Documentation Guide for Ivanti Neurons for GRC

Release 2022.1

December 13, 2022

TOC

About Ivanti Neurons for GRC 2022.1

Use Neurons for GRC as a Governance, Risk, and Compliance (GRC) software to provide a centralized platform for your organization to assess risk and manage compliance against numerous authoritative sources.

Minimum platform version requirements: Ivanti Neurons for GRC 2021.4

Prerequisites: Contact Ivanti Professional Services Organization (PSO) to obtain and install the Ivanti Neurons for GRC package.

This software provides the following benefits:

- Analysis and mitigation of risks.
- Streamlined audits, findings, reports, and processes for appropriate actions.
- Rapid containment of any breaches and documentation of steps taken in a secure, need-to-know process.

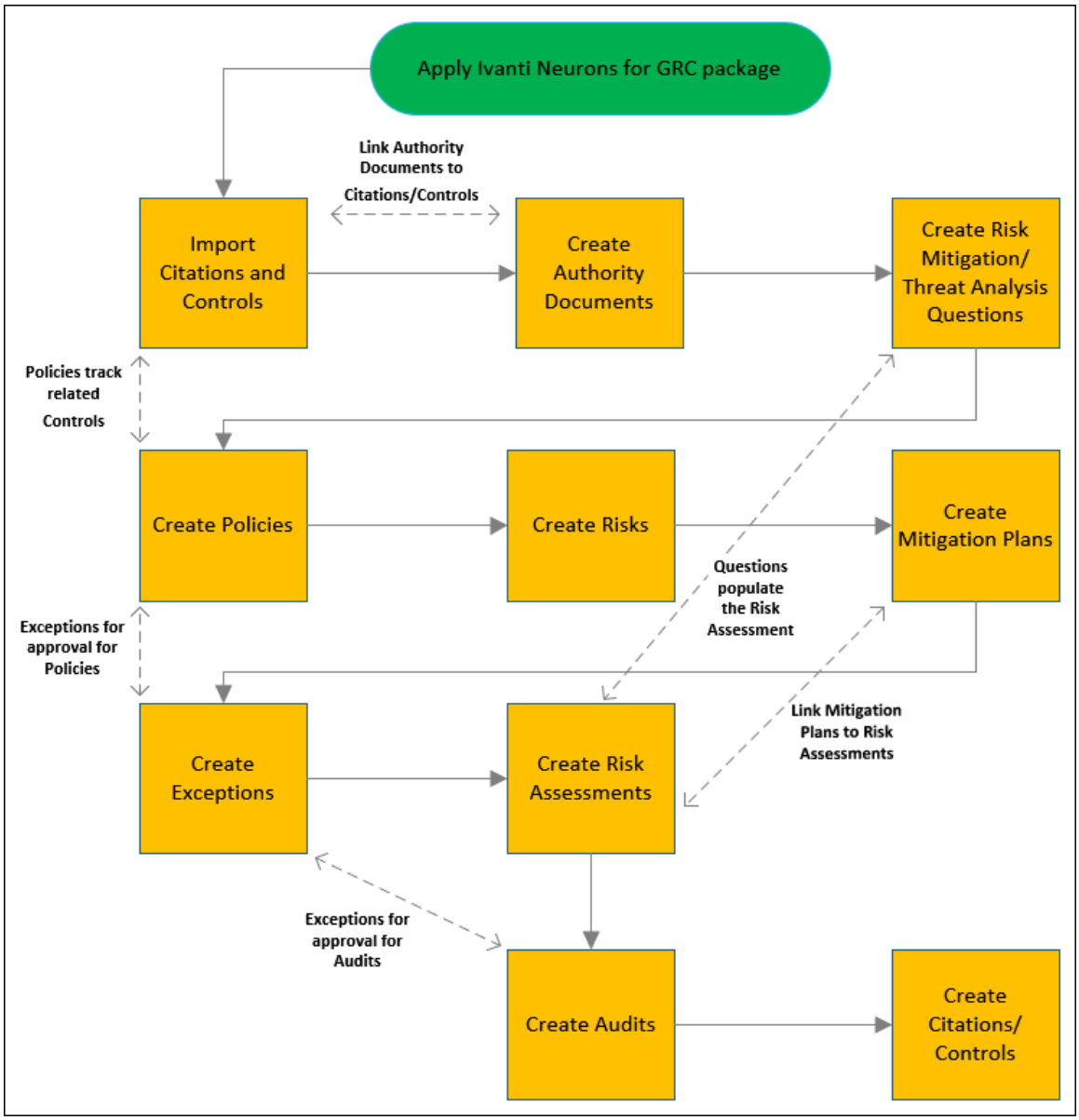
Neurons for GRC is associated with the GRC Manager role and the following Business Objects:

- Approvals
- Audit
- Audit Calendar
- Authority Documents
- Citation
- Controls
- Exception
- Mitigation Plans
- Policy
- Risk
- Risk Assessment

How Ivanti Neurons for GRC Works

This is a high-level overview of how you can use this software. The steps and order vary depending on your organization's approach and requirements for risk and compliance management.

Neurons for GRC Workflow



1. After you apply the software package, import Citations and Controls. You can manually create them, but we recommend you utilize the import for consistency and ease of entry. You'll need Citations and Controls in the system before you can link them to Authority Documents.
2. Create Authority Documents to link to Citations and Controls.
3. Create questions and assign Risk Values, Question Impact, and Question Sequence to use the Risk Assessment form. Risk Mitigation Questions and Threat Analysis Questions populate the Risk Assessment.

4. Create Policies to track related Controls.
5. Create Risks to manage potential problems.
6. Create Mitigation Plans to use with other Neurons for GRC Business Objects to ensure compliance with Audits, Risks, Citations, and Controls.
7. Create Exceptions to gain approval for non-compliance with an Audit or Policy.
8. Create a Risk Assessment to discover, correct, or prevent security problems.
9. Create Audits for scheduled review of compliance related to an industry standard such as ISO 20071:2013 or key Configuration Items (infrastructure, supporting services, or collateral).
10. Manually create Controls and Citations and link Citations to Controls.

Use Ivanti Neurons for GRC

This software helps you manage records to track risks and streamline processes.

Use the software to:

Import Controls and Citations Group Data

Before you create Authority Documents, import Citations and Controls via the **Data Import Wizard**.

Create Control Groups that align with current industry standards such as FedRAMP:2014, ISO 27001:2013, and ISO 9001:2015.

Citations are passages or expressions in a document that are quoted or cited and express a specific requirement from the Authority Document. Controls are the specific steps or actions within a compliance mandate that must be met to fulfill a compliance requirement. Controls can be mapped to multiple Citations from multiple Authority Documents.

To import Citations and Controls:

1. Set up the Data Import Connection.

   See *Setting Up a Data Import Connection* in Data Import Connections.

2. Use **Manual File Upload** for the **Connection Type** and upload the Excel spreadsheet.
3. The **Source Unique Key** is **ID**.
4. The **Target Business Object** is **GRC Citation**.
5. No **Filter Setting** is necessary.
6. Add a row for the **Reference ID** and the corresponding field is **CitatationID**.
7. Select **Publish & Run Now**.

   This imports the data from an outside source into the Neurons for GRC database and creates new records. Each record needs a unique ID (Control_RecID or Citation_RecID).

You must have permissions for shared access to both the file (and its enclosing directories) and the Neurons for GRC server receiving the data.

Create or Edit an Authority Document

Create an Authority Document so you can link Citations to them. Authority Documents can be a combination of statuses, regulations, directives, principles, standards, best practices, policies, and procedures.

To create an Authority Document:

1. Open the Authority Document workspace.
2. Select **New GRC Authority Document** to create a new Authority Document.

   A blank form opens.
3. Enter the information into the fields as required.

   a. **Owner Email** and **Sponsor Email** autopopulate based on the **Owner** and **Sponsor** fields.
4. In the **Details** tab, enter a **Document Title** field.
5. Select **Save**.
6. Use the **Supervisory Authorities**, **Citations**, and **Controls** tabs to link Supervisory Authorities, Citations, and Controls to the Authority Document.

   You can also use the tabs to create new Supervisory Authorities, Citations, and Controls.
7. Select **Save**.

Edit an Authority Document

To edit an Authority Document:

1. Double-click an Authority Document to open the details.
2. Change the information as needed.
3. Select **Save**.

Create Risk Mitigation and Threat Analysis Questions

You must create questions and assign Risk Values, Question Impact, and Question Sequence to use the Risk Assessment form. The questions help assess risk and threat and the current state of requirements.

Risk Mitigation Questions and Threat Analysis Questions populate the Risk Assessment. We recommend that you align Risk Assessment Questions with current industry standards such as FedRAMP:2014, ISO 27001:2013, or ISO 9001:2015.

To create Risk Mitigation and Threat Analysis Questions:

1. In **Administrator**, select the **Risk Assessment Business Object**, and then select **Quick Actions**.

    a. Select **Subset of Action Questions**, and then select **Edit**.

    The description indicates **Threat** or **Risk** and **#**.

    - Select an existing question to modify or edit.
    - Select **Add** to add a new question.

    b. Select **Save** when you're finished.

Create or Edit a Policy

Create a Policy for written guidelines your organization communicates to its employees about how they execute security strategy. Policies formalize your organizational approach to archiving Control requirements.

To create a Policy:

1. Open the Policy workspace.
2. Select **New GRC Policy** to create a new Policy.

   A blank form opens.
3. Enter the information into the fields as required.

   a. **Owner Email** and **Business Owner Email** autopopulate based on the **Owner** and **Business Owner** fields.
4. Select **Save**.
5. In the **Details** tab, enter the information into the fields as required.
6. Use the **Risk Assessments**, **Audits**, **Assets**, **Compliances**, and **Controls** tabs to link Risk Assessments, Audits, Assets, Compliances, and Controls to the Policy.

   You can also use the **Control** tab to create new Controls.
7. Select **Save**.

Edit a Policy

To edit a Policy:

1. Double-click a Policy to open the details.
2. Change the information as needed.
3. Select **Save**.

Create or Edit a Risk

Create a Risk to define and manage issues and potential problems.

To create a Risk:

1. Open the Risk workspace.
2. Select **New GRC Risk** to create a new Risk.

   A blank form opens.
3. Enter the information into the fields as required.
   a. **Owner Email** autopopulates based on the **Owner** field.
   b. **Review Cadence** creates a Task based on how often the Risk needs to be reviewed.
   c. Select the **Create Review Tasks** checkbox to create review Tasks.
   d. **Grade** autopopulates based on Impact and Likelihood.
   e. **Grade change** displays a graphic that shows if the grade has increased with a green arrow or decreased with a red arrow.
4. Select **Save**.
5. In the **Details** tab, enter the information into the fields as required.
6. Use the **Controls**, **Mitigation Plans**, **Assets**, **Risk Assessments**, **Audits**, and **Policies** tabs to link Controls, Mitigation Plans, Assets, Risk Assessments, Audits, and Policies to the Risk.
   a. Use the **Controls** and **Mitigation Plans** tabs to create new Controls and Mitigation Plans.
   b. You can restore hidden tabs using the **plus** sign (to the right of the tabs).
7. Select **Save**.

Edit a Risk

To edit a Risk:

1. Double-click a Risk to open the details.
2. Change the information as needed.
3. Select **Save**.

Create or Edit a Mitigation Plan

Use Mitigation Plans in conjunction with other GRC Business Objects to track proactive actions or ensure compliance with Audits, Risks, and Citations. You can link Mitigation Plans to Tasks and Risk Assessments.

To create a Mitigation Plan:

1. Open the Mitigation Plan workspace.
2. Select **New GRC Mitigation Plan** to create a new Mitigation Plan.

   A blank form opens.
3. Enter the information into the fields as required.
   a. **Owner Email** autopopulates based on the **Owner** field.
   b. **Incomplete Tasks** will have a number below it if there are incomplete Tasks associated with the Mitigation Plan. Those Tasks must be completed before you can complete the Mitigation Plan. The Tasks associated with the Mitigation Plan are listed in the **Tasks** tab.
4. Select **Save**.
5. Use the **Tasks**, **Controls**, **Risks**, **Risk Assessments**, and **Audit** tabs to link Task, Controls, Risks, Risk Assessments, and Audits to the Mitigation Plan.

   Use the **Tasks** and **Controls** tabs to create new Task and Controls.
6. Select **Save**.

Edit a Mitigation Plan

To edit a Risk:

1. Double-click a Mitigation Plan to open the details.
2. Change the information as needed.
3. Select **Save**.

Create or Edit an Exception

Create an Exception to document and gain approval for non-compliance with an Audit or Policy.

To create an Exception:

1. Open the Exceptions workspace.
2. Select **New GRC Exception** to create a new Exception.

   A blank form opens.
3. Enter the information into the fields as required.
   a. **Requester Email** and **Owner Email** autopopulate based on the **Requester Email** and **Owner Email** fields.
   b. **Status** autopopulates as **New**.
4. The approver can vote to Approve or Deny. The Approver needs to provide approval before the Exception can move to the next step. The approver for the Exception is determined by the **Exception Type**.
   a. After you select an **Exception Type**, a tab is added for that type.
   b. Based on the **Exception Type**, an **Audit** or **Policy** field is added to choose a record.
5. Select **Save**.
6. In the **Details** tab, enter the information into the fields as required.
7. Use the **Assets**, **Controls**, and **Risk Assessments** tabs to link Assets, Controls, and Risk Assessments to the Exception.
   a. Use the **Controls** tab to create new Controls.
   b. The **Audit/Policy** tab displays a summary form of the Audit or Policy.
   c. The **Approval** tab displays the approval details. Every Exception must be approved by the Owner of the Audit or Policy.
   d. You can restore hidden tabs using the **plus** sign (to the right of the tabs).
8. To approve or deny the Exception, from the **Action Menu**, select **Approve my vote** or **Deny my vote**.
9. Select **Save**.

Edit an Exception

To edit an Exception:

1. Double-click an Exception to open the details.

2. Change the information as needed.
3. Select **Save**.

Create or Edit a Risk Assessment

Create a Risk Assessment to discover, correct, and prevent security problems. Complete analysis questions and calculate Risk scores (mitigated and unmitigated). Accept the Risk and mitigate with Controls or a Mitigation Plan, or transfer or avoid the Risk.

Create a Risk Assessment

To create a Risk Assessment:

1. Open the Risk Assessment workspace.
2. Select **New GRC Risk Assessment** to create a new Risk Assessment.

   A blank form opens.
3. Enter the information into the fields as required.
   a. The questions for Threat Analysis and Risk Mitigation are based on the **Risk Assessment Type**.
   b. **% of Threat Analysis Assessment Complete** is based on the total number of questions answered.
   c. **% of Risk Mitigation Assessment Complete** is based on the total number of questions answered.
   d. **Current Unmitigated Risk** and **Current Mitigated Risk** are based on the questions weighted response.
4. Select **Save**.
5. In the **Threat Analysis** tab, there are a set of sample questions.
   a. Select each question, and then select a Threat Analysis Level from the **Select Threat Analysis Level** drop-down list.
   b. Select a question, and then select **No Impact** to change the impact.
      - If a Threat Analysis Question is set to **No Impact**, it's removed from the percentage complete. You can select **No Impact** for all but one question, and then select the level of threat and your analysis will be 100% complete.
6. In the **Risk Mitigation** tab, there are a set of sample questions.
   a. Follow steps a-b above to change the Risk Mitigation Level or Impact.
7. Use the **Threat Analysis**, **Risk Mitigation**, **Risks**, **Tasks**, **Journals**, **Controls**, **Mitigation Plans**, **Exceptions**, and **Linked Risk Assessments** tabs to link Threat Analyses, Risk Mitigations, Risks, Task, Journals, Controls, Mitigation Plans, Exceptions, and other Risk Assessments to the Risk Assessment.
8. You can restore hidden tabs using the **plus** sign (to the right of the tabs).

9. Select **Save**.

Edit a Risk Assessment

To edit a Risk Assessment:

1. Double-click a Risk Assessment to open the details.
2. Change the information as needed.
3. Select **Save**.

Create or Edit an Audit

Conduct an Audit for review of compliance related to an industry standard or key Configuration Items.

To create an Audit:

1. Open the Audit workspace.
2. Select **New GRC Audit** to create a new Audit.

   A blank form opens.
3. Enter the information into the fields as required.
   a. **Lead Auditor Email** autopopulates based on the **Lead Auditor** field.
   b. **Status** autopopulates as **New**.
   c. **Priority** autocalculates based on **Probability** and **Impact**.
4. Select **Save**.
5. In the **Details** tab, enter the information into the fields as required.
6. Use the **Participants**, **Assets**, **Linked Audits**, **Controls**, **Mitigation Plans**, **Authority Documents**, **Risk Assessments**, and **Scheduled Audits** tabs to link Participants, Assets, Linked Audits, Controls, Mitigation Plans, Authority Documents, Risk Assessments, and Scheduled Audits to the Audit.

   Exceptions are linked from the Exception Business Object, not from the Audit.
   a. If the **Recurring Audit** checkbox is selected in the **Details** tab, the **Scheduled Audits** tab displays the recurring Audits.
   b. Use the **Tasks** and **Controls** tabs to create new Task and Controls.
   c. You can restore hidden tabs using the **plus** sign (to the right of the tabs).
7. Select **Save**, and then **Refresh**.
8. Change the **Status** to **Approving**.
9. Once the Audit is approved, you can change the **Status** to **Active**.

Edit an Audit

To edit an Audit:

1. Double-click an Audit to open the details.
2. Change the information as needed.

3. Select **Save**.

Create or Edit a Control

Use Controls as security mechanisms to ensure adherence to Policies and assist with compliance to laws, regulations, and other authoritative standards.

To create a Control:

1. Open the Control workspace.
2. Select **New GRC Control** to create a new Control.

   A blank form opens.
3. Enter the information into the fields as required.
4. Select **Save**.
5. Use the **Policies**, **Citations**, **Tasks**, **Audits**, **Exceptions**, and **Mitigation Plans** tabs to link Policies, Citations, Task, Audits, Exceptions, and Mitigation Plans to the Control.
   a. Use the **Citations**, **Tasks**, and **Mitigation Plan** tabs to create new Citations, Tasks, and Mitigation Plans.

Edit a Control

To edit a Control:

1. Double-click a Control to open the details.
2. Change the information as needed.
3. Select **Save**.

Create Citations and Link to Controls

Citations are the individual records that represent the statement, articles, and laws associated with an Authority Document. Controls state how the organization will comply with the Citations that require evidence.

You can manually create Citations or import them through a .csv import. We recommend you utilize the import for consistency and ease of entry.

See "Import Controls and Citations Group Data" on page 7

To manually create a Citation:

1. Open the Citation workspace.
2. Select **New GRC Citation** to create a new Citation.

   A blank form opens.
3. Enter the information into the fields as required.
   a. **Reference Group** and **Reference ID** are from the Authority Document. Your organization's strategy determines these values. For example, Information Technology 13250:2000 or the ISO Reference Group is IEC and the Reference ID is 12232:2002.
   b. **Control Implemented** is selected based on if there's a Control linked.
   c. **Policy Defined** is selected based on if the Policy linked has a Control that's linked to the Citation.
4. Select **Save**.
5. Use the **Controls**, **Authority Document**, **Policies**, and **Audits** tabs to link Controls, Authority Documents, Policies, and Audits to the Citation.
   a. Use the **Controls** tab to create new Controls.

Edit a Citation

To edit a Citation:

1. Double-click a Citation to open the details.
2. Change the information as needed.
3. Select **Save**.

Ivanti Neurons for GRC Dashboards

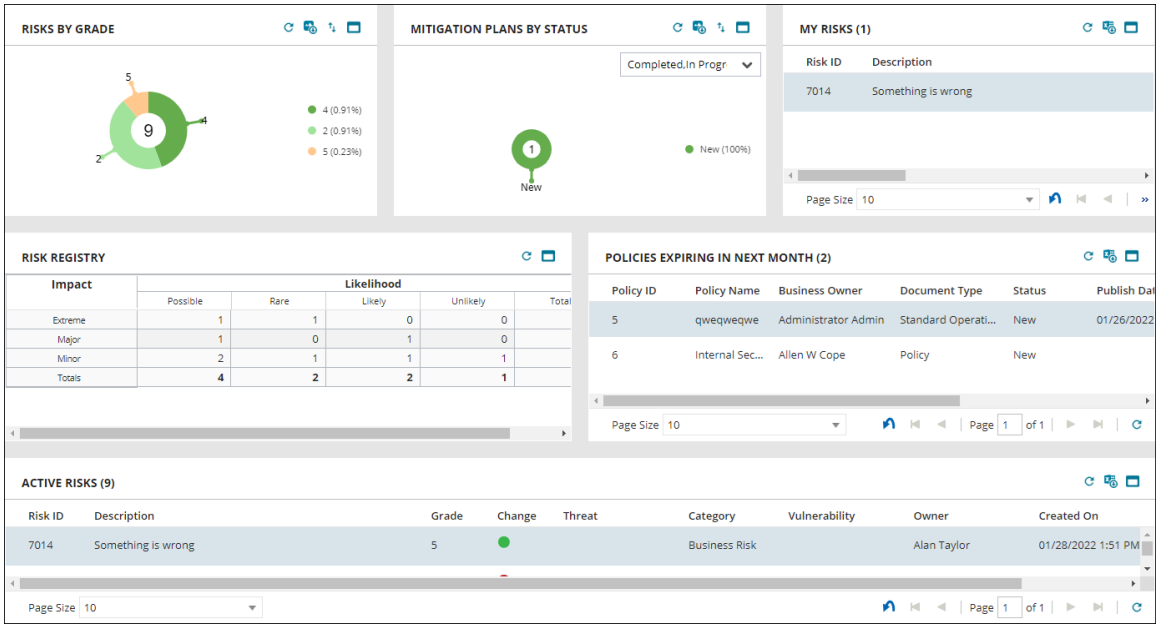
This software provides five dashboards for overview and at-a-glance metrics.

GRC Risks Dashboard

This dashboard aims to provide a Security Manager or Chief Information Security Officer (CISO) with an overall view of the organization's current risk assessments. The following information is available on this dashboard:

- Risk by Grade
- Mitigation Plans by Status
- My Risks
- Risk Registry
- Policies Expiring Next Month
- Active Risks

GRC Risks Dashboard



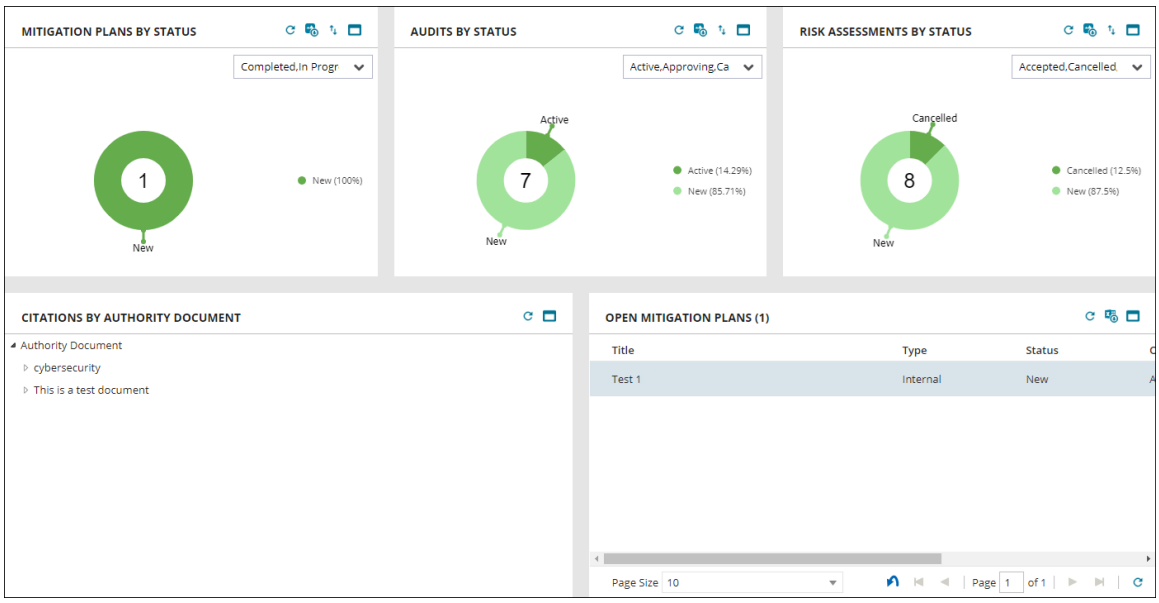
GRC Mitigation Plans Dashboard

This dashboard provides an overall view of the organization's current mitigation plans. The following information is available:

- Mitigation Plans by Status
- Audits by Status

- Risk Assessments by Status
- Citations by Authority Document
- Open Mitigation Plans

GRC Mitigation Plans Dashboard

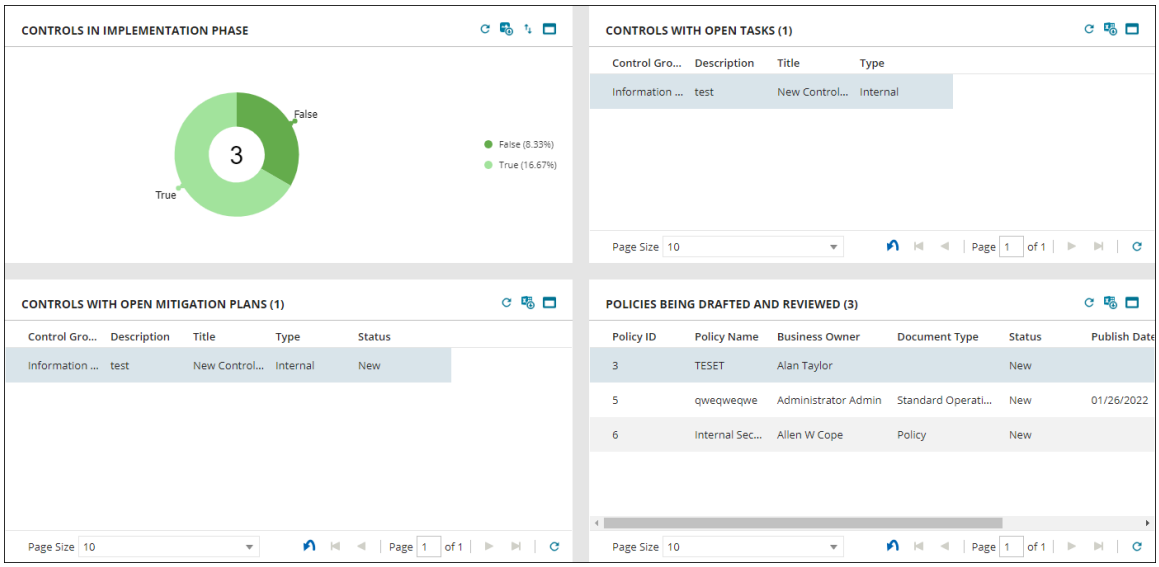


GRC Controls Dashboard

This dashboard provides an overview of the organization's current Controls and Policies status. The following information is available:

- Controls in Implementation Phase
- Controls with Open Mitigation Plans
- Controls with Open Tasks
- Policies being Drafted and Reviewed

GRC Controls Dashboard

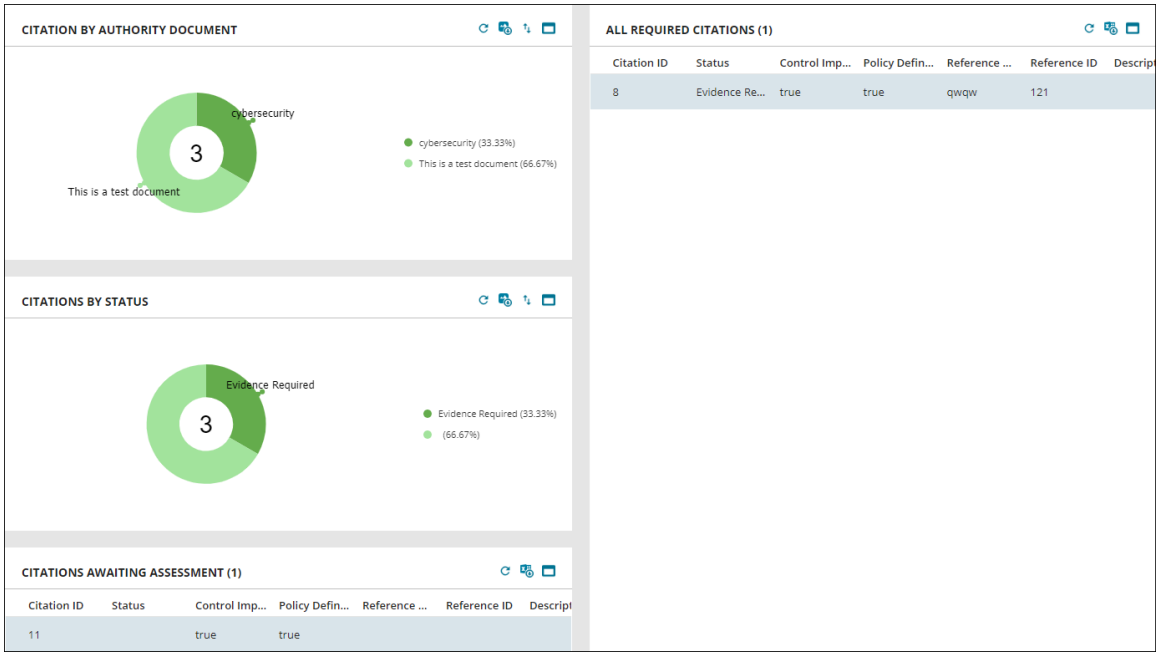


GRC Citations Dashboard

This dashboard provides an overview of the GDPR-related Citations and Risk Assessments. The following information is available:

- Citations by Authority Documents
- Citations by Status
- Citations awaiting Assessment
- All Required Citations

GRC Citations Dashboard

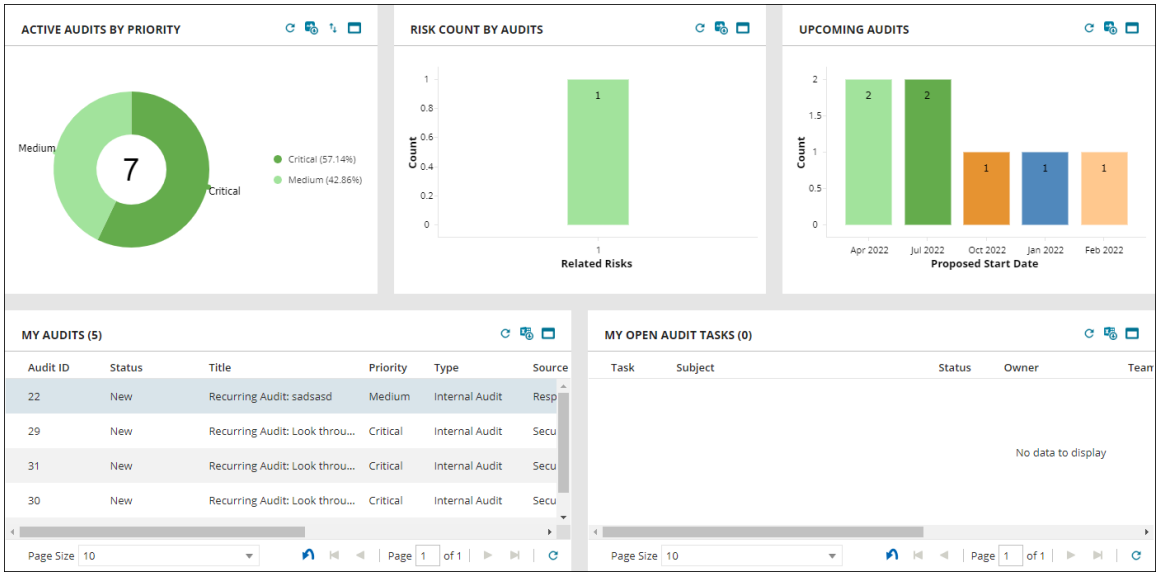


GRC Audit Dashboard

This dashboard provides an incite as to where Audits are currently. The following information is available:

- Active Audits by Priority
- Risk County by Audits
- Upcoming Audits
- My Audits
- My Open Audit Tasks

GRC Audit Dashboard



Audit Calendar

Use the Audit Calendar to view a calendar of proposed and actual start and end dates for Audits.

- Open the Audit Calendar workspace to view the Audit dates.