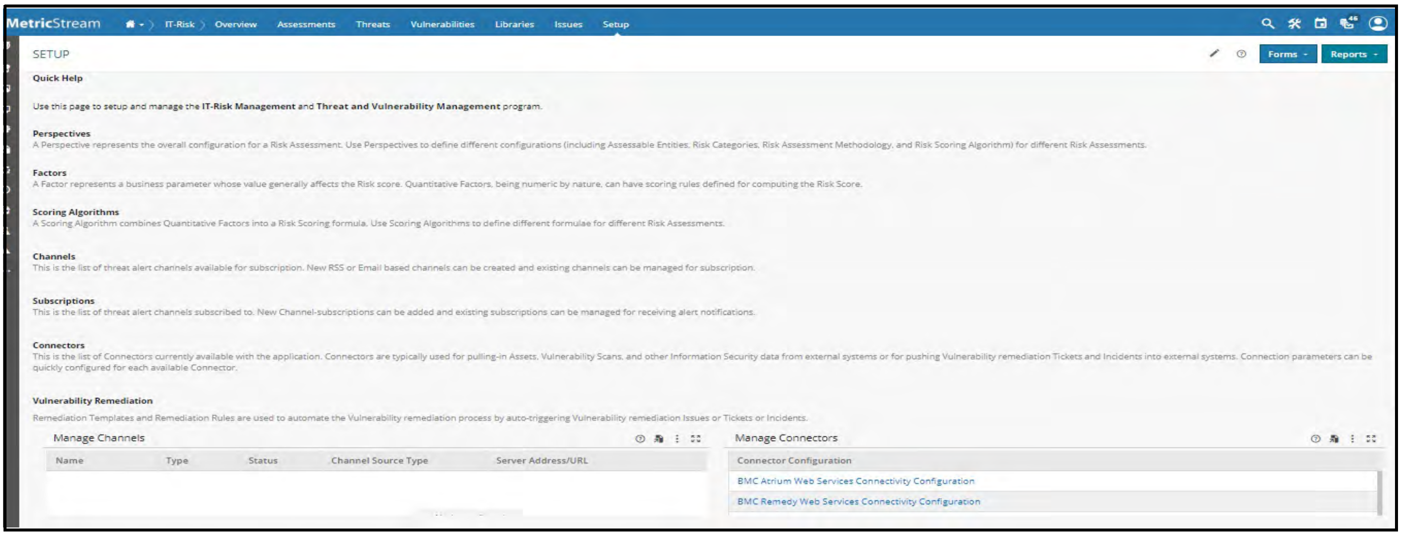
IT-GRC Apps Configuration Report

Use this report to:
View the IT-GRC Apps configuration and edit the configuration, if required. For more information on editing the IT-GRC Apps Configuration, refer Editing IT-GRC Apps Configuration.

Setup (for other users)

Use the **Setup** page to perform various administrative functions related to IT-Risk management. A quick help is also available for you to set up and manage connectors and the Threat and Vulnerability Management program.

The following **Setup** page is available for IT - Risk Manager and IT - Risk Analyst. For more information on the role-infocenter/privilege mapping, see Roles, Privileges, and Infocenters.



Quick Help

Use this page to setup and manage the **IT-Risk Management** and **Threat and Vulnerability Management** program.

Perspectives
A Perspective represents the overall configuration for a Risk Assessment. Use Perspectives to define different configurations (including Assessable Entities, Risk Categories, Risk Assessment Methodology, and Risk Scoring Algorithm) for different Risk Assessments.

Factors
A Factor represents a business parameter whose value generally affects the Risk score. Quantitative Factors, being numeric by nature, can have scoring rules defined for computing the Risk Score.

Scoring Algorithms
A Scoring Algorithm combines Quantitative Factors into a Risk Scoring formula. Use Scoring Algorithms to define different formulae for different Risk Assessments.

Channels
This is the list of threat alert channels available for subscription. New RSS or Email based channels can be created and existing channels can be managed for subscription.

Subscriptions
This is the list of threat alert channels subscribed to. New Channel-subscriptions can be added and existing subscriptions can be managed for receiving alert notifications.

Connectors
This is the list of Connectors currently available with the application. Connectors are typically used for pulling-in Assets, Vulnerability Scans, and other Information Security data from external systems or for pushing Vulnerability remediation Tickets and Incidents into external systems. Connection parameters can be quickly configured for each available Connector.

Vulnerability Remediation
Remediation Templates and Remediation Rules are used to automate the Vulnerability remediation process by auto-triggering Vulnerability remediation Issues or Tickets or Incidents.

Manage Channels

Name	Type	Status	Channel Source Type	Server Address/URL

Manage Connectors

Connector Configuration
BMC Atrium Web Services Connectivity Configuration
BMC Remedy Web Services Connectivity Configuration

Figure 66 Setup Page

Note: The Setup page provides a brief help text about various features available in the page.

Forms

Use the links within the **Forms** drop-down list, as shown in the following figure, to access various forms that help in the setting up the product before you begin with the IT- Risk Management assessments.

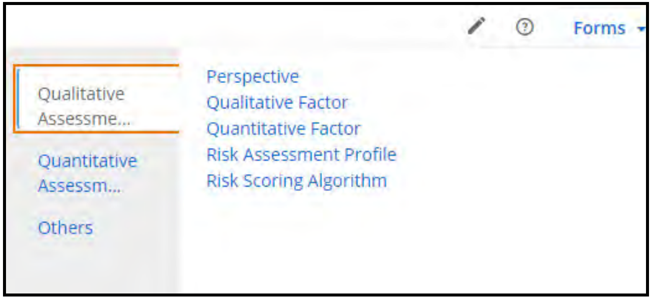


Figure 67 Forms of Setup Page

You can create:

- **Perspective:** Opens the **Perspective** form. Perspectives enable organizations to perform various types of risk assessments by using different types of risk scoring algorithms and risk configuration matrix.
- **Qualitative Factor:** Opens the **Qualitative Factor** form. A qualitative factor represents a question, whose responses can be a text, number, date and so on. Use this form to define questions and the corresponding response. The qualitative factors do not carry any weightage.
- **Quantitative Factor:** Opens the **Quantitative Factor** form. Quantitative assessment factors are those factors that are assessed, and the assessment of these factors determines the overall risk score and rating. The two types of quantitative factors are standard and non-standard factors.

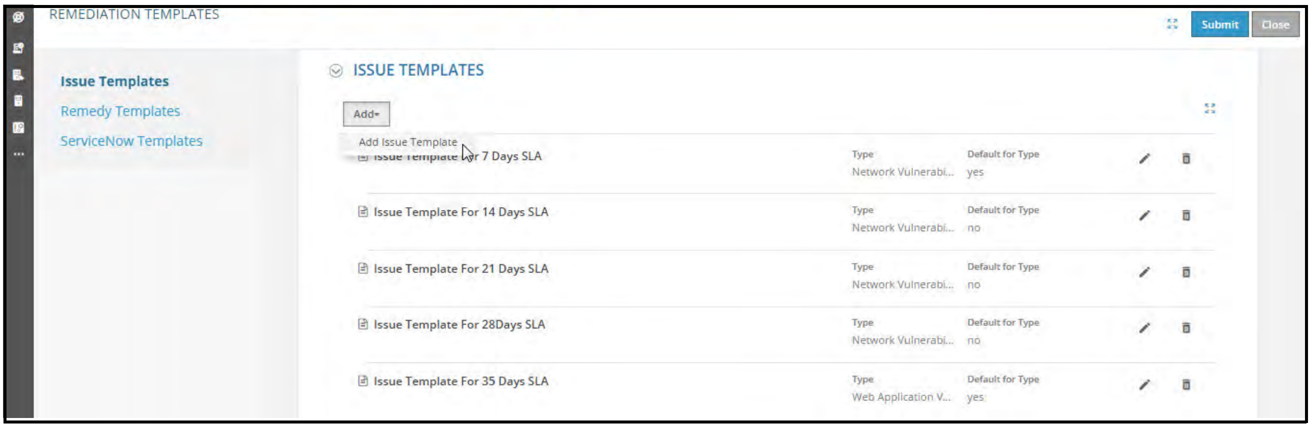
- **Risk Assessment Profile:** Opens the **Risk Assessment Profile** form, allows you to specify the risk assessment methodology, scoring algorithm, roll-up logic, risk ranges, configuring risk matrix, setting up control assessment, and configuring heat map.
- **Risk Scoring Algorithm:** Opens the **Risk Scoring Algorithm** form, allows you to define the IT-specific risk scoring algorithm based on which the risk assessment is conducted.
- **Create Channel:** Opens the **Channel** form. By using this form, you can create threat alert channels. For more information, refer to the MetricStream Arno Release Spring ‘21 - GRC Intelligence - User Guide.
- **Channel Subscription:** Opens the **Channel Subscription** form. Use this form to subscribe to the threat alert channels. You can add new channel subscriptions and view the existing channel groups to which you are subscribed. You can add new RSS or email based channels for subscriptions. Additionally, use the **Channel Group Subscriptions** section to create and manage a group of channels.
- **Remediation Rules:** Opens the **Remediation Rules** form, provides an intuitive rule builder that lets you combine the business context for your assets with the vulnerability context for those assets.
- **Remediation Template:** Opens the **Remediation Templates** form. Use this form to create either remedy template or an issue template to trigger incidents or issues. For more information, refer Remediation Templates.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Risk Assessments - User Guide.

Remediation Templates

The first step of managing your threat and vulnerability management program, is to define remediation templates. These are essentially blueprints for tickets that you want to automatically trigger based on remediation rules (which we will get to shortly). You can choose to manage the tickets using MetricStream's Issues capability or the service desk tool (for example, BMC Remedy) that is already deployed in your organization. These options are described next.

Adding Issue Template



	Type	Default for Type
Issue Template For 7 Days SLA	Network Vulnerabi...	yes
Issue Template For 14 Days SLA	Network Vulnerabi...	no
Issue Template For 21 Days SLA	Network Vulnerabi...	no
Issue Template For 28Days SLA	Network Vulnerabi...	no
Issue Template For 35 Days SLA	Web Application V...	yes

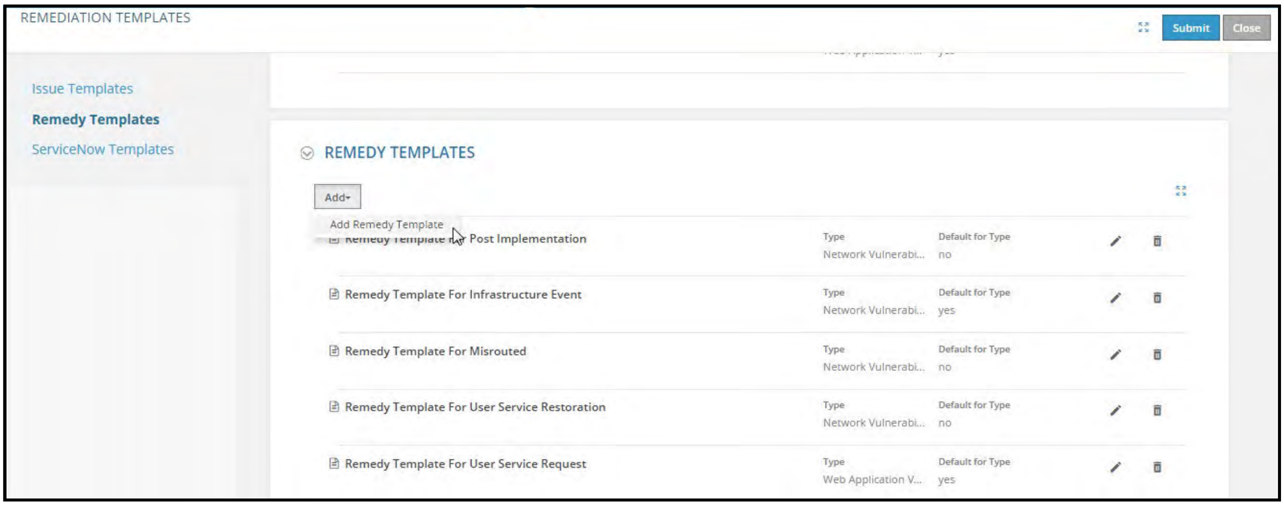
Figure 68 Adding Issue Template

Field	Description
Click **Add** and click **Add Issue Template** to add a new issue template.	
Name	Type the name of the issue template.
Type	Select the type of issue template. The available options are: • Network Vulnerability Remediation • Web Application Vulnerability Remediation
Default for Type	Select this check box if you want to mark the current template as default to create an issue manually.
Title	Displays the title of the issue.

Field	Description
Owner Organization	Select owner organization responsible for maintaining the issue. This field displays the various levels of organizations available to the current user. To select the owner organization: **1.** Click **Add** icon associated with the field. The **Owner Organization** window appears displaying the defined organization structure. **2.** Select the required organization structure, and then click **Add**. **Note:** For more details on multidimensional organization structure, see MetricStream Arno Release Spring '21 - Threat and Vulnerability Management - User Guide.
Owner	Select a user who is responsible for addressing the reported issue. When you submit the form, the selected issue owner receives a task to review the issue. The list of users available for selection is based on the selected organization structure.
Issue Type	Select the type of the issue.
Due Date	Type the number of days after which the issue is due.
Issue Approver Section	
Initial Approver - Organization	Select the organization to which the initial approver of the issue belongs to. To select the initial approver organization: **1.** Click **Add** icon associated with the field. The **Initial Approver Organization** window appears displaying the defined organization structure. **2.** Select the required organization structure, and then click **Add**. **Note:** For more details on multidimensional organization structure, see MetricStream Arno Release Spring '21 - Threat and Vulnerability Management - User Guide.
Initial Approver	Select the initial approver owner of the issue. The list of users available for selection is based on the selected organization structure.
Action Plan Approver Organization	Select the organization to which the action plan approver of the issue belongs to. **Note:** This section will display based on global ISM configuration. To select the action plan approver organization: **1.** Click **Add** icon associated with the field. The **Action Plan Approver Organization** window appears displaying the defined organization structure. **2.** Select the required organization structure, and then click **Add**. **Note:** For more details on multidimensional organization structure, see MetricStream Arno Release Spring '21 - Threat and Vulnerability Management - User Guide.

Field	Description
Action Plan Approver	Select the action plan approver owner of the issue. The list of users available for selection is based on the selected organization structure. For more information, refer to MetricStream Arno Release Spring ‘21 - Threat and Vulnerability Management - User Guide.
Final Approver Organization	Select the organization to which the final approver of the issue belongs to. To select the final approver organization: **1.** Click **Add** icon associated with the field. The **Final Approver Organization** window appears displaying the defined organization structure. **2.** Select the required organization structure, and then click **Add**. **Note:** For more details on multidimensional organization structure, see MetricStream Arno Release Spring ‘21 - Threat and Vulnerability Management - User Guide.
Final Approver	Select the final approver owner of the issue. The list of users available for selection is based on the selected organization structure.

Adding Remedy Template



	Type	Default for Type
Remedy Template for Post Implementation	Network Vulnerabi...	no
Remedy Template For Infrastructure Event	Network Vulnerabi...	yes
Remedy Template For Misrouted	Network Vulnerabi...	no
Remedy Template For User Service Restoration	Network Vulnerabi...	no
Remedy Template For User Service Request	Web Application V...	yes

Figure 69 Adding Remedy Template

Field	Description
From **Add**, click **Add Remedy Template** to add a new Remedy template.	
Name	Select the remediation template name that you want to add in the rule.
Type	Select the remediation template type corresponding to the remediation template that you want to add in the rule. The available options are: • Network Vulnerability Remediation • Web Application Vulnerability Remediation
Default for Type check box	Select this check box if you want to mark the current template as default to create an incident manually.

Field	Description
Service Type	Select the type of service. This field provides the list of service type values available in BMC remedy. The available options are: • User Service Restoration • User Service Request • Infrastructure Restoration • Infrastructure Event • Misrouted • Post Implementation
Reported Source	Select the source from which the remedy incident is reported. This field provides the list of service type values available in BMC remedy. The available options are: • Direct Input • Email • External Escalation • Fax • Self Service • Systems Management • Phone • Voice Mail • Walk In • Web • Other • BMC Impact Manager Event
Description	Select vulnerability information for description of remedy incident. The available options are: • Vulnerability Title • Vulnerability Type • Vulnerability Source • Vulnerability Severity • Vulnerability Category
Detailed Description	Select detailed vulnerability information for Notes field of the remedy incident. The available options are: • Vulnerability Title • Vulnerability Type • Vulnerability Description • Vulnerability Source • Vulnerability Severity • Vulnerability Category • Vulnerability Solution • Vulnerability Consequence • CVE Information • CVSS Information

Adding ServiceNow Template

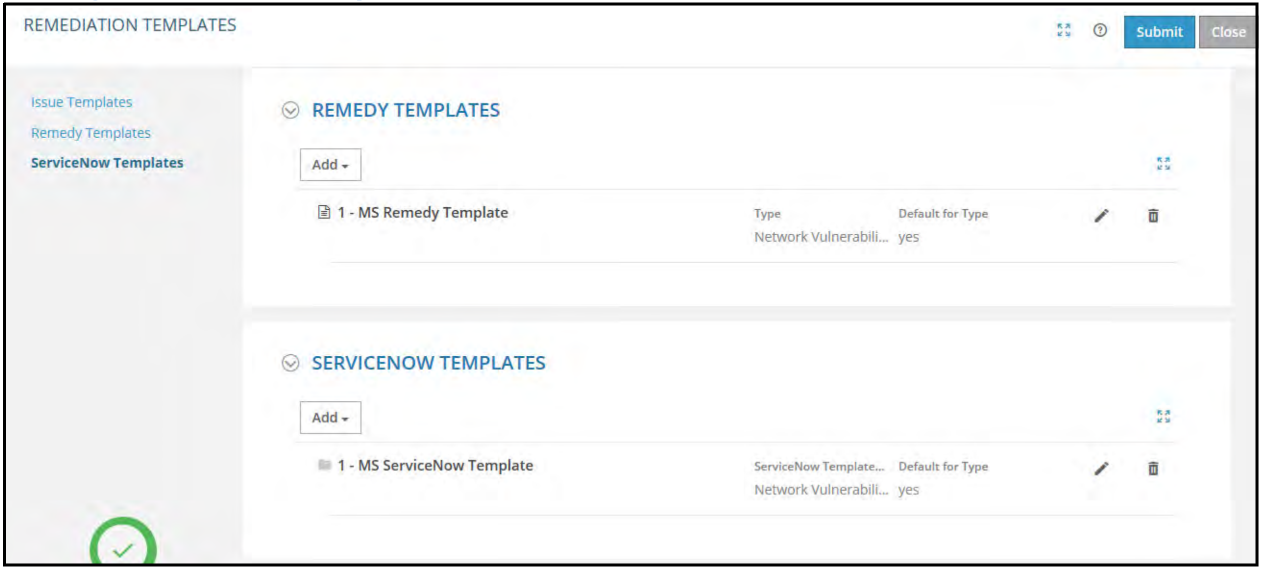


Figure 70 Adding ServiceNow Templates

Field	Description
From **Add**, click **Add ServiceNow Templates** to add a new ServiceNow template.	
ServiceNow Template Name	Enter the ServiceNow template name that you want to add in the rule.
ServiceNow Template Type	Select the type of issue template. The available options are: • Network Vulnerability Remediation • Web Application Vulnerability Remediation
Default for Type	Select this check box if you want to mark the current template as default to create an incident manually.
Caller	Enter the details of the caller who has reported the incident.
Opened By	Enter the details of the authorized person who has opened the ticket to address the incident.
Contact Type	Select the type of contact used to report the incident. The available options are: • Email • Phone • Self-service • Walk-in
Category	Select the category of the ServiceNow incident. The available options are: • Request • Inquiry/Help • Software • Hardware • Network • Database

Field	Description
Short Description	Select information for description of incident. The available options are: • Asset Name • Vulnerability Title
Description	Select detailed vulnerability information for Notes field of the incident. The available options are: • Asset Name • IPv4 Address • IPv6 Address • Vulnerability Title • Vulnerability Type • Vulnerability Description • Vulnerability Source • Vulnerability Severity • Vulnerability Category • Vulnerability Solution • Vulnerability Consequence • CVE Information • CVSS Information

Reports

Use the links within the **Reports** drop-down list to access respective reports, as shown in the following figure.

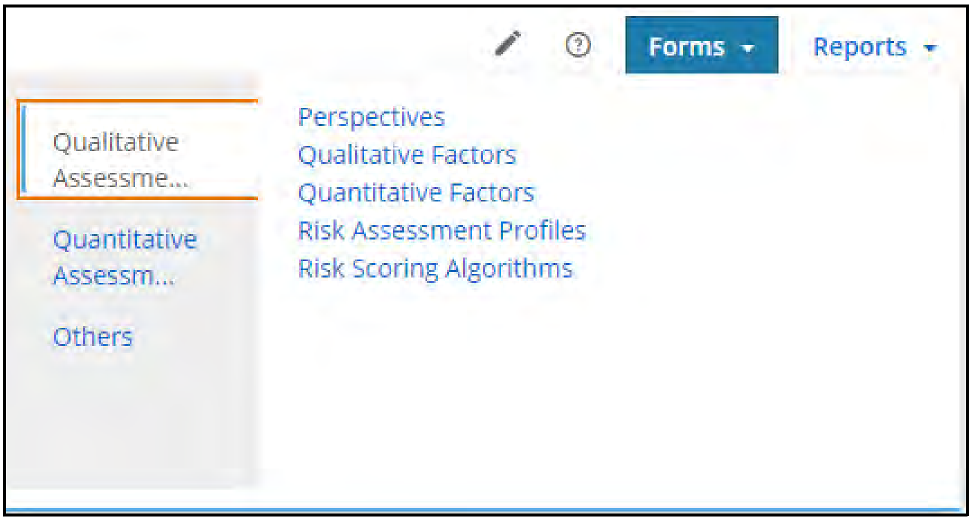


Figure 71 Reports of Setup page

You can manage:

- **Perspectives:** Opens the Perspectives report, which displays all the published perspectives that are applicable for your organization. It also displays the assessment type and the assessment methodology used for each Perspective.

  Note: A **Perspective** defines the assessment types (Org-Assessable Item-Risk or Org-Risk or Assessable Item-Risk) and the assessment methodology (Scoring Algorithm / Rating / Scoring and Rating / Scoring Algorithm and Rating / Ranking and Rating) to be used.

- **Qualitative Factors:** Opens the **Qualitative Factors** report, which displays all the published qualitative assessment factors, useful for the risk assessments performed for your organization.

  Note: **Qualitative Factors** are usually bunch of questions, the response type of which can be a simple text, date, options such as Yes/No, a paragraph, and so on. The responses to these factors do not directly contribute to the risk score or rating. Instead, these factors help guide the assessor in determining the overall score for the assessment. The qualitative factor responses are typically used for reference, reporting, and documentation purposes.

- **Quantitative Factors:** Opens the **Quantitative Factors** report, which displays all the published quantitative assessment factors, useful for the risk assessments performed for your organization.

  Note: **Quantitative Factors** are those factors that are directly assessed and the assessment ratings have a direct effect on the overall risk score and rating. Examples of quantitative factors are DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability) and STRIDE (Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges).

- **Risk Assessment Profiles:** Opens the **Risk Assessment Profiles** report, which displays the available risk profiles in the system.
- **Risk Scoring Algorithms:** Opens the **Risk Scoring Algorithms** report, which displays all the defined risk scoring algorithms, useful for the risk assessments performed for your organization.

  Note: The **Risk Scoring Algorithm** component is used to define the inherent, control, and residual scoring formula. This component supports definition of simple to moderate complex formula. Using the Risk Scoring Algorithm interface, you can define the risk scoring algorithm specific to your organization to conduct risk assessments on a periodic or ongoing basis.

- **Remediation Template Configuration:** Open the Remediation Template Configuration report, view and edit the configuration, if required. For more information on editing the Remediation Template Configuration, refer Remediation Templates.

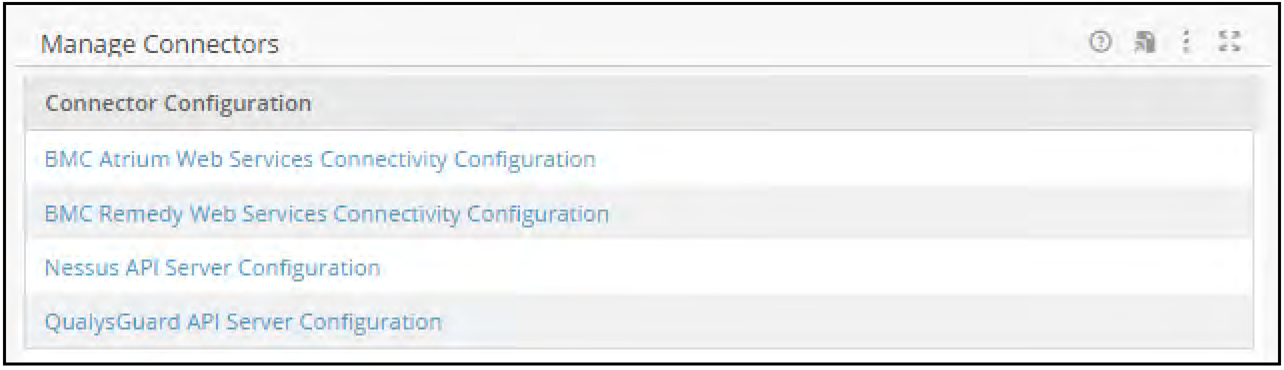
Note: For details, refer to the MetricStream Arno Release Spring ‘21 - Risk Assessments - User Guide.

Managing Connectors Dashboard

The **Managing Connectors** dashboard displays the available connectors which can be used for pulling in vulnerability assessments from external scanning tools.

MetricStream recommends API-based connectivity into vulnerability assessment tools, CMDBs, and service desk or help desk systems. This ensures that the flow of information can be automatically orchestrated by MetricStream across these external systems. For example, asset repositories flow in from CMDBs into the MetricStream application and vulnerability scan data flows in from vulnerability assessment tools into the MetricStream application. Then, prioritized remediation tickets flow out from the MetricStream application into your service or help desk system.

Note: The actual connectors available in your environment depends on your subscriptions.



Manage Connectors

Connector Configuration

BMC Atrium Web Services Connectivity Configuration

BMC Remedy Web Services Connectivity Configuration

Nessus API Server Configuration

QualysGuard API Server Configuration

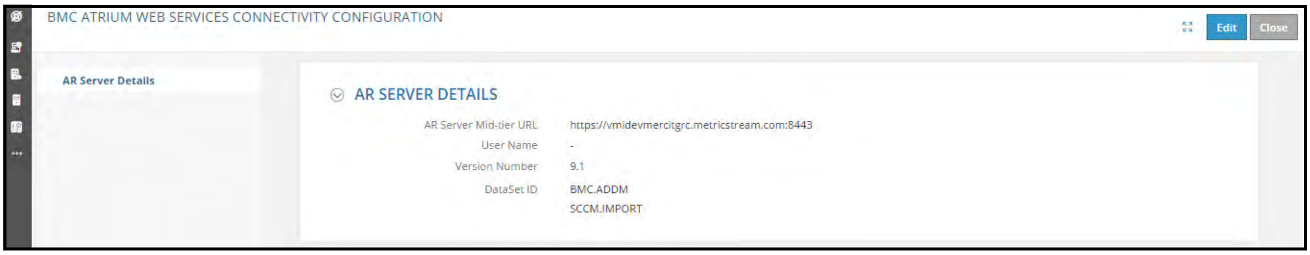
Figure 72 Manage Connectors Dashboard

You can configure the following connectors through Manage Connectors dashboard:

- BMC Atrium Web Services Connectivity Configuration
- BMC Remedy Web Services Connectivity Configuration
- ServiceNow REST API Configuration (CMDB)
- ServiceNow REST API Configuration (Incidents)
- QualysGuard API Server Configuration
- Nessus API Server Configuration
- Rapid 7 Nexpose API Server Configuration
- Tenable SecurityCenter Configuration

BMC Atrium Web Services Connectivity Configuration

Use the BMC Atrium Web Services Connectivity Configuration form to configure web services connection parameters for BMC Atrium. You can configure the connection parameters for BMC Atrium by providing the user credentials in this form.


BMC ATRIUM WEB SERVICES CONNECTIVITY CONFIGURATION

AR Server Details

AR SERVER DETAILS

AR Server Mid-tier URL https://vmidevmercitgrc.metricstream.com:8443
User Name -
Version Number 9.1
DataSet ID BMC.ADDM
SCCM.IMPORT

Figure 73 BMC Atrium Web Services Connectivity Configuration Form

Field	Description
Click **Edit** to modify the form.	
AR Server Mid-tier URL	Select the mechanism to log into the remedy web service.
User Name	Type the first name of the remedy user.
Password	Type the password.
Version Number	Select the relevant BMC atrium version number.
DataSet ID	Select the available CMDB dataset ID. **Note:** This field can be configured based on your requirement.
After entering all the required details in the form, click **Submit** to submit the form.	

Running Infolet of BMC Atrium

After submitting the form, you can fetch Asset Classes and Assets from BMC Atrium CMDB into MetricStream GRC libraries by running the related infolets. They are:

1. **MS ITG BMC WS FETCH**
2. **MS_ITG_CMD_CREATE_GRCF_OBJECTS**

Once the data is fetched, run the next infolet to update the relationships between the fetched GRC libraries.

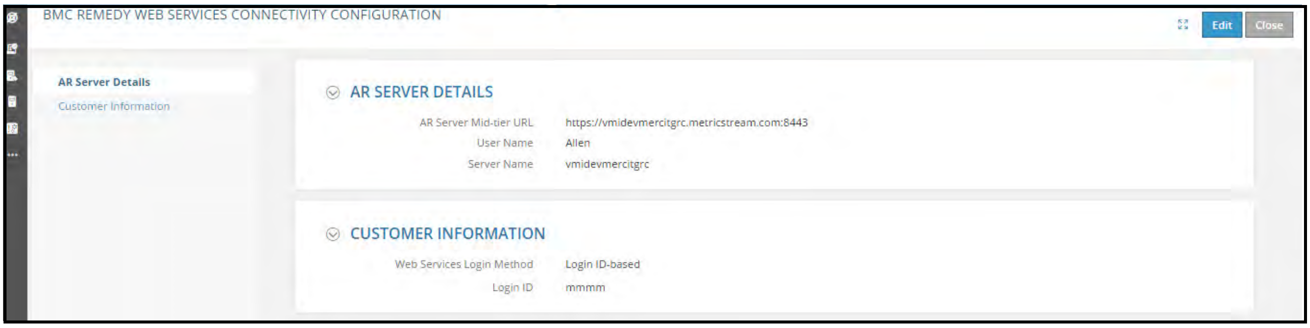
3. **MS ITG CMD UPDATE GRCF OBJECTS**

BMC Remedy Web Services Connectivity Configuration

Use the BMC Remedy Web Services Connectivity Configuration form to configure web services connection parameters for BMC Remedy. You can configure the connection parameters for BMC Remedy by providing the user credentials in this form.

After submitting the Configuration Form, create a default Remedy Template in the Remediation Template Form. In the form, set the default Remediation Target as **Remedy**.

Note: This form should be configured before setting up Remedy Templates and Rules, for creating incidents into BMC Remedy Management system.



BMC REMEDY WEB SERVICES CONNECTIVITY CONFIGURATION

AR SERVER DETAILS

AR Server Mid-tier URL: https://vmidevmercitgrc.metricstream.com:8443
User Name: Allen
Server Name: vmidevmercitgrc

CUSTOMER INFORMATION

Web Services Login Method: Login ID-based
Login ID: mmmm

Figure 74 BMC Remedy Web Services Connectivity Configuration Form

Field	**Description**
Click **Edit** to modify the form.	
AR Server Details	
AR Server Mid-tier URL	Type the BMC mid-tier URL.
User Name	Type the user name.
Password	Type the password.
Server Name	Type the host name of the server hosting the BMC remedy.
Customer Information	
Web Services Login Method	Select the mechanism to log into the remedy web service.
First Name	Type the first name of the remedy user.
Middle Initial	Type the middle name of the remedy server user.
Last Name	Type the last name of the remedy user.

After entering all the required details in the form, click **Submit** to submit the form.

Running Infolet of BMC Remedy

After submitting the form, setup the remediation templates and rules. Next, run the following infolets:

- MS_ITG_GRC_DATA_PUB_EVENT
- MS_APPSUTILS_PUSH_CIF_EVENT_JOB
- MS_ITS_ITSLP_STATISTICS_INFOLET

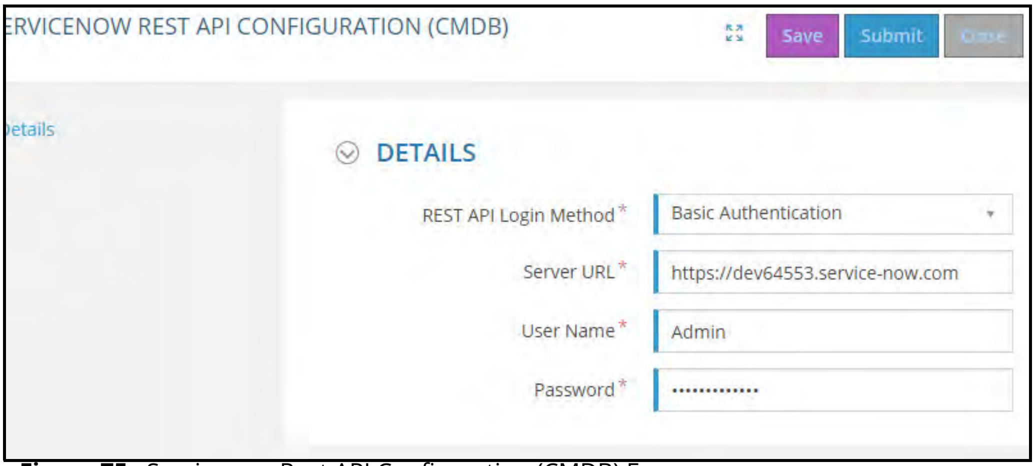
Finally, run **MS_ITS_INCIDENT_SCHEDULED_INFOLET** to view the incidents in charts and reports of the product.

ServiceNow REST API Configuration (CMDB)

Use the **ServiceNow REST API Configuration (CMBD)** form to configure the ServiceNow setup access to your organization. You should set up the REST API Login Method (Basic Authentication or OAuth2Authentication) and User Name and Password for the ServiceNow (CMDB) API server from which you want to import Asset Classes, Assets, and Business Processes into the MetricStream Foundation Libraries.

After you submit the form:

1. Run the **MS_ITG_SRVC_FETCH_CMDB_DATA** Infolet to fetch the data and import it into the ServiceNow tables.
2. Run **MS_ITG_CMD_CREATE_GRCF_OBJECTS** infolet to import Asset Classes, Assets, and Processes data dynamically into the MetricStream Foundation Libraries.
3. If there are updates to name, type, and so on, run the **MS_ITG_CMD_UPDATE_GRCF_OBJECTS** infolet to fetch the modified data and update the MetricStream Foundation Libraries.



ERVICENOW REST API CONFIGURATION (CMDB)

DETAILS

REST API Login Method*	Basic Authentication
Server URL*	https://dev64553.service-now.com
User Name*	Admin
Password*	•••••••••••••

Figure 75 Servicenow Rest API Configuration (CMDB) Form

Field	Description
REST API Login Method	Select the login method based on your requirement. The following methods are available. • Basic Authentication • OAuth2 Authentication
Server URL	Provide the ServiceNow API Server URL.
User Name	Provide the user name of the ServiceNow.
Password	Provide the password of the ServiceNow.

Notes: Asset class is derived from the ServiceNow attributes, such as CI Class, Model Category, Version, and so on. Asset class is not exactly mapped with the Class field from ServiceNow.

Running Infolet of ServiceNow REST API Configuration (CMDB)

After you submit the form:

- Run the **MS_ITG_SRVC_FETCH_CMDB_DATA** infolet to fetch the data and import it into the ServiceNow tables.
- Run the **MS_ITG_CMD_CREATE_GRCF_OBJECTS** infolet to import Asset Classes, Assets, and Processes data dynamically into the MetricStream Foundation Libraries.

1. Login as SYSTEMI.
2. Navigate to the **Infolets** page.
3. Click the **Run Infolet** link corresponding to the ServiceNow infolet.

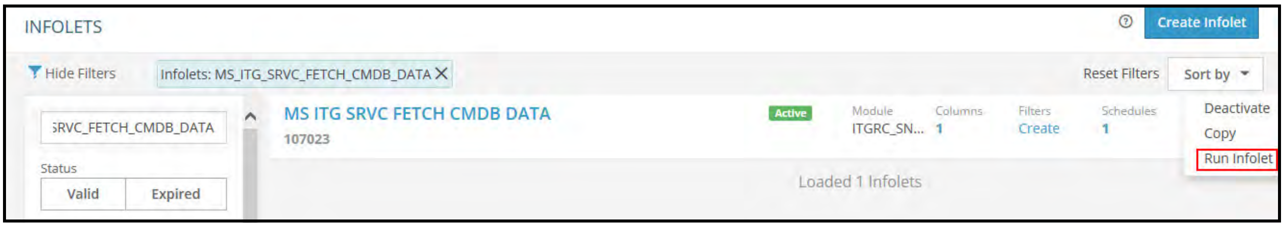
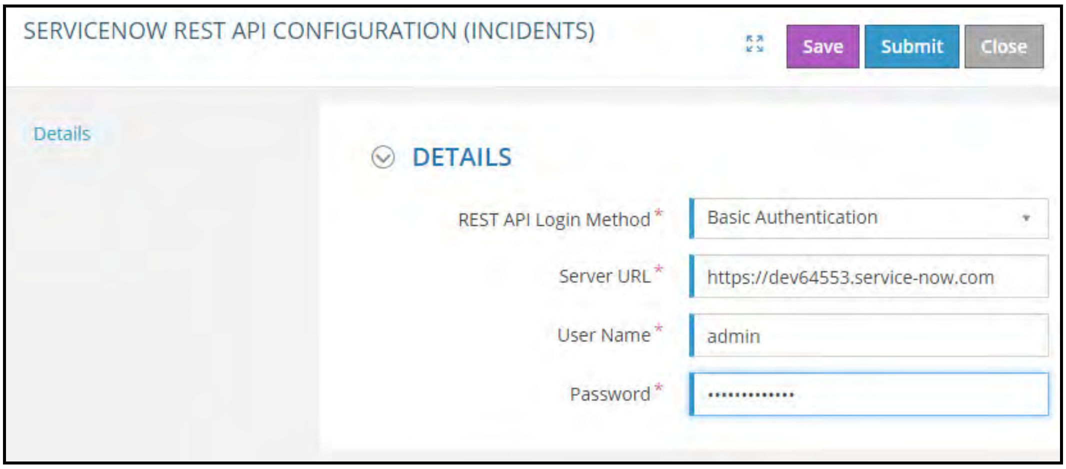


Figure 76 ServiceNow REST API Configuration (CMDB) Infolet

Note: Once you click **Run Infolet**, the data is imported.

ServiceNow REST API Configuration (Incidents)

Use the **ServiceNow REST API Configuration (Incidents)** form to configure the ServiceNow setup access to your organization. You should set up the REST API Login Method (Basic Authentication or OAuth2Authentication) and User Name and Password for the ServiceNow (Incidents) API server to trigger Vulnerability Remediation Incidents from MetricStream Security Threat and Vulnerability Management into ServiceNow Incident Management system.



REST API Login Method*	Basic Authentication
Server URL*	https://dev64553.service-now.com
User Name*	admin
Password*	•••••••••••••

Figure 77 Servicenow Rest API Configuration (Incidents) Form

Field	Description
REST API Login Method	Select the login method based on your requirement. The following methods are available. • Basic Authentication • OAuth2 Authentication
Server URL	Provide the ServiceNow API Server URL.
User Name	Provide the user name of the ServiceNow.
Password	Provide the password of the ServiceNow.

Triggering Incidents Automatically

After submitting the **ServiceNow REST API Configuration (Incidents)** form, perform the following steps to trigger vulnerability incidents automatically in the Incident management system.

1. From **Setup** page, click **Configure / Setup** and click **Remediation Templates**.
2. Select the **ServiceNow Templates** tab and create a ServiceNow template.
3. Click **Submit**.
4. Navigate to **Setup**, from **Configure / Setup** click **Remediation Rules**.
5. Select the required connector - for example, QualsGuard, Nessus.
6. Define the rule condition to auto trigger incidents to ServiceNow Incident Management system. This rule should be tied the template that is created in the Step 2.

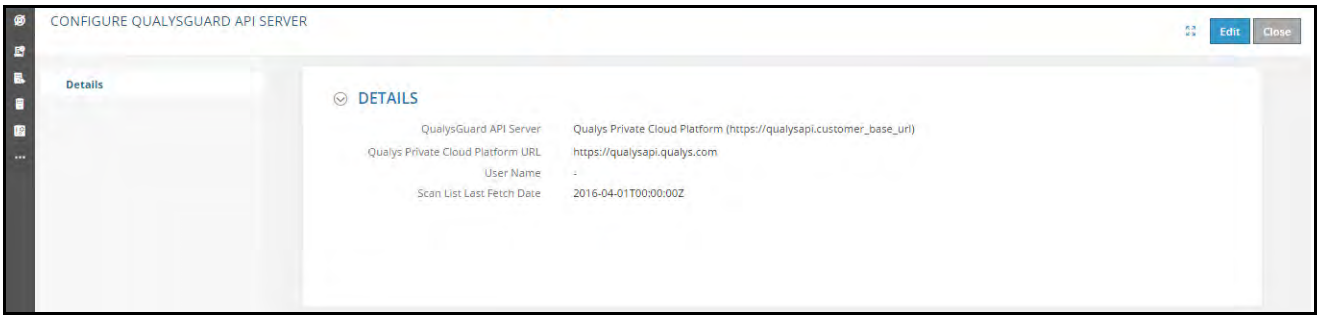
   Note: Ensure that the **ServiceNow** option is selected in the **Remediation Target**.

7. Click **Submit**.

QualysGuard API Server Configuration

By using the **Configure QualysGuard API** Server form, you can configure the QualysGuard connector access to your organization. You should set up the API Server URL, User Name and Password, and Scan List Last Fetch Date for the QualysGuard API server from which you want to retrieve the vulnerability details for the specified duration. Once you submit the form and run the **MS_ITG_QUALYS_SYNC_TAV** infolet, the vulnerability data for the set of assets scanned is retrieved from the QualysGuard server. The retrieved information is saved in the Mongo database.

The TaV related data is saved in the “**MsItgCommonTaV**” collection such as the asset details, related TaV details, scan records, and so on. The Timestamp and the IP addresses of the scanned details are saved in the **MsItgLatestAssetAndLatestTimeStamp** collection.



DETAILS

QualysGuard API Server: Qualys Private Cloud Platform (https://qualysapi.customer_base_url)
Qualys Private Cloud Platform URL: https://qualysapi.qualys.com
User Name: -
Scan List Last Fetch Date: 2016-04-01T00:00:00Z

Figure 78 Configure QualysGuard API Server Form

Field	Description
Click **Edit** icon to modify the form.	
QualysGuard API Server	Provide the QualysGuard API Server URL. The available options are: • Qualys US Platform 1 (https://qualysapi.qualys.com) • Qualys US Platform 2 (https://qualysapi.qg2.apps.qualys.com) • Qualys EU Platform (https://qualysapi.qualys.eu) • Qualys Private Cloud Platform (https://qualysapi.<customer_base_url>)
User Name	Provide the user name of the QualysGuard API Server.

Field	Description
Password	Provide the password of the QualysGuard API Server.
Scan List Last Fetch Date (YYYY-MMDDTHH:MM:SSZ)	Provide the duration of the past date that you want to retrieve the scan results. For example, if you want to retrieve the scan results of June 23, 2015 10 AM 10 Minutes and 10 seconds, you can provide input as: **2015-02-23T10:10:10Z** **Note:** - A UI Configuration Parameter is provided for troubleshooting options such as **Download Scanned Host List**, **Check Knowledgebase Status**, and **View API Rate Limit** to QualysGuard server to specify the timestamp from which Scan Results should be pulled into the system. - The details that you have provided for the QualysGuard API Server, User Name, Password, Scan List Fetch Date are stored in the MS_ITG_Config table. After you submit the form and run the **MS_ITG_QUALYS_SYNC_TAV** infolet, the TaV data is fetched. For more information on running the infolet, see Running Infolet of QualysGuard.
Test Connection	Test the connection with QualysGuard API server. The message "**Connection successful. Please continue**." appears on successful connection.
Download Scanned Host List *(appears if the **Test Connection** is successful)*	You can download the CSV file that contain the list of assets scanned along with IPv4 addresses. Perform these steps to configure this option: 1. Click **Settings** icon, click **Configuration and** select **Parameter Category**, to open the list of parameter categories. 2. Type **MS_ITG_QG_API_CALLS** in the search field. 3. Click the parameter category. 4. Select **Yes** in **Editable** field, in **Basic Information** section. 5. Click **Save Changes**.
Check Knowledgebase Status *(appears if the Test Connection is successful)*	You can view the status of knowledge base. **Note:** Ensure that the status is **Active**, to retrieve the Scanned Summary onto Mongo database.
View API Rate Limit *(appears if the Test Connection is successful)*	You can view the number of APIs allowed per day. **Note:** Minimum Remaining Rate limit should be 60-80. Only then scanned summary will be retrieved onto Mongo Data base.

After entering all the required details in the form, click **Submit** to submit the form.

Notes:

- If any mandatory field remains blank in the Configure QualysGuard API Server form, an error massage displays as '**Please provide details for all required fields**'.
- If any mandatory field value is incorrect in the Configure QualysGuard API Server form, an error massage displays as '**Connection failed. Error: 401 Unauthorized. Please check provided details**'.

Running Infolet of QualysGuard

After submitting the form, you can fetch the TaV data from QualysGuard by running the **MS_ITG_QUALYS_SYNC_TAV** infolet.

The system administrator performs the following steps to retrieve the TaV data from QualysGuard:

1. Login as SYSTEMI.
2. Navigate to the **Infolets** page.
3. Click the **Run Infolet** link corresponding to the **MS ITG QUALYS SYNC TAV** infolet.

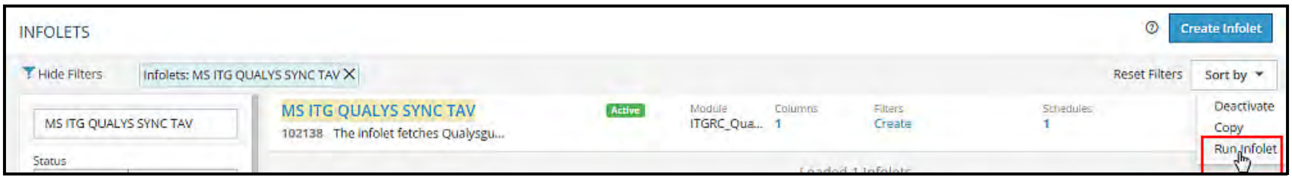


Figure 79 Running QualysGuard Infolet

Note: Once you click **Run Infolet**, the retrieved data from QualysGuard is stored in the MsItgCommonTaV collection.

Setting up Remediation Templates - QualysGuard Connector

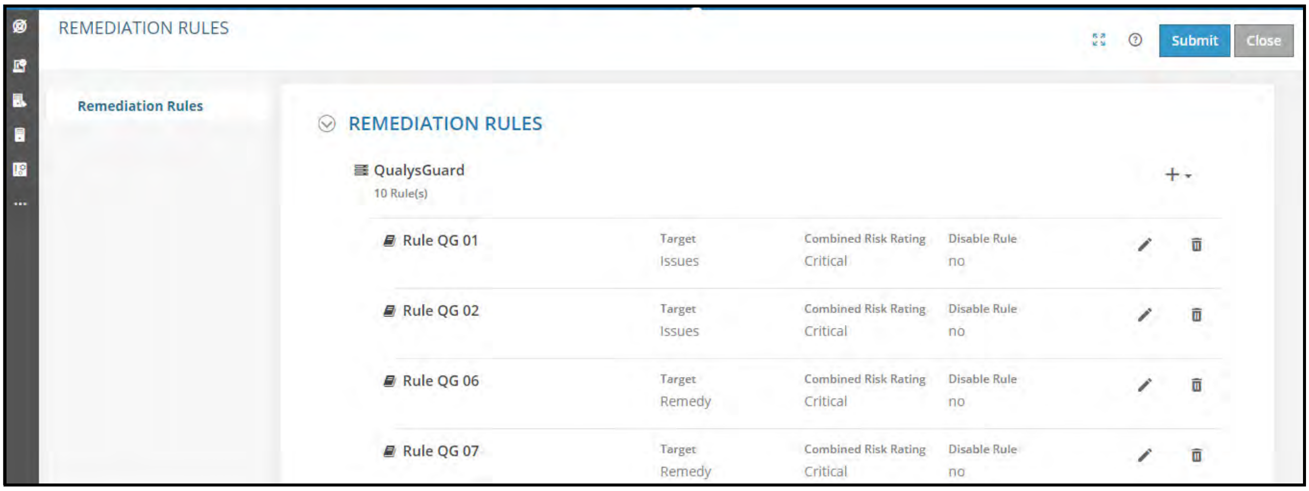
The first step of managing your threat and vulnerability management program, is to define remediation templates. For setting up templates, refer Remediation Templates.

Note: The **Remedy** template and **ServiceNow** template is available in your environment based on your subscription.

Adding Remediation Rules - QualysGuard Connector

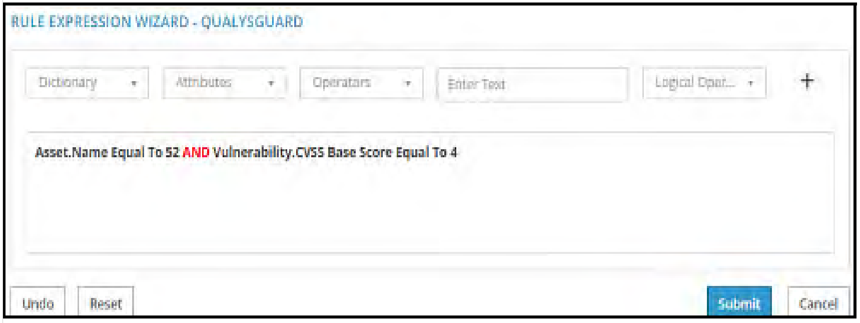
After configuring your remediation templates, you need to setup business rules that helps you to prioritize the vulnerabilities to be remediated. The product provides an intuitive rule builder that lets you combine the business context for your assets with the vulnerability context for those assets. A remediation rule (when to trigger the ticket), then ties to a remediation target (where to trigger the ticket) and a remediation template (to whom, to trigger the ticket).

The following rules have been set up for the QualysGuard connector:



Rule	Target	Combined Risk Rating	Disable Rule
Rule QG 01	Issues	Critical	no
Rule QG 02	Issues	Critical	no
Rule QG 06	Remedy	Critical	no
Rule QG 07	Remedy	Critical	no

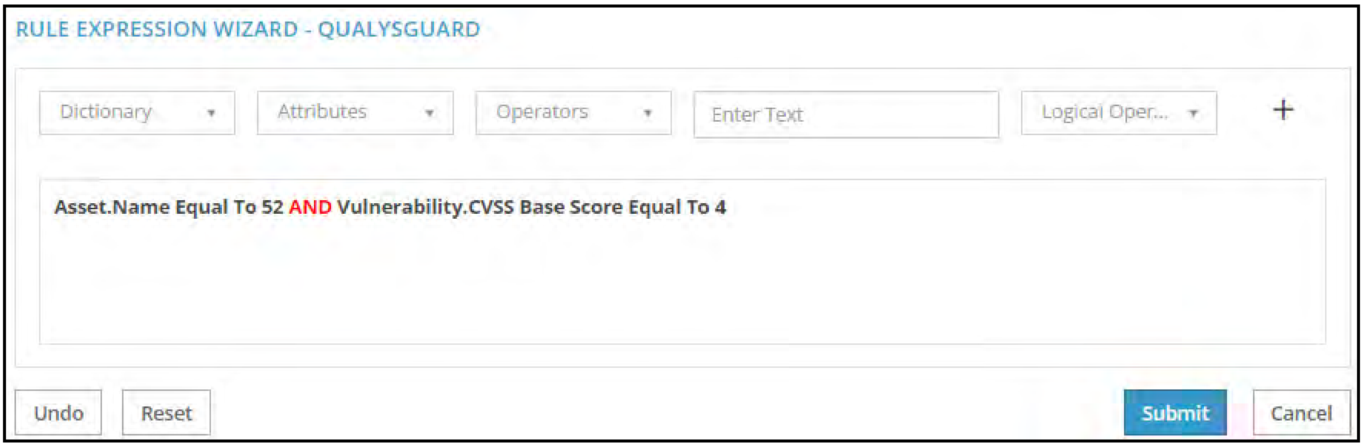
Figure 80 Adding Remediation Rules - QualysGuard

Field	Description
Click + icon to add new remediation rules	
Remediation Action	
Name	Type the name of the rule.
Disable Rule check box	Select this check box if you do not want to apply the defined rule to create issues or incidents.
Condition	Displays the rule that is added by using the Rule Expression Wizard window.
Rule Expression Wizard	Click this button to define remediation rules for issues or incidents. To define rules, perform the following steps: **1.** Click the **Rule Expression Wizard** button. The **Rule Expression Wizard - QualysGuard** window appears.  RULE EXPRESSION WIZARD - QUALYSGUARD Dictionary Attributes Operators Enter Text Logical Oper... + Undo Reset Submit Cancel Asset.Name Equal To 52 AND Vulnerability.CVSS Base Score Equal To 4 **2.** Define the rule as required. **3.** Click **Submit** to create the rule. For more information on Rule Expression Wizard - QualysGuard window, see Rule Expression Wizard - QualysGuard Window.

Field	Description
Combined Risk Rating	Select the combined risk rating. The available options are: • Critical • High • Medium • Low
Target	Select the remediation target. Remediation target defines the target system for issue/incident. • **Issues**: Select this option if you want to trigger issues in the Issues module. Note: You can select remediation target for manual issue/incident creation by configuring the parameter **MS_ITG_RMD_CONFIG**. • **Remedy**: Select this option if you want to trigger incident in BMC remedy.
Template Type	Select the remediation template type corresponding to the remediation template that you want to add in the rule. The available options are: • Network Vulnerability Remediation • Web Application Vulnerability Remediation
Template Name	Select the remediation template name that you want to add in the rule. Note: Template names are available for selection based on the selected template type.
Incident Priority **Appears only when you select Remedy in the Remediation Target field.**	**Urgency**: Select the urgency of the incident. The available options are: • 1-Critical • 2-High • 3-Medium • 4-Low **Impact**: Select the impact of the incident. The available options are: • 1-Extensive/Widespread • 2-Significant/Large • 3-Moderate/Limited • 4-Minor/Localized

Rule Expression Wizard - QualysGuard Window

Use this window to define remediation issue creation rules.



Asset.Name Equal To 52 AND Vulnerability.CVSS Base Score Equal To 4

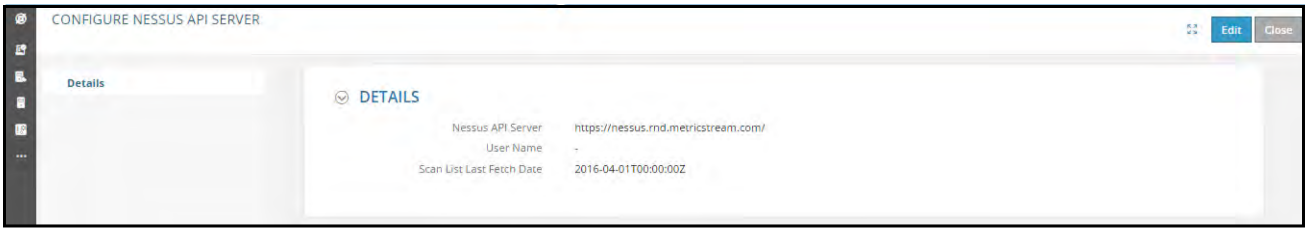
Figure 81 Rule Expression Wizard - QualysGuard Window

Field	Description
Dictionary	Select if you want to create a rule for an Asset or Vulnerability.
Attributes	Select the attribute for which you want to create the rule. This field displays the values based on the value that you select in the Dictionary field.
Operator	Select the operator. This field displays the operators based on the values that you select in the Dictionary and Attributes fields. The available options are: • Equal To • Not Equal To • Greater Than • Less Than • Greater Than Equal To • Less Than Equal To
Value	Define the value in this field. This field displays the values based on the attribute that you select in the Attributes field.
Add icon	Click this icon to add the rule.
Connecting Operator	Select the connecting operator. The available operators are: • **AND**: Select this option to “AND” (combine) two different rules. • **OR**: Select this option to “OR” (either of the options) two different rules.
ADD button	Click this button to add the connecting operator.
Buttons	
Submit	Click this button to submit the created rule and close. Once you submit, the created rule appears in the Rule Condition field of the Remediation Rules form.
Undo	Click this button to clear the last-entered expression.
Reset	Click this button to clear the defined rule and reset.

Nessus API Server Configuration

Use the **Configure Nessus API Server** form to configure the Nessus connector. You should set up the API Server URL, User Name and Password for the Nessus API server from which you want to retrieve the vulnerability details for the specified duration. Once you submit the form and run the **MS ITG NESSUS SYNC TAV** infolet, the identified vulnerability data for the set of assets scanned is retrieved from the Nessus server. The retrieved information is saved in the Mongo database.

The TaV related data such as the asset details and related vulnerability details, scan records, and so on are saved in the “**MsItgCommonTaV**” collection. The Timestamp and the IP addresses of the scanned details are saved in the **MsItgLatestAssetAndLatestTimeStamp** collection.



Nessus API Server https://nessus.rnd.metricstream.com/
User Name -
Scan List Last Fetch Date 2016-04-01T00:00:00Z

Figure 82 Configure Nessus API Server Form

Field	**Description**
Click **Edit** icon to modify the form.	
Nessus API Server	Type the Nessus API Server URL.
User Name	Type the user name of the Nessus API Server.
Password	Type the password of the Nessus API Server.
Scan List Last Fetch Date(YYYY-MMDDTHH:MM:SSZ)	Provide the duration of the past date that you want to retrieve the scan results. For example, if you want to retrieve the scan results of June 23, 2016 10 AM 10 Minutes and 10 seconds, you can provide input as: **2016-02-23T10:10:10Z** **Note:** The details that you have provided for the Nessus API Server, User Name, Password, Scan List Fetch Date are stored in the **MS_ITG_Config** table. After you submit the form and run the **MS ITG NESSUS SYNC TAV** infolet, the TaV data is fetched. For more information on running the infolet, see Running Infolet Nessus.
Test Connection to Nessus API Server	Test the connection with Nessus API Server. The message “**Connection successful. Please continue.**” appears on successful connection.

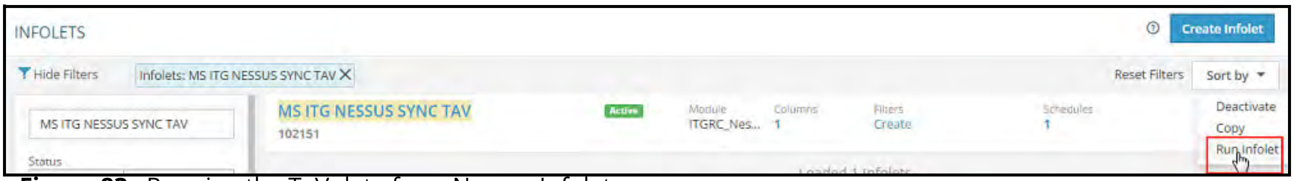
After entering all the required details in the form, click **Submit** to submit the form.

Running Infolet Nessus

After submitting the form, you can fetch the TaV data from Nessus by running the **MS ITG NESSUS SYNC TAV** infolet.

The system administrator performs the following steps to retrieve the TaV data from Nessus:

1. Login as SYSTEMI.
2. Navigate to the **Infolets** page.
3. Click the **Run Infolet** link corresponding to the **MS ITG NESSUS SYNC TAV** infolet.



MS ITG NESSUS SYNC TAV
102151
Active

Module	Columns	Filters	Schedules
ITGRC_Nes...	1	Create	1

Figure 83 Running the TaV data from Nessus Infolet

Note: Once you click **Run Infolet**, the retrieved data from Nessus is stored in the **MsItgCommonTaV** collection.

Setting up Remediation Templates - Nessus Connector

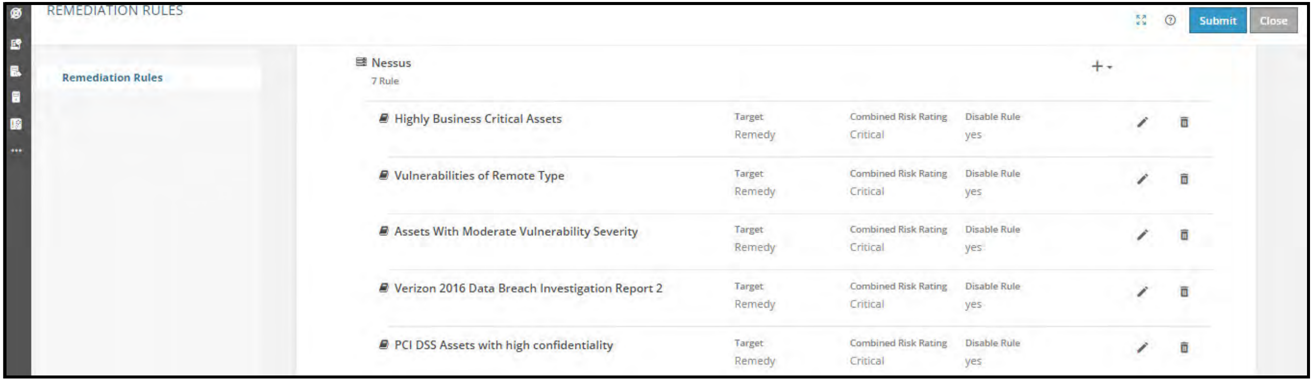
The first step of managing your threat and vulnerability management program, is to define remediation templates. For setting up remediation templates, refer Remediation Templates.

Note: The **Remedy** template and **ServiceNow** template is available in your environment based on your subscription.

Adding Remediation Rules - Nessus Connector

After configuring your remediation templates, you need to setup business rules that helps you to prioritize the vulnerabilities to be remediated. The product provides an intuitive rule builder that lets you combine the business context for your assets with the vulnerability context for those assets. A remediation rule (when to trigger the ticket), then ties to a remediation target (where to trigger the ticket) and a remediation template (to whom, to trigger the ticket).

The following rules have been set up for the Nessus connector:

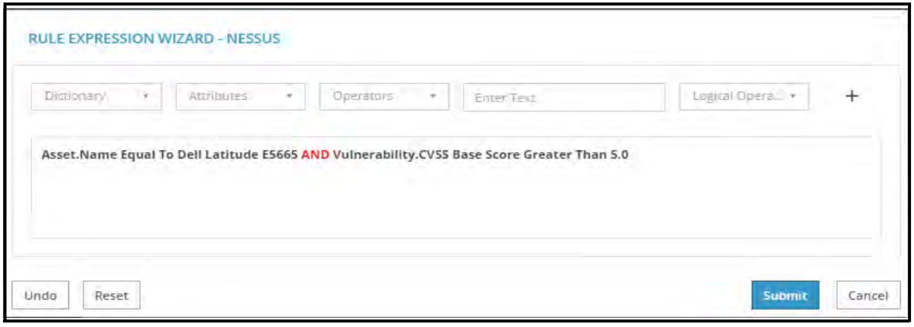


Nessus
7 Rule

	Target	Combined Risk Rating	Disable Rule
Highly Business Critical Assets	Remedy	Critical	yes
Vulnerabilities of Remote Type	Remedy	Critical	yes
Assets With Moderate Vulnerability Severity	Remedy	Critical	yes
Verizon 2016 Data Breach Investigation Report 2	Remedy	Critical	yes
PCI DSS Assets with high confidentiality	Remedy	Critical	yes

Figure 84 Adding Remediation Rules - Nessus

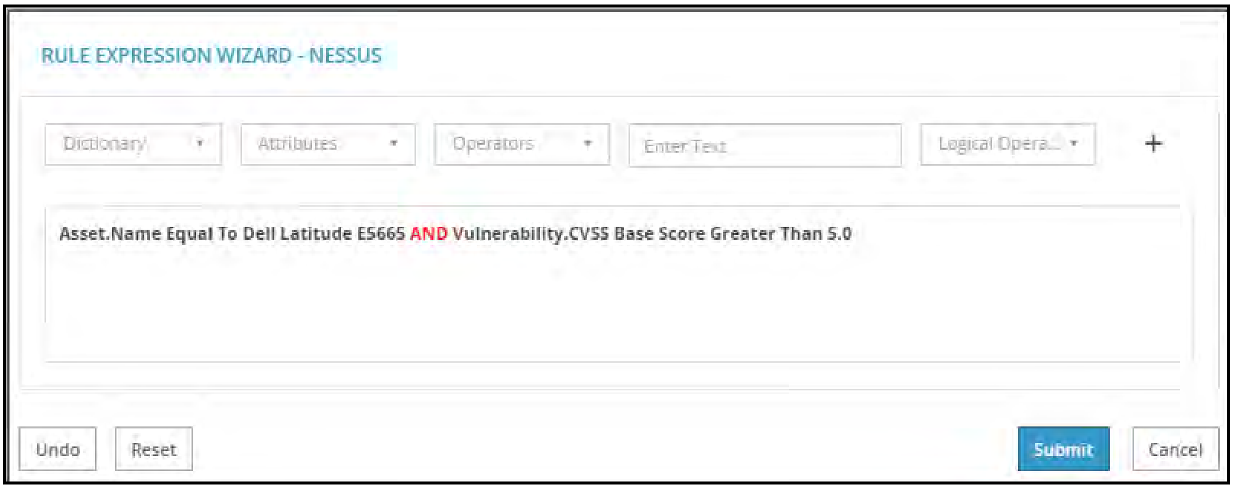
Field/Button Name	Description
Click + icon to add new remediation rules	
Remediation Action	

Field/Button Name	Description
Name	Type the name of the rule.
Disable Rule check box	Select this check box if you do not want to apply the defined rule to create issues or incidents.
Condition	Displays the rule that is added by using the Rule Expression Wizard window.
Rule Expression Wizard button	Click this button to define remediation rules for issues or incidents. To define rules, perform the following steps: **1.** Click the **Rule Expression Wizard** button. The **Rule Expression Wizard - Nessus** window appears.  RULE EXPRESSION WIZARD - NESSUS Asset.Name Equal To Dell Latitude E5665 AND Vulnerability.CVSS Base Score Greater Than 5.0 Dictionary Attributes Operators Enter Text Logical Opera... + Undo Reset Submit Cancel Define the rule as required. **2.** Click **Submit** to create the rule. For more information on Rule Expression Wizard - Nessus window, see Rule Expression Wizard - Nessus Window.
Combined Risk Rating	Select the combined risk rating. The available options are: • Critical • High • Medium • Low
Target	Select the remediation target. Remediation target defines the target system for issue. • **Issues**: Select this option if you want to trigger issues in the Issues module. **Note:** You can select remediation target for manual issue creation by configuring the parameter **MS_ITG_RMD_CONFIG**. • **Remedy**: Select this option if you want to trigger issues in BMC remedy.
Template Type	Select the remediation template type corresponding to the remediation template that you want to add in the rule. The available options are: • Network Vulnerability Remediation • Web Application Vulnerability Remediation

Field/Button Name	Description
Template Name	Select the remediation template name that you want to add in the rule. **Note:** Template names are available for selection based on the selected template type.
Incident Priority *(Appears only when you select **Remedy** in the Remediation Target field.)*	**Urgency**: Select the urgency of the incident. The available options are: • 1-Critical • 2-High • 3-Medium • 4-Low **Impact**: Select the impact of the incident. The following options are available: • 1-Extensive/Widespread • 2-Significant/Large • 3-Moderate/Limited • 4-Minor/Localized

Rule Expression Wizard - Nessus Window

Use this window to define remediation issue creation rules.



Asset.Name Equal To Dell Latitude E5665 AND Vulnerability.CVSS Base Score Greater Than 5.0

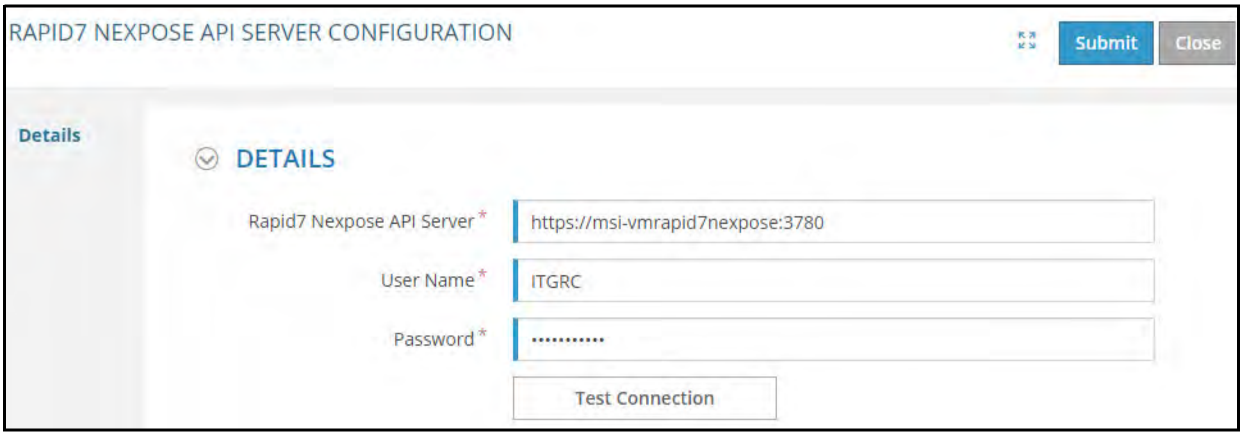
Figure 85 Rule Expression Wizard - Nessus Window

Field Name	Description
Dictionary	Select if you want to create a rule for an **Asset** or **Vulnerability**.
Attributes	Select the attribute for which you want to create the rule. This field displays the values based on the value that you select in the Dictionary field.

Field Name	Description
Operators	Select the operator. This field displays the operators based on the values that you select in the Dictionary and Attributes fields. The available options are: • Equal To • Not Equal To • Greater Than • Less Than • Greater Than Equal To • Less Than Equal To
Value	Define the value in this field. This field displays the values based on the attribute that you select in the **Attributes** field. **Note:** For attributes like Asset Business Criticality, CIA, Location, Type and Vulnerability Severity, Category, Type value gets auto-populated.
Add icon	Click this icon to add the rule.
Connecting Operator	Select the connecting operator. The following operators are available: • **AND**: Select this option to “AND” (combine) two different rules. • **OR**: Select this option to “OR” (either of the options) two different rules.
ADD	Click this button to add the connecting operator.
Buttons	
Submit	Click this button to submit the created rule and close. Once you submit, the created rule appears in the Rule Condition field of the Remediation Rules form.
Undo	Click this button to clear the last-entered expression.
Reset	Click this button to clear the defined rule and reset.

Rapid 7 Nexpose API Server Configuration

Use the **Rapid7 Nexpose API Server Configuration** form to configure the Rapid7 Nexpose setup access to your organization. You should set up the API Server URL, User Name, and Password for the Rapid7 Nexpose API server from which you want to retrieve the vulnerability details, for the assets scanned through Rapid7 Nexpose for the specified duration. After you submit the form and run the **MS_ITX_NEXPOSE_SYNC_REPORT** infolet, the vulnerability data is retrieved from the Rapid7 Nexpose sever. The retrieved information is saved in the Mongo database. The vulnerability data, such as the scanned asset details and related vulnerability information, and scan records, is saved in the **“MsItgCommonTaV”** collection. The Timestamp and the IP addresses of the scanned assets are saved in the **MsItgLatestAssetAndLatestTimeStamp** collection.


RAPID7 NEXPOSE API SERVER CONFIGURATION

DETAILS

Rapid7 Nexpose API Server* https://msi-vmrapid7nexpose:3780

User Name* ITGRC

Password* •••••••••••

Figure 86 Rapid 7 Nexpose API Server Configuration Form

Field	Description
Rapid7 Nexpose API Server	Type the Rapid7 Nexpose API Server URL.
User Name	Type the user name of the Rapid7 Nexpose API Server.
Password	Type the password of the Rapid7 Nexpose API Server.
Test Connection	Click **Test Connection** to test the connection between the product and Rapid7 Nexpose API Server. If the connection is successful, then a successful message is displayed before proceeding to fetch the scan data. If the connection is not successful, then an error message is displayed.

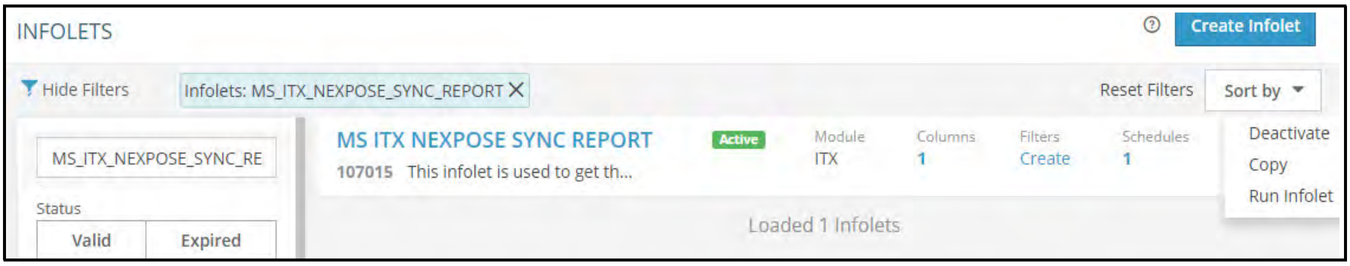
After entering all the required details in the form, click **Submit** to submit the form.

Running Infolet of Rapid 7 Nexpose

After submitting the form, you can fetch the vulnerability data from Rapid7 Nexpose by running the **MS_ITX_NEXPOSE_SYNC_REPORT** infolet.

To retrieve the vulnerability data from Rapid7 Nexpose by running the infolet, perform the following:

1. Login as SYSTEMI.
2. Navigate to the **Infolets** page.
3. Click the **Run Infolet** link corresponding to the **MS_ITX_NEXPOSE_SYNC_REPORT** infolet.


INFOLETS

Infolets: MS_ITX_NEXPOSE_SYNC_REPORT

MS_ITX_NEXPOSE_SYNC_RE

MS ITX NEXPOSE SYNC REPORT Active

107015 This infolet is used to get th...

Module ITX | Columns 1 | Filters Create | Schedules 1

Loaded 1 Infolets

Figure 87 Running Rapid 7 Nexpose Infolet

Note: Once you click **Run Infolet**, the retrieved data from Rapid 7 Nexpose is stored in the **MsItgCommonTaV** collection.

Setting up Remediation Templates - Rapid 7 Nexpose Connector

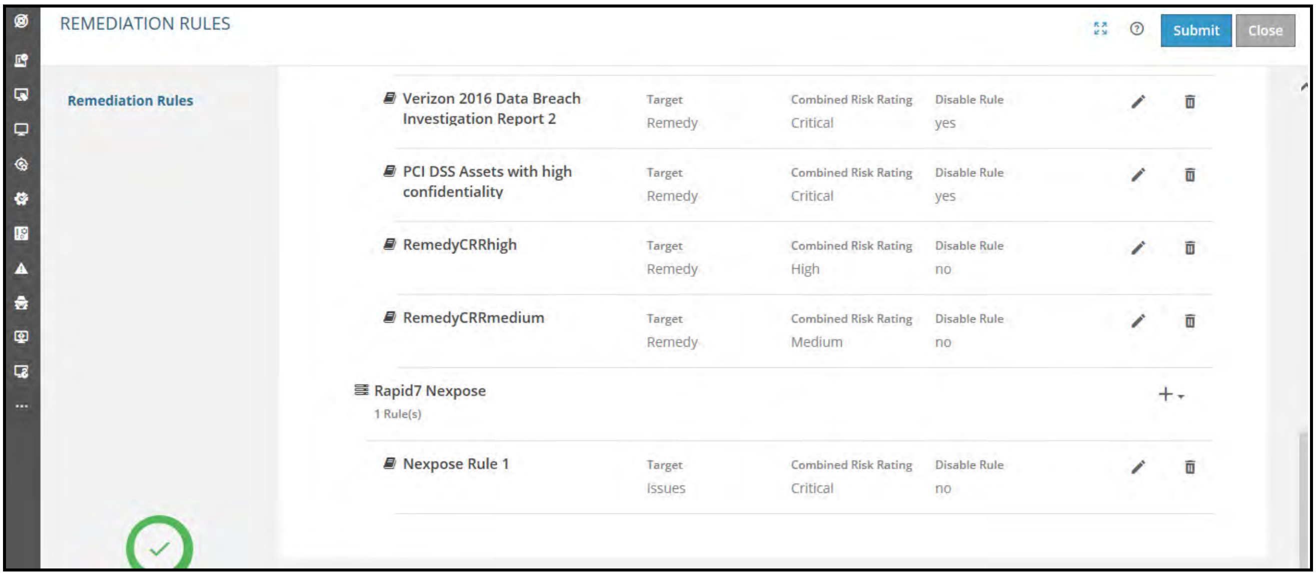
The first step of managing your threat and vulnerability management program, is to define remediation templates. For setting up template, refer Remediation Templates.

Note: The **Remedy** template and **ServiceNow** template is available in your environment based on your subscription.

Adding Remediation Rules - Rapid 7 Nexpose Connector

After configuring your remediation templates, you need to setup business rules that helps you to prioritize the vulnerabilities to be remediated. The product provides an intuitive rule builder that lets you combine the business context for your assets with the vulnerability context for those assets. A remediation rule (when to trigger the ticket), then ties to a remediation target (where to trigger the ticket) and a remediation template (to whom, to trigger the ticket).

The following rules have been set up for the Rapid 7 Nexpose connector:



REMEDIATION RULES

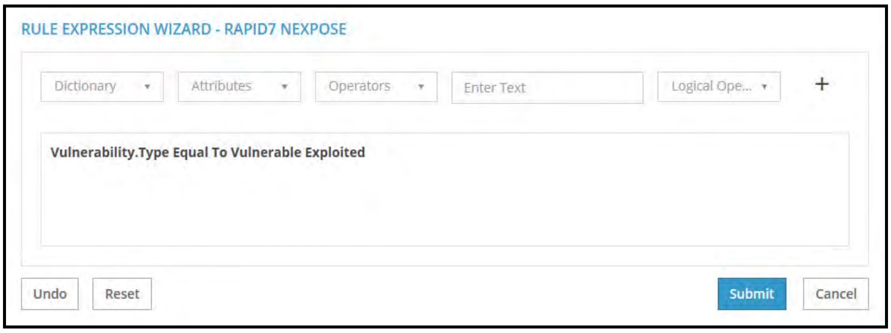
Verizon 2016 Data Breach Investigation Report 2	Target Remedy	Combined Risk Rating Critical	Disable Rule yes
PCI DSS Assets with high confidentiality	Target Remedy	Combined Risk Rating Critical	Disable Rule yes
RemedyCRRhigh	Target Remedy	Combined Risk Rating High	Disable Rule no
RemedyCRRmedium	Target Remedy	Combined Risk Rating Medium	Disable Rule no

Rapid7 Nexpose
1 Rule(s)

Nexpose Rule 1	Target Issues	Combined Risk Rating Critical	Disable Rule no

Figure 88 Adding Remediation Rules - Rapid 7 Nexpose Connector

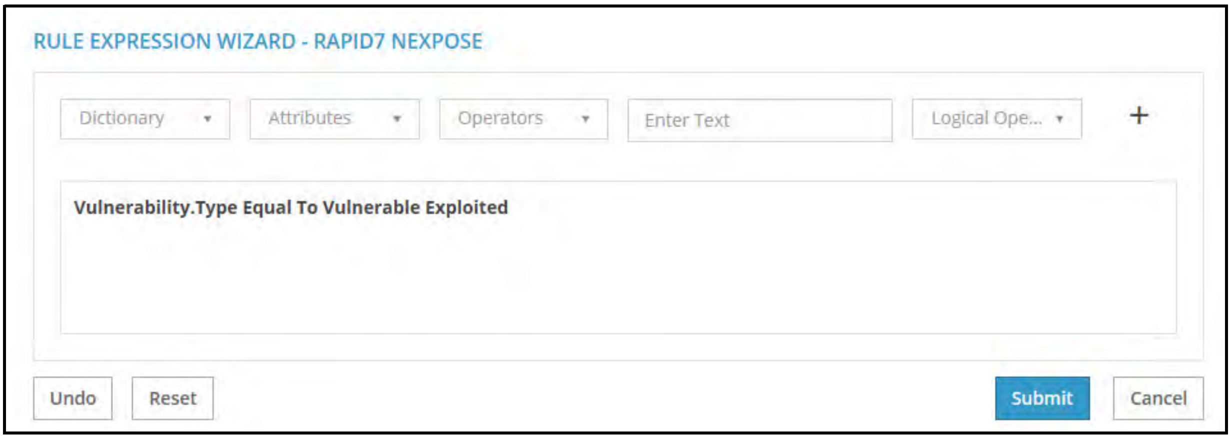
Field	Description
Click + icon to add new remediation rules	
Remediation Action	
Name	Type the name of the rule.
Disable Rule	Select the check box if you do not want to apply the defined rule to create issues or incidents.
Condition	Displays the rule that is added by using the Rule Expression Wizard window.

Field	Description
Rule Expression Wizard	Click this button to define remediation rules for issues or incidents. To define rules, perform the following steps: **1.** Click the **Rule Expression Wizard** button. The **Rule Expression Wizard - Rapid7 Nexpose** window appears.  RULE EXPRESSION WIZARD - RAPID7 NEXPOSE Dictionary Attributes Operators Enter Text Logical Ope... + Undo Reset Submit Cancel Vulnerability.Type Equal To Vulnerable Exploited **2.** Define the rule as required. **3.** Click **Submit** to create the rule. For more information on **Rule Expression Wizard - Rapid7 Nexpose** window, see Rule Expression Wizard - Tenable SecurityCenter Window.
Combined Risk Rating	Select the combined risk rating. The available options are: - Critical - High - Medium - Low
Target	Select the remediation target. Remediation target defines the target system for issue/incident. - **Issues**: Select this option if you want to trigger issues in the Issues module. **Note:** You can select remediation target for manual issue/incident creation by configuring the parameter **MS_ITG_RMD_CONFIG**. - **Remedy**: Select this option if you want to trigger incident in BMC remedy. - **ServiceNow:** Select this option if you want to trigger incident in ServiceNow.
Template Type	Select the remediation template type corresponding to the remediation template that you want to add in the rule. The available options are: - Network Vulnerability Remediation - Web Application Vulnerability Remediation
Template Name	Select the remediation template name that you want to add in the rule. **Note:** Template names are available for selection based on the selected template type.

Field	Description
Incident Priority *Appears only when you select the Remedy option in the Remediation Target field.*	**Urgency**: Select the urgency of the incident. The available options are: • 1-Critical • 2-High • 3-Medium • 4-Low **Impact**: Select the impact of the incident. The available options are: • 1-Extensive/Widespread • 2-Significant/Large • 3-Moderate/Limited • 4-Minor/Localized

Rule Expression Wizard - Rapid7 Nexpose Window

Use this window to define remediation issue creation rules.



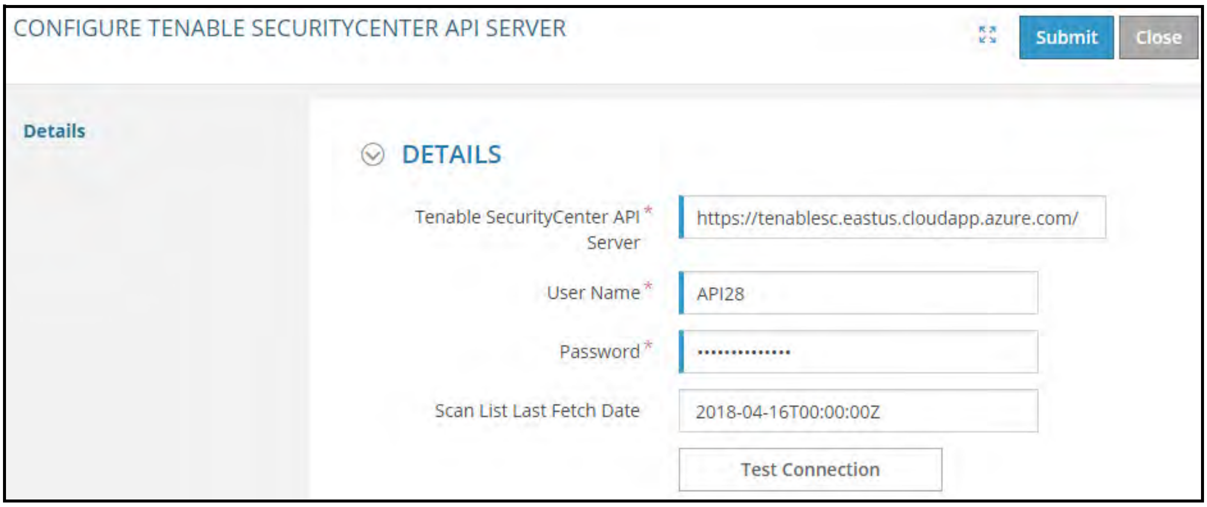
Vulnerability.Type Equal To Vulnerable Exploited

Figure 89 Rule Expression Wizard - Rapid7 Nexpose Window

Field	Description
Dictionary	Select if you want to create a rule for an Asset or Vulnerability.
Attributes	Select the attribute for which you want to create the rule. This field displays the values based on the value that you select in the Dictionary field.
Operators	Select the operator. This field displays the operators based on the values that you select in the Dictionary and Attributes fields. The available options are: • Equal To • Not Equal To • Greater Than • Less Than • Greater Than Equal To • Less Than Equal To
Value	Define the value in this field. This field displays the values based on the attribute that you select in the Attributes field.
Add icon	Click this icon to add the rule.
Connecting Operator	Select the connecting operator. The available operators are: • **AND**: Select this option to “AND” (combine) two different rules. • **OR**: Select this option to “OR” (either of the options) two different rules.
ADD button	Click this button to add the connecting operator.
Buttons	
Submit	Click this button to submit the created rule and close. Once you submit, the created rule appears in the Rule Condition field of the Remediation Rules form.
Undo	Click this button to clear the last-entered expression.
Reset	Click this button to clear the defined rule and reset.

Tenable SecurityCenter Configuration

Use the **Configure Tenable SecurityCenter API Server** form to configure the SecurityCenter setup access to your organization. You should set up the API Server URL, User Name and Password for the SecurityCenter API server from which you want to retrieve the vulnerability details, for the assets scanned via Tenable SecurityCenter for the specified duration. Once you submit the form and run the **MS_TSC_SECURITYCENTER_SYNC_TAV** infolet, the vulnerability data is retrieved from the SecurityCenter sever. The retrieved information is saved in the Mongo database. The vulnerability data, such as the scanned asset details and related vulnerability information, scan records, and so on, is saved in the “**MsItgCommonTaV**” collection. The Timestamp and the IP addresses of the scanned assets are saved in the **MsItgLatestAssetAndLatestTimeStamp** collection.



Tenable SecurityCenter API Server *	https://tenablesc.eastus.cloudapp.azure.com/
User Name *	API28
Password *	•••••••••••••••
Scan List Last Fetch Date	2018-04-16T00:00:00Z

Figure 90 Configure Tenable SecurityCenter API Server Form

Field	Description
Tenable SecurityCenter API Server	Type the SecurityCenter API Server URL.
User Name	Type the user name of the Tenable SecurityCenter API Server.
Password	Type the password of the Tenable SecurityCenter API Server.
Scan List Last Fetch Date (YYYY-MM-DDTHH:MM:SSZ)	Provide the duration from past date to current date that you want to retrieve the scan results. For example, if you want to retrieve the scan results of May 05, 2017 10 AM 10 Minutes and 10 seconds, you can provide input as below: 2017-05-05T10:10:10Z **Note:** The details that you have provided for the Tenable SecurityCenter API Server URL, User Name, Password, Scan List Fetch Date are stored in the **MS_ITG_Config** table. After you submit the form and run the **MS_TSC_SECURITYCENTER_SYNC_TAV** infolet, the Vulnerability data is fetched.
Test Connection	Test the connection with Tenable SecurityCenter API Server.

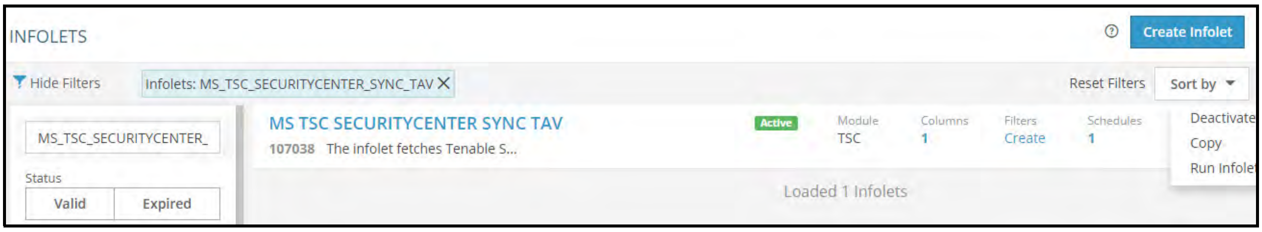
After entering all the required details in the form, click **Submit** to submit the form.

Running Infolet of Tenable SecurityCenter

After submitting the form, you can fetch the vulnerability data from Tenable SecurityCenter by running the **MS_TSC_SECURITYCENTER_SYNC_TAV** infolet.

To retrieve the vulnerability data from Tenable SecurityCenter by running the infolet, perform the following:

1. Login as SYSTEMI.
2. Navigate to the **Infolets** page.
3. Click the **Run Infolet** link corresponding to the **MS_TSC_SECURITYCENTER_SYNC_TAV** infolet.



INFOLETS

Infolets: MS_TSC_SECURITYCENTER_SYNC_TAV

MS_TSC_SECURITYCENTER_

Status

MS TSC SECURITYCENTER SYNC TAV

107038 The infolet fetches Tenable S...

Module TSC

Columns 1

Filters Create

Schedules 1

Loaded 1 Infolets

Figure 91 Running Tenable SecurityCenter Infolet

Note: Once you click **Run Infolet**, the retrieved data from Tenable SecurityCenter is stored in the **MsItgCommonTaV** collection.

Setting up Remediation Templates - Tenable SecurityCenter Connector

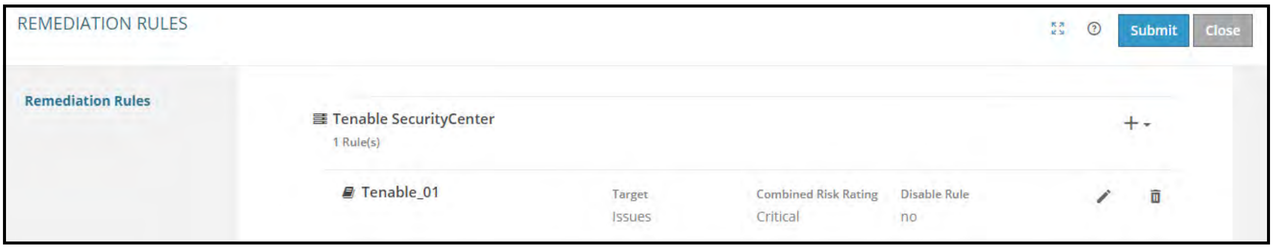
The first step of managing your threat and vulnerability management program, is to define remediation templates. For setting up template, refer Remediation Templates.

Note: The **Remedy** template and **ServiceNow** template is available in your environment based on your subscription.

Adding Remediation Rules - Tenable SecurityCenter Connector

After configuring your remediation templates, you need to setup business rules that helps you to prioritize the vulnerabilities to be remediated. The product provides an intuitive rule builder that lets you combine the business context for your assets with the vulnerability context for those assets. A remediation rule (when to trigger the ticket), then ties to a remediation target (where to trigger the ticket) and a remediation template (to whom, to trigger the ticket).

The following rules have been set up for the Tenable SecurityCenter connector:



REMEDIATION RULES

Remediation Rules

Tenable SecurityCenter
1 Rule(s)

Tenable_01

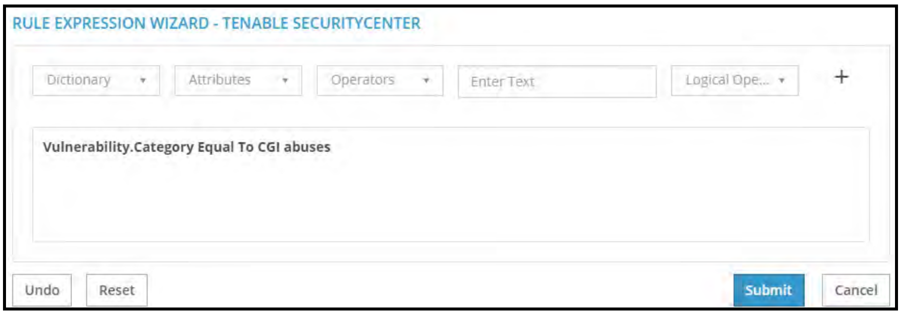
Target Issues

Combined Risk Rating Critical

Disable Rule no

Figure 92 Adding Remediation Rules - Tenable SecurityCenter

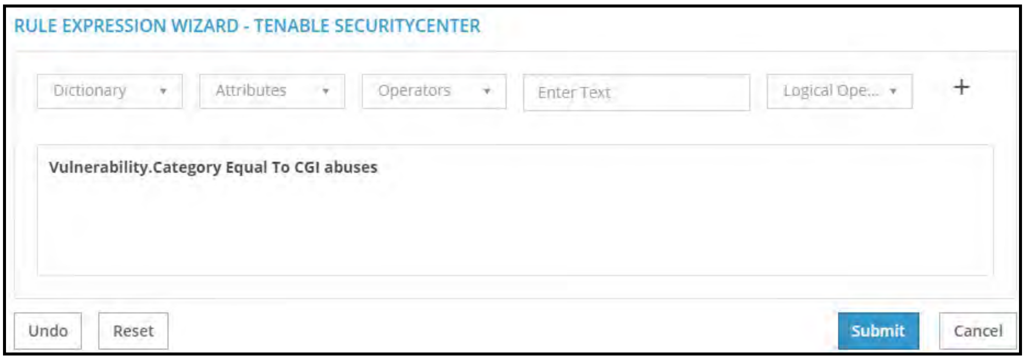
Field	Description
Click + icon to add new remediation rules	
Remediation Action	
Name	Type the name of the rule.

Field	Description
Disable Rule	Select the check box if you do not want to apply the defined rule to create issues or incidents.
Condition	Displays the rule that is added by using the Rule Expression Wizard window.
Rule Expression Wizard	Click this button to define remediation rules for issues or incidents. To define rules, perform the following steps: **1.** Click the **Rule Expression Wizard** button. The **Rule Expression Wizard - Tenable SecurityCenter** window appears.  RULE EXPRESSION WIZARD - TENABLE SECURITYCENTER Dictionary Attributes Operators Enter Text Logical Ope... + Undo Reset Submit Cancel Vulnerability.Category Equal To CGI abuses **2.** Define the rule as required. **3.** Click **Submit** to create the rule. For more information on Rule Expression Wizard - Tenable SecurityCenter window, see Rule Expression Wizard - Tenable SecurityCenter Window.
Combined Risk Rating	Select the combined risk rating. The available options are: • Critical • High • Medium • Low
Target	Select the remediation target. Remediation target defines the target system for issue/incident. • **Issues**: Select this option if you want to trigger issues in the Issues module. **Note:** You can select remediation target for manual issue/incident creation by configuring the parameter **MS_ITG_RMD_CONFIG**. • **Remedy**: Select this option if you want to trigger incident in BMC remedy. • **ServiceNow:** Select this option if you want to trigger incident in ServiceNow.
Template Type	Select the remediation template type corresponding to the remediation template that you want to add in the rule. The available options are: • Network Vulnerability Remediation • Web Application Vulnerability Remediation

Field	Description
Template Name	Select the remediation template name that you want to add in the rule. **Note:** Template names are available for selection based on the selected template type.
Incident Priority *Appears only when you select the Remedy option in the Remediation Target field.*	**Urgency**: Select the urgency of the incident. The available options are: • 1-Critical • 2-High • 3-Medium • 4-Low **Impact**: Select the impact of the incident. The available options are: • 1-Extensive/Widespread • 2-Significant/Large • 3-Moderate/Limited • 4-Minor/Localized

Rule Expression Wizard - Tenable SecurityCenter Window

Use this window to define remediation issue creation rules.



Vulnerability.Category Equal To CGI abuses

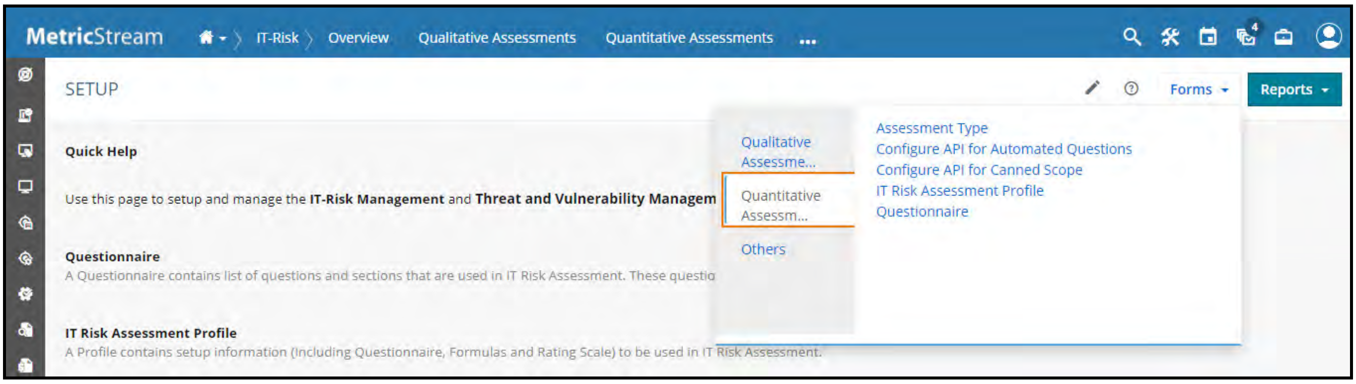
Figure 93 Rule Expression Wizard - Tenable SecurityCenter Window

Field	Description
Dictionary	Select if you want to create a rule for an Asset or Vulnerability.
Attributes	Select the attribute for which you want to create the rule. This field displays the values based on the value that you select in the Dictionary field.
Operators	Select the operator. This field displays the operators based on the values that you select in the Dictionary and Attributes fields. The available options are: • Equal To • Not Equal To • Greater Than • Less Than • Greater Than Equal To • Less Than Equal To
Value	Define the value in this field. This field displays the values based on the attribute that you select in the Attributes field.

Field	Description
Add icon	Click this icon to add the rule.
Connecting Operator	Select the connecting operator. The available operators are: • **AND**: Select this option to "AND" (combine) two different rules. • **OR**: Select this option to "OR" (either of the options) two different rules.
ADD	Click this button to add the connecting operator.
Buttons	
Submit	Click this button to submit the created rule and close. Once you submit, the created rule appears in the Rule Condition field of the Remediation Rules form.
Undo	Click this button to clear the last-entered expression.
Reset	Click this button to clear the defined rule and reset.

Setup (Quantitative Assessment)

Use the **Setup** page (Quantitative Assessment) to perform various quantitative assessment functions related to IT-Risk management.



Quick Help

Use this page to setup and manage the **IT-Risk Management** and **Threat and Vulnerability Managem**

Questionnaire

A Questionnaire contains list of questions and sections that are used in IT Risk Assessment. These questio

IT Risk Assessment Profile

A Profile contains setup information (Including Questionnaire, Formulas and Rating Scale) to be used in IT Risk Assessment.

Figure 94 Setup Page - Quantitative Assessment

Forms

Use the links within the **Forms** drop-down list, as displayed in the following figure, to access various forms that help in the setting up the IT Risk quantitative assessments.

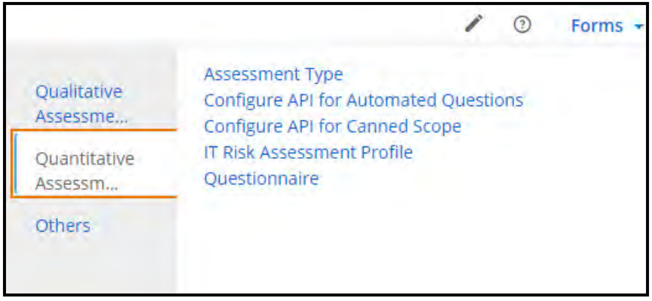

Forms
Qualitative Assessme...
Quantitative Assessm...
Others
Assessment Type
Configure API for Automated Questions
Configure API for Canned Scope
IT Risk Assessment Profile
Questionnaire

Figure 95 Forms of Quantitative Assessment Setup Page

You can access the following forms:

- **Questionnaire** - Opens the Questionnaire form. This form allows you to create a questionnaire.
- **IT Risk Assessment Profile** - Opens the IT Risk Assessment Profile form. This form allows you to create an IT Risk assessment profile. This form determines the Questionnaire to be used, and configures the level of automation in assessment response. It also configures the summary formulas and the associated risk ratings.
- **Assessment Type** - Opens the Assessment Type form. This form allows you to create an assessment type which defines the objects that take part in the scope of the IT Risk assessment.
- **Configure API for Automated Questions** - Opens the Configure API for Automated Questions form. This form allows you to configure API that can be used to automatically compute the response to the questions. The API association is not mandatory for each question. Only the questions which are supposed to be responded automatically need to be associated with an API.
- **Configure API for Canned Scope** - Opens the Configure API for Canned Scope form. This form allows you to configure API that can be used for canned scope selection. This is a one-time configuration process, and it does not allow you to configure it again.

Note: For details, refer to the MetricStream Arno Release Spring ‘21 - IT and Cyber Risk - User Guide.

Reports

Use the links within the **Reports** drop-down list to access the reports available in the **Quantitative Assessment** section, as displayed in the following figure.

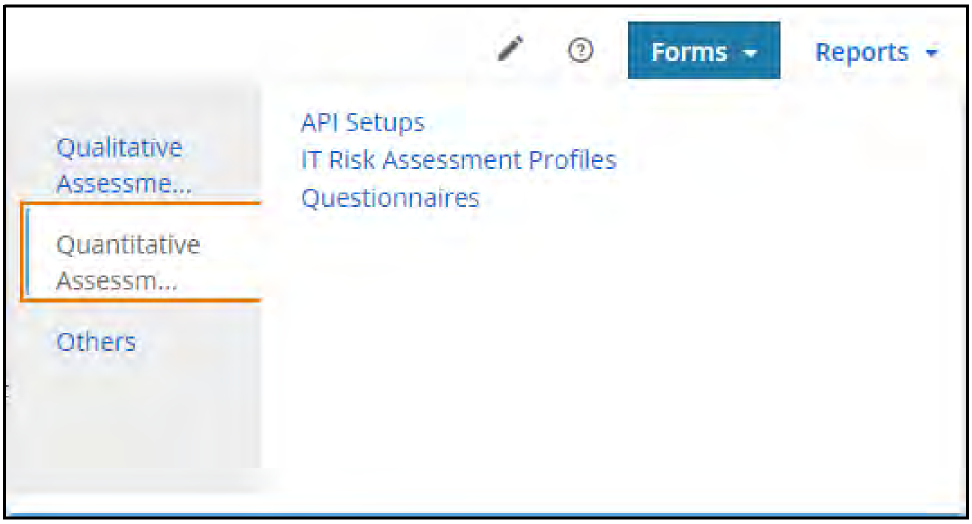


Figure 96 Reports of Quantitative Assessments

The **Reports** button has the following reports within it:

- **API Setups** - Opens the API Setups report, which displays the API setup details available in the system.
- **IT Risk Assessment Profiles** - Opens the IT Risk Assessment Profiles report, which displays all risk assessment profiles available in the system.
- **Questionnaires** - Opens the Questionnaires report, which displays the IT risk assessment questionnaire available in the system.

Note: For details, refer to the MetricStream Arno Release Spring '21 - IT and Cyber Risk - User Guide.

Appendix

This section provides the list of supported special characters.

Sections:

- Restricted Special Characters

Restricted Special Characters

The following table provides the special characters that are not allowed in the specified form fields and in the template used for data upload.

<table>
<tr><th>Field</th><th>Restricted special character combinations</th></tr>
<tr><td><b>Threat</b> form -
• <b>General</b> section → <b>Name</b> field
• <b>Issue</b> section → <b>Add Issue</b> → <b>Title</b> field
• <b>Issue</b> section → <b>Add Action</b> → <b>Title</b> filed
<b>Threat Actor</b> form → <b>General</b> section → <b>Title</b> field
<b>Vulnerability</b> form -
• <b>General</b> section → <b>Name</b> field
• <b>Issue</b> section → <b>Add Issue</b> → <b>Title</b> field
• <b>Issue</b> section → <b>Add Action</b> → <b>Title</b> filed</td><td>^&^   , and ~   #_#   @@   @@<-   >@@
$^^$   \\|\\|\\| $#$ ||| @#@   _$$_
$$$ %#%   &#&   ;#~   ;#,   #~#
[|] |@^| ||^|| !^()^!   ^^   <~>
||!|| <!>   <::>   <* |? |#|</td></tr>
</table>

For more details on special characters, refer to the MetricStream Arno Release Spring ‘21 - Platform - Configuration Guide.

Glossary

Chart

A graphical representation of data

GRC

Governance, Risk, and Compliance

Infocenter

A common and user specific page that appears to users after they login to the MetricStream application. The individual items in the infocenter, such as user forms, assignments, and reports appear on this page.

Infoport

All related user objects, which are grouped in a single section of the infocenter, that facilitate work.

Reports

A tabular representation of data.

References

You can refer to the following documents:

- MetricStream Arno Release Spring ‘21 - Issues - User Guide
- MetricStream Arno Release Spring ‘21 - Risk Assessments - User Guide
- MetricStream Arno Release Spring ‘21 - Platform - User Guide

Feedback

MetricStream welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important to us. For any documentation-related comments and suggestions, write to: TechPubs