Cyntegrity My**RBQM**® Portal

User Manual

Platform Version 9.3.2 May 2026

Gateway to Clinical Operational Excellence & Performance Control

Table of Contents

Contents

Introduction

Risk varies inversely with knowledge.

Irving Fischer – American Economist

Clinical Trial Risk Management in the Modern Clinical Trial Landscape

In the dynamic landscape of clinical trials, pharmaceutical companies have traditionally outsourced aspects of trial implementation to contract research organizations (CRO) for efficiency and cost-effectiveness. However, a transformative approach known as Risk-based Quality Management (RBQM) has emerged, offering innovative strategies for managing clinical trials.

RBQM integrates quality by design principles and necessitates changes in clinical monitoring, data management, and project management. By implementing RBQM effectively, transparency in decision-making improves, proactive trial controls are enabled, and lessons are learned from previous trial data. RBQM drives efficiency, prioritizes patient safety, and adopts a proactive management approach.

Successful implementation of RBQM requires significant changes across all stages of clinical research, demanding effective management and oversight to seamlessly integrate it into trial operations.

What is Risk-based Quality Management?

Risk-based Quality Management (RBQM) has become a pivotal concept in pharmaceutical clinical research, offering the potential to improve data quality, patient safety, and expedite the time-to-market for medicines. RBQM involves adaptive monitoring practices based on critical key risk indicators (KRI), enabling a focused approach to areas with the highest potential impact on subject safety and data quality.

RBQM encompasses centralized monitoring, remote monitoring, reduced monitoring through targeted source data verification (SDV), and triggered monitoring based on predefined KRI or QTL thresholds. Both the FDA and the European Medicines Agency (EMA) recognize the importance of RBQM, emphasizing its role in human subject protection, trial integrity, and the facilitation of existing quality practices and standards, such as the ICH E6 and E8 guidelines.

Cyntegrity, in alignment with regulatory guidelines, considers RBQM as a profound change in the way clinical trials are conducted. It is seen as a preventive approach to trial management, aimed at avoiding negative surprises and enhancing overall trial efficiency.

What is the MyRBQM® Portal?

The **MyRBQM® Portal** is a comprehensive cloud-based software solution that empowers organizations with the tools to implement Risk-based Quality Management (RBQM) seamlessly. Serving as a pivotal element, the MyRBQM Portal automates the entire RBQM process, enabling efficient management of clinical trials.

With the MyRBQM Portal, users can effectively apply RBQM principles, integrate quality by design practices, and streamline clinical trial operations. The portal facilitates transparent decision-making, proactive trial controls, and the utilization of previous trial data for continuous improvement. By leveraging the MyRBQM Portal, organizations can enhance patient safety, optimize trial efficiency, and navigate the complex landscape of modern clinical trials.

With the guidance of the MyRBQM Portal's built-in clinical process workflows, study teams can easily detect, assess, mitigate, control, report, and archive risks. The Portal's integrated RBQM methodology encourages its users to think and act proactively, reducing "data noise" and accelerating statistical significance.

The MyRBQM Portal equips study teams with corrective and preventive actions following the CAPA principle. All activities and processes within the MyRBQM Portal are easy-to-audit since they are logged and tracked

automatically, providing full traceability and are human-readable.

Along with AI-driven statistical algorithms for fraud detection and misconduct, predictive and retrospective data analytics, and clinical indication-focused risk indicators, the MyRBQM Portal uniquely facilitates ICH GCP compliant risk management.

System Requirements and Installation

System Requirements

MyRBQM® is designed as a cloud-based solution and, thus, has minimal impact on the customer's infrastructure.

Installation of MyRBQM® Portal

The MyRBQM® Portal is a web-based application and therefore needs no installation on your computer or device. No data will be installed on your system. It is solely entered via web access.

Web Access

MyRBQM® can be accessed via any web browser. All functions, including study setup and administration, is provided via web access. The system features a modern web user interface with responsive design and a fallback strategy for older browsers.

The best experience will be delivered with recent versions of the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer
- Apple Safari

- Microsoft Edge
- Opera
- Chrome for Android
- iOS Safari
- Android

Older browser versions are generally supported (down to Internet Explorer 11), but certain advanced features, such as report template design, might be disabled due to missing features. Cyntegrity cannot guarantee an acceptable performance on web browsers older than Internet Explorer 8.

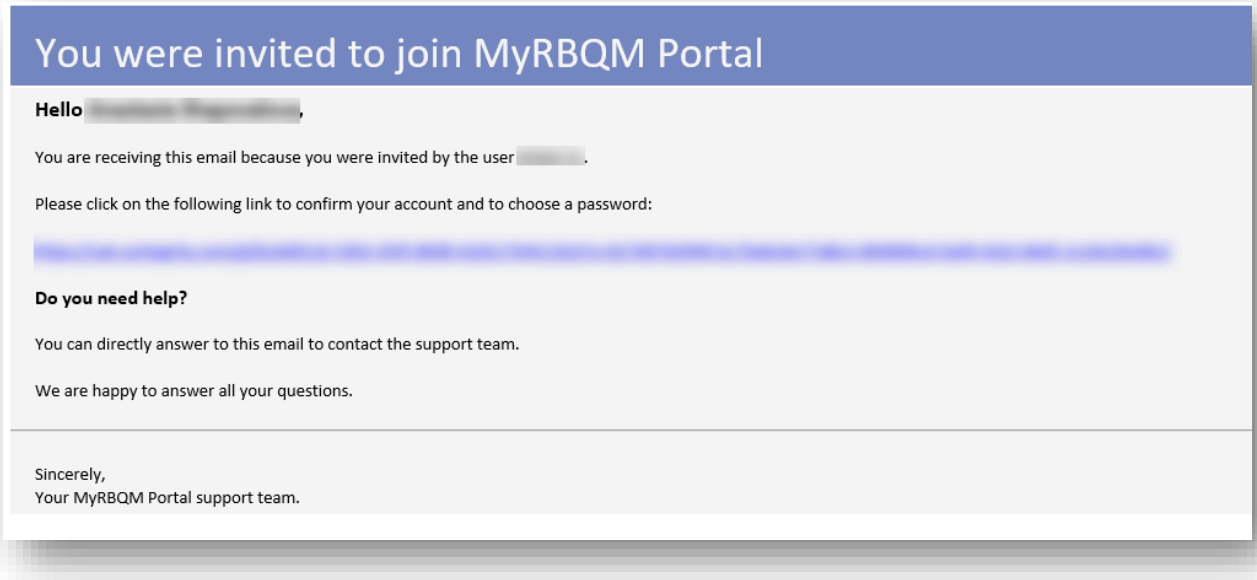
MyRBQM® Portal does not need to offer a separate specialized portal for mobile devices. We use a special design technique called Responsive Design which optimizes the user interface dynamically for any device screen size. Therefore, users will navigate to the same WebURL, regardless of device used.

Setting Up MyRBQM® Portal

To access the **MyRBQM® Portal** software, the user needs to create an account.

Create an Account

To create an account, you must have received an invitation from an administrator with the email subject: "You were invited to join MyRBQM Portal!"


You were invited to join MyRBQM Portal

Hello [redacted],

You are receiving this email because you were invited by the user [redacted].

Please click on the following link to confirm your account and to choose a password:

[redacted]

Do you need help?

You can directly answer to this email to contact the support team.

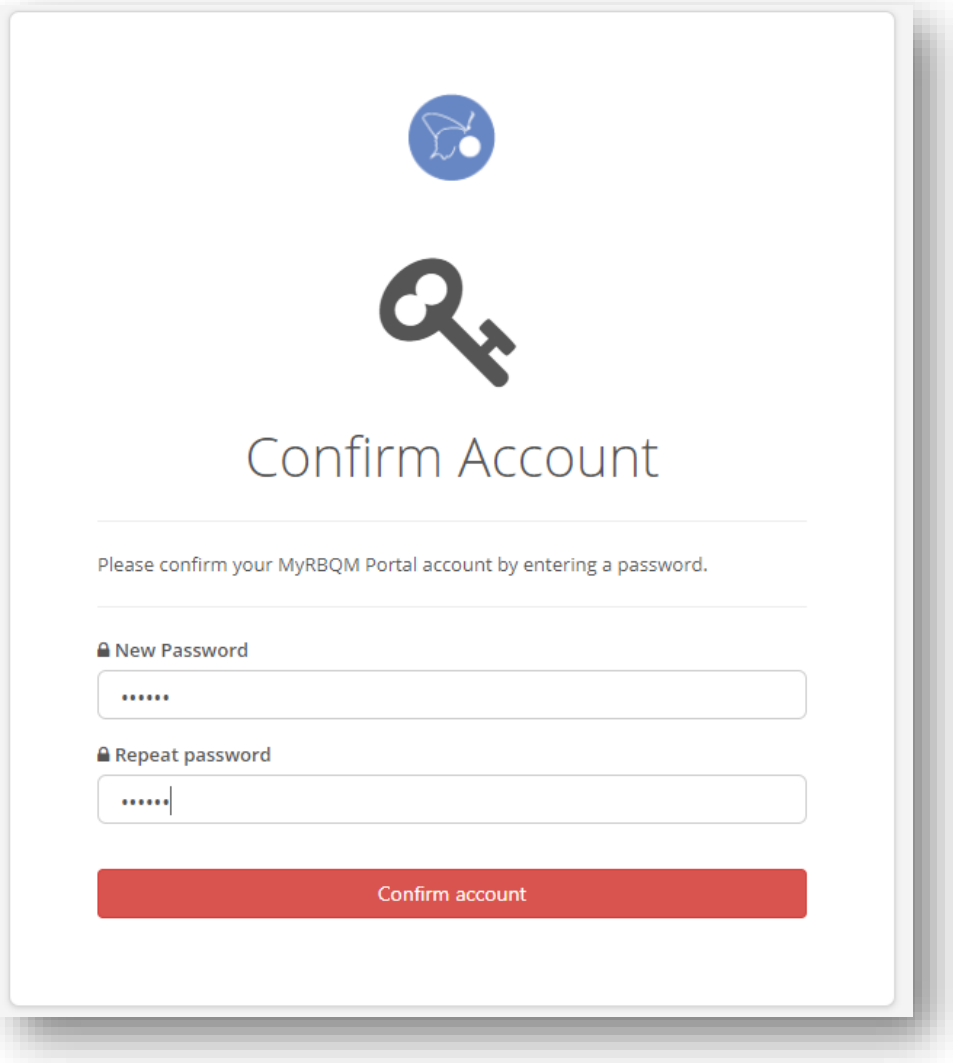
We are happy to answer all your questions.

Sincerely,
Your MyRBQM Portal support team.

NOTE: If you cannot find an invitation, check your SPAM folder.

1. Click the provided link or copy & paste it into a browser.
2. Confirm your invitation by entering your new password and repeating it.

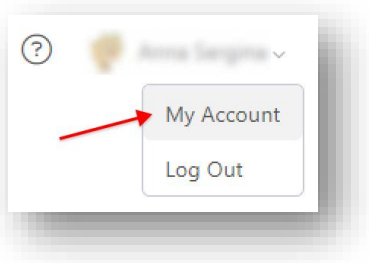
3. Click **Confirm account**.



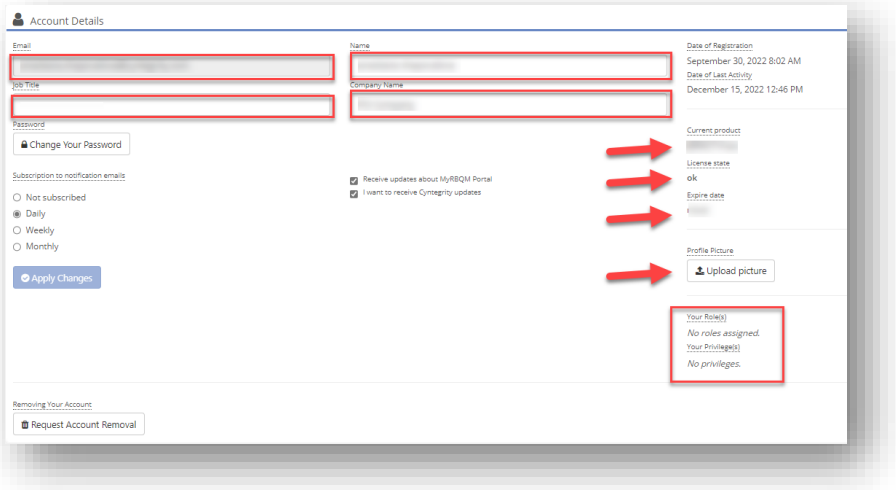
Manage Your Account

To manage your **MyRBQM® Portal** account:

1. Click your **Username** in the upper right corner and choose **My Account**.



2. The **Account Details** show your registered email address (this cannot be changed), date of registration, date of last activity, the current product, license state, and expiry date.
3. To complete your account details, enter your **Name** (display name), **Job Title**, **Company Name**, **Roles** and **Privileges, select a subscription to notification emails frequency and if you want to receive updates from Cyntegrity**.



4. If you like, upload a profile picture to your account:
   A. Click **Upload picture**.
   B. Click **Choose File**, select the desired picture and confirm by clicking **Open**.
   C. If required, zoom the image using the slider beneath the picture until satisfied and confirm by clicking **Upload Image** (the circle confines the visible part of the picture).
   D. Confirm all changes by clicking **Apply Changes**.

Change Your Password

To change the password of your account (if SSO is not configured for your company):

1. Click the **Account Symbol** in the upper right corner and choose **My Account**.

2. Click **Change Your Password**.
3. Enter your new password into the field **Password** and repeat in the field **Repeat Password**.
4. Confirm the password change (and all other changes made along with it) by clicking **Apply Changes**.

NOTE: The password should contain a minimum of 11 characters/symbols.

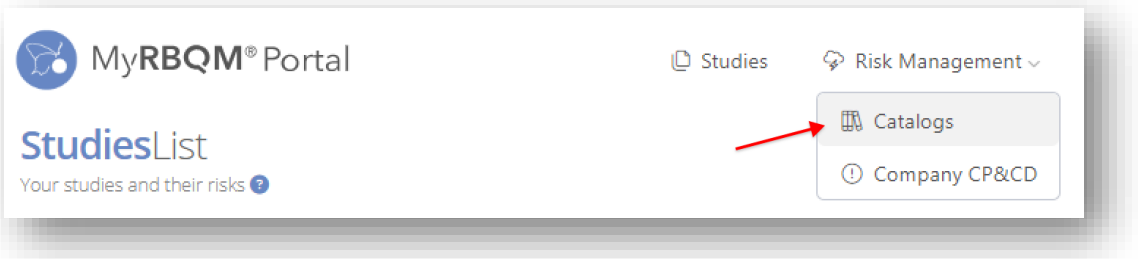
Catalogs and Questions for Risk Assessment

The **MyRBQM® Portal** can support many catalogs with risk assessment questions. Each catalog provides risk assessment guidelines (impact, probability, and detectability of a risk) for a set of risk categories by defining risks through questions for each category. New users of **MyRBQM® Portal** have some predefined catalogs, however, users of @RACT and @RACT-PRO (depending on license type) have access to a few standard catalogs. Most studies will need individual catalogs that you need to create.

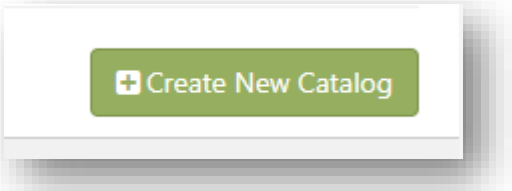
Create a New Catalog

To create a new specialized catalog:

1. Go to **Risk Management** → **Catalogs** in the menu bar.



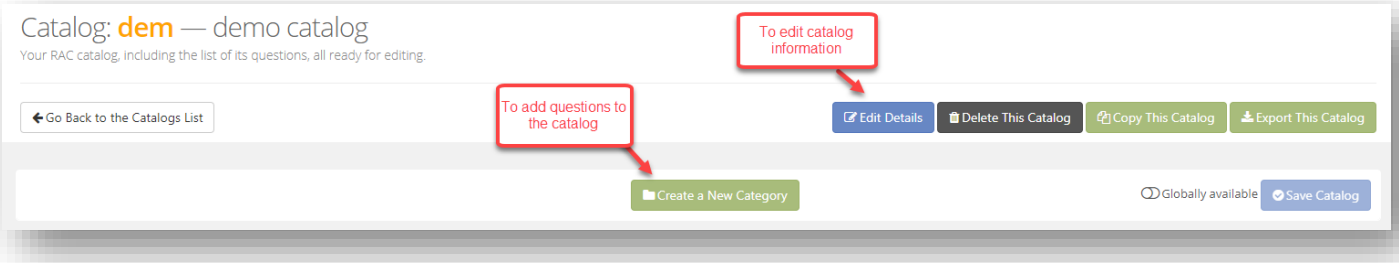
2. Click **Create New Catalog**.

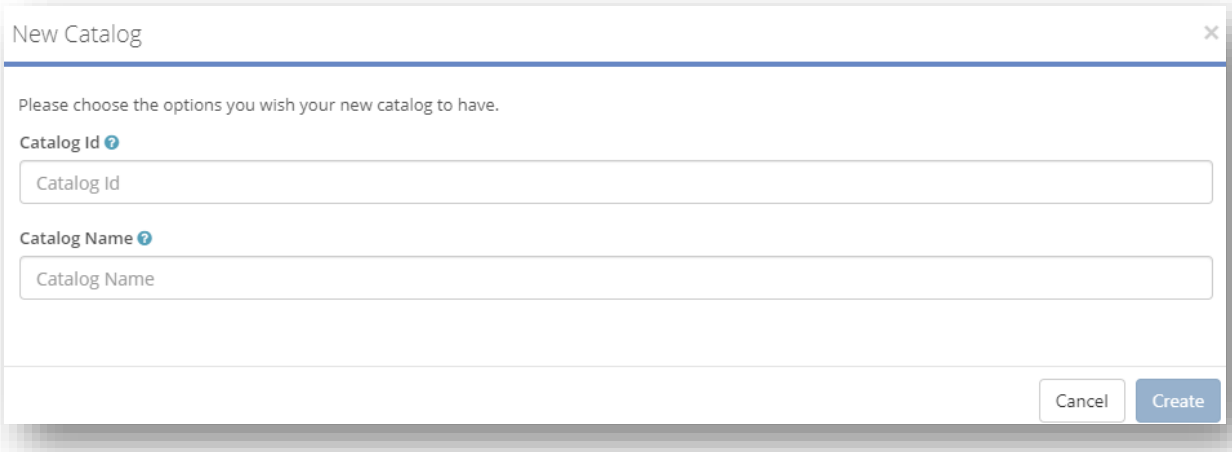


3. Enter a unique **Catalog Id** and **Catalog Name** and confirm by clicking on **Create**.

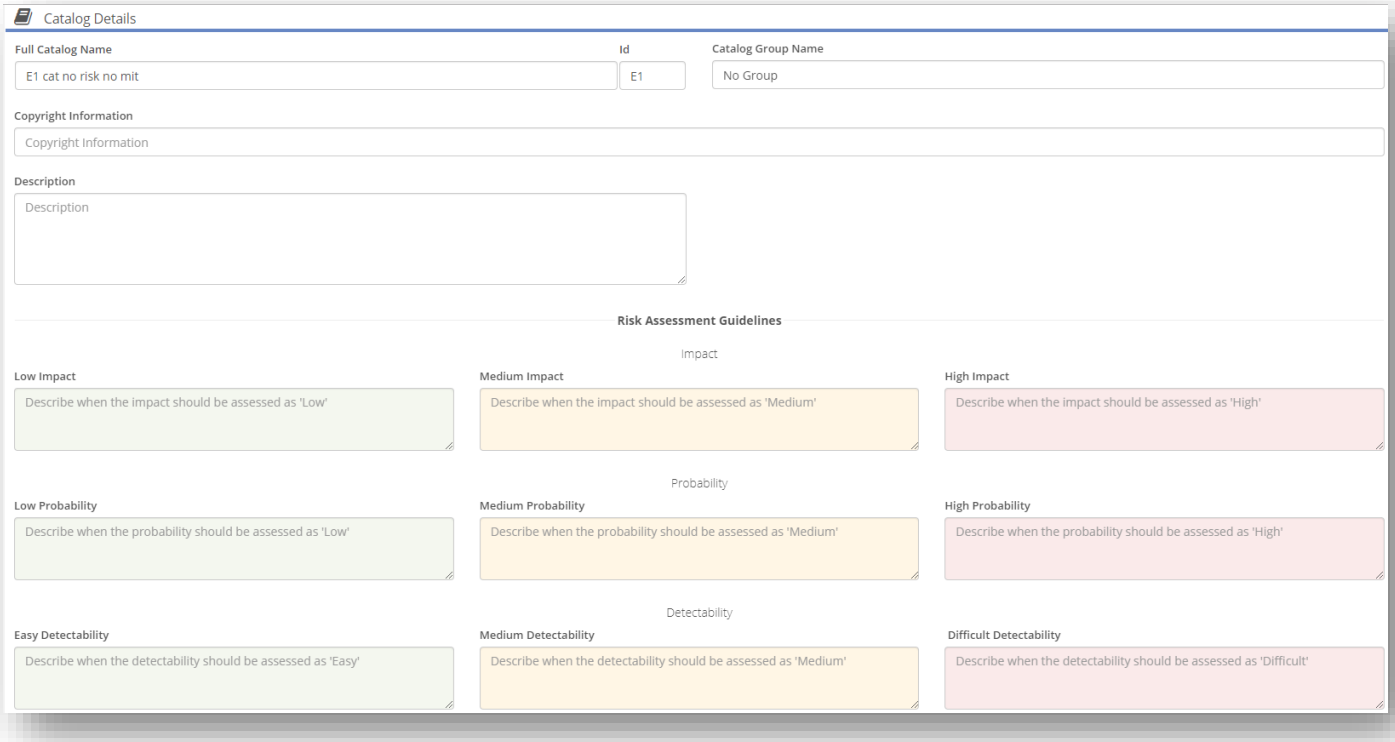
NOTE: The system will only accept unique Ids and names that do not duplicate already existing ones to ensure an unambiguous correlation of Ids, names, and internal system data.

4. Optional: Fill in the **Catalog Details**, such as **Copyright Information** and a **Description**. With the field **Catalog Group Name**, the new catalog can be assigned to a catalog group for a hierarchy in the **Catalogs List**.





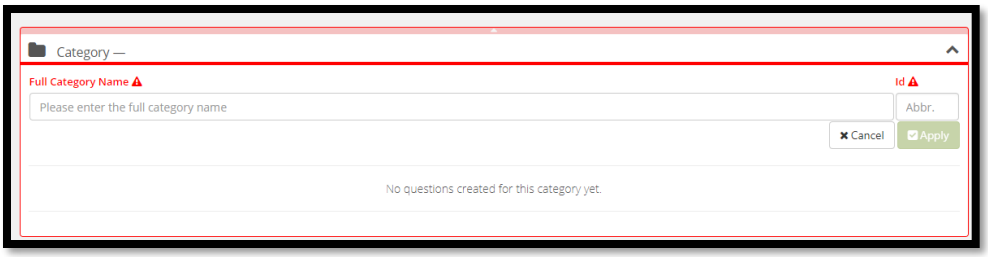
Fill in the **Risk Assessment Guidelines**, which are shown as tooltips near the risk assessment area.



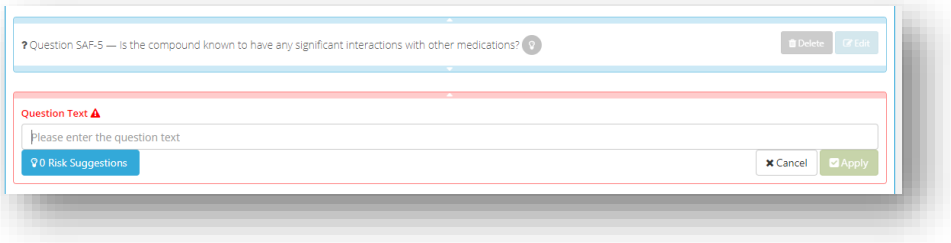
NOTE: Filling in the risk assessment guidelines is optional, however, thoroughly entered guidelines help to ensure that the risk assessment is objective.

5. Create a new **Category** for your catalog. An abbreviation will be generated automatically, which you can change. Categories contain one or more questions that describe risks.

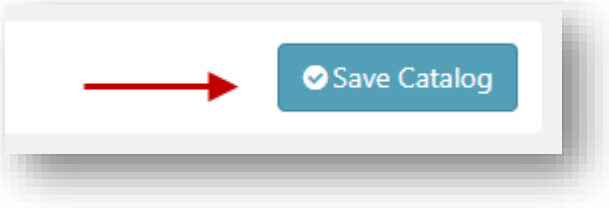
Important: The category name and the abbrev. must stay unique. The system will not allow you to save the category or catalog without all data points being unique.



6. Add a new Question to your catalog:



7. When all categories and questions are entered, click Save **Catalog**:



Edit an Existing Catalog

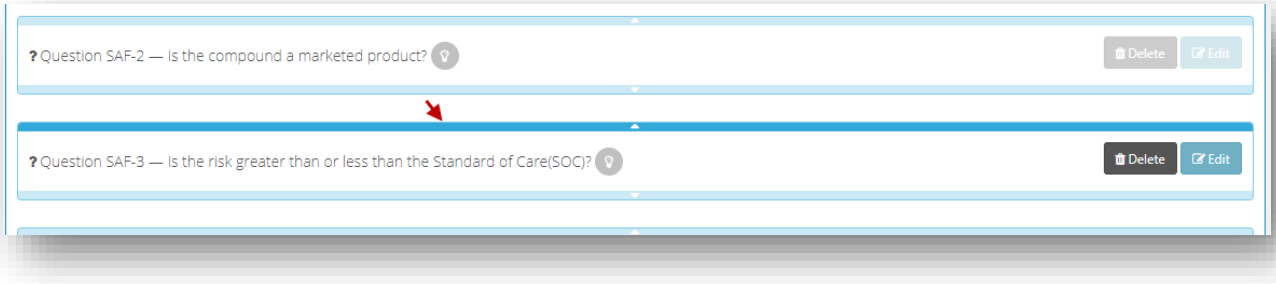
The edit mode of an existing catalog is required for adding or changing any questions in it.

NOTE: Questions in already existing studies will not be affected by editing the affiliated catalog. Only newly created studies that use the edited catalog will include updated questions!

To edit an existing catalog:

1. Go to **Risk Management** → **Catalogs** in the menu bar.

2. Choose an existing catalog from the **Catalogs List** and click **Edit**.
3. Perform the desired changes.
4. Add new categories and/or questions if desired.
5. To change the order of the questions/categories, click the slim bar (arrow) above or below a question/category.



Copy an Existing Catalog

Catalogs do not need to be created from scratch. You can copy and then edit a catalog with a similar configuration to the one you want.

To copy an existing catalog:

1. Go to **Risk Management** → **Catalogs** in the menu bar.
2. Choose a catalog from the **Catalogs List** and click **Edit**.
3. Click **Copy This Catalog** in the header of the **Catalog Details**.

4. Confirm by clicking **Copy**.
5. Enter a unique **Catalog Id** and **Catalog Name** for the copied catalog (which is regarded as a new catalog).
6. Now that the catalog has been copied, the new catalog can be edited.

Export / Import a Catalog

Catalogs in **MyRBQM® Portal** can be exported or imported in the .json-file format. Exported catalogs are only intended for sharing to different Cyntegrity systems or users by importing; they are not intended to be opened outside of **MyRBQM® Portal**.

To export a catalog:

1. Go to **Catalogs** in the menu bar.
2. Choose a catalog from the **Catalogs List** and click **Edit**.
3. Click **Export This Catalog** in the header of the **Catalog Details**.
4. Confirm by clicking **Export**.
5. You can find the exported catalog in your configured download destination folder (browser setting).

To import a catalog:

1. Go to **Catalogs** in the menu bar.
2. Click **Import Catalog** in the header of the **Catalogs List**.

3. Choose the desired catalog from the explorer and confirm with **Open**.
4. Enter a unique **Catalog Id** and **Catalog Name** for the imported catalog and confirm with **Create**.
5. The imported catalog is now listed in your **Catalogs List** and can be edited.

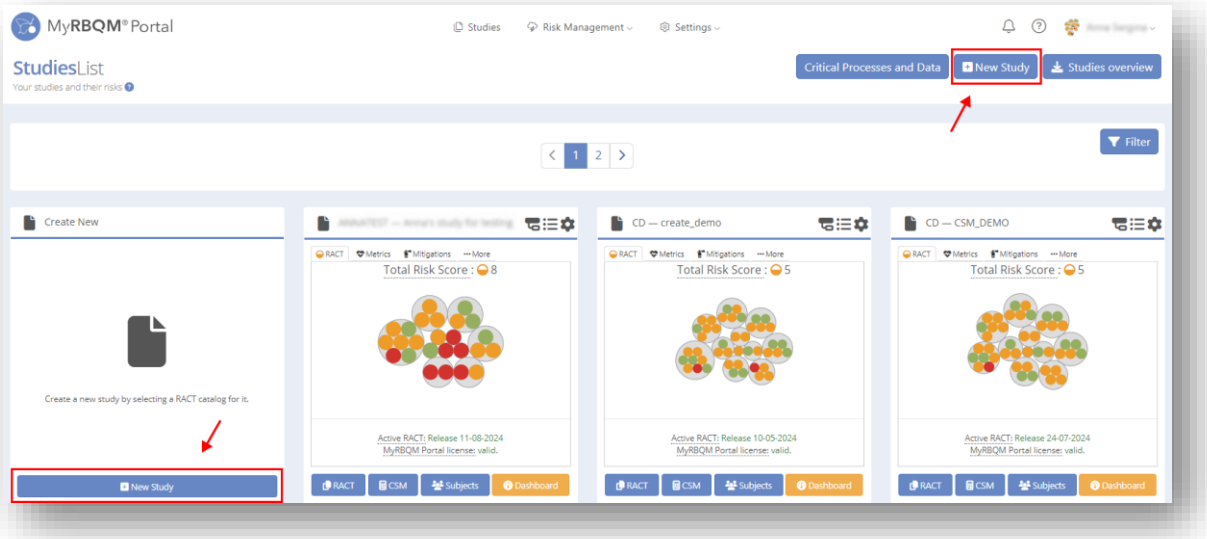
Study Management in MyRBQM® Portal

MyRBQM® Portal helps you to manage your RBM issues for all your studies. As a new user, you will either need to be assigned to studies or create your own.

Create a Study

To create a new study:

1. Go to **Studies** in the menu bar.
2. Click either on **New Study** in the Studies bar or on the StudiesList section (either option will bring you to the **Study Wizard**).



3. Enter a unique **Study Name** and **Study Id** (both are required).

NOTE: These symbols can't be used in Study name and Study ID: <, >, ,, &

4. Select a **Catalog** for your study.
5. Optionally select the **Study Type**.

NOTE: Only one catalog per study can be selected. Catalogs must be created before they can be used for a study or imported.

Cyntegrity offers commercially available catalogs tailored for specific indications.

6. Confirm by clicking on **Create Study**.

The next step is to set up risk scores with @RACT. You are automatically brought here after creating a study (if you have imported RACT from other studies, please follow instructions from the Export and Import of RACT chapter below). However, you do not have to set up risk scores now. There are multiple ways to leave @RACT and return later. Clicking **Go Back to Version Overview** or **Risk Management → RACT** in the menu bar will bring you to the **RiskManagementOverview** of the study. Clicking **a blue circled arrow-up** icon in the menu bar brings you back to the **StudiesList**.

You can come back any time and set up the risk scores. To complete the risk scores:

1. Go to **Studies** in the menu bar.
2. Click **RACT** on your study tile.

Set Up Risk Scores

To set up risk scores for your study in @RACT:

1. Navigate through the risk categories in the **RiskManagementOverview wizard** at the top of the page, or by clicking on **Next Category**/**Previous Category** at the bottom of the page.
2. Enter **event**, **cause**, and **impact** for each question and define the values for **Impact**, **Probability**, and **Detectability** of a risk (low, medium, high).

NOTE: Navigate through the questions by using the Question Summary in the wizard mode, the Next open question button, the Search bar, and the Answered, Unanswered, and Disabled buttons.

3. If required, new risks to each question can be added by clicking **Add another risk** and deleted by clicking **Delete this risk**.

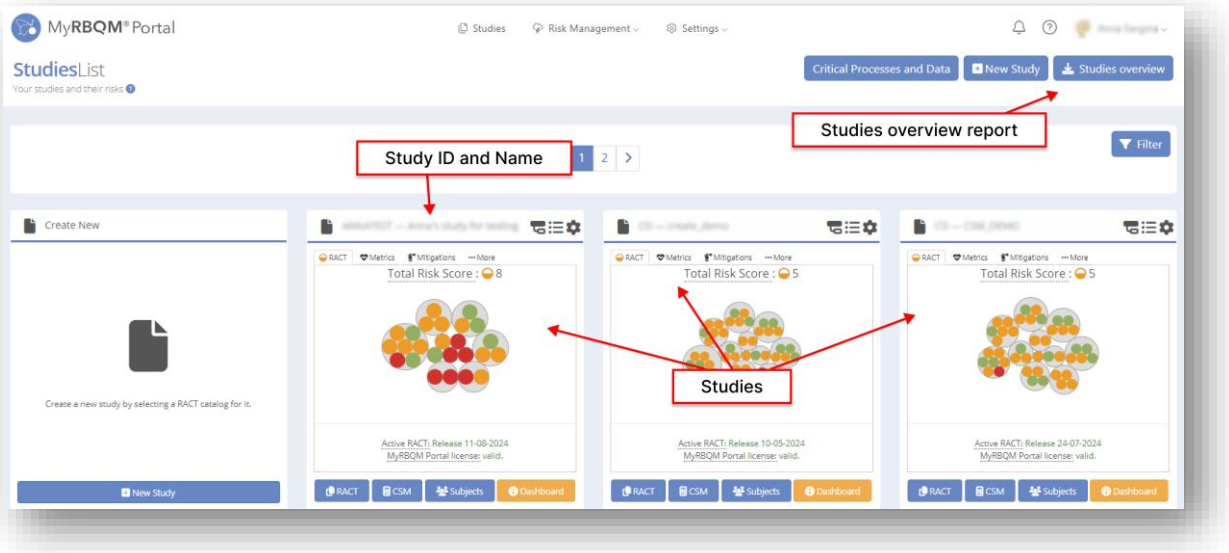
NOTE: To avoid adding risk data to the knowledge base upon successful release of a draft, deactivate the switch Add this Risk's data to the Knowledge Base (activated by default).

NOTE: Questions can be disabled by clicking on Disable Question. Disabling a question inactivates it for all internal processes but does not delete it. If needed later, a disabled question can be enabled again by clicking on Enable Question.

4. When everything has been filled in, Release the draft by clicking on **Release Draft**.

Study Overview

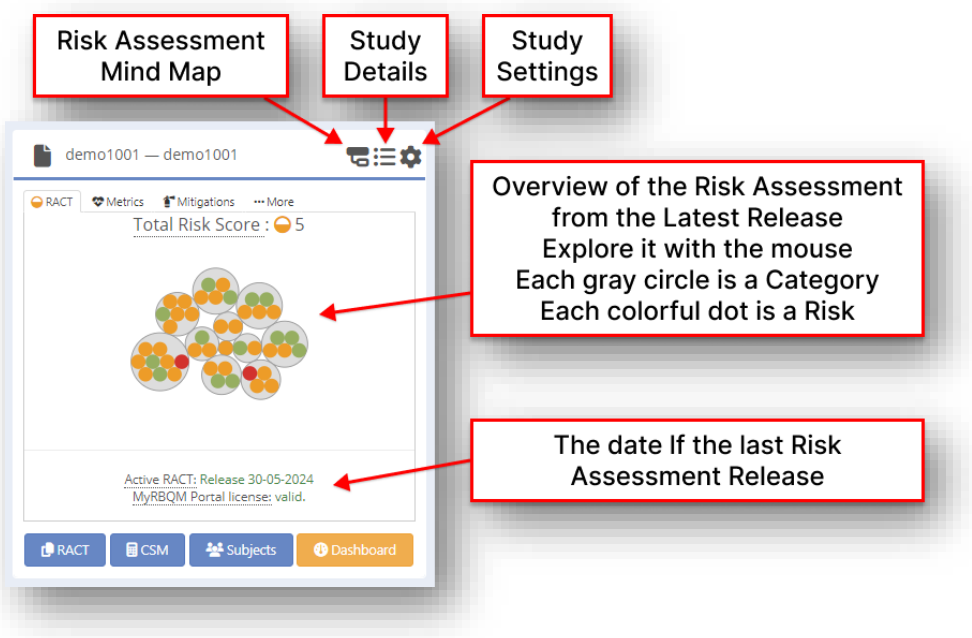
StudiesList in MyRBQM® Portal can be accessed in the menu bar via **Studies** outside of a study context or via **a blue circled arrow-up icon** inside a study.



Apart from the information about the company's studies presented on the **StudiesList** page, there is a studies overview report available for download via **Studies**

overview button on top of the page. It contains detailed information about each study, such as study status, key dates, the use of Subject Profile, data upload, and information about RACT, etc.

Some of the studies already have a released risk assessment, depicted by the colorful bubble graph in the center of a **Study Overview Tile** (presentation may vary depending on the system configuration). Cyntegrity calls this bubble graph **"The Risk Flower"**.



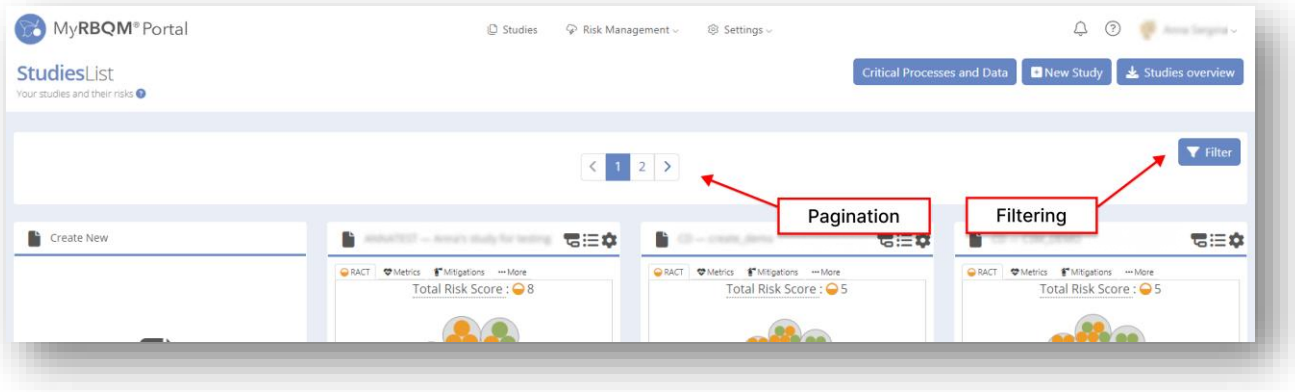
The **Study Overview Tile** provides a lot of information about a running study at a glance. Besides the title of the

study, it presents the most recent release of the risk assessment and categorization (RAC) in the **RACT** tab, the most important metrics in the **Metrics** tab, statistics of the mitigation actions in the **Mitigations** tab, and the option for additional actions in the **…More** tab for a study.

Moreover, it depicts risk categories and risks as colorful dots within the Risk Flowers, together with the overall numerical risk score. The date of the latest active RAC and the study status are shown under the Risk Flower. Besides that, there is a tree-view risk assessment interactive visualization. It can be accessed by clicking the **Mind Map** icon next to study's name. It shows the RACT structure, having a study cell in the center of the map, and the following levels coming from it: Risk Categories → Risk Questions → Risk Statements → Mitigation Actions. Disabled questions, accepted risks and closed mitigation actions are colored gray. It is possible to filter the items and download the map.

Study Navigation

For user convenience, filtering and pagination functions are offered in **StudiesList**.



Filtering options:

- Study ID or Name
- Live AND/OR Non-Live Studies
- Active AND/OR Retired Studies

NOTE: Please remember that Retired Studies are available for only 1 month after the retirement date.

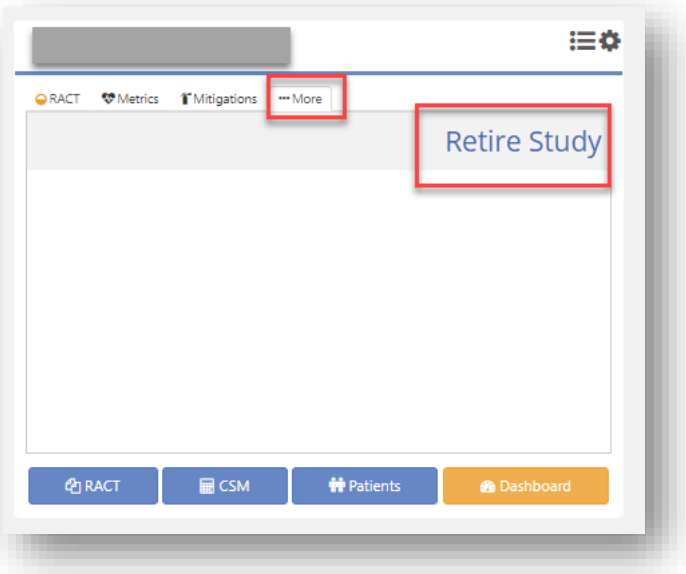
Retire Study

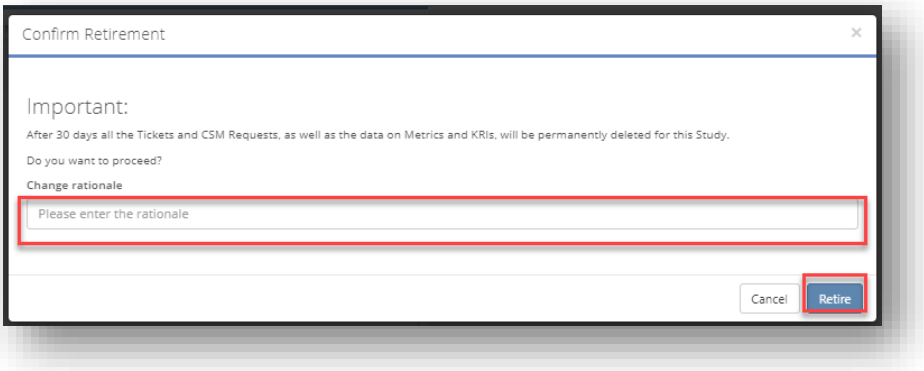
NOTE: Live study can't be retired.

To Retire a Study:

1. Go to **StudiesList**.
2. Select the **Study** to be retired.

3. On the **Study Overview Tile** select **More...**.
4. Select **Retire Study**.
5. Provide **Change Rationale** in a free text area in the pop-up window.
6. Click **Retire** in the popup window.





Retired Study can be shown if the filter is set up to show retired studies.

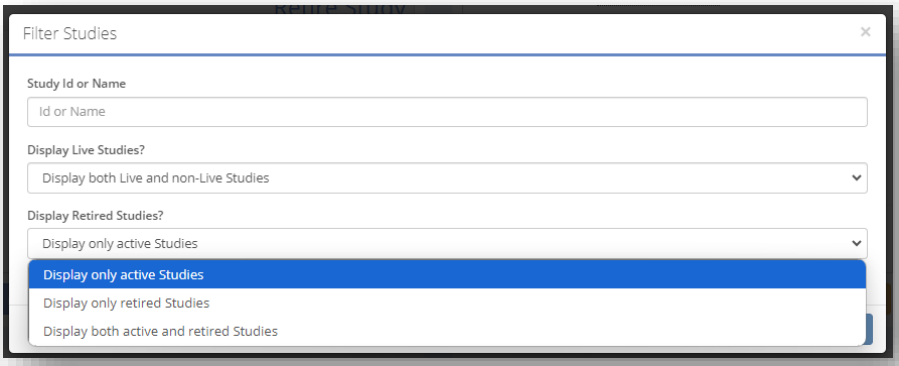
NOTE: An authorized user can see the Retired Study Data in Read-Only mode for 1 month after study retirement.

Unretire Study

MyRBQM® Portal users can **unretire** a study.

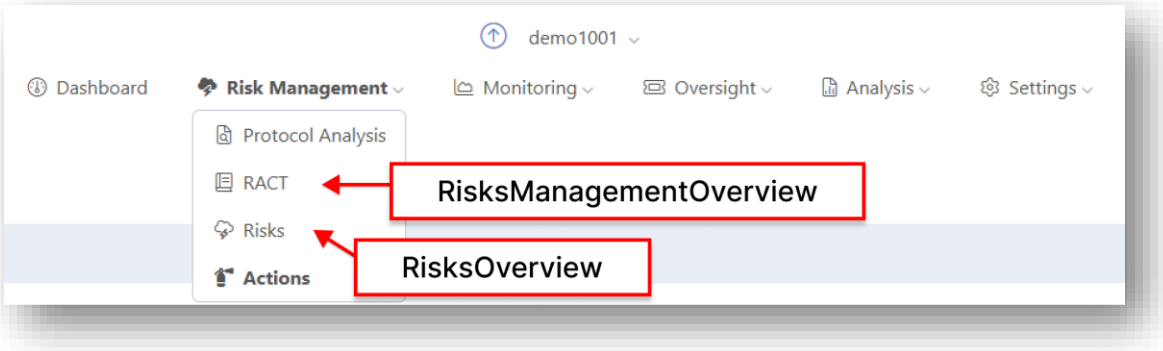
To Unretire a study:

1. Go to **Filter** and filter for **Retired Studies**.
2. Find the Study you want to unretire (it is also possible to set the **Study ID or name** in the Filter).
3. On the **Study Overview Tile**, click **Unretire**.
4. Set up the filter to see **Active Studies.**



RACT

The RACT Overview



RACT is an acronym for Risk Assessment Categorization Tool.

The **RiskManagementOverview** contains the Study Details, the Risk Flower of the study, information about all released versions of the RAC, the Risks Overview of the study, which summarizes all study risks, their events, causes and effects, and their risk scores, and the Questions Overview, which summarizes all risk categories and questions defining risks for the study.

Detailed information about the risk assessment and categorization (RAC) of a study are given in the **RiskOverview**.

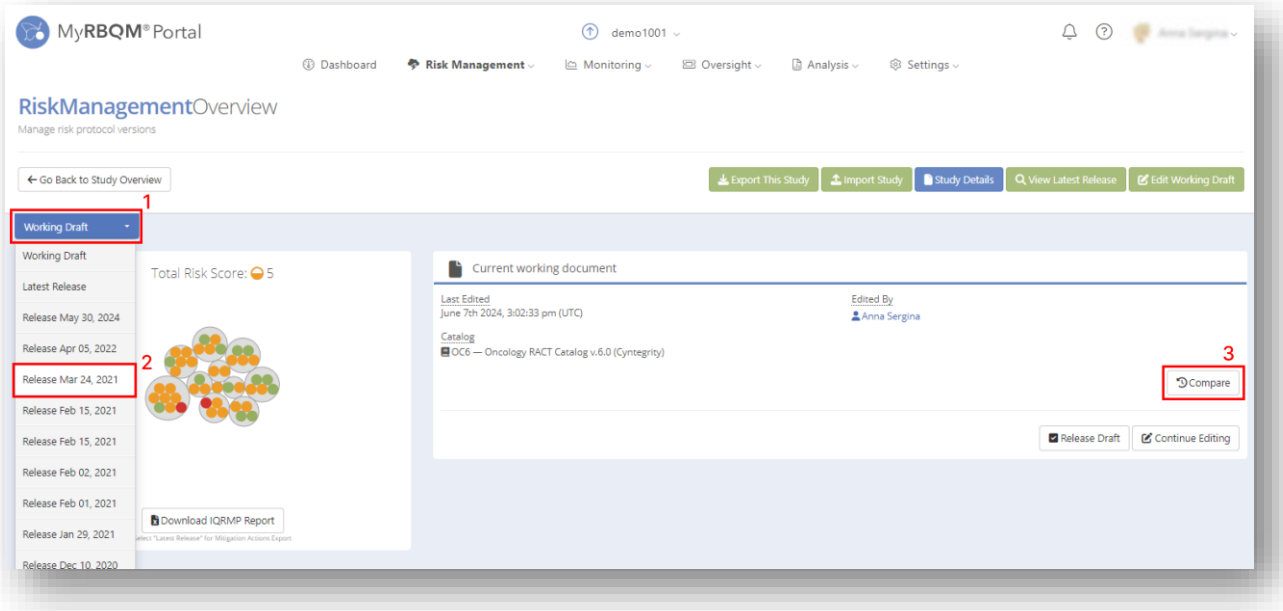
The Release Overview

The latest working draft and all previously released versions of a study are saved by **MyRBQM® Portal** and can be reviewed at any time. Clicking on **Working Draft** and selecting the desired version from the drop-down menu immediately takes you to the desired version of the study. Releases are named with "Release" followed by the release date; the latest release and the working draft do not have a date in their name. The latest release can also be viewed by clicking on **View Latest Release**.

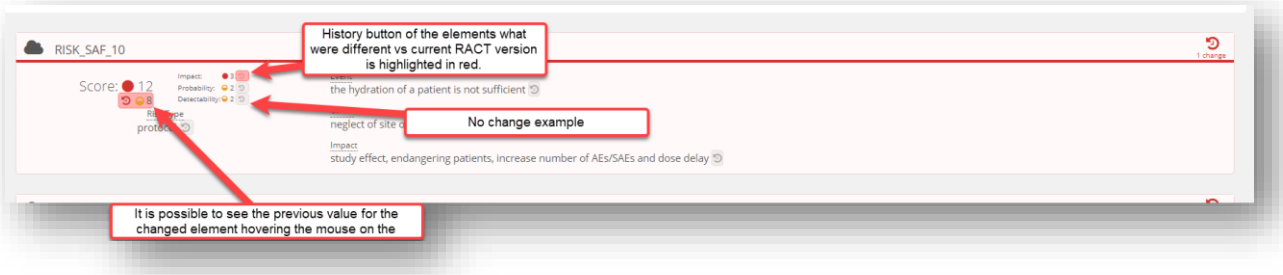
Compare a Working Draft to a Release

Every release version of a study can be compared to the working draft. To compare them:

1. Click **Working Draft** and select the desired release version.
2. Click **Compare** in the current working document.



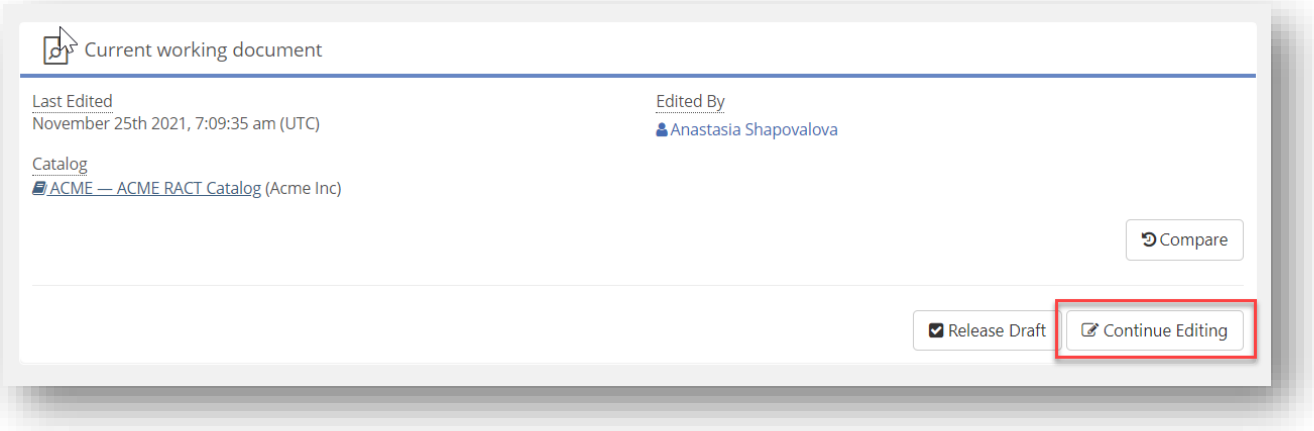
The current working document is extended by information about the compared release version, including the number of edits incorporated in the working draft since the compared release. Detailed information about the changes made can be viewed by scrolling down to the **Risks Overview** and **Questions Overview**. All changes are marked red.



Enhance RACT

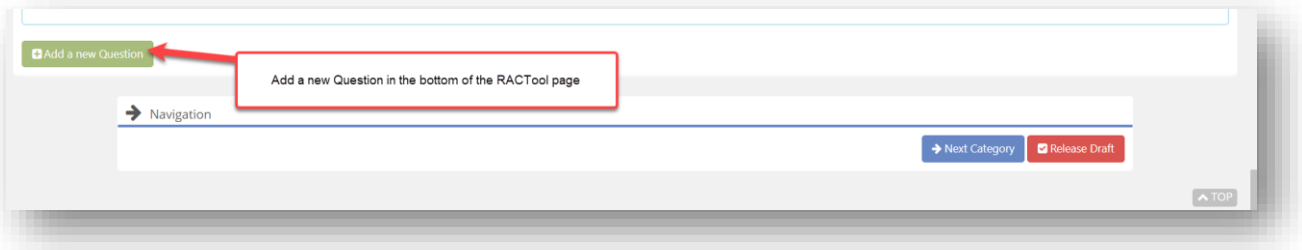
It is possible to edit the RACT of an already created study.

- Category Name
- Question Header and/or text
- Add a New Question
- Add a New Category

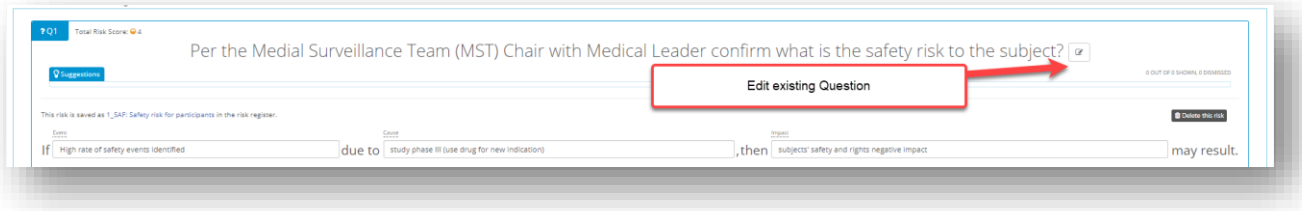


To edit Category Name AND/OR add a New Category:

To add a New Question to the Category:



To edit existing Question in the Category:



Export and Import of RACT

Users can export a selected study RACT to a file and import the file into another study.

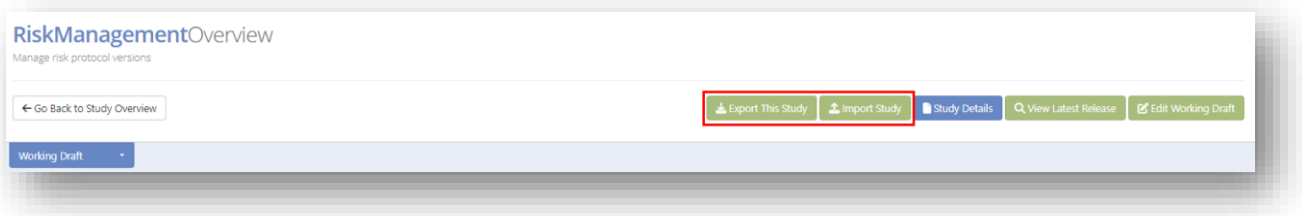
To Export RACT:

1. Go to **StudiesList.**
2. Choose a study with a risk assessment.
3. Complete the risk assessment and release it.
4. Go to **RACT**.
5. Click **Export This Study** in the header of the RiskManagementOverview.
6. Confirm by clicking **Export** in the dialogue box.

You can find the exported RACT in your configured download destination folder (browser setting).

To Import RACT**:**

1. Go to **StudiesList**.
2. Create a new study with any catalog.
3. Go to the **RACT** page.
4. Click **Import Study** in the header of the RiskManagementOverview.
5. Choose the study that you have exported from the explorer and confirm with **Open.**
6. Stay on the RisksOverview page and check if all actions match the original study which was imported.



Edit an Existing Study

The working draft of a study can be edited until its release. To edit the working draft:

- Click **Edit Working Draft**.

OR:

- Click **Continue Editing** in the Document Information Window, after having selected Working Draft from the Release Overview.

All properties of the risks of the study can be changed and completed as described in the chapter **Set Up Risk Scores** and confirmed by clicking **Release Draft**. All changes will then be applied in the latest release of the study. A draft can also be released by clicking **Release Draft** in the Document Information Window.

By default, the system requires a separate rationale when disabling a question, accepting a risk, and one general rationale when releasing a RACT Working Draft. However, it is also possible to configure the system to require a rationale for any saved change in a RACT Working Draft. This can be enabled in: **Company Settings** → **Company Management** → **RACT Customization**, by ticking the checkbox Ask for a rationale for any saved change in RACT Working Draft. All saved rationales for changes can be tracked at any time in the Study Audit.

NOTE: Drafts can also be released without any prior changes to the latest version.

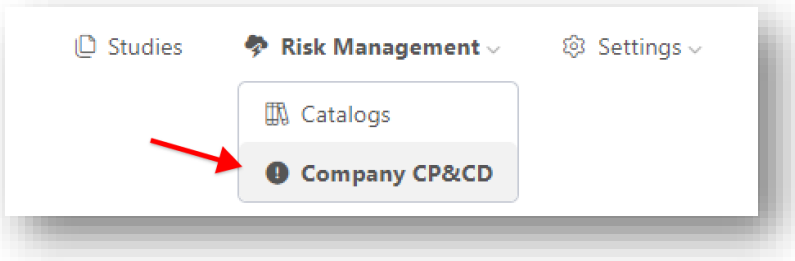
NOTE: Every released draft of the same day will be named with the same name. Thus, it can happen that more than one version with the same name occurs in the Release Overview.

Critical Processes and Data

In a risk assessment, not every process and data point are similarly important for defining a risk. Some processes and data points are critical for elevating a risk score, while others may be insignificant, or even detached. To conduct successful risk management, it is important to be aware of, define, and give these critical processes extra attention. In **MyRBQM® Portal,** it is easy to manage the critical processes and data of your studies.

Manage Critical Processes and Data

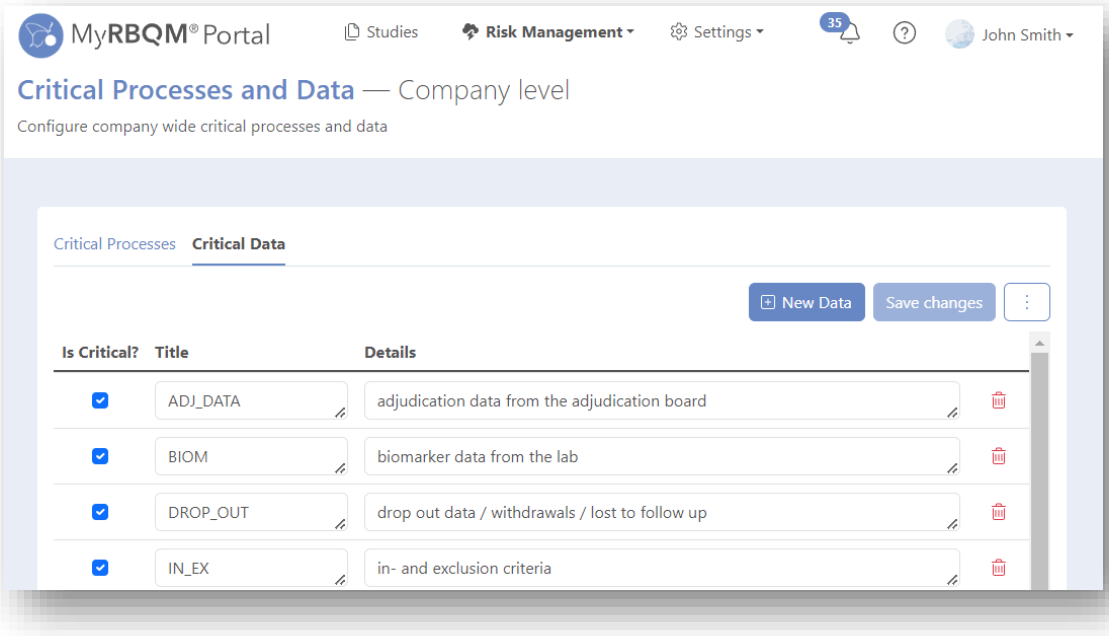
Critical Processes and Data in the MyRBQM® Portal are presented at two levels: Company and Study. To manage your critical processes and data on company level go to **Risk Management** → **Company CP&CD** in the menu bar.



To manage your critical processes and data on study level navigate to the **relevant study** and select **Risk Management** → **Study CP&CD** in the menu bar.

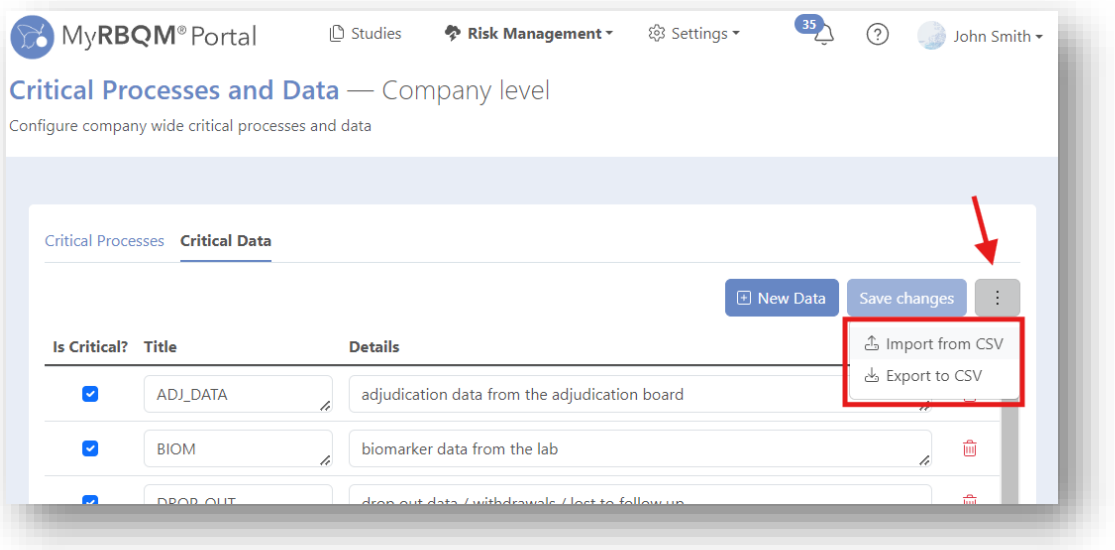
When creating a study, critical processes and data are automatically imported from the Company level. As a result, company-defined critical processes and data are available from the outset and do not need to be redefined for each study.

To create a new critical data or process click New Process or New Data and enter a Title and Details for each new entry. To delete an entry, click the **Trash bin** icon in the end of the row. If a data point is critical, activate the **Check Mark** on the left side beside it. Don't forget to **save changes** separately in each tab.



Import/Export Critical Processes and Data

Defined critical processes and data can be exported and imported from .csv-format (Microsoft Excel Comma-Separated Values file).



The **Export** and **Import** options are available via the three-dot menu.

To export, select **Export to CSV**

To import, select **Import from CSV**, then choose a file that follows the required table structure:

- .csv format with a semicolon delimiter
- Column headers must match system fields
- Mandatory fields (Label/Title) must not be empty and must be unique (separately for CP and CD)

The exported file can be used as a template for import.

NOTE: Imported CPs or CDs **fully replace** any existing ones.

IQRMP Report

MyRBQM® Portal documents all RAC data of a study. The latest data summary can be exported as an excel file.

Download an Excel IQRMP Report

To download a report for your study in Excel format:

1. Go to **StudiesList**.
2. Select the appropriate study.
3. In the **RiskManagementOverview**, click **Download IQRMP Report**.

Open and View Your IQRMP Report

Excel reports are structured in thematic worksheets listing the History, Risk Assessment, Critical processes, Critical data, KRI and QTL.

1. **History Worksheet:**
    - **IQRMP Report** section: study ID and name, an overview of the account details of the user that downloaded the excel report and the version number of the downloaded report.
    - **Release History** section: provides information about the all previous reports version numbers, their release dates, by whom the reports were released and their release notes.

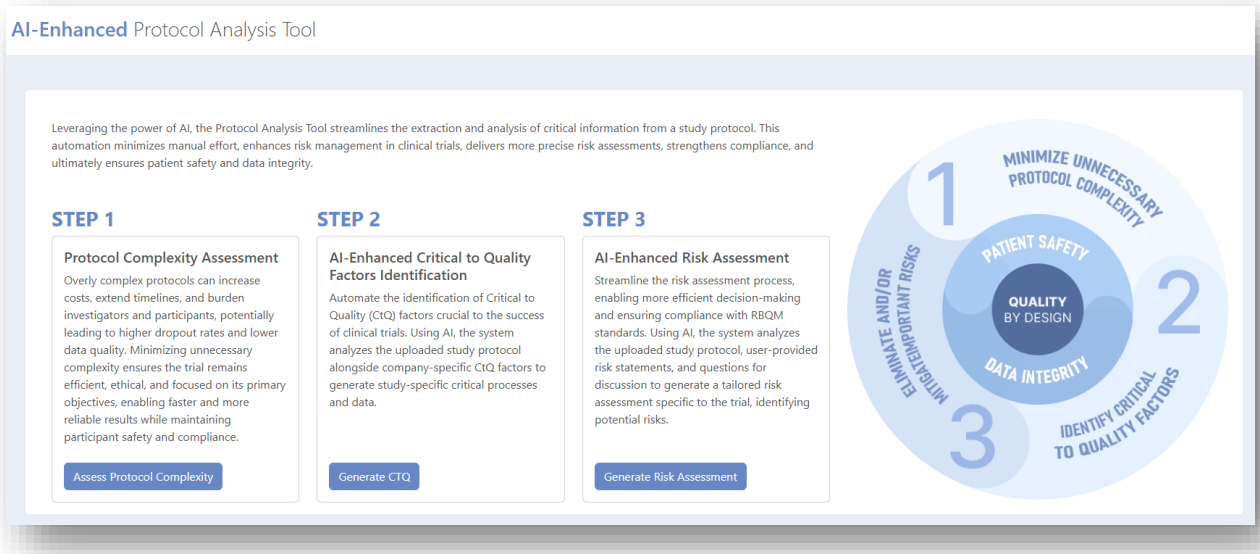
2. **Risk Assessment Worksheet:** detailed information about the RACT version, implemented risk categories, questions, risk assessment guidelines, their risk score, from which the overall risk level is calculated and full information about each mitigation action created.
3. **Critical processes Worksheet:** summarizes all applied critical processes of the study with their names and descriptions.
4. **Critical data Worksheet:** information about the calculated critical data of the study, their labels and descriptions.
5. **KRI and QTL Worksheet:** the list of all the KRI their ID, the brief description of how it is calculated, an associated risk (if any), the actual thresholds (medium, high) for each level (site, study, etc.) along with the mitigation IDs and review timelines associated with KRI.

AI-Enhanced Protocol Analysis Tool

The **Protocol Analysis Tool** is an AI-driven solution designed to enhance the quality and efficiency of clinical trials by automating key aspects of protocol evaluation and early risk detection.

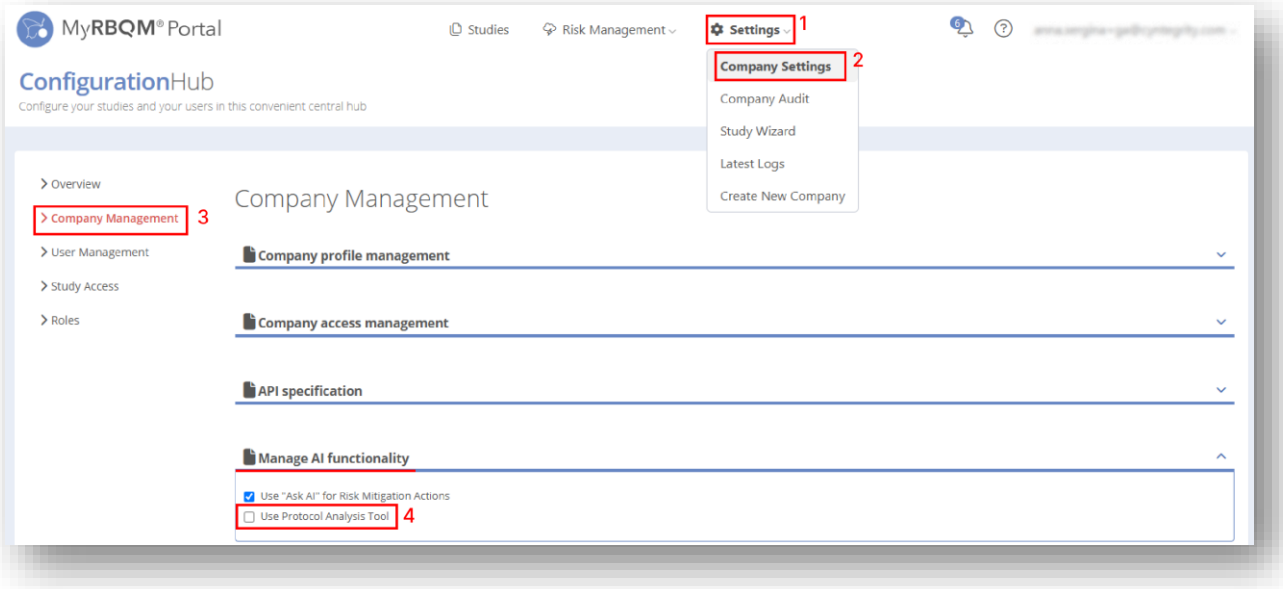
The tool operates in three intelligent steps, where the output of each step serves as the input for the next. This

streamlined automation reduces manual effort, improves risk management, enhances compliance, and ultimately supports patient safety and data integrity.

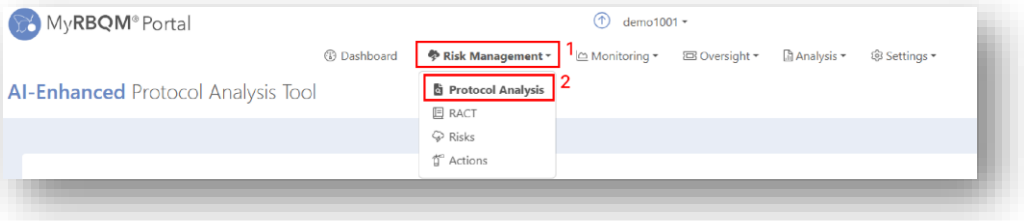


To use the **Protocol Analysis Tool**, it must first be enabled in your **Company Settings** by your Administrator (This functionality is **disabled** in MyRBQM by default).

To enable the Protocol Analysis Tool for those users assigned the privilege navigate to **Company Management** → **Manage AI functionality** and check the box labeled **Use Protocol Analysis Tool** (see below).



Carefully read and accept the terms of use before enabling the Protocol Analysis Tool. Once the Protocol Analysis Tool has been enabled, navigate to the study for which you want to create or enhance the Risk Assessment. Click on the **Risk Management** menu drop-down item: **Protocol Analysis**, as below.



AI-Enhanced Critical to Quality Factors Identification

Identification of Critical to Quality (CtQ) factors is crucial to the success of clinical trials. Generating CtQ with the help of AI is meant to minimize unnecessary complexity, ensure that the trial remains efficient, ethical, and focused on its primary objectives, and enable faster and more reliable results while maintaining participant safety and compliance.

Navigate to the **Protocol Analysis Tool** and click **Generate CtQ**. To identify study-specific Critical to Quality (CtQ) factors, **upload your Study Protocol** in .docx or native (machine-readable) .pdf format and **choose a set of example CP&CD** to support identification between:

- Company CP&CD from MyRBQM (recommended if available)
- Predefined examples provided by the Cyntegrity team

Once the request is processed (usually within a few minutes), the requestor will receive and email with a link to the generated Critical to Quality Factors Report.

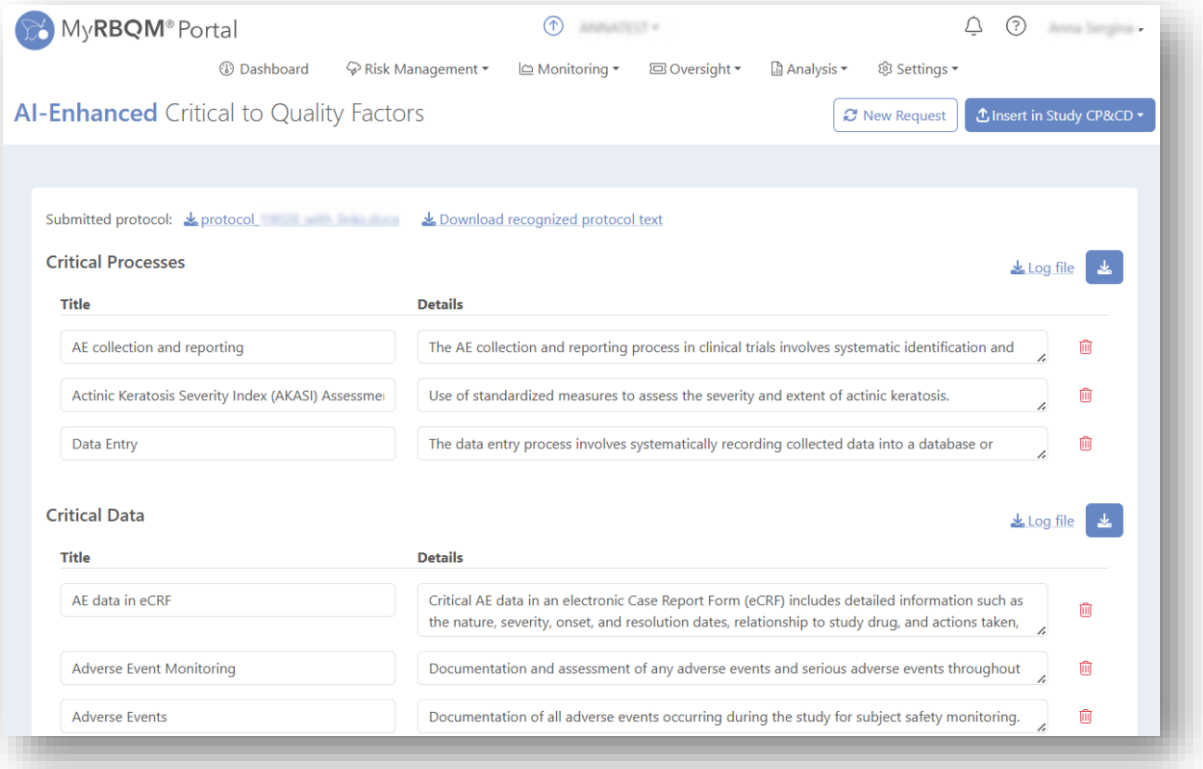
The generated Critical to Quality Factors Report contains a list of Critical Processes and a list of Critical Data. Edit the Title and Detail fields or delete entries (by clicking on its Trash Can icon) as appropriate.

From here you can:

1. Download the finalized CP&CD
2. Insert in MyRBQM Study CP&CD by clicking **Insert in Study CP&CD** (Newly inserted CP&CD will be added to existing ones).
3. Download:
    a. The original Protocol file
    b. The recognized protocol text
    c. The Log file(s)

Start a new request by clicking **New Request**. The CtQ generation process will start from the beginning.

Previously generated (unedited) results are accessible any time via the original email link.



AI-Enhanced Risk Assessment Generation

AI-Enhanced Risk Assessment Generation allows to streamline the risk assessment process, enabling more efficient decision-making and ensuring compliance with RBQM standards.

To generate Risk Assessment with the help of AI navigate to the **Protocol Analysis Tool** and click **Generate Risk Assessment**. There **upload your Study Protocol** in .docx or native (machine-readable) .pdf format.

Similarly to generating CtQ, once the request is processed (usually within a few minutes), the requestor will receive and email with a link to the generated Risk Assessment.

The generated Risk Assessment contains a list of Risk Statements in the "if-due to-then" format. Each Risk Statement has an associated Risk Question and an allocated Risk Category from the TransCelerate Categories List.

You can edit the Risks by:

- Selecting a Risk Category from the drop-down list
- Editing the Risk Question
- Editing the Risk Statement
- Deleting the Risk entirely

When all edits have been made, insert the Risk Assessment into RACT by clicking **Insert in RACT**. (The newly

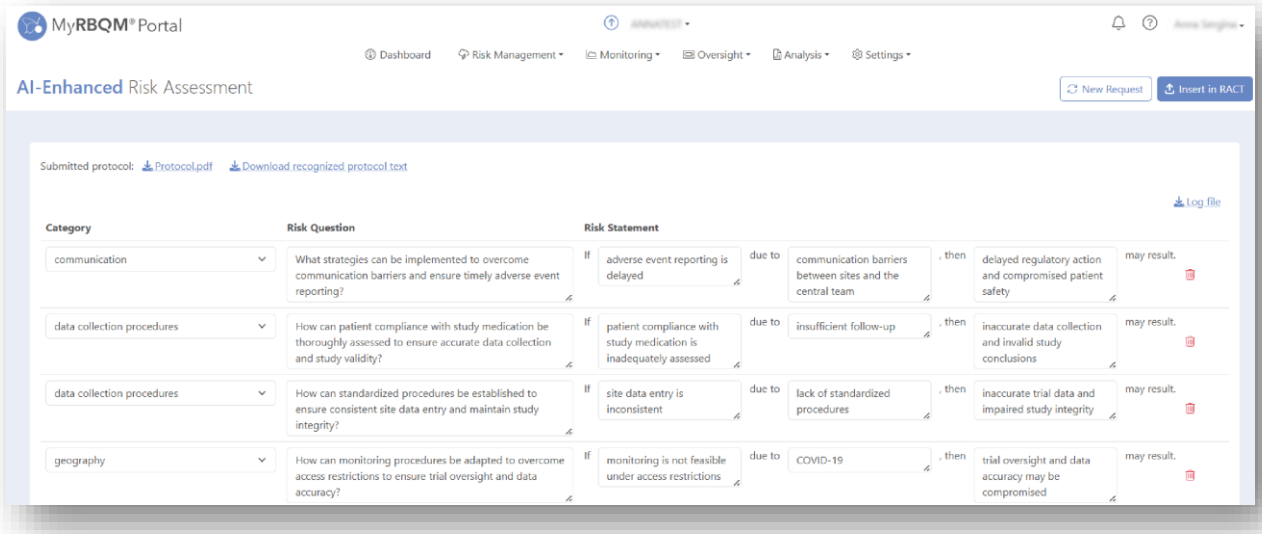
identified risks, risk questions and risk categories will be added to the existing ones in your RACT).

To download:

- The uploaded Protocol file, click **Download [Protocol name]**.
- The recognized protocol text, click **Download Recognized Protocol text**.
- The Log file(s), click **Download Log file**.

To start a new request, click **New Request**. The Risk Assessment generation process will start from the beginning.

Unedited results of any previous request can be accessed using the link in the email.



Risk Assessment & Mitigation Actions

Risk Assessment and Mitigation Actions – Explanation

The **MyRBQM® Portal** contains the integrated risk assessment tool RACT+, which is based on TransCelerate's Risk Assessment and Categorization Tool (RACT).

Team members involved in risk identification should, above all, focus on the identification of risk threats:

- human subject safety
- human subject rights
- critical study processes and
- critical data of the pertinent clinical study
- risks to:
  - quality requirements
  - scope
  - schedule
  - budget
  - team
  - deliverables
  - outcome and
  - IT systems (e. g., communication tools, electronic files, data capture systems)

TransCelerate Biopharma Inc.[i], a non-profit organization comprising the world's leading biopharmaceutical companies, has created an RBM Knowledge Center freely available online. This Knowledge Center includes RACT used mainly for risk identification and evaluation based on the failure mode and effects analysis (FMEA) method[ii].

Although RACT is a sufficient tool for systematically reviewing all clinical study critical aspects for risk evaluation and identification, it has clear drawbacks[iii]. Risk levels are assessed with high subjectivity and in disagreement with other study team members' evaluations. This generates a bias in the risk prioritization process.

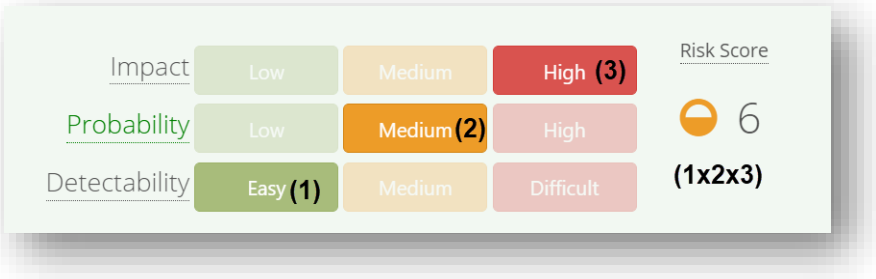
Cyntegrity found the need for a consensus of risk level assignments that RACT was not covering. Thus, Cyntegrity developed RACT+ based on an enhanced version of RACT, featuring objective definitions for low, medium and high-risk levels for each risk concerning three risk attributes:

- The severity of risk **impact** (I)
- The **probability** of risk occurrence (P), and
- Risk **detectability** (D).

RACT+ is a list of questions that facilitate the identification and the qualitative assessment of clinical trial risks, organized in 13 to 15 risk categories (as per TransCelerate's RACT):

- Safety
- Study Phase
- Study Complexity
- Subject Population
- Technology
- Data Collection Procedures
- Study Endpoints
- Organizational Experience
- Imp
- Imp Supply Chain
- Blinding
- Operational Complexity
- Geography.

RACT+ enables the study team to identify risks and to evaluate the severity of risk impact (I), the probability of occurrence (P) and detectability (D) by assigning a score (from 1 to 3, higher scores meaning higher risk) to each of these three attributes. I, P and D scores are multiplied to obtain a single score for each risk, the so-called "Risk Priority Number" (RPN).



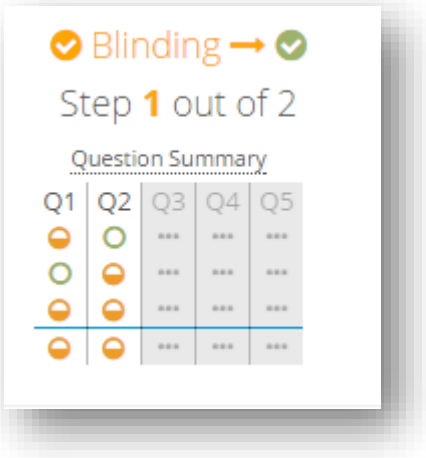
The assigned risk scores allow for single and grouped risk prioritization and the calculation of a total risk score for each clinical study.

RACT+ checks the severity of the risk outcomes, risk occurrence likelihood and the ability to detect the risk timely, following a system more in accordance to the failure mode, effects and criticality analysis (FMECA) method. In comparison with TransCelerate's RACT, RACT+ will be able to inform whether a high-risk level is due to the severity of the risk impact, to a high probability of occurrence or to a combination of both (I and P). This is an extremely relevant assessment that will be documented in @RACT+ for each risk. Additionally, the complementary risk detectability scores enable an evaluation of the feasibility to respond timely to risks.

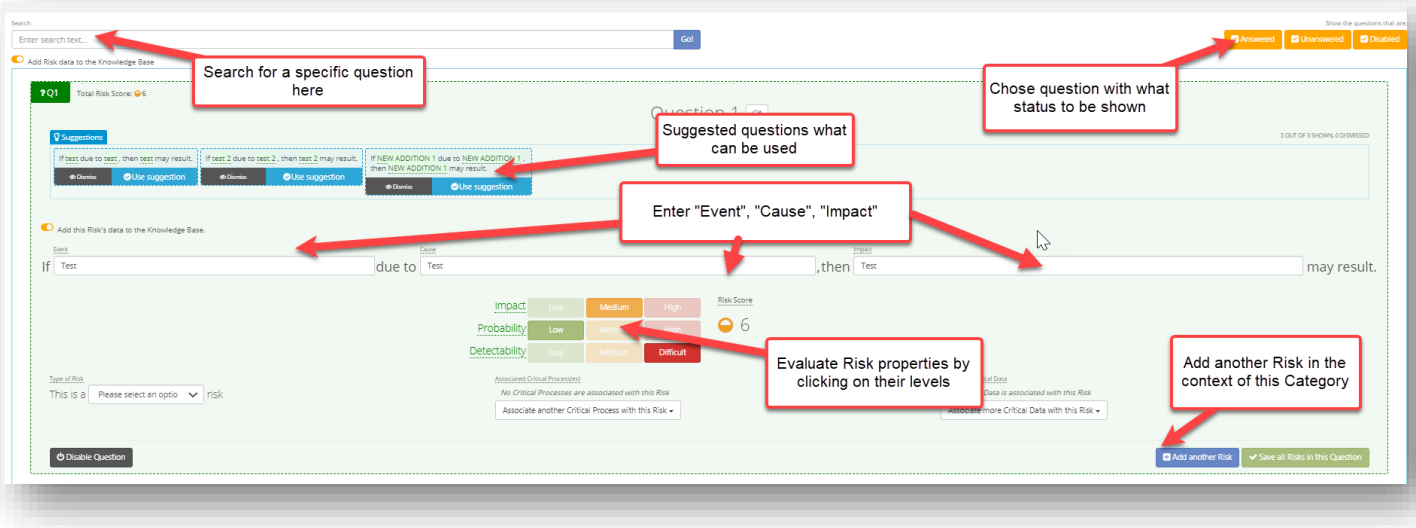
Edit the Risk Assessment

1. When you choose the option **Edit Working Draft** in the **RiskManagementOverview,** you will be taken to the edit mode of the risk evaluation and identification.
2. The first object that meets your eye is the summary of already finished risk assessments. It shows the categories, the evaluated properties of risks (Impact,

Probability, Detectability) and the risk priority number.



3. To identify a risk in **MyRBQM® Portal** you can find the questions from TransCelerate's RACT, which act as a guide for risk identification. The risk itself is identified with three elements – event, cause, and impact:

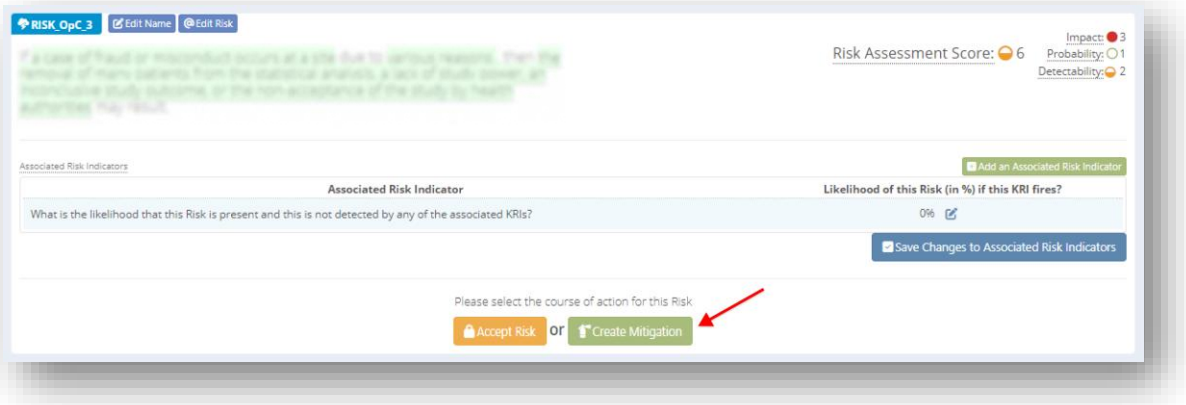


There are different ways to calculate the risk score, however, the most common one (best practice) is to multiply all given properties: *impact * probability * detectability

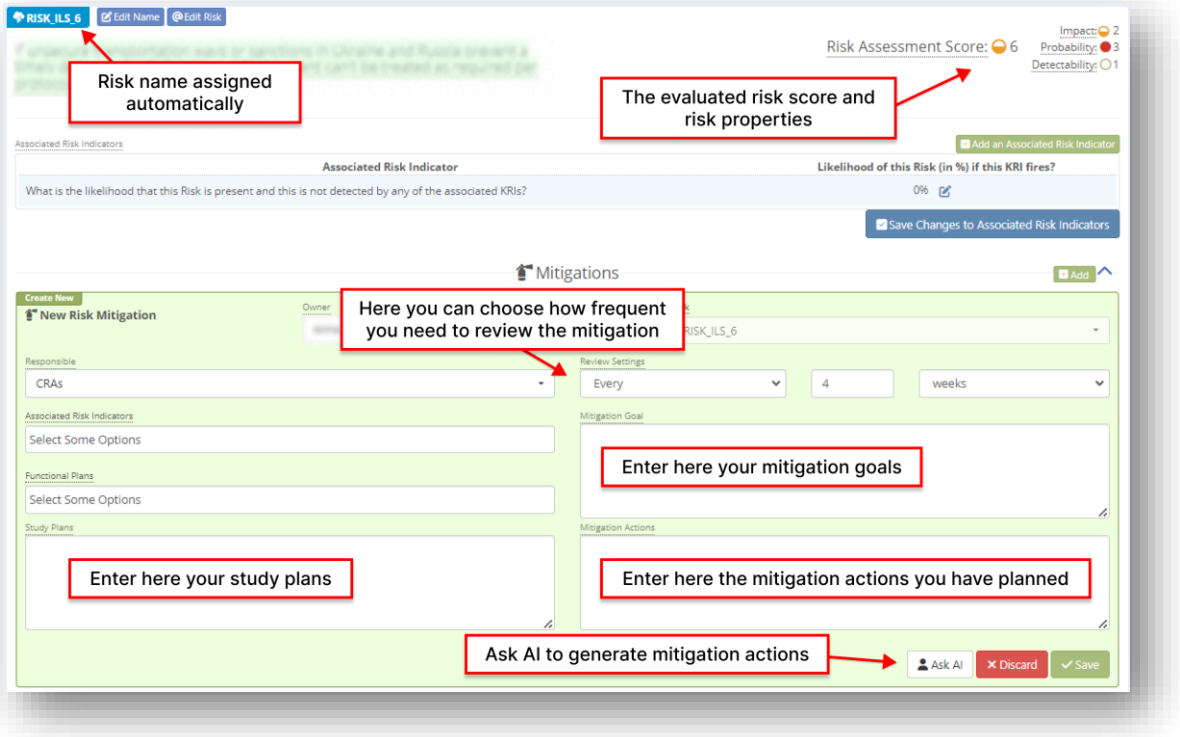
4. After filling in a risk, its properties can be assessed: Probability, Impact, and Detectability. The Risk Score (Risk Priority Number) is automatically calculated.
5. When done with all questions within one category, move to the next one, until the assessment is finished.

Associate the Identified Risks with Mitigation Actions

1. Go to **Risk Management** → **Risks** from the menu bar.
2. Now you can see the risks that you identified and evaluated previously from the latest release.
3. Create mitigation actions for them by clicking **Create Mitigation**. Mitigation actions must reduce the probability, improve detectability, or reduce impact.



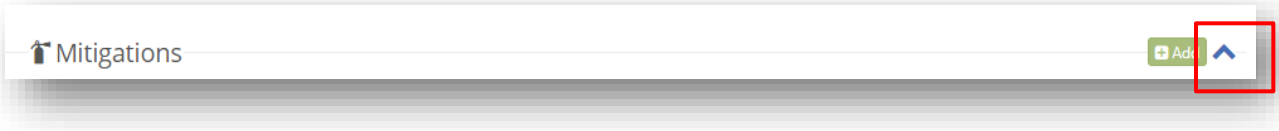
4. Click **Ask AI** to get an **AI-generated mitigation action text suggestion**. Enable this functionality in Company or Study settings to be able to use it.



NOTE: When a Review Setting Once at [Vital Timeline date] is selected, the system will prompt you to choose the Vital Timeline event for reviewing the progress of your action goals. If the selected Vital Timeline date is not defined in the study protocol, the system will immediately notify you. In this case, neither push notifications nor emails will be sent to remind the user to review the progress of the mitigation goals. The same happens if the selected event date is removed from the Vital Timeline.

5. Click **Save** when ready.

6. If required, add additional mitigation actions for the same risk by moving the mouse to the plus sign (+) and clicking **Add**:



Actions List - Manage Risk Mitigation Actions

Risk mitigation actions are listed in the actions list, along with ticket actions (see Actions List - Manage Ticket Actions section).

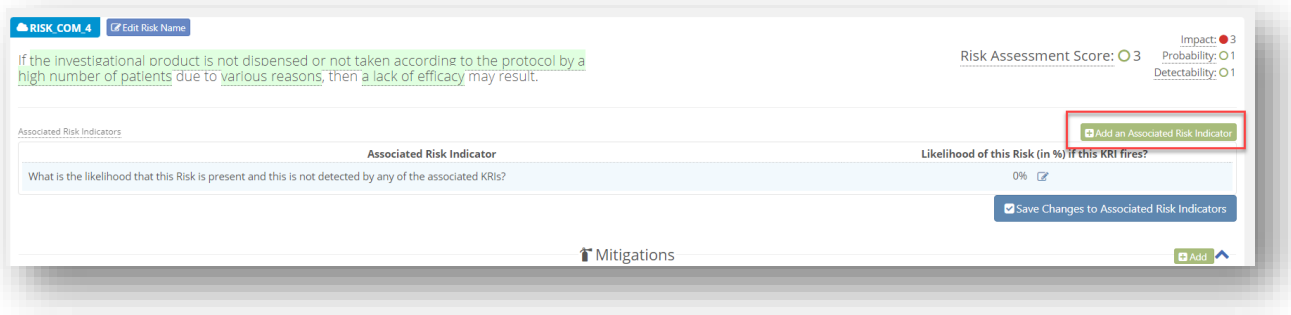
1. Go to **Risk Management** → **Actions** from the menu bar.
2. Investigate the table of available actions. All created risk mitigation actions are listed, together with ticket actions. Risk mitigations are indicated with a special icon and the MA_X, e.g. MA_791 .
    - To enter the **Mitigation Details** page, click the corresponding Id.
    - To enter the **RiskOverview** page, click the **Parent Id** and you will be auto-scrolled to the corresponding risk.
3. Managing (e.g. edit, activate, review, close) risk mitigation actions can be done via the **RiskOverview** and the **Mitigation Details** pages.

Risk Assessment & Key Risk Indicators

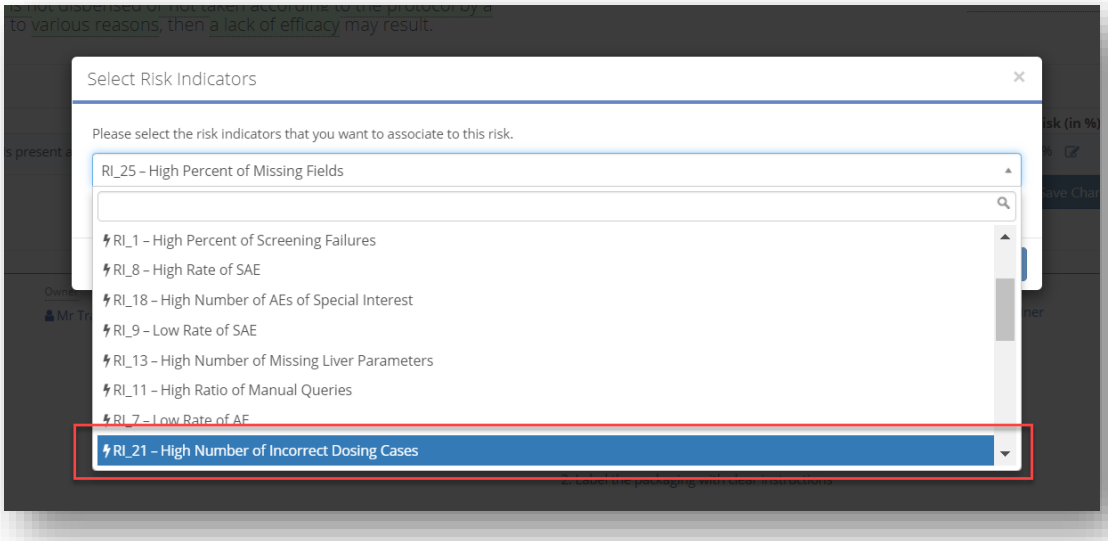
Risks that are not accepted should be controlled. The **MyRBQM® Portal** allows users to manage risks using **Risk Indicators (RIs)**, which can be associated with a specific risk.

To associate RIs with a Risk:

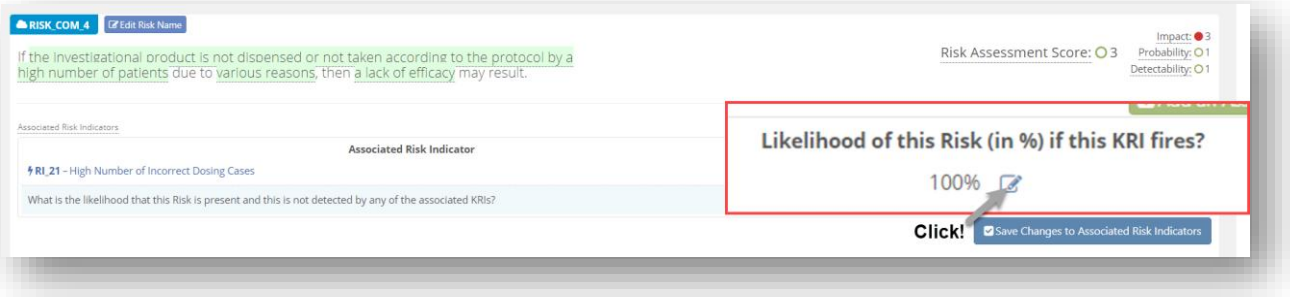
1. Identify which RIs can help indicate that the risk may occur.
2. Set up the system:
   a. Go to **Risk Management** → **Risks** Tab.
   b. Find the Risk and click **Add an Associated Risk Indicator.**



   c. In the drop-down list select a RI, then click **Save**.



d. By default, the likelihood of the RI fire together with the Risk is 100% but it is not always true, so you need to adjust it.

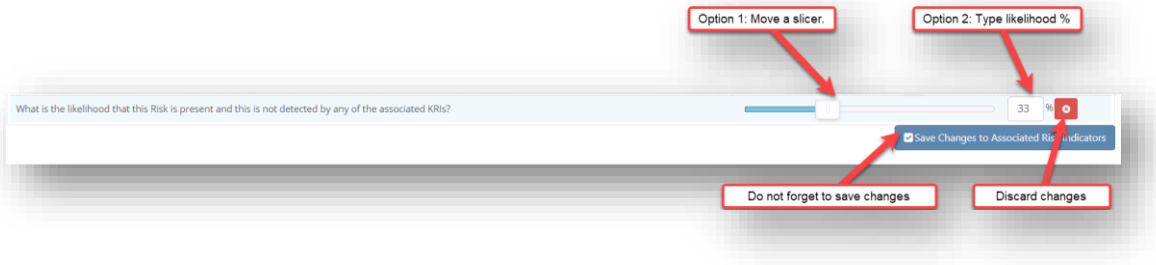


- **High likelihood** (close to 100%): If this KRI fires, it is **very probable** that the Risk is also present. A KRI is strongly correlated with the Risk.
- **Medium likelihood** (around 50%): If this KRI fires, the Risk **might be** present, but other causes are also possible.

- **Low likelihood** (close to 0%): If this KRI fires, it **does not strongly indicate** that the Risk is present.

In addition, you also need to define the opposite case: **What is the likelihood that this Risk is presented, and this is not detected by any of the associated KRI?** This captures the possibility that the Risk occurs without being detected by the KRIs:

- **High likelihood** (close to 100%): The Risk is **largely independent** of the defined KRIs, so it may often occur without them being triggered.
- **Medium likelihood** (around 50%): The Risk is **somewhat tied** to KRIs, but there are still considerable external factors that may cause it without any indicator firing.
- **Low likelihood** (close to 0%): The Risk is **almost always linked** to at least one KRI, so if no KRI fires, it is very unlikely the Risk occurs.



→ **Tip:** Look at the **Detectability** score of the Risk. If the Risk is **easy to detect** (Detectability = 1), then the likelihood of "Risk without KRI" should be **low**.

Note: the percentages for different KRIs **do not have to add up to 100%**.

The likelihood for a KRI firing and the likelihood for the Risk occurring without any KRIs firing cannot both be high or both low — they should reflect a realistic balance.

Centralized Statistical Monitoring (CSM)

About CSM

WHAT is it?

CSM - a statistical approach to central monitoring of clinical trials.
It includes a large number of statistical tests performed on **all variables** collected in the database.
Entities that **differ from the pool of all other entities** can be objectively identified.
→Outliers can be identified that would not be detectable by other methods.

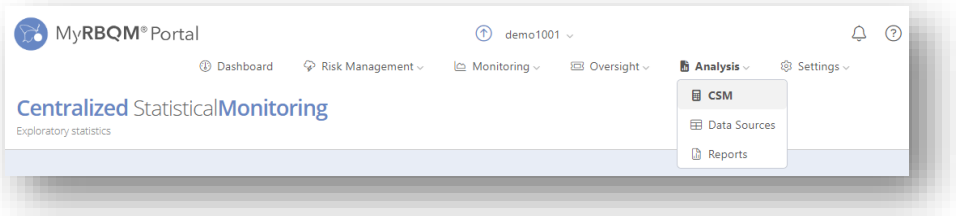
HOW does it work?

Multiple statistical tests generate a high-dimensional matrix of p-values.
Analysis by complex statistical methods enables identification of extreme entities. (outliers).

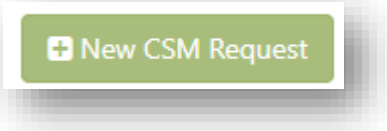
Centralized Statistical Monitoring combines Centralized Monitoring with Statistical Monitoring. Centralized monitoring is when site data is evaluated for risks in real time from a single off-site location, rather than reviewing risks directly on site at each investigative site. Statistical Monitoring is the complex statistical algorithms recommended by TransCelerate to discover data outliers and anomalies.

Create a CSM request

1. Select a study and enter the CSM page. It can be accessible from the main navigational menu by clicking **Analysis** → **CSM**.



2. Click **+New CSM Request** button on the right top of the page.



Individual test sets are used for different entity levels.

Most common CSM tests in the literature are Multivariate Outliers / Bivariate Outliers (identify differences between entities) **Digit Preference** (identifies data fraud, mis-calibrated equipment, subjective measurements)

3. Enter a Name for the CSM request. Click **Save and Go to Next Step.**
4. Choose from where you want to get data for the Request:
   A. **From the file:** Select **Data File** and upload the .csv file (max limit 512 MB) with all the data and click **Upload and Go to Next Step.**
   B. **Study Data:** You will see 2 options:
      - **Select the latest value** (latest Value means that the CSM Request will use for calculation the data points what have the latest day and (if available) time stamps in the latest uploaded Study Data Set. It means that if there are several records in the latest Study Data Set for the selected Data Item the last one will be taken for the CSM Request calculation.)
      - **Select Study Day/Range** (concept is explained below)

   C. Once you have selected one of the options above, click **Save & Go to Next Step.**

5. Create the number of columns needed for the Request that you plan to run.

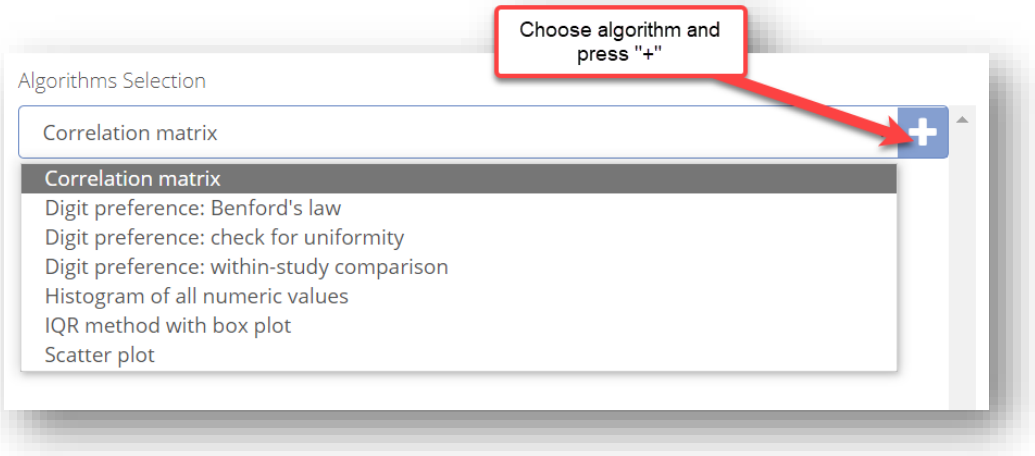
   A. Assign a Column Title, Level (Study, Country, Site etc.), Data Item (from drop-down list),

Field (Value or other parameters depending on selected Data item), Counting Number (if several measurements/records were made for the Data item type, choose one (for example 1,2,5). If there was just one measurement/record, type 1).

B. Click **Save.**

C. To set up another column(s), click **Add a New Column**. When all needed columns are created, click **Save & Go to Next Step.**

6. Select an algorithm option from the drop-down menu of the **Algorithm selection** and click the **+** sign.



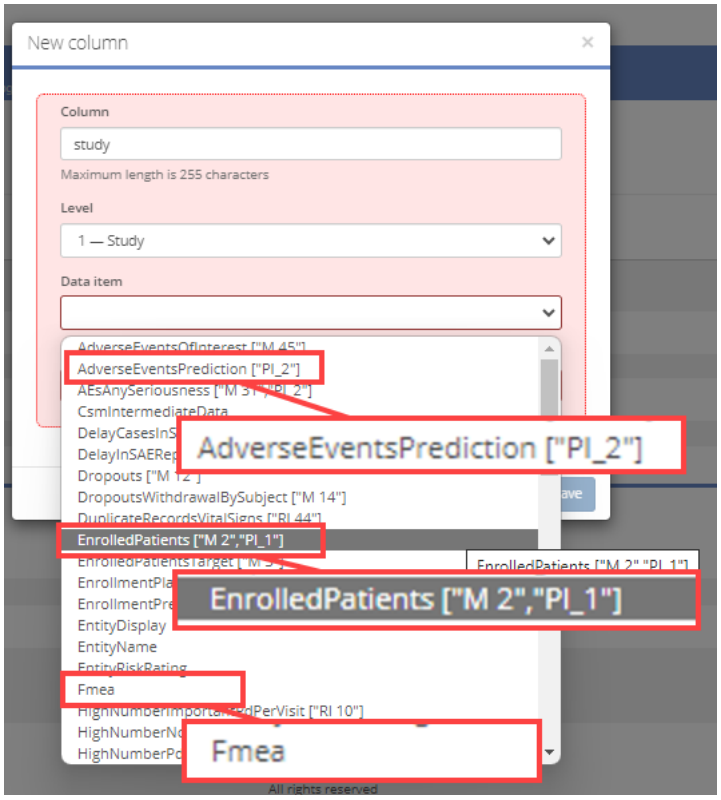
7. Select the drop-down menu in the **Label** column (optional) and choose any one column.

This function is available for **IQR box plots** and **scatterplots**. Select either a single column or to make the selection from the range of columns, i.e., select the range and click **+** every time to complete the selection.

8. Click **Save Changes and Send Request.**

NOTE: If Study Data is selected as Data Source. The Data item drop-down list will be formed based on the latest data set loaded in the system.

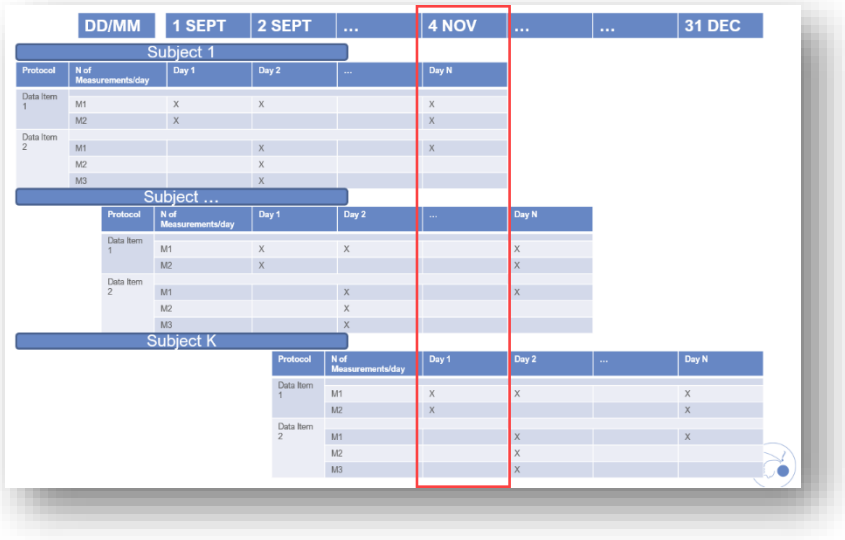
Data items what are also used as metrics calculated in MyRBQM (metric, KRI, QTL, PI etc.) have reference information in the drop-down list.



Study Day/Range

In clinical studies, subject enrollment takes some time, usually months. This means that one Subject can be at the end of his/her treatment protocol while others are in the beginning or in the middle of theirs, which means that it might not be correct to analyze their vital signs or any other parameters for a specific date.

For example, in the case of an oncology study with very high probability, the Subject who has just finished chemo-therapy had lost a lot of weight, and if we compare his/her weight with other Subjects who have just started their treatment, the first Subject might be considered as an out-lier (due to the significant weight difference), but it is not correct.

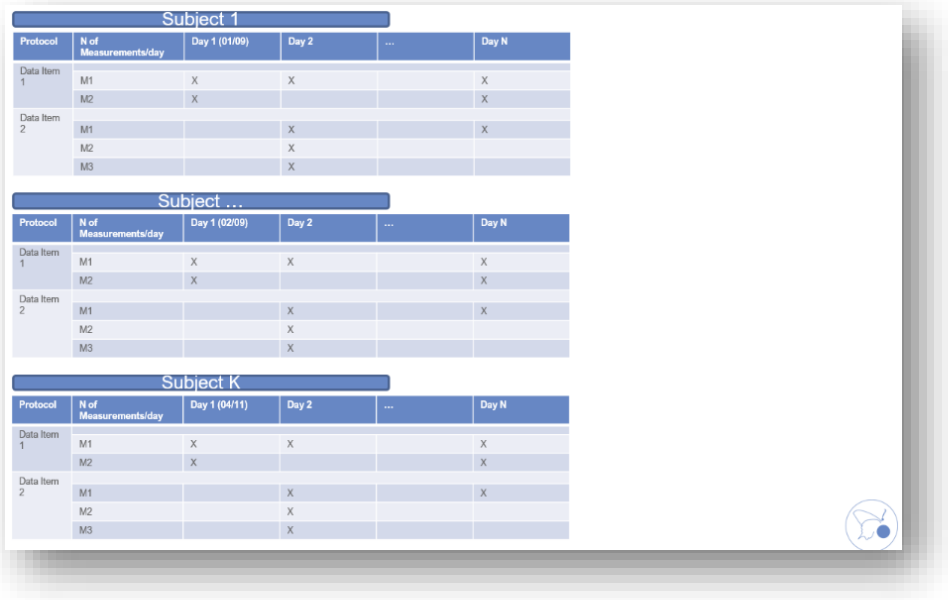


To solve this problem for a retrospective analysis, we need a **unified time parameter** that will allow us to compare Subjects who entered the Study at different times. This unified time parameter is named **"Study Day"**.

The date on which a Subject first appeared in the Study Data Set is considered the "Study Day 1".

So, we take Subject 1 and assign Study days for him/her:
Sept 1st = Study Day 1
Sept 2nd = Study Day 2, etc.

And we do the same for all Subjects
Subject K:
Nov 4th = Study Day 1
Nov 5th = Study Day 2, etc.



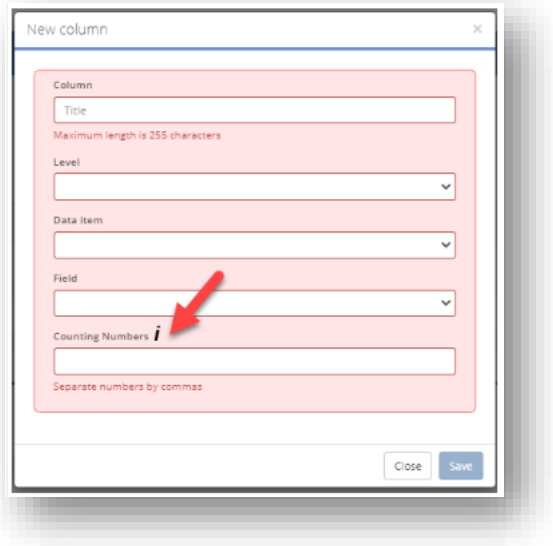
In this case, if we select the same **Study Day** for all Subject, we will compare Data item values properly (i.e., weight will be compared for 5th Study Day for all Subjects) and probability of statistical errors that can be caused by different enrollment days will be significantly lower.

It is also possible to select not only a single Study Day but **Study Day Range**. For example, Study Day 1 to Study Day 10.

Please note that Cyntegrity doesn't recommend selecting a long Study Day Range.

NOTE: For other levels (Site, Country, Study) the first Study Day will be calculated as the first date when an entity (for example Site N1) at the selected level (Site) appeared in the Study Data Set.

Counting Number



It is possible the Data Item was measured several times during a Study Day (for example, Heart Rate).

Values of these measurements might be very different (for example before and after injection). In this case, if a user makes a CSM Request for all measurements that were made during the **Study Day** it may cause statistical errors and incorrect conclusions.

To allow users to analyze concrete measurements, the **Counting Number** parameter was added.

Imagine that, following the protocol, there were 5 measurements of Heart Rate made.

The 1st, 2nd and 3d measurements were made before and between injections of an Investigational Product while the

2nd and 4th measurements were made just *after* the injection, and it is expected that IP should affect the Heart Rate significantly.

This means that statistical analysis for measurements 1,2,3 and 2,4 should be made separately or used as separate Data Items (i.e., presented in separate columns) in the CSM Request.

NOTE: If the Study Day/Range Option was selected, the Counting number field can't be empty.

Explore CSM Results

You will receive an email from the **MyRBQM® Portal** when your given task is completed, saying "**Your CSM request was finished!".** Open the mail and click the link, **or** you can periodically refresh the CSM tab to see the report progress.

1. Once the CSM Request is opened, the Algorithm Details section will appear blue. A small "spike" symbol indicates a "short cut" view of the result page.

2. Alternatively, you can click the CSM algorithm you had chosen to expand the Algorithm Details section. Click **View Results**. The CSM results page will open.
3. Explore the results:

Algorithms	Results
IQR Box Plot	For IQR algorithm the Portal shows the boxplot charts and details table for each selected column. On the plot you can find a collection of inliers, outliers, and a predicted mean (line). The box plot labels outliers and inliers. A label column can be selected as an option for the IQR algorithm. It must contain the following: The details in the table are the four quartiles and the median value. • Q1 • Q2 • Median • Q3 • Q4 • Amount Amount is calculated as the total number of inliers and outliers added to the number of filtered out inliers and outliers.
Correlation Matrix	For the Correlation Matrix algorithm, you can find a heatmap of the selected columns' data correlation. For demonstration purposes, a crosshair appears when hovering over this image with a mouse. There are ellipses in cells of a matrix (unless number of selected variables is 50 or more, in that case there are just colored cells). The greater the value of the correlation, the more oblong the ellipsis.

	Positive correlations are displayed in blue and negative correlations in red color. Color intensity is proportional to the correlation value.
Histogram of All Numeric Values	For the Histogram Algorithm, a histogram chart and Details table for each selected column are shown. The details in the table are: Minimum (Min), Maximum (Max), Range, Mean, Median, 3rd Quartile (3rd Qu.), 1st Quartile (1st Qu.), Total Number, Variance, Standard Deviation (Std. Dev.), and the Number of Missing Values (Missing). Similar to the IQR algorithm, each chart in the histogram should be labeled with the name of the column to which it correlates. The charts on the **CSM Results** page must show an additional graph: a black spline displaying the kernel density estimate overlaid on top of the histogram columns. An additional Y-axis for its values will be shown on the right side of the chart. A tool-tip for this chart should display both the count (based on the bin being hovered over) and the density estimate (based either on a specific point of the spline being hovered over, or, if the user is hovering over a histogram column, based on the spline point that is closest to the middle-point of the column/bin). It must also show the current bin as a range of values and, if the user is hovering over a specific point on the density graph, it will show the specific value (i.e., the value on the X-axis).
Scatterplot	You see a Raster Plot which is a two-dimensional data visualization that uses dots to represent the values obtained for two different variables - one plotted along the x-axis, and the other plotted along the y-axis. Also, you will see:

	• A linear regression line reflecting dependency between variables • A kernel density estimate curve reflecting density of points for each axis • Colored ticks near coordinate axes reflecting density of points for every label • A list of outlier points under the plot. (For many variables selected), you see a table with a list of all the possible variables, from which you can click and select a scatter plot for the specific chosen combination. Below the table you will find the scatter plot and there should a folded table with outliers for that pair of variables under the scatter plot (if any).
Digit Preference - within study comparison	Depending on what label field is specified by a user, the algorithm is able to compare leading or trailing digits between user-defined groups in a clinical trial, e.g., for sites or for randomization arms (for checking whether randomization is correct).The algorithm calculates a contingency table for the frequency distribution of digits of interest (either 1 or 2 leading or trailing digits). That table is defined as follows. Every column contains 2 values: 1) A count of occurrences of every digit (or sequence of digits) for a label value (e.g., if labels are site IDs, it is a count for a specific site), 2) A count of that digit (sequence) for all other values of label (if labels are site IDs, it is a count for all other sites, except for the site we are looking at). Calculates standardized mid-rank scores for columns of the table. Performs Cochran-Mantel-Haenszel Row Mean Scores Differ test, which effectively compares rows of the contingency table between each other using

	Chi-squared test, which is calculated from standardized mid-rank scores. Considering all tests that are executed in a scope of a CSM Request, whether for trailing or leading digits are parts of a single experiment, it's needed to perform adjustment for multiple comparisons. It is done by using the Benjamini-Yekutieli method for control of the false discovery rate. Adjusted p-values are calculated using that method. Scores are calculated from the p-values using the formula -log10(p-value), which provides values that have a more convenient and useful scale than the p-values, themselves. Scores are highlighted in a report if a p-value is lower than a user-defined significance level, which means that the data is suspicious, and the case should be investigated. If the number of observations is small (50 or less), a cell is highlighted with a lighter color. If the number of highlighted cells is too big, then the highlights are additionally filtered by finding outliers of the distribution of test results and highlighting them only. In the report, the user can also examine the distribution of digits in data and, for any digit, find out the difference (in percent) between actual and expected counts (the expected counts are taken from the distribution of digits for all other label values).
Digit Preference - Benford's Law	The algorithm is able to detect fraud by checking that the first significant digit (FSD) frequency distribution complies with Benford's Law, which is true for many clinical data variables. The first thing needed to apply this algorithm is learning whether a variable of interest follows the law in general. The algorithm will leave a warning in the warnings list if some of the properties of data complying with

	Benford's Law are not observed. When deciding on whether to use the algorithm, consider the origin of the data: • Data should have values covering several orders of magnitude (this is also checked by the algorithm). • Data which is distributed normally typically does not follow Benford's Law. • The law is usually followed for numbers that result from a mathematical combination of numbers, first of all multiplicative. • The law is not followed for numbers assigned sequentially; numeric distributions constrained by some threshold, so that threshold heavily affects histogram of data; numbers distributed very unevenly across their range. The algorithm: 1. Finds frequencies of values of one or two leading digits in data. 2. Finds second-order frequencies of two leading digits. For that, it first removes duplicates from the set of numbers, sorts them in ascending order and finds differences of numbers neighboring in a sequence. Then it runs a test on a sequence of differences. 3. Compares these frequencies with the expectation of following Benford's Law. The algorithm performs different statistical tests to compare FSD distribution with Benford's Law. In every case, a statistical test is selected based on the number of analyzed rows, whether in the whole dataset if Label column is not selected, or in a group otherwise (that is especially important if some of the groups are small), every test is the most sensitive and unbiased in its range. 4. Achieves the best results on big datasets (500 rows or more). For them, the Excess MAD test is used, which answers the question of how

	similar the actual distribution is to the expected distribution, so the result of it is an effect size statistic. This result is compared with marginal conformity and nonconformity thresholds for MAD specified in [3] but is also corrected for the size of the sample using the method from [4]. Effect size is useful because besides Benford sets of numbers, which follow Benford's Law with high confidence, there are almost Benford sets, and certain effect size can be observed for certain data. Even if the threshold is not crossed, issues can be found by comparing an effect size with an expectation found from a similar but proven for correctness set of data. For a small dataset size, it is difficult to detect effect size precisely. Other 2 tests produce p-value and answer a different question, which is whether a distribution follows Benford's Law with a given significance level. p-values produced by statistical tests are adjusted for multiple comparisons by the Benjamini-Yekutieli method and are compared with the significance level specified by a user. Very small dataset size tests are even less powerful. For that reason, p-value correction for G-test and d* test is performed separately. This increases the probability of a single error but helps to preserve statistical power. Scores are calculated from the p-values using the formula -log10(p-value), which provides values that have a more convenient and useful scale than the p-values themselves. Scores are highlighted in a report if a p-value is lower than a user-defined significance level, which means that the data is suspicious, and the case should be investigated. If the number of observations is small (50 or less), a cell is highlighted with a lighter color.

	In the report, the user can also examine the distribution of digits in data and find out for any digit the difference (in percent) between actual and expected counts (the expected counts are taken from the distribution of digits for all other label values). An effective number of numbers processed by the algorithm is affected by NA values in data and specifically for the second-order test also by duplicated numbers. So, regarding the second-order test, if there is a big number of duplicates in data, then that test is not very useful.
Digit Preference - Check for Uniformity	The algorithm detects data collection errors and fraud by checking that the trailing digits frequency distribution is uniform. The following should be considered whether a set of data is eligible for that test. Many clinical variables allow expecting that their trailing digits are distributed uniformly, which means the probability of occurrence of all digits is equal. But we need to be careful: for some measurements, it is not the case, and it is sometimes not yet known why. On the other hand, if the leading digits follow Benford's Law, and data consists of numbers with more than 3 digits, then it can be expected that trailing digits have Uniform Distribution because that is specified by Benford's Law for higher decimal places. You can look at the manual page for Digit Preference: Benford's Law to learn more about the applicability of Benford's Law. Most common use case of the test is data given with a specific precision (number of decimal places after the decimal separator). Though if rounding of numbers is abnormal, that will also be found by the test.

	The last two-digit test is generally run on data tables where we are looking for signs of number invention., so this test shouldn't be run on data for which last digits are normally affected by some psychological thresholds or rounding. The algorithm: Finds frequencies of values of one or two trailing digits in data. • Compares these frequencies with the expectation of Uniform Distribution. • p-values produced by statistical tests are adjusted for multiple comparisons by the Benjamini-Yekutieli method and compared with the significance level specified by a user. For a very small dataset size, tests are less powerful. For that reason, p-value correction for G-test and KS test is performed separately, to increase the probability of a single error, but help to preserve statistical power. • Scores -log10(p-value) are calculated, which are in a more convenient scale than p-value itself. Scores are highlighted in a report if a p-value is less than a significance level, which means that the data is suspicious, and the case should be investigated. If the number of observations is small (50 or fewer), a cell is highlighted with a lighter color.

Create a Ticket Based on CSM Results

1. Click **New Ticket**, Enter the details (Scope, Associated Entity, Designee, Alert level and Description) and click **Create Ticket**.

2. Enter the details of the newly created ticket by clicking on the ticket number. You will be redirected to the **Ticket Details** page with the following information:
    - Responsible
    - Created at
    - Last Update
    - Description
    - Affected Study
    - Associated CSM Request Details

    The created ticket can be subscribed, activated, assigned, closed.

Archive CSM Request

1. From the **CentralizedStatisticalMonitoring** page, open a finished CSM request, select a CSM request in process or one that is already done by clicking on the check box.
2. Click **Archive this request.**
3. Press **Ok.**

Cancel CSM Request

1. From the study's **CSM** page, click **+New CSM request** button on the right top of the page.
2. Enter the basic CSM **Request Details.**
3. Upload the data file/select study data.
4. Select an algorithm.

5. Click **Save and Send Request**.
6. Click **Cancel** from the **CentralStatisticalMonitoring** page.

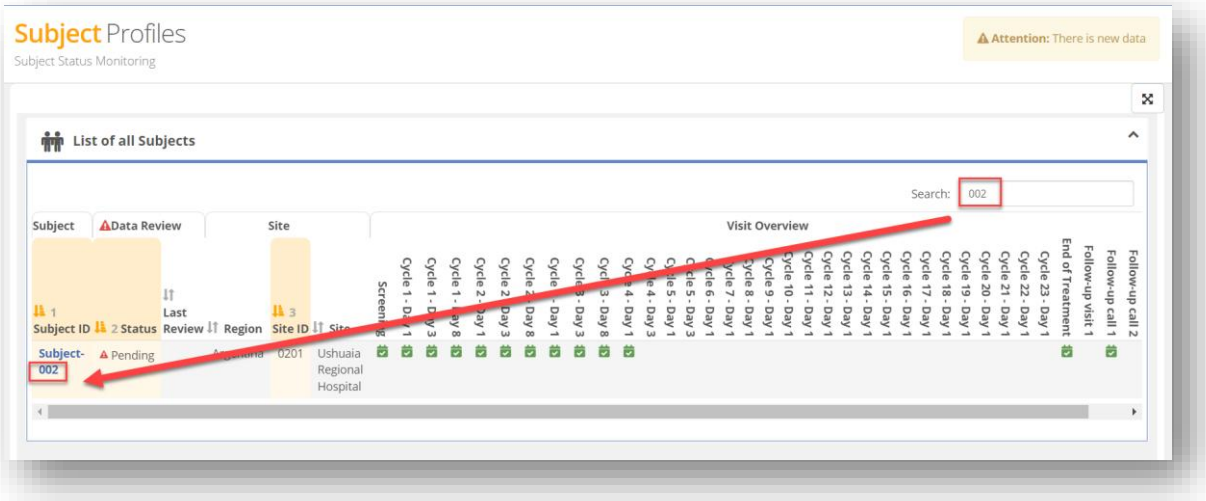
Subject Profile

Subject - centered R&D in pharma begins with understanding your patients, and Subject Profiles is the feature that enables that. The Subject Profile module allows oversight of all study-relevant parameters for all study subjects. By facilitating a bird's eye view on subject history, the module helps you improve clinical trial data quality and particularly patient safety.

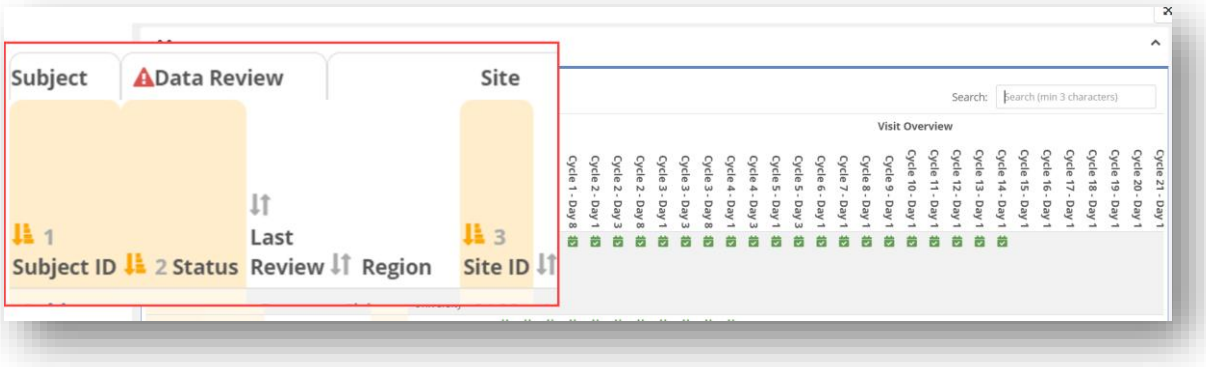
For a single site and for each Subject Profiles displays detailed subject information, a comprehensive medical history, and a graphical profile listing in Gantt and line charts, Visits, Adverse Events, Concomitant Medication, and Laboratory Measurements.

Explore List of Subjects

1. Open a study.
2. Got to **Oversight** → **Subjects** on the upper menu.
3. Enter text into the Search field (min 3 characters). The table will filter data.
4. Clear the Search field. The table will display all data.



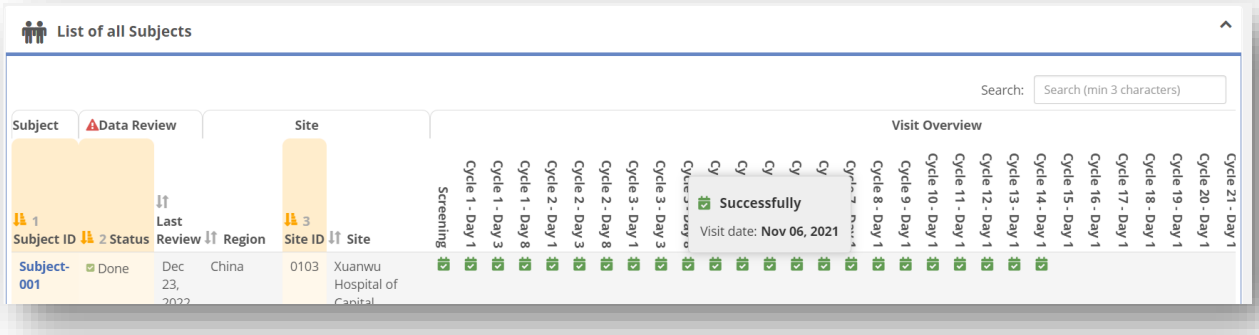
Default column is sorted with 1- Status, 2-Site ID.



Click any column to sort direction, order, priority.

Visits Status elements will display different states as different icons in color.

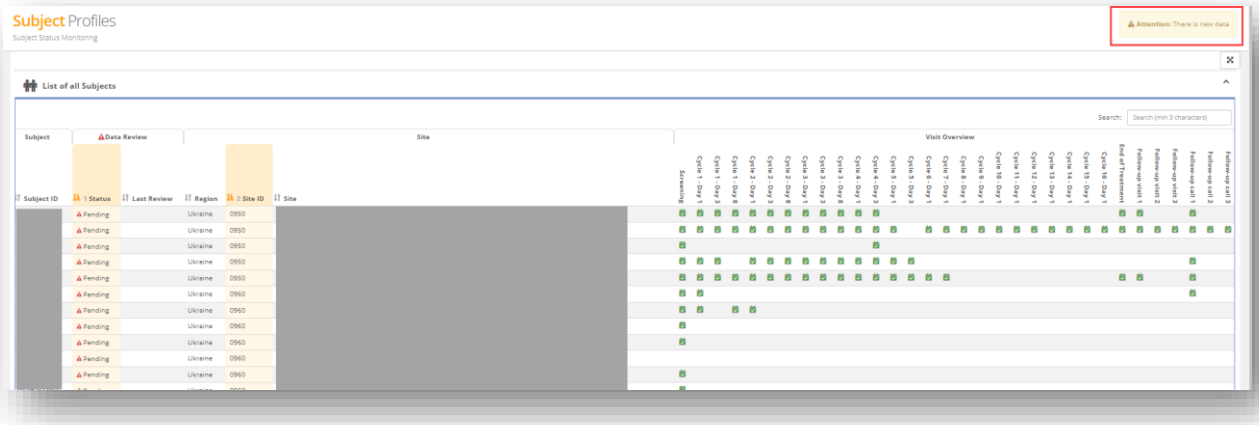
To display **Visit Status Tooltips**, hover over the visits. When hovering over any visit, a hint about the status of the visit will display.



Color Key for Visit Statuses:

- Green - visit performed as scheduled
- Orange - visit performed out of schedule or unplanned
- Red - missing visit
- Blue - future scheduled visit.

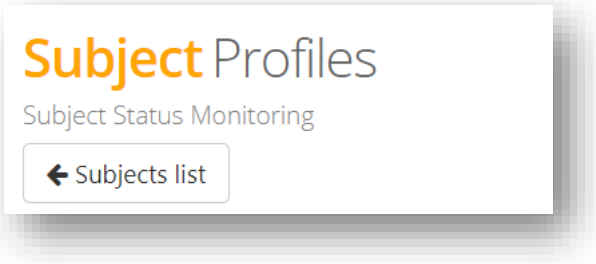
The overview status indicator shows progress of the new data calculation, which begins immediately after the Subjects Profile page is loaded.

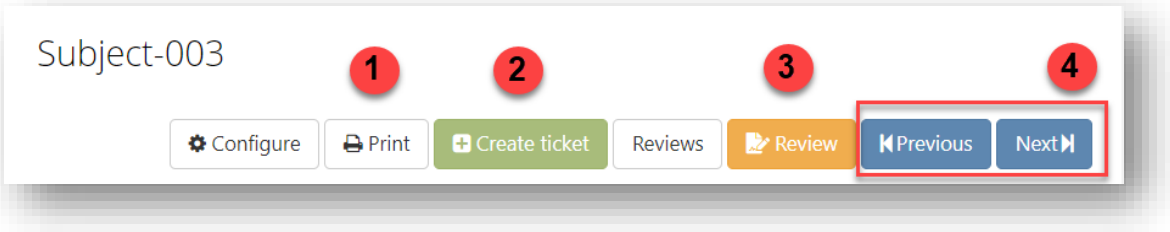


NOTE: To open a Subject Profile in a new tab, click central button/wheel of a computer mouse.

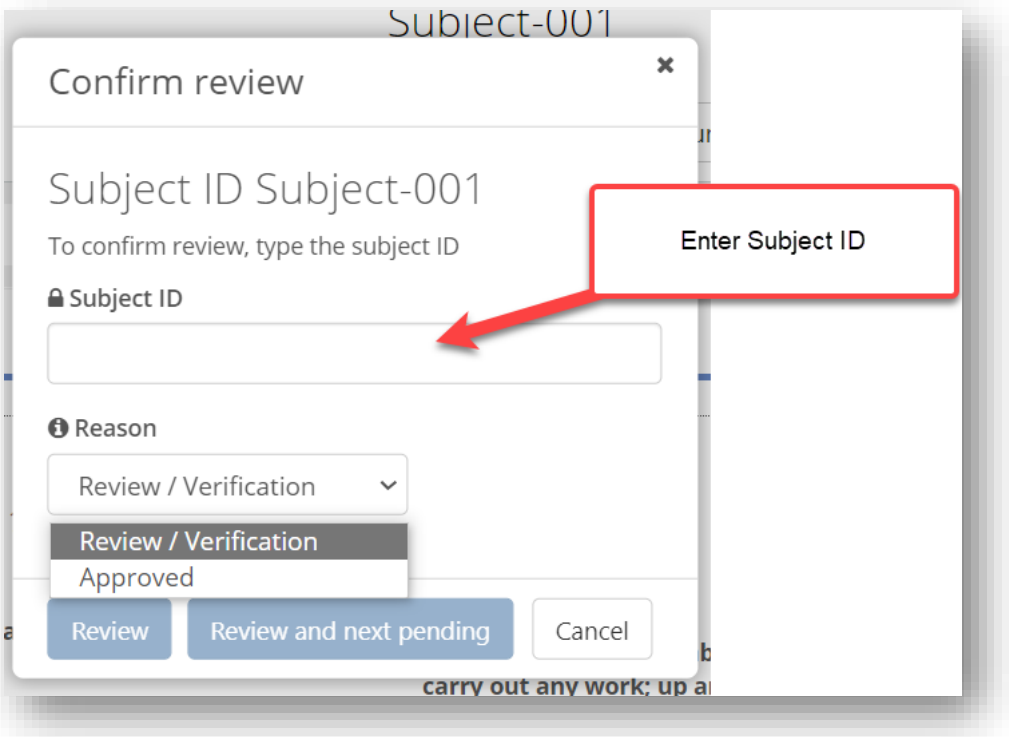
Subject Profile toolbar

The ← **Subjects list** button takes you to the **Subjects list.**

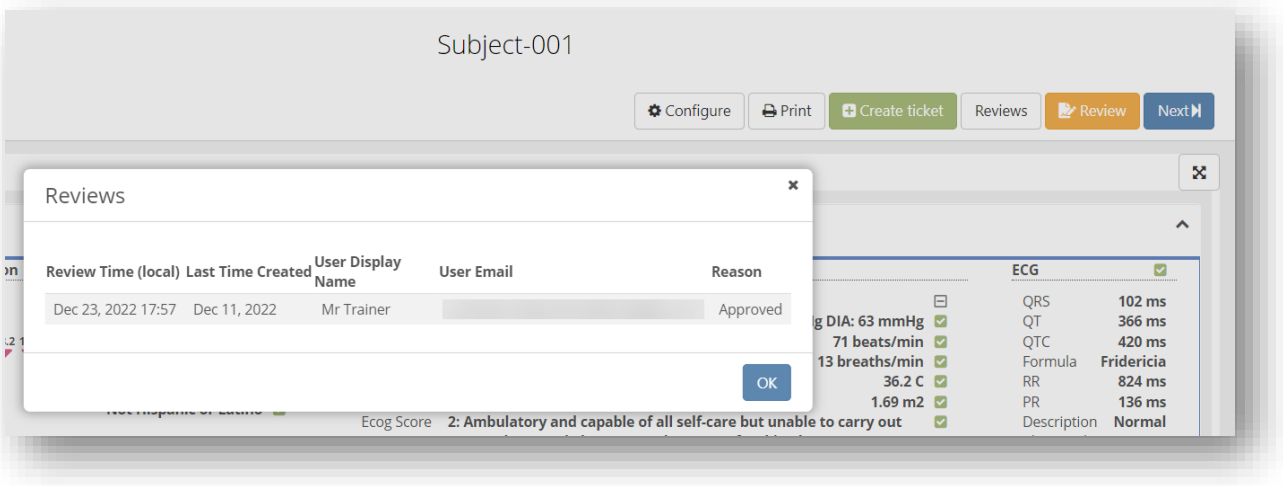




1. **Print** opens a new browser with Print Dialog. Click **Print** to print or **Save** the profile as a file.
2. **Create Ticket** opens the Create Ticket Dialog box. Create a ticket and check the ticket in the Tickets list.
3. **Review** displays a Confirm Review Dialog box.



1. Select the **Reason**: Approve, Review/Verification
2. Select **Review** or **Review and next Pending** to confirm revision of the subject data or confirm the revision of the subject data and go to the next subject.
3. To check the Reviews history, click **Reviews**.



4. The **Next** and **Previous** buttons take you to the next or previous pending profiles. "No more pending profiles" will appear if all profiles are signed.

Subject Data

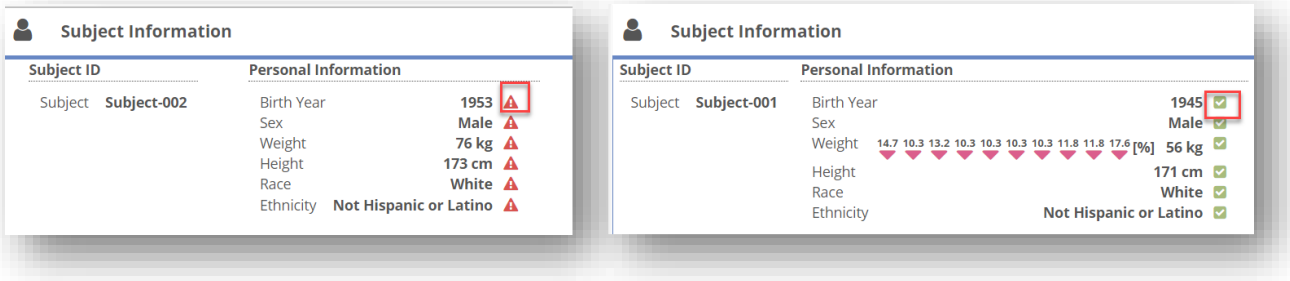
Open any Subject Profile. Click a subject hyperlink in the **Subject ID** column.

The Subject Profile page usually contains:

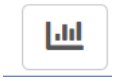
- Subject Information
- Subject Visits
- Medical History
- Adverse Events
- Concomitant Medication
- Laboratory Measurements
- Physical Examination

New data is indicated by a red icon.

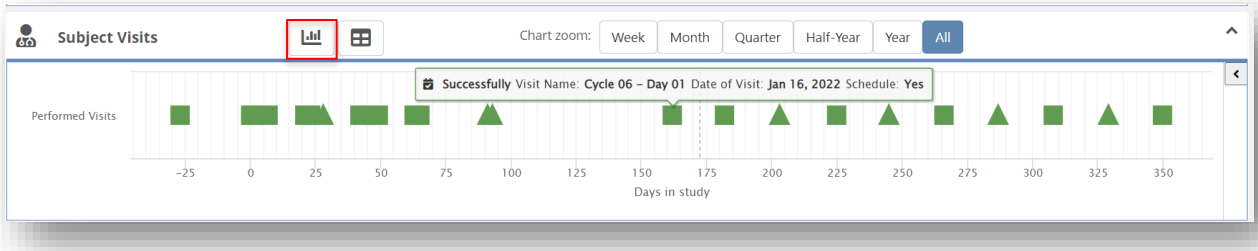
Reviewed data is displayed with or without a green icon.

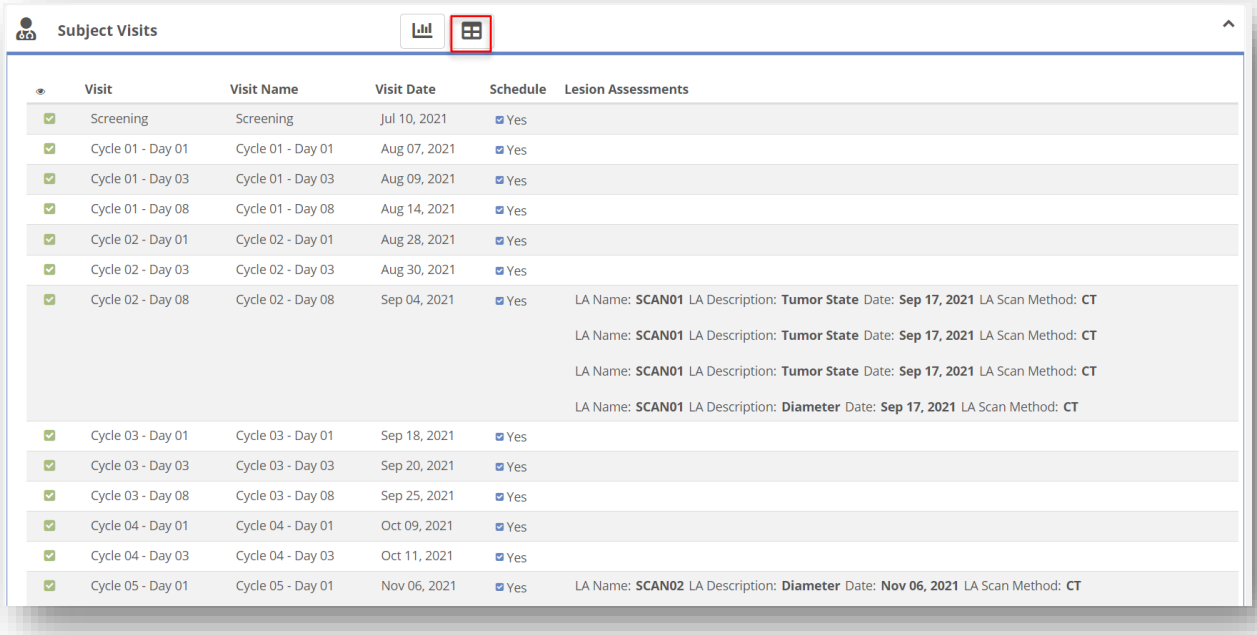


Click the **Table**  shown in the section data table.

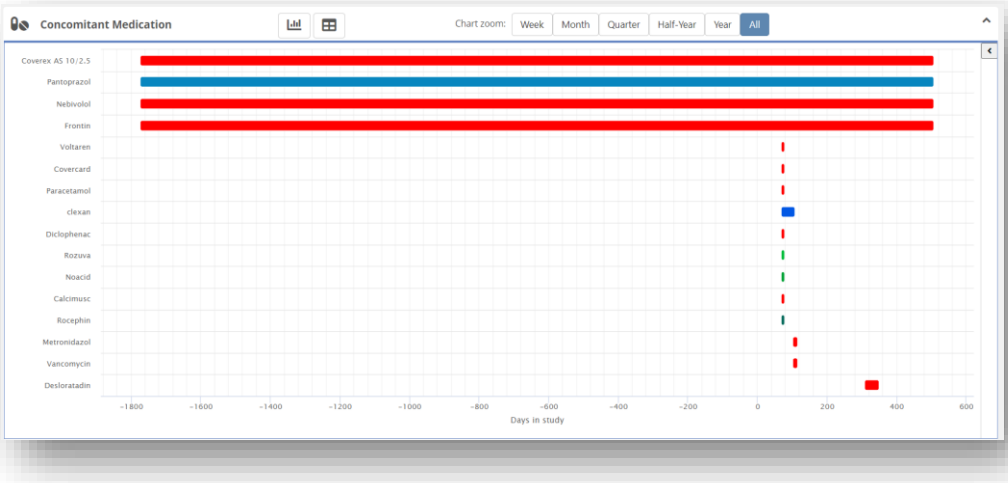
Click **Chart**  to show the section chart.

When hovering over any point on the chart, an information Tooltip will display.

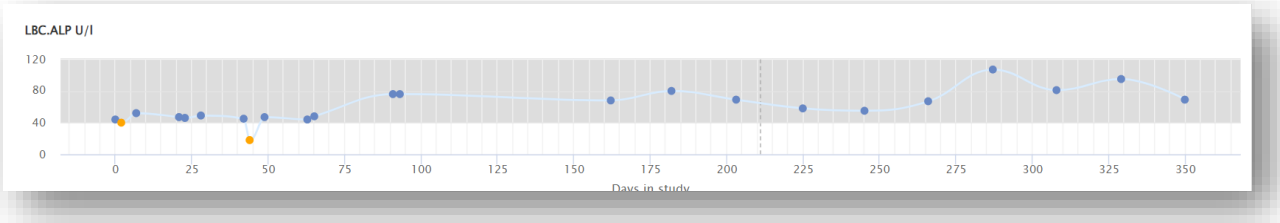




Concomitant Medication can display related Adverse Events and Medical Conditions. Such markers are marked in red on the chart. Other elements are displayed in a blue-green palette.



The Laboratory Measurements section has one graph for each measurement.



Each graph displays a Laboratory Value in bold gray line, Confidence Interval in light blue area.

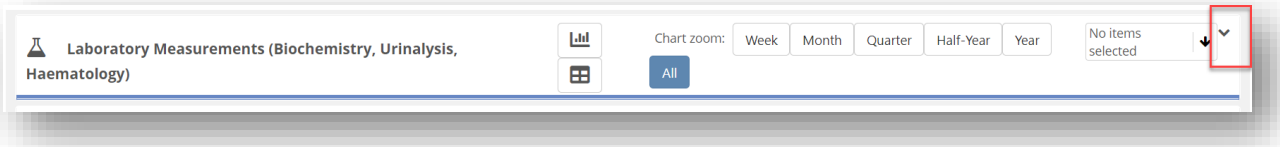
Each graph displays a Range Values in light gray band.

The Laboratory Value points out from Range Values point orange.

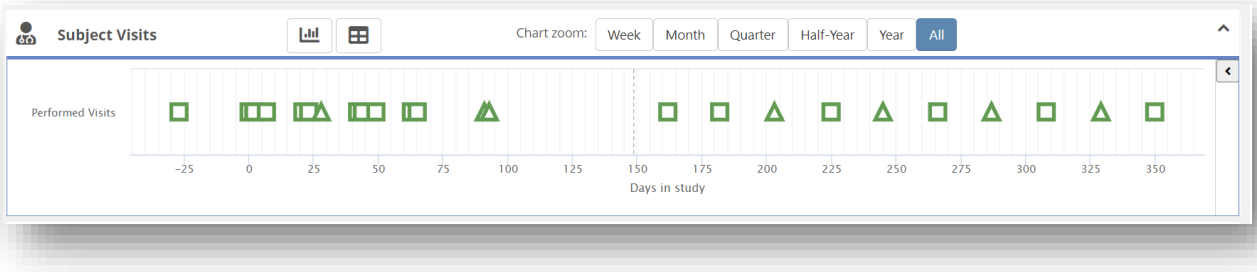
The Laboratory Value point displays as a circle when new data is present. The Laboratory Value point is solid when reviewed.

The Laboratory Value point is a triangle when Is Significant.

The Laboratory measurements section is closed when the patient profile is displayed. To open the section, click the down arrow:



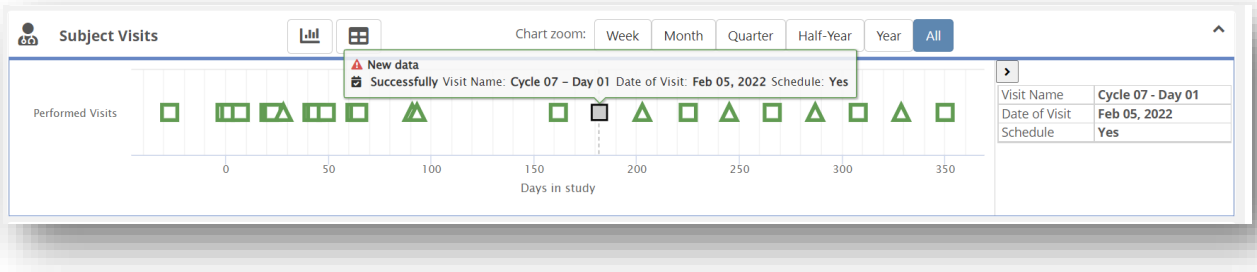
The Subject Visits chart contains Performed Visits statuses.



Triangle point when the imaging was taken (CT Scan). Box point is a regular visit.

Purple color means unscheduled visits, green color means scheduled visits.

Click the **Visit Marker** to display additional data.



Subject Profile settings

To enable the Subject Profile:

1. Click **Settings** → **Study Settings** → **Study Protocol**.
2. Click the checkbox: **Is Subject Profile Enabled?**

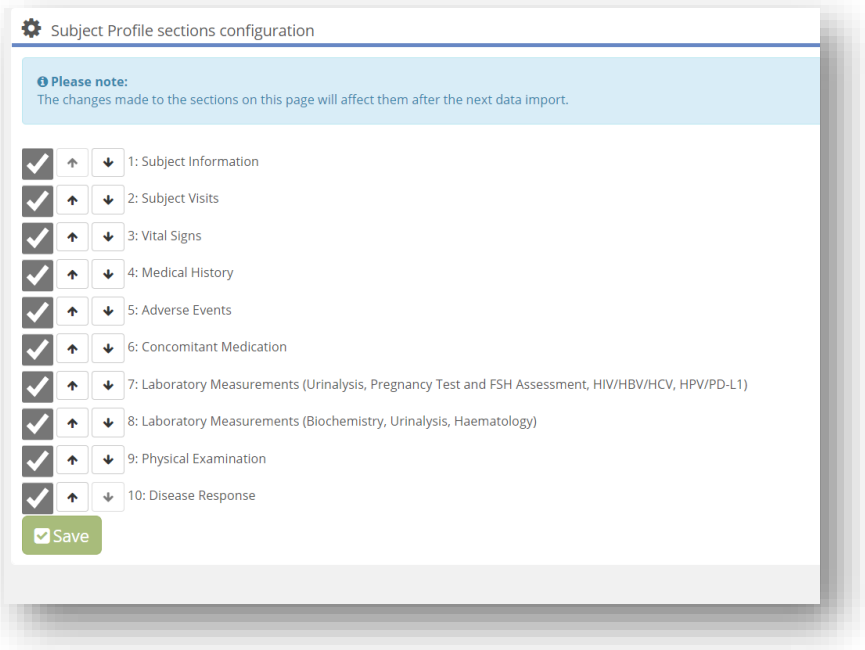
3. **Save**.

When the SubjectProfile availability is confirmed, the user can manage the Subject Profile view and sections to be displayed.

Setup the Subject Profile View

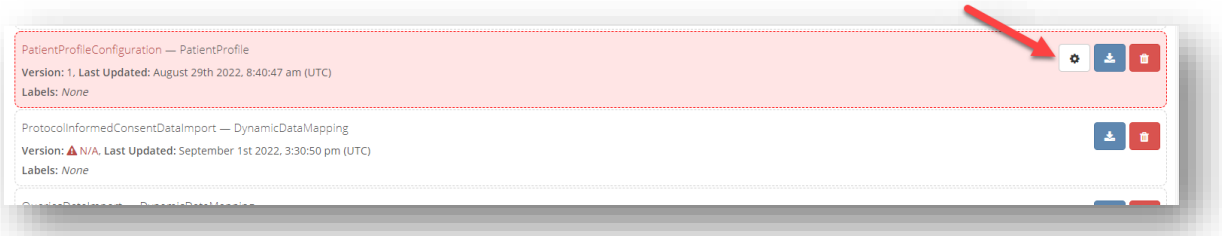
1. Go to **Subjects**, open any Subject Profile, click **Configure.**
2. In the Subject Profile section, click the **arrow up or down** button to reorder sections.
3. Select a section to be displayed.
4. **Save.**

NOTE: Changes will be available after the next import.



There is another way to reach the Subject tab configuration using Studies Settings Setup:

1. Go to **Study Settings.**
2. In left-hand menu, select **Technical Config.**
3. **Patient Profile Configuration**.



Compliance & Data Quality Check

The Compliance & Data Quality Check module is designed to help study teams quickly identify and manage potential protocol deviations using advanced AI-driven detection algorithms. Whenever the system flags an issue, users can access detailed contextual information, review supporting data, and determine the appropriate follow-up actions directly within the module.

Each detected issue moves through a structured review process. Users with the appropriate permissions can update the issue status, document review decisions, assign responsible reviewers, and set due dates for further evaluation. Every action is fully traceable: status changes are recorded in the study audit trail and displayed in the Status Change History section on the issue details page, ensuring complete transparency and easy monitoring of the issue’s lifecycle.

This module provides a streamlined workflow for confirming, reviewing, and resolving protocol deviations — supporting both operational efficiency and regulatory compliance.

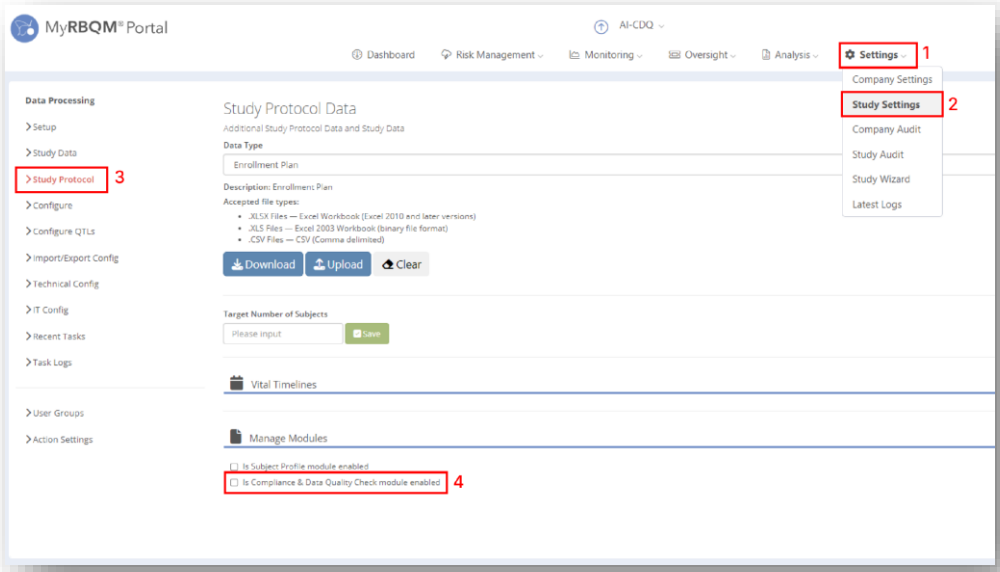
How to enable and access the Compliance & Data Quality Check module

To use the **Compliance & Data Quality Check** functionality:

1. it must first be enabled in the current **study configuration** by Cyntegrity team.
2. then in your **Study Settings** by your Administrator (This functionality is **disabled** in MyRBQM by default).
3. a **privilege CDQ - Access Compliance and Data** has to be granted by your Administrator.

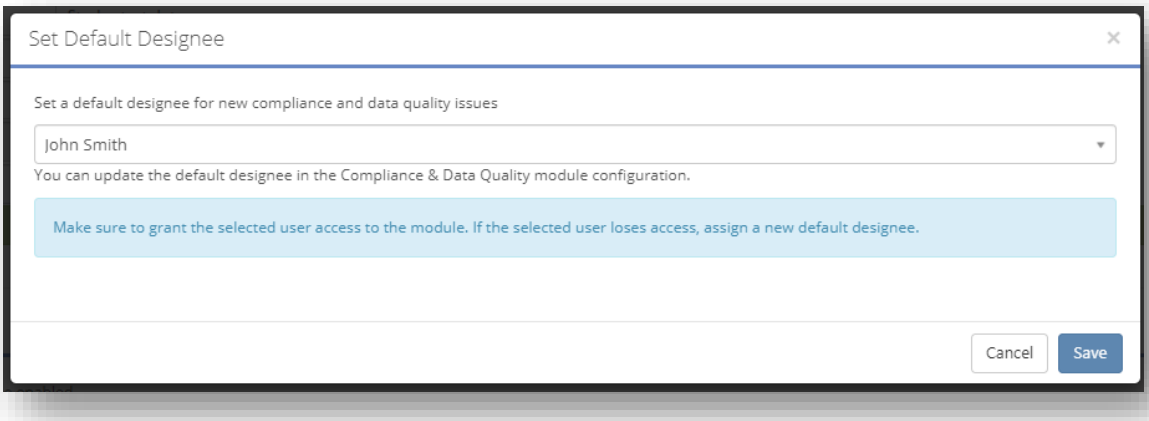
To enable the **Compliance & Data Quality Check** if it is setup in your study configuration:

Navigate to **Study Settings** → **Study Protocol** tab → **Manage Modules** section → and check the box labeled **Is Compliance & Data Quality Check module enabled** (see below).



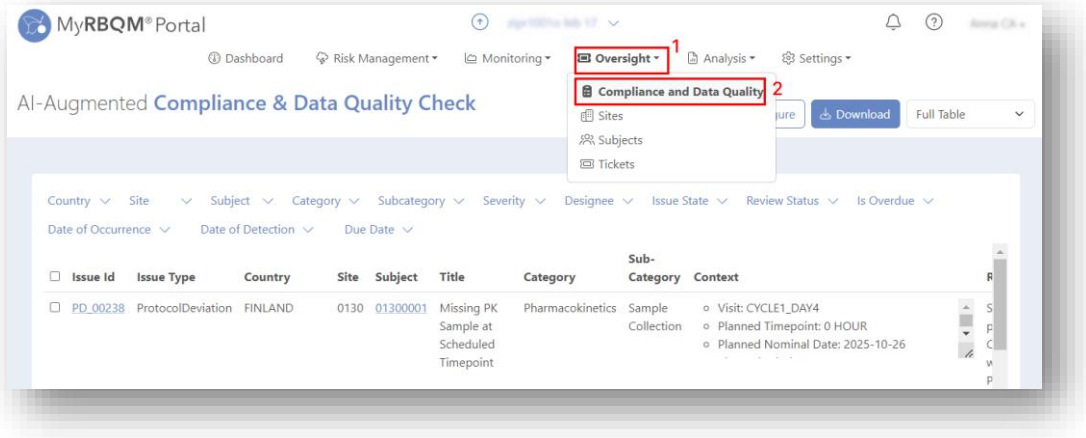
Carefully read and accept the **terms of use** before enabling the Compliance & Data Quality Check module.

After accepting the terms of use the system will ask you to select a default designee who will be responsible for newly created issues.



Don't forget to **save** changes after selecting the default designee:

Once the module has been enabled, click on the **Oversight** menu drop-down item: **Compliance & Data Quality**, as below.



Updating Issue Status in the Compliance & Data Quality Check Module

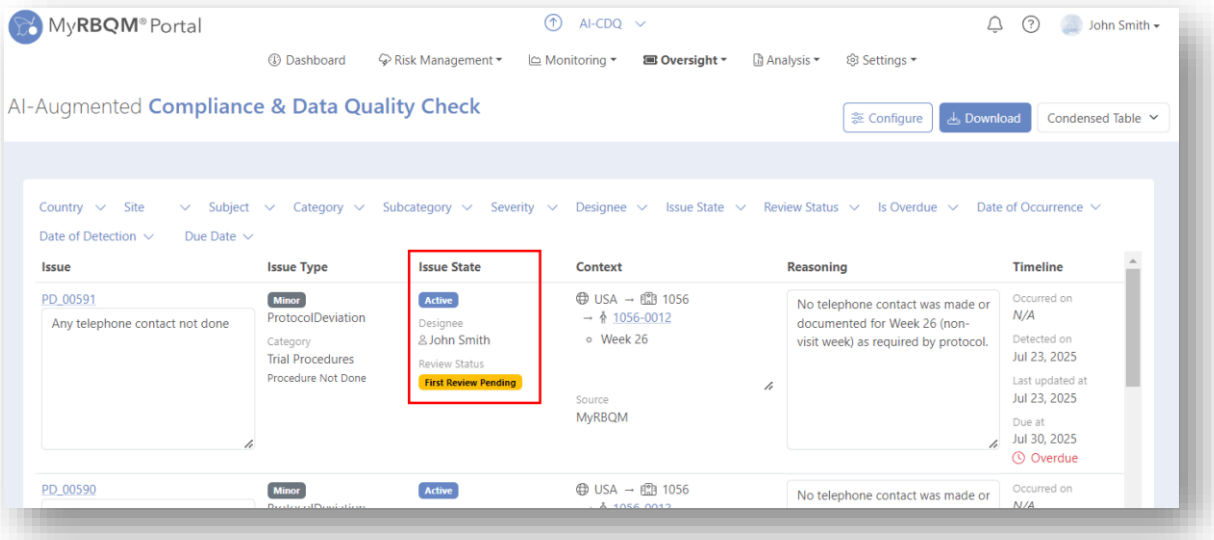
The Compliance & Data Quality Check module includes an Issue Status Update workflow that allows users to review detected deviations and manage their follow-up actions. The Update Status functionality ensures that each issue progresses through a clear and traceable review cycle.

The current status of each identified issue can be viewed on the **Issues List** page (as shown in the image below). When a new issue is created in the system, it automatically receives the **state: Active** and the **status: First Review Pending**. The assigned default designee is notified that a new issue requires attention.

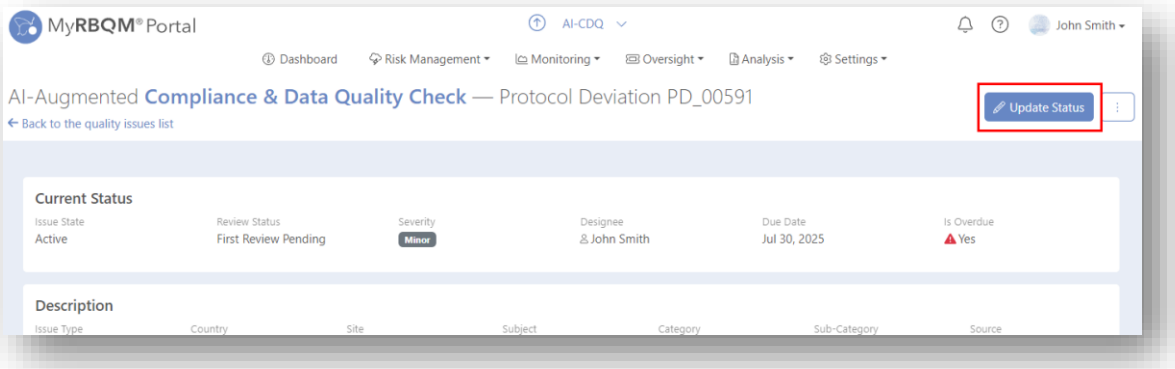
You can change the default designee for new issues by clicking **Configure** on the **Issues List** page. The functionality is available with the assigned privilege **CDQ - Configure Workflow**.

All users who have access to the module and the assigned privilege **CDQ - Status Change** are authorized to update an issue status. This can be done individually for each issue or in bulk.

To update a single issue status, open the **Issue Details** page by clicking the issue ID in the first column.



When you click **Update Status** on the **Issue Details** page, a **Status Update** window opens. This window displays the issue's current state and review status, and allows you to define the next steps.



Current Status Overview

At the top of the dialog, you will see two read-only fields:

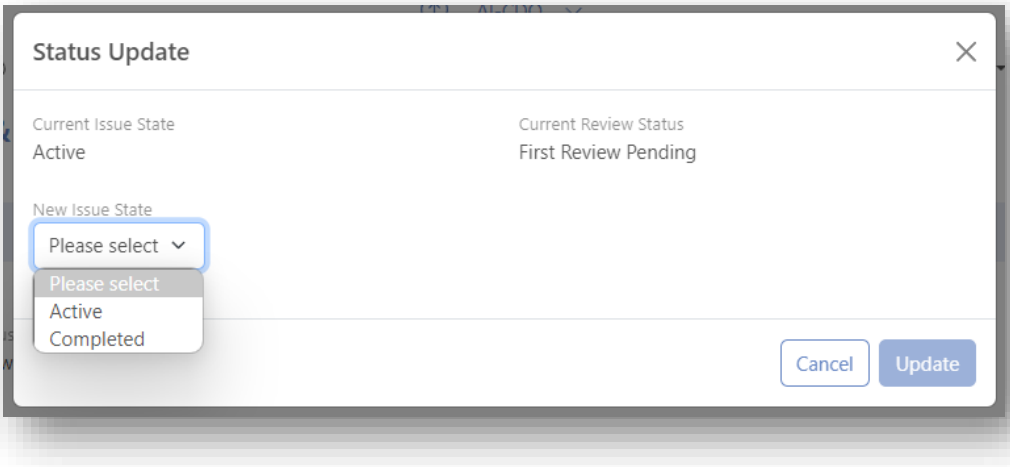
- **Current Issue State** – shows whether the issue is currently Active or Completed.
- **Current Review Status** – displays the latest review decision associated with the issue.

These fields help you understand the issue's present position before making any changes.

Choosing the New Issue State

The first editable field is **New Issue State**, where you select whether the issue should be moved to **Active** or **Completed**.

- Use **Active** when the issue still requires attention or additional review.
- Use **Completed** when the issue is fully resolved or accepted and no further action is needed.



Updating Active Issues

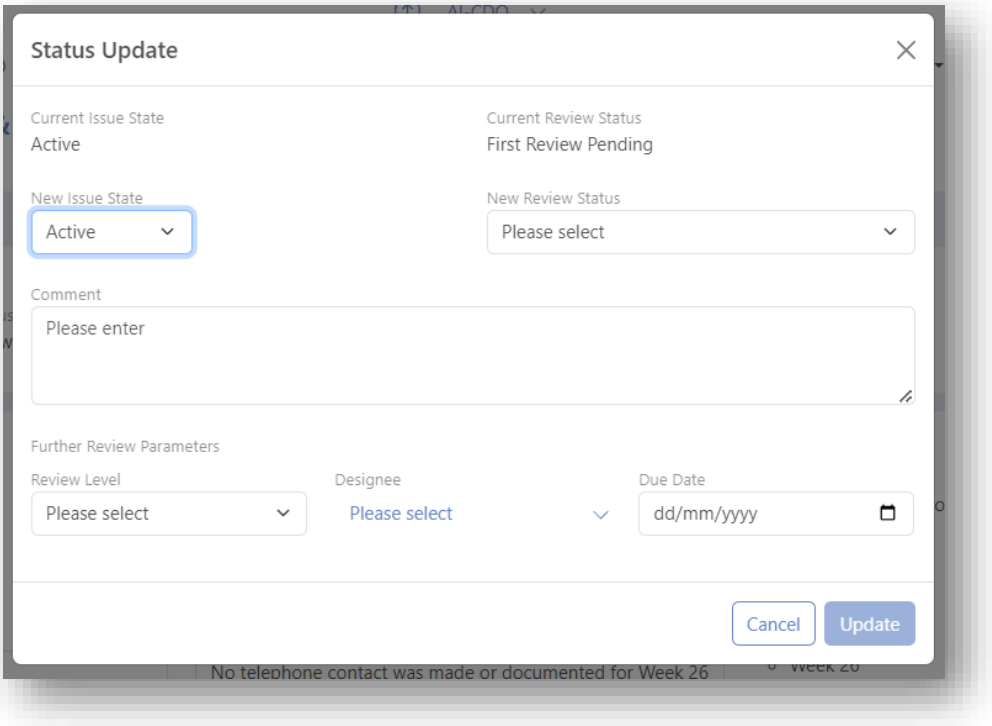
If you set the New Issue State to **Active**, several additional fields appear. These fields allow the reviewer to define the next steps in the follow-up process:

- **New Review Status** – document your decision on the issue by selecting one of the available review statuses: *Reviewed*, *Verified*, or *Rejected* .
- **Comment** – provide a mandatory explanation for the update.

In addition, the **Further Review Parameters** section becomes visible. This section helps assign responsibility and timelines for the next review stage:

- **Review Level** – select the appropriate review level (*Next, Final, Sponsor*).
- **Designee** – assign the next reviewer by selecting a user from the study's list of individual users (user groups are not supported yet). Make sure that selected user was given access to the module and granted the privileges.
- **Due Date** – select the deadline for the next review.

These parameters ensure that every Active issue has a defined owner and a clear timeline for resolution.



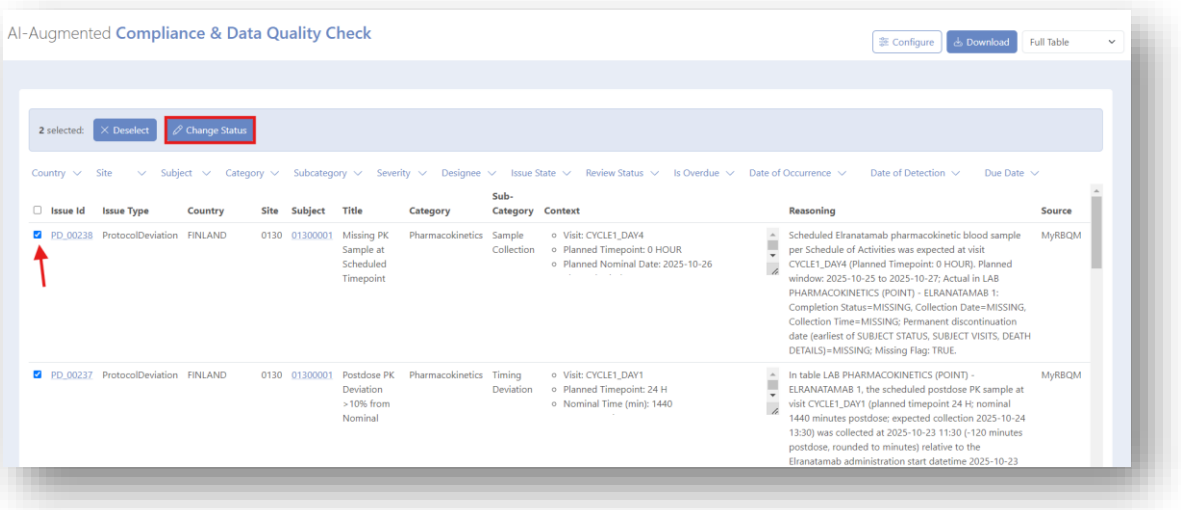
Completing an Issue

If you set the New Issue State to **Completed**, a simplified set of fields is shown:

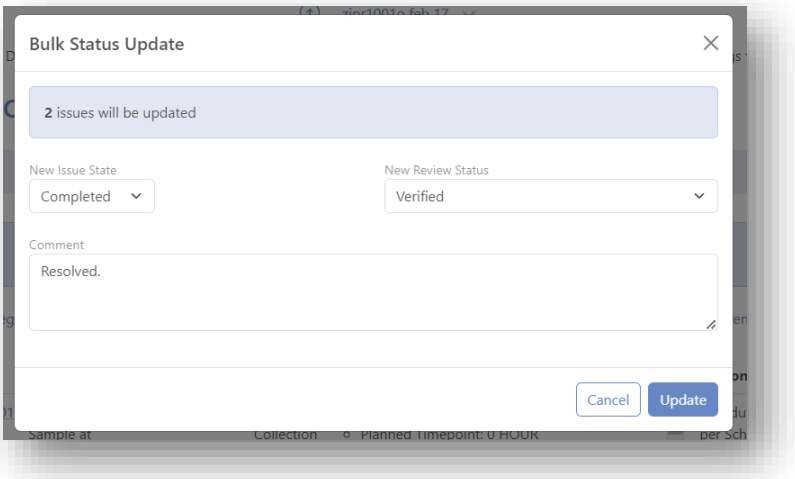
- **New Review Status** – choose either *Verified* or *Rejected*.
- **Comment** – provide the mandatory explanation for completing the issue.

This ensures that the final disposition of the issue is clearly documented.

To perform a **bulk update**, select all issues in the overview table that require a status change, then click **Change Status** in the section that appears above the table.



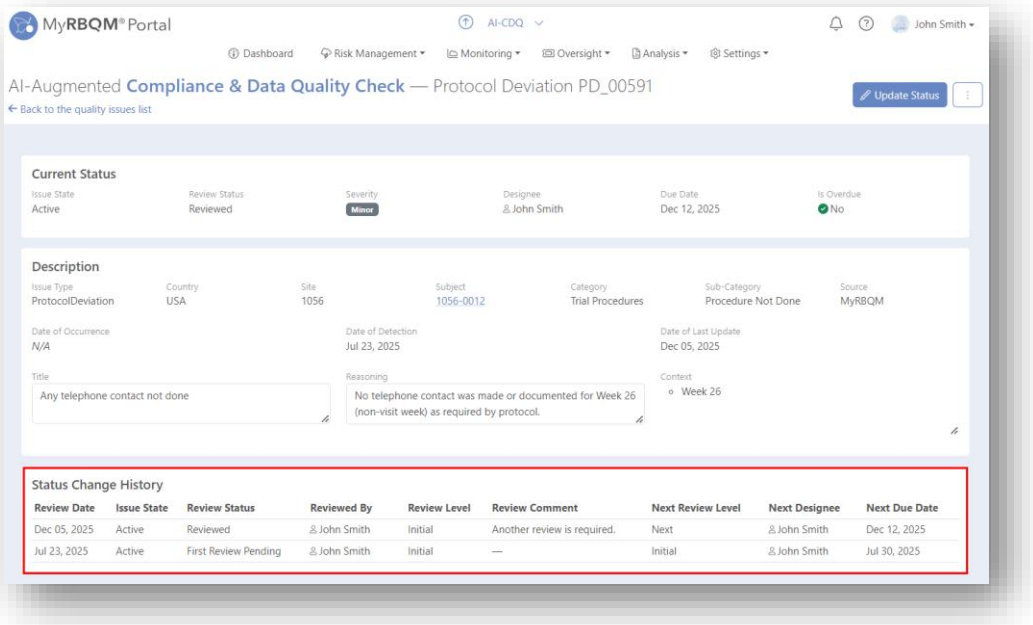
In the **Status Update** window, set the new parameters similarly to editing a single issue. The newly set parameters will be applied to all selected issues, regardless of their current status.



NOTE: Bulk status update is only available in the **Full Table** and **Condensed Table** display modes.

Every time you perform a **Status Update**, the action is recorded in the study audit trail under the action name **Update Compliance & Data Quality Issue Status**. This ensures full traceability of all decisions and changes made to the issue.

In addition, each successful status update automatically appears in the **Status Change History** section on the **Issue Details** page (as shown in the image below). This allows users to easily track the progression of the issue, understand who performed each update, and review how the issue evolved over time.



This streamlined workflow ensures that every update to an issue is consistent, auditable, and aligned with the study's review processes.

Risk Control

Risk Control – Explanation

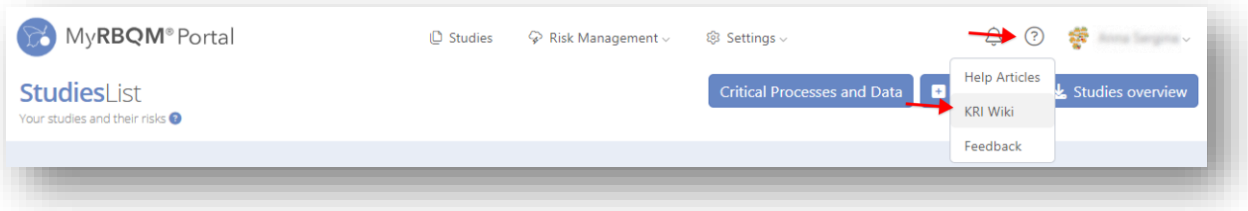
Controlling risks is the process of overseeing risks to timely identify and prevent foreseeable and new risks, control risk occurrence, and validate risk response efficacy during the study conduct phase.

Risk monitoring and control is not a novelty in clinical trials. However, risk control was lacking a systematized procedure for a sound deployment in clinical research.

In order to apply a systematic approach to risk-based quality management, clinical trials rely on "risk indicators". A risk indicator could be defined as a metric used to measure a specific risk, with its relevant control limits (thresholds) and alerts. These alerts are signals sent to the risk owner and relevant team members that are triggered when a pre-defined risk level or threshold has been reached. Sometimes, identified risks are not clearly linked to the risk indicators used by a monitor. The relationship

between critical metrics and potential risk indicators should have been established already in the clinical study planning phase.

NOTE: Cyntegrity provides MyRBQM users with suggestions of the Risk Indicators that can be used for Risk control via KRIWIKI (Help icon → KRI Wiki).



To fill this gap, a coherent procedure has been developed in which each risk that has been identified and assessed by RACT+, has been listed in a risk register with the assigned KRI (Key Risk Indicators) and their respective RPN. This procedure enhances monitoring efficiency and medical data review by clearly highlighting those data of highest risk. This risk register provides clear instructions on risk monitoring and risk control measures, comprising the required responses to risks (mitigating and corrective actions).

The timely implementation of actions to ensure risk control requires an unambiguous risk communication plan in which all involved team members are informed about their roles, responsibilities and respective communication channels.

Each study team member must be aware of what group of risks is assigned to his/her area of competence. Each risk should be clearly assigned to an accountable **risk owner**. In order to facilitate these assignments, risks might be categorized (as per @RACT+, integrated into **MyRBQM® Portal**) in groups according to knowledge areas or functions.

Each risk must be measurable, via a KRI, and have clearly defined risk tolerance or control limits as reference thresholds. Once a KRI is close to reaching a threshold, an alert should be triggered. This should happen timely for the effective prevention of threats. Additionally, the timelines for regular risk monitoring and reporting should be clarified.

The type of alerts, the IT systems, and the communication method (i.e., phone call, automated email notifications, online platforms, etc.) should be well-known. Likewise, the clinical study team must have an available description of actions and procedures to follow (i.e., root cause analysis, investigation of serious issues or corrective and preventive actions (CAPA)).

Cyntegrity fine-tuned the online platform **MyRBQM® Portal**, an automated system that continuously scans the clinical study database (comprising all type of data captured by means of electronic data capture - EDC -, comprising the eCRF, ePRO or even eTMF, if available),

checks risk control thresholds for each data type, and triggers alerts to the relevant study team members (or risk owners) if any threshold has been reached or exceeded. Thus, **MyRBQM® Portal** deploys KRI with a statistical engine that detects data anomalies of statistical nature. The deviations from risks and quality control limits, typically depicted in summary tables, are now enhanced by automated risk alerts and streamlined visualizations that prioritize risks according to their respective RPN. In some cases, multiple KRI have been used to monitor a single risk, based on the risk priority, to enable closer monitoring.

Cyntegrity developed an issue management system (ticketing system) based on KRI assisted by the statistical engine. Each time that **MyRBQM® Portal** detects that a KRI reaches the defined risk threshold, the system triggers an automated alert, an email communication to the person that has been assigned as risk owner. Thus, immediate risk alerts are distributed to the relevant study team members avoiding delays caused by manual checks and manual communications. The issue management system is designed to document, track, and share all preventive and corrective actions, root cause analyses and contingency plans, which are related to an issue with the relevant team. The **MyRBQM® Portal** cloud solution allows a team to timely and efficiently deal with expected and unexpected risk events. Moreover, it provides the essential audit trail, enabling to present a plausible story to auditors: when the

issue was triggered, who was involved in its mitigation and what actions were taken.

Two different alert threshold levels have been defined for most KRI:

- **Medium risk alert threshold** – The risk is still under control (risk lower/upper control limits not yet reached), however, there is a relevant increase in the probability of the risk to materialize. This alert informs about the need to deploy **preventive** actions.
- **High risk alert threshold** – The risk has reached the lower or upper-risk control limit and **corrective** actions should be implemented without undue delay.

As an example, assuming that for the KRI named rate of screening failures too high, the risk control limit is 15% subject screening failures at a site:

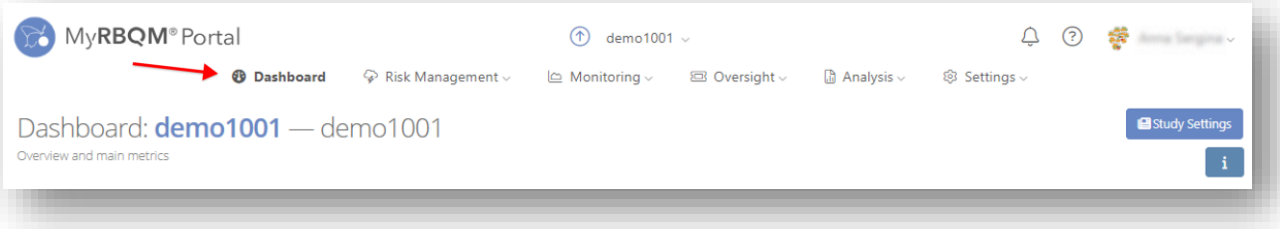
- **Medium risk** - KRI threshold is within the risk control limits, e.g., the warning signal will be displayed if 10% screening failures have been observed.
- **High risk** - KRI threshold is exactly on or above the risk control limit, e.g., the warning signal will be triggered if 15% screening failures have been reached or exceeded.

The selected KRI thresholds must be documented in a KRI Register. KRI thresholds will be determined prior to planning the actions to be implemented, given that risk

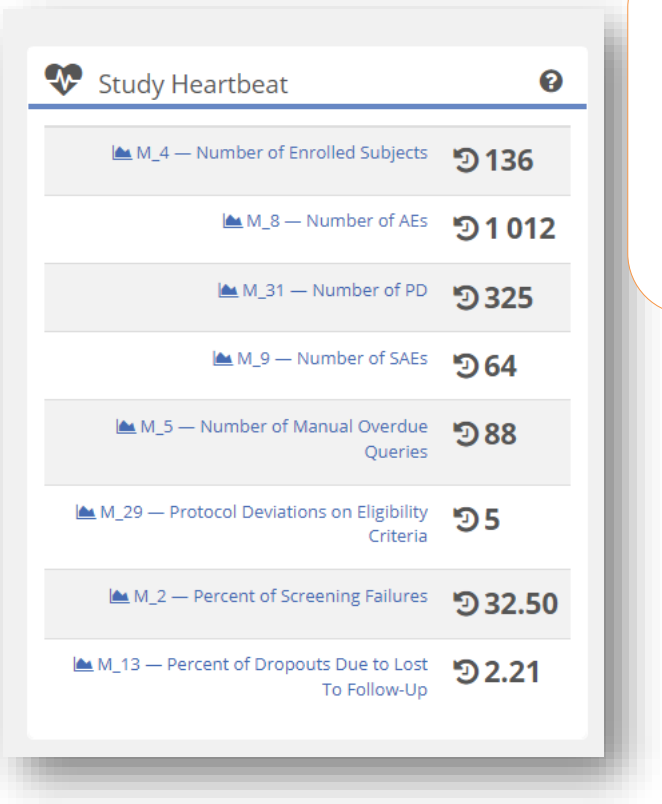
tolerability will influence the selection of the most suitable preventive and corrective actions (risk response).

An appropriate frequency and method, system or IT tool for the monitoring of each KRI is defined in the KRI Register. KRI related to high risks must be closely monitored, as a minimum on a weekly basis, to ensure effective risk mitigation (e.g., critical risks need to be reported immediately to the Data Safety Monitoring Board) and prompt implementation of actions if necessary.

The Main Dashboard



Study Heartbeat



The **Study Heartbeat** is the main summary of the most important metrics that are pre-selected for a trial.

Study Predictions

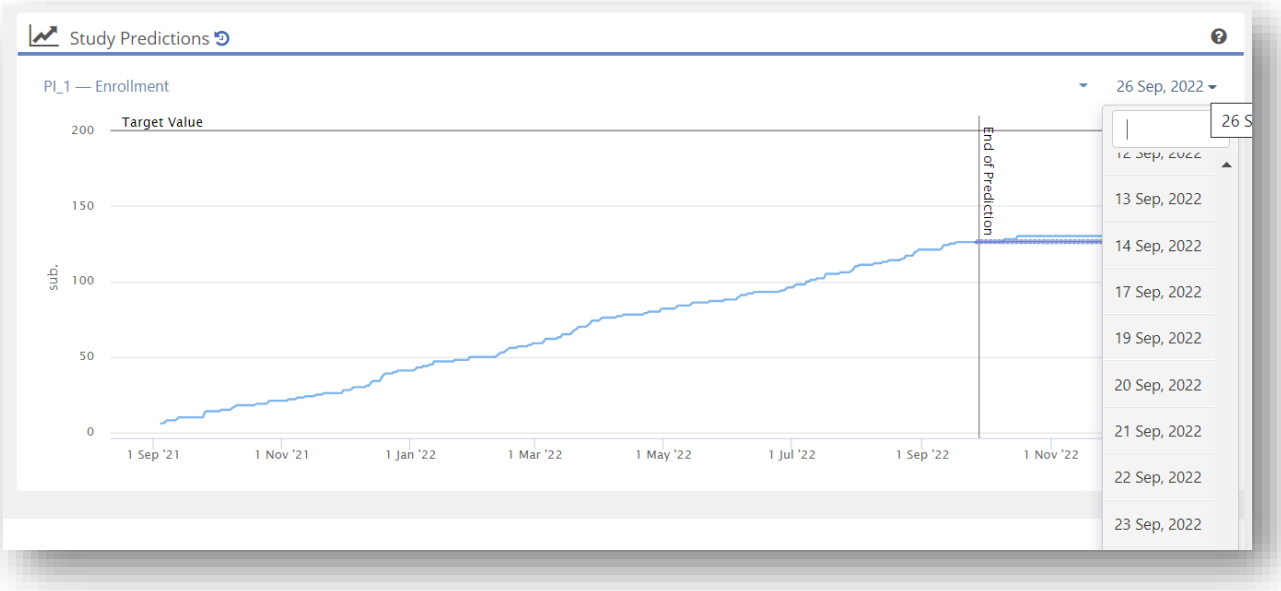
The **Study Predictions Graph** shows various chosen Prediction Indicators (PI) on a time axis with data prediction.

- Y-axis – value of a chosen PI
- X-axis – weeks/months/years (depends on chosen time periods)
- Target value – a pre-configured boundaries allow you to control the target values (available not for all PIs)

- End of prediction – a pre-configured final deadline of a clinical trial.

The choice of the date in the top right corner allows you to test the prediction accuracy retrospectively in the past vs. the currently available actual data.

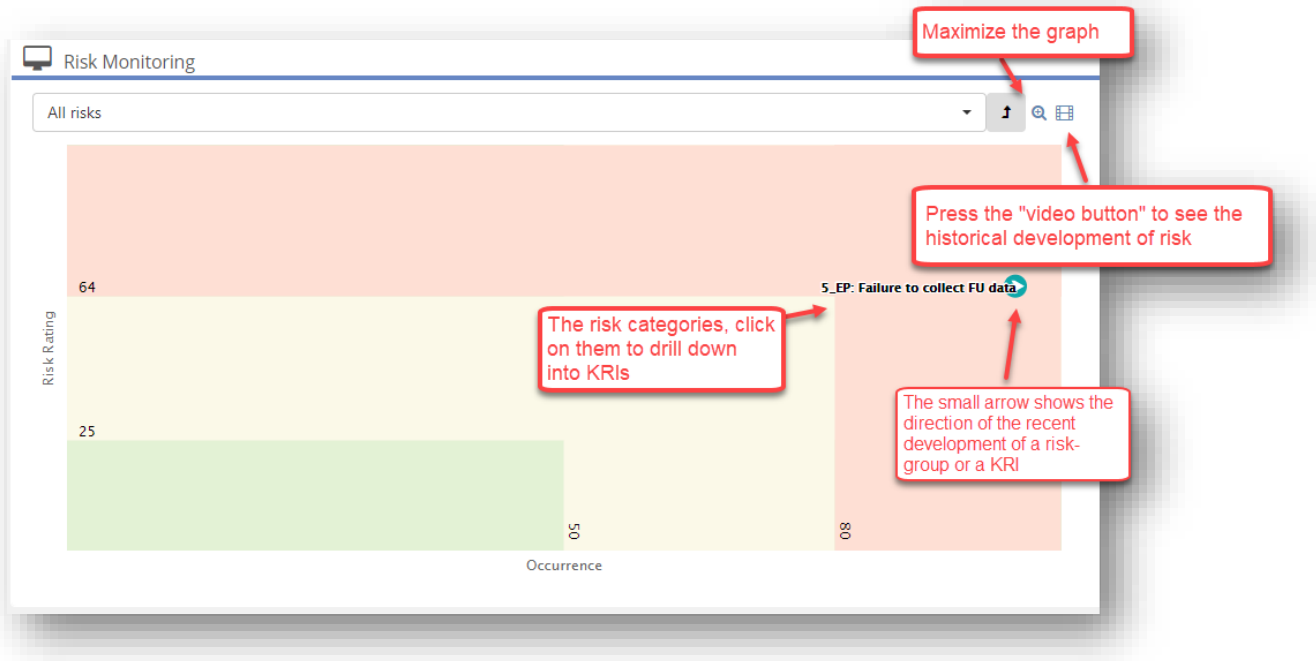
NOTE: If too few data for the prediction's calculation are available, the user will be informed.



Risk Graph – Understanding and Interpreting

The risks on the risk graph in the Risk Monitoring section are designed using the FMEA guidelines showing the risk indicators in Risk Rating vs. Occurrence.

The green zone shows the low-risk area, yellow shows the medium-risk area, and the red zone represents the zone of severe escalation.



Click the **Video** button in the right top corner to see the historical development of the risks.

FMEA Score Graphs – Understanding and Interpreting

The Risk rating graphs on the Dashboard allow capturing a different picture of the study's current status. Instead of simply accumulating the binary information about whether the threshold of certain risk indicators was breached, a special preprocessing step was introduced. This step allows users to investigate the status of sites for systematic behavior in the breaches of risk indicators.

A score for occurrence and risk rating is introduced.

The occurrence describes how often and how long thresholds were breached and takes into consideration past breaches as well. This way the score reflects systemic issues of a risk indicator and of individual sites.

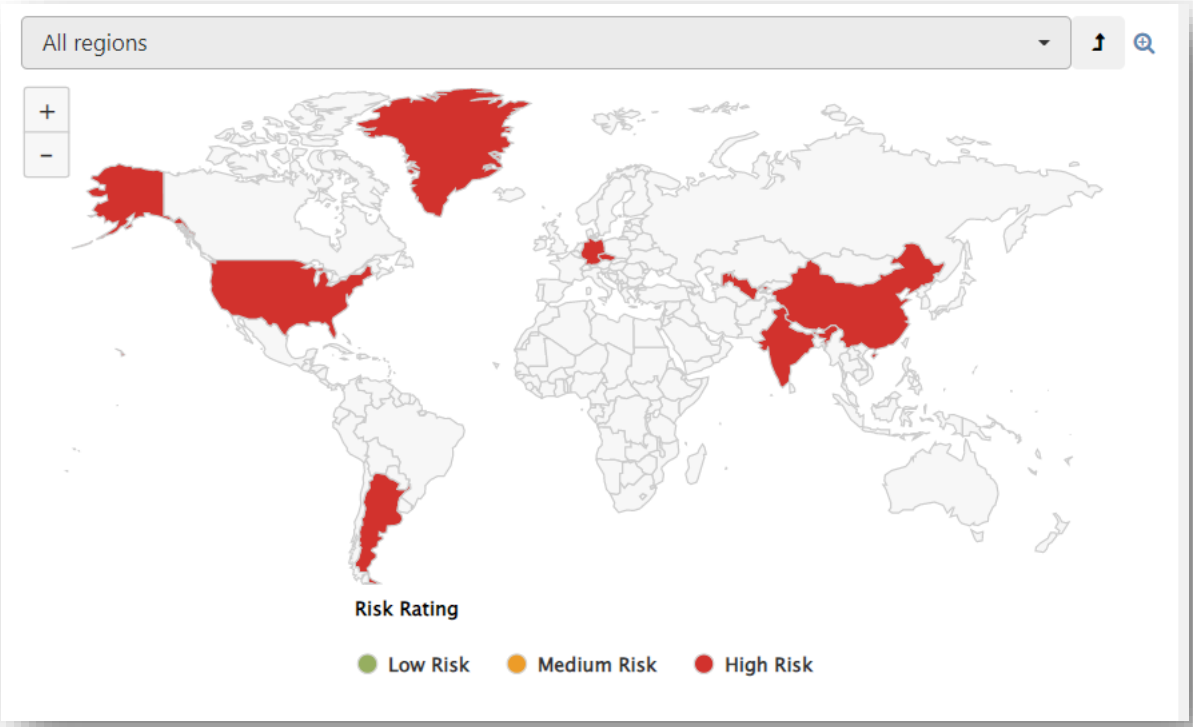
For example: a high occurrence score of a risk indicator suggests that the thresholds were breached by many sites and that the breaches are of systematic nature.

The Risk Rating score can be viewed by choosing a concrete risk indicator in the Risk Monitoring section and in the Site-to-Site Comparison section (breakdown by sites).

If a risk is selected instead, the graph in the Risk Monitoring section represents the mean occurrence and risk rating of each affected site and indicator.

If nothing is selected in the FMEA overview graph (Risk Monitoring section), an overall mean risk is displayed.

Geographical Risk Presentation



MyRBQM® Portal can present the risks by geographical region.

Clicking on any risk in the risk graph (Risk Monitoring Section), will display the updated distribution of the risks among countries that are involved in the study.

You can select any country from the drop-down list or click the map.

In the Site-to-Site Comparison, you will see the highlighted sites from this country or region.

Site-to-Site Comparison Section – Understanding and Interpreting

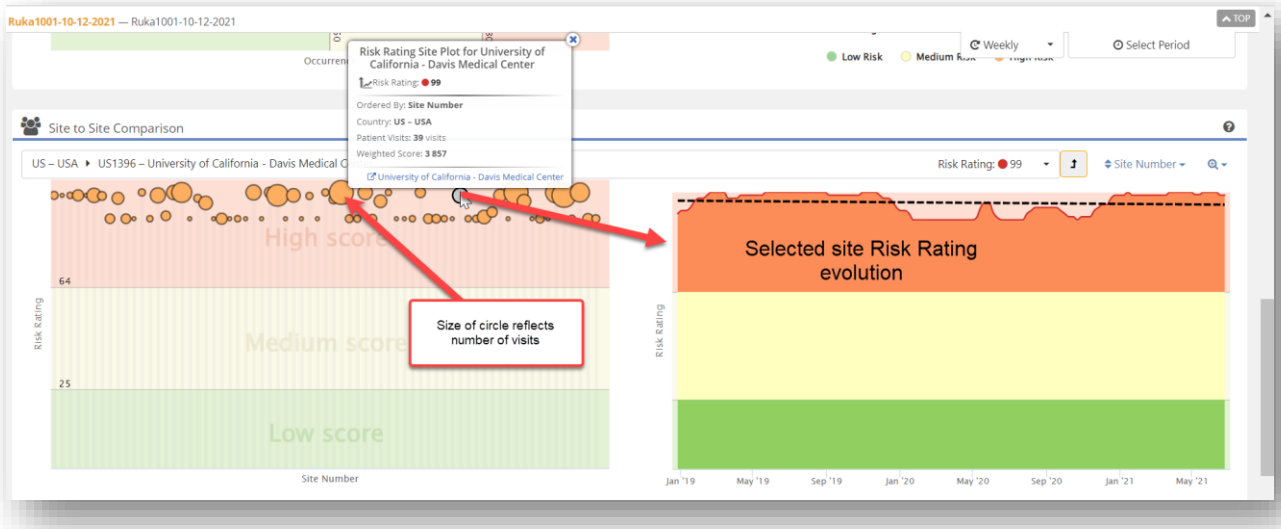
The Site-to-Site Comparison is useful for understanding which sites are classified by which risk levels. This information is required for targeted and triggered monitoring.

The size of the "bubble" represents the number of visits (key metric).

By clicking on a site bubble, the historical development of the risk rating will appear near the Site-to-Site Comparison graph.

To choose a different sorting presentation of the sites, see the top right corner.

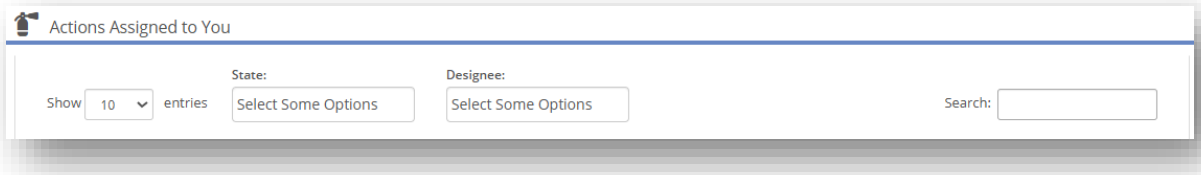
By hovering with a mouse over a site bubble, a Tooltip with the detailed information appears. From there, you can enter the detailed Site Profile.



Actions in the Main Dashboard

On the main Dashboard, all actions assigned to you or your groups, based on risks (risk mitigations) and on tickets (investigative/corrective actions and preventive actions) are listed in a table.

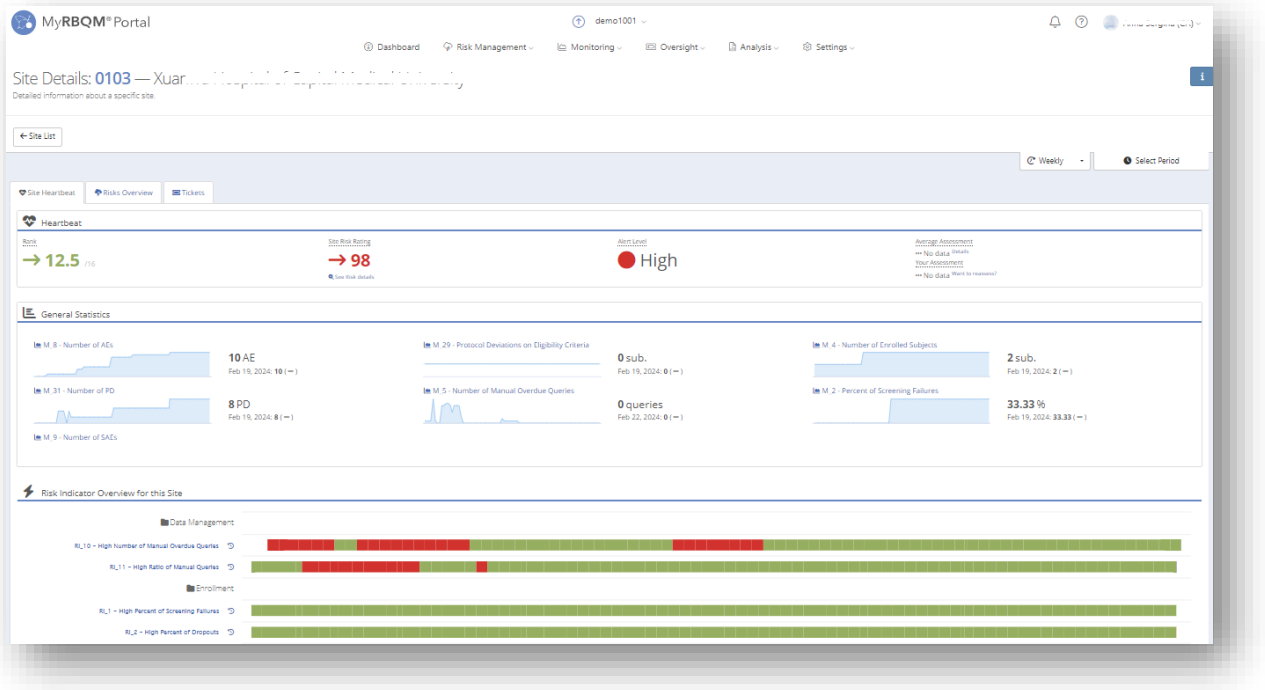
Filter actions by their **State** and/or **Designee**.



Sites

Site Profiles – Understanding and Interpreting

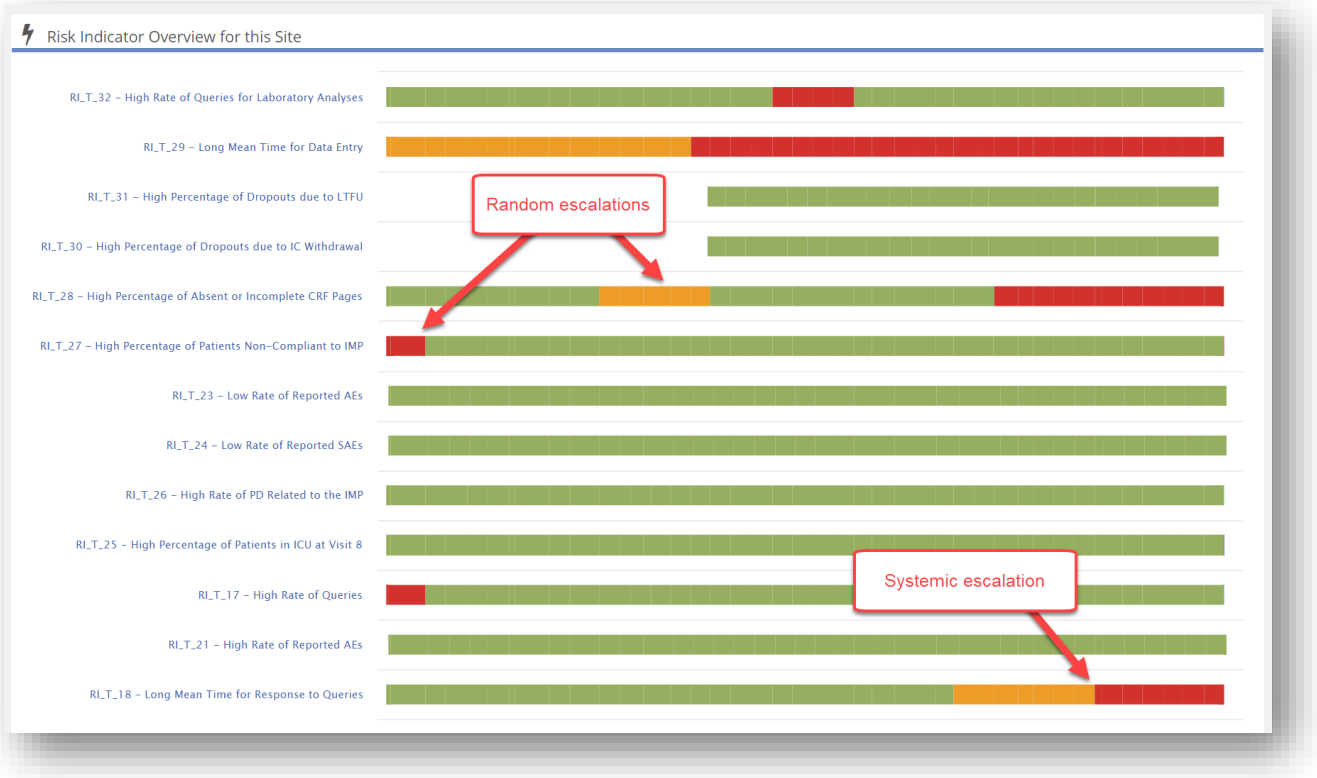
To access the **Sites** page go to **Oversight → Sites.**



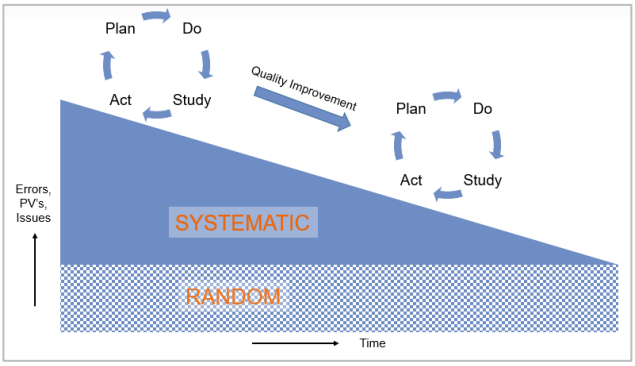
MyRBQM® Portal creates detailed profiles for each clinical site (**Sites** page → **Select a site** → **Site Details** page):

- Site profiles provide information about the performance, quality and risk profile of a site.
- This information helps to adjust monitoring activities and to document the personal evaluation of a CRA or clinical project manager.

- Site profiles contain the performance indicators, tickets for the selected sites and risk indicators with a historical overview.



- The Historical Overview graph is important to see which KRI escalations happen systematically, and which happen randomly. The focus of a CRA must be on systematic escalations first because illuminating the systematic issues brings the largest quality improvement effect for a clinical trial:



Site Risk Rank.

Why max rank of 62.5?

How are ties resolved?

What is better: 1 or 62.5?

Description

The FMEA scores of a site are ranked. This means that all sites are sorted by their FMEA score (from highest to lowest), and the rank represents the position in this list. A rank of 1 represents the highest FMEA score on the list.

Several sites can have the same FMEA score. This is called a "tie". A tie is resolved by giving each involved site the same rank. **MyRBQM® Portal** uses the highest rank of the tied group and a .5 is appended to the number to indicate a tie.

As an example: a rank of 2.5/10.5 means that the current site is ranked with the second highest risk rank, but has ties, so other sites share the same rank. The number

following the '/' character represents the maximum of all ranks. In this case, the maximum rank is 10.5 and there are several sites who share the same rank.

Example 1 (all scores show a tie)

FMEA scores of a site: 1, 1, 2, 2, 4, 4

Ranks of FMEA scores: 5.5, 5.5, 3.5, 3.5, 1.5, 1.5

Example 2 (some scores show a tie)

FMEA scores of a site: 1, 500, 530, 30, 30

Ranks of FMEA scores: 5, 2, 1, 3.5, 3.5

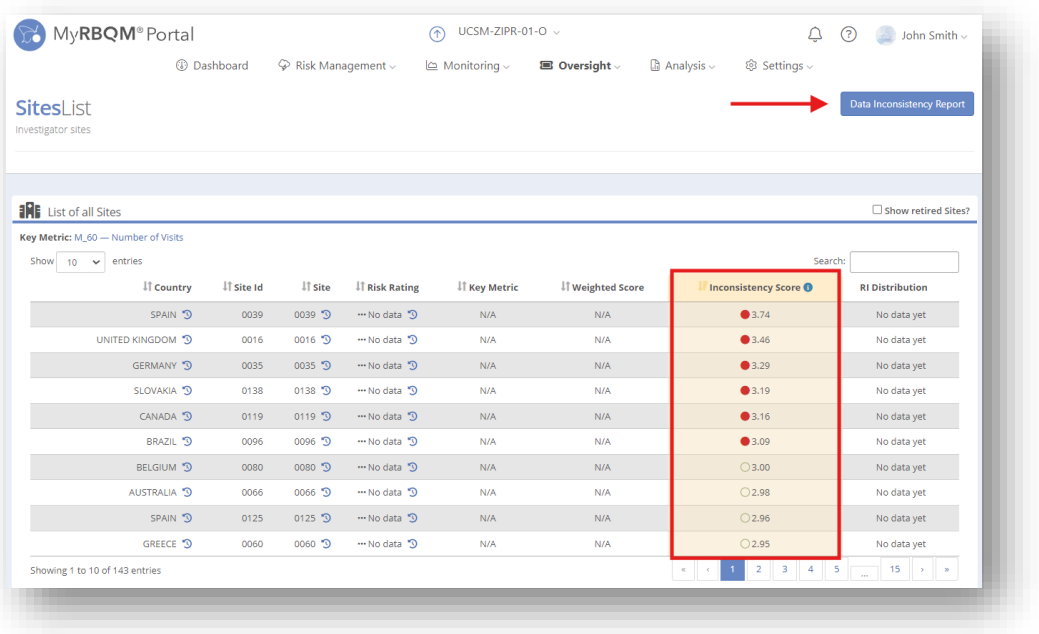
Sites Data Inconsistency Score Report

The **Sites Data Inconsistency Score Report** helps to identify sites whose data distributions and/or time patterns differ from the study-wide reference more than expected by random variation.

In other words, it is designed to find sites that "look different" (too high/low, unusual spread, odd visit timing trends), so you can check for process issues, measurement differences, or data problems.

To access the report navigate to the **Sites List** page and click Data Inconsistency Report. The **Combined Data Inconsistency score (Z-score)** per site is displayed in

the sites overview table and indicates standardized distance from the reference (the higher the score the more unusual the site behaves).



How to read the report

1. Start with the **Combined Z-score chart**: pick the sites above the confidence threshold.

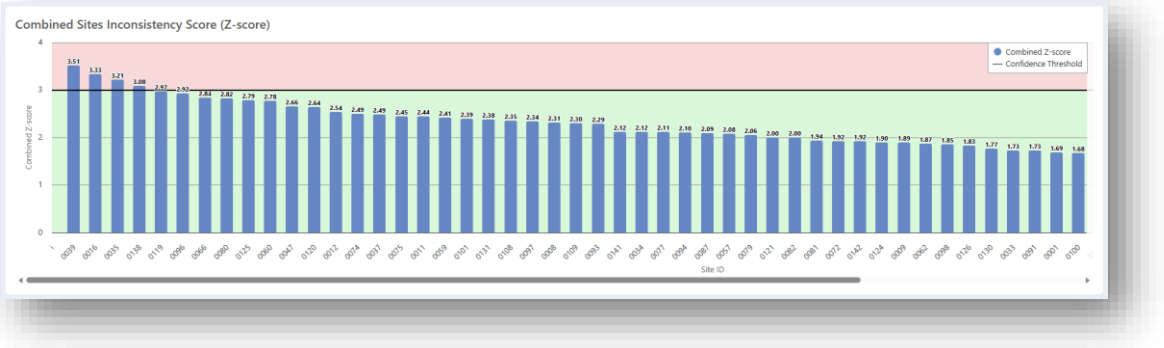
2. Use the **Overview heatmap table**: see which test(s) drive the site's overall score.

3. Click a cell: the **Statistical Test Details** section updates to explain that specific signal (distribution or time trend).

4. Interpret with context: confirm if differences are clinically plausible or suggest data capture / lab /

operational issues.

Chart 1 — Combined Sites Inconsistency Score (Z-score)



What you see

- A bar chart by Site ID, sorted from highest to lowest.
- A horizontal "Confidence threshold" line (value 3).
- Background shading indicating "below vs above threshold".

How to interpret

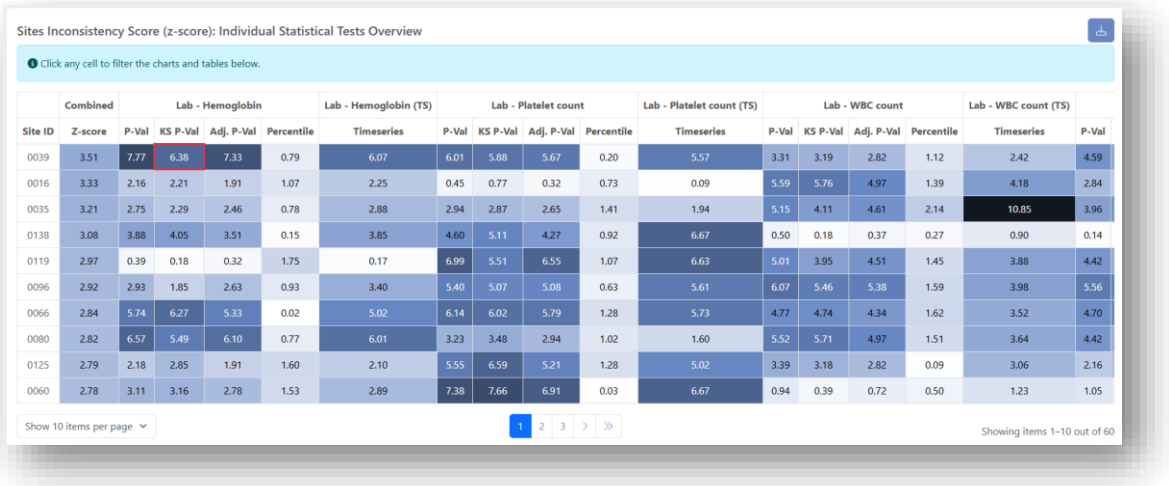
Z-score = standardized distance from the reference (in SD units). Higher Z-score ⇒ more unusual site overall.
Example intuition: Z = 3 means "about 3 standard deviations away" (rare under normal assumptions).

Use this chart to **prioritize**:

- Above threshold: investigate first.

- Just below threshold: monitor, especially if trending up over time.

Table 1 — Individual Statistical Tests Overview (heatmap table)



	Combined	Lab - Hemoglobin				Lab - Hemoglobin (TS)	Lab - Platelet count				Lab - Platelet count (TS)	Lab - WBC count				Lab - WBC count (TS)	
Site ID	Z-score	P-Val	KS P-Val	Adj. P-Val	Percentile	Timeseries	P-Val	KS P-Val	Adj. P-Val	Percentile	Timeseries	P-Val	KS P-Val	Adj. P-Val	Percentile	Timeseries	P-Val
0039	3.51	7.77	6.38	7.33	0.79	6.07	6.01	5.88	5.67	0.20	5.57	3.31	3.19	2.82	1.12	2.42	4.59
0016	3.33	2.16	2.21	1.91	1.07	2.25	0.45	0.77	0.32	0.73	0.09	5.59	5.76	4.97	1.39	4.18	2.84
0035	3.21	2.75	2.29	2.46	0.78	2.88	2.94	2.87	2.65	1.41	1.94	5.15	4.11	4.61	2.14	10.85	3.96
0138	3.08	3.88	4.05	3.51	0.15	3.85	4.60	5.11	4.27	0.92	6.67	0.50	0.18	0.37	0.27	0.90	0.14
0119	2.97	0.39	0.18	0.32	1.75	0.17	6.99	5.51	6.55	1.07	6.63	5.01	3.95	4.51	1.45	3.88	4.42
0096	2.92	2.93	1.85	2.63	0.93	3.40	5.40	5.07	5.08	0.63	5.61	6.07	5.46	5.38	1.59	3.98	5.56
0066	2.84	5.74	6.27	5.33	0.02	5.02	6.14	6.02	5.79	1.28	5.73	4.77	4.74	4.34	1.62	3.52	4.70
0080	2.82	6.57	5.49	6.10	0.77	6.01	3.23	3.48	2.94	1.02	1.60	5.52	5.71	4.97	1.51	3.64	4.42
0125	2.79	2.18	2.85	1.91	1.60	2.10	5.55	6.59	5.21	1.28	5.02	3.39	3.18	2.82	0.09	3.06	2.16
0060	2.78	3.11	3.16	2.78	1.53	2.89	7.38	7.66	6.91	0.03	6.67	0.94	0.39	0.72	0.50	1.23	1.05

What you see

- Rows = sites
- Columns grouped by domain/parameter (e.g., Lab Hemoglobin, Platelet count, WBC count, Neutrophils, etc.)
- Within each group you typically see:
  - P-Val
  - KS P-Val
  - Adj. P-Val
  - Percentile
  - For some tests: Timeseries (TS)

How to interpret the color + numbers

Darker cells = stronger signal (more inconsistent vs reference) for that statistic.

Click any cell to open the exact supporting plot below.

higher = more significant.

Once a Z-score exceeds conventional significance thresholds (around 3), further increases primarily indicate greater statistical certainty rather than proportionally greater practical severity. In applied site inconsistency, Z-scores beyond this range are therefore better interpreted as confirming the presence of inconsistency rather than scaling its magnitude.

Empty cells are shown for those sites and statistics that have too less values to be statistically meaningful.

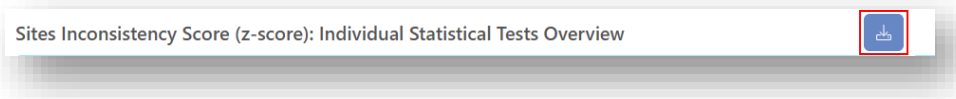
Column meanings

Column	Statistical meaning	Plain-language meaning
P-Val	Evidence against "site matches reference" for a selected test	"How unlikely is this difference if the site were normal?"
KS P-Val	P-value from Kolmogorov–Smirnov test	"Does the whole distribution look different (not just the mean)?"

	(distribution shape difference)	
Adj. P-Val	P-value adjusted for multiple comparisons (controls false positives)	"Significance after correcting for many tests/sites"
Percentile	A percentile-based extremeness comparison (site vs reference)	"How different is this the two tails of site's distribution compared with others/reference?"
Timeseries (TS)	Time-pattern anomaly score (based on model vs observed over visit time)	"Does this site's trend over time look unusual?"

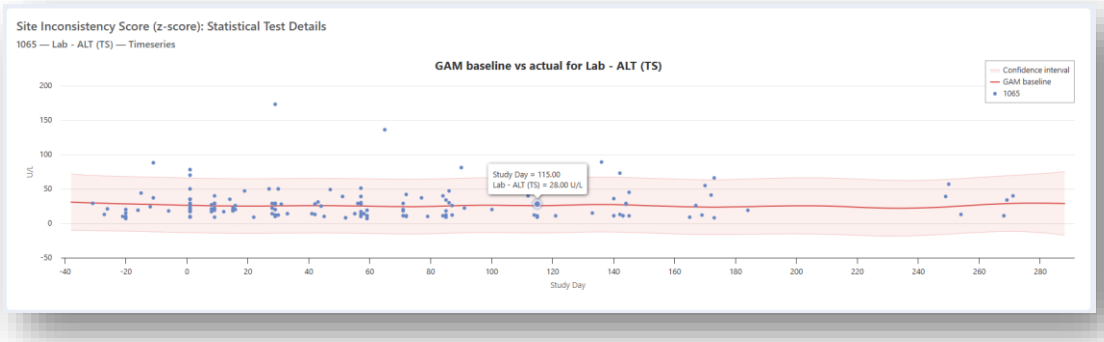
Export Data

The table with all sites can be exported as csv file by clicking the download button in the header of the table.



Section — Statistical Test Details (updates when you click a cell)

A) Timeseries details — "GAM baseline vs actual … (TS)"



What you see

- Scatter points for the selected site across relative study day / data value.
- A smooth baseline curve labeled GAM baseline (Generalized Additive Model).
- A shaded 95% confidence interval band around the baseline.

How to interpret

- If points mostly stay within the band: site follows the expected time pattern.
- If points systematically shift above/below the baseline: possible site-specific bias (e.g., consistently higher values).
- If deviations appear only in certain time windows: possible phase-specific issue (startup training, device change, local lab change, visit scheduling artifacts).

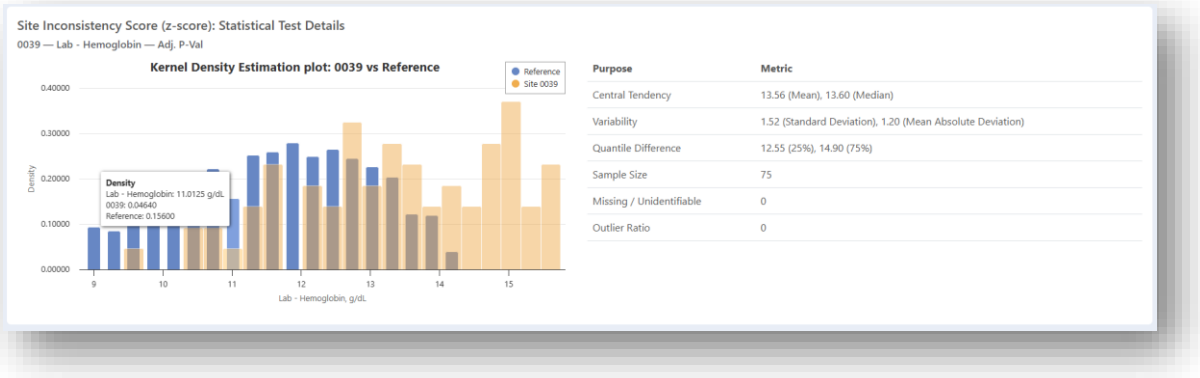
- Wider confidence band typically means less information / more uncertainty in that time region.

Typical follow-ups

Check lab vendor / calibration, collection timing, unit conversions, visit window handling, data entry delays, protocol deviations at that site.

B) Distribution details — "Kernel Density Estimation plot: Site vs Reference"

(Shown when selecting **P-Val** or **Adj. P-Val**)



What you see

- Overlaid **density/histogram-like** distributions:
  - **Reference** (all other sites or pooled data)
  - **Selected site**
- A small summary table with metrics such as:
  - **Central Tendency** (mean/median-like)

Mean < Median: left/negative skew; investigate low values.

- **Variability** (Standard Deviation, Mean Absolute Deviation)
  - Standard deviation ≈ Mean Absolute Deviation: variability is evenly distributed; few extreme values.
  - Standard deviation >> Mean Absolute Deviation: large number of outliers and heavy tails

- **Quantile Difference (25% and 75%)**
- **Sample Size**, **Missing/Unidentifiable**
  Number of data points with NA values
- **Outlier ratio (%)**
  Percentage of data source values which are 3*1.4826·MAD from median

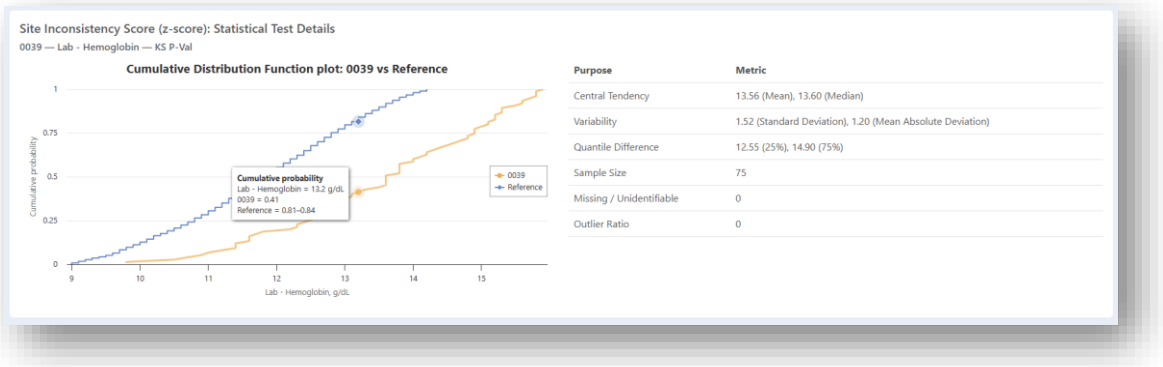
How to interpret

- Shift left/right: site has lower/higher typical values.
- Narrower/wider shape: site has less/more variability than reference.
- Different shape (skew/multimodal): may indicate mixed populations, data mixing, measurement/process differences, or data quality issues.

- Small sample size: treat signals cautiously (higher noise / instability).

C) Distribution details — "Cumulative Distribution Function (CDF): Site vs Reference"

(Shown when selecting **KS P-Val** and also in the Percentile example.)



What you see

- Two step-like curves:
  - Reference CDF
  - Site CDF
- The KS test is driven by the maximum vertical gap between these curves.

How to interpret

- Curves overlap closely: distributions are similar.

- Consistent separation across the range: systematic difference (location/scale).

- Separation mainly in tails: site differs in extremes/outliers (e.g., unusually high values).

- Largest vertical gap point: where the site diverges most from reference.

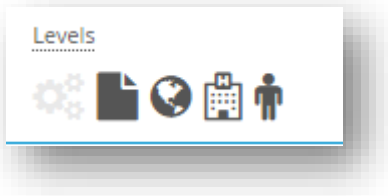
Metrics

Metric List

To explore the list of Metrics available in a Study, go to **Monitoring → Metrics.**

Metric is a measurement of a property from data. It contains no information about the thresholds yet. A KRI unites a metric (or even several), a risk and typically one or two thresholds.

- Load metrics and explore the list.
- The same metric can be captured on different levels: patient, study, program or even country levels.

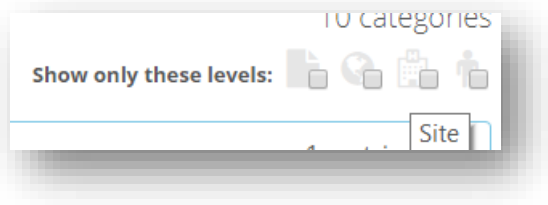


- Metrics are grouped by Categories, e.g., enrollment or data quality.

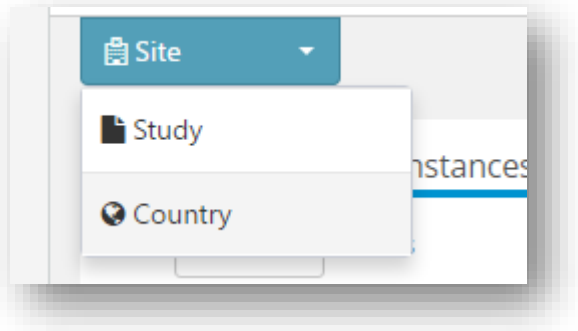
- Search or filter the metric list as required.

Metric – Overview

1. Open a metric from the **Metrics Overview** grouped in categories.
2. Sort metrics by level.



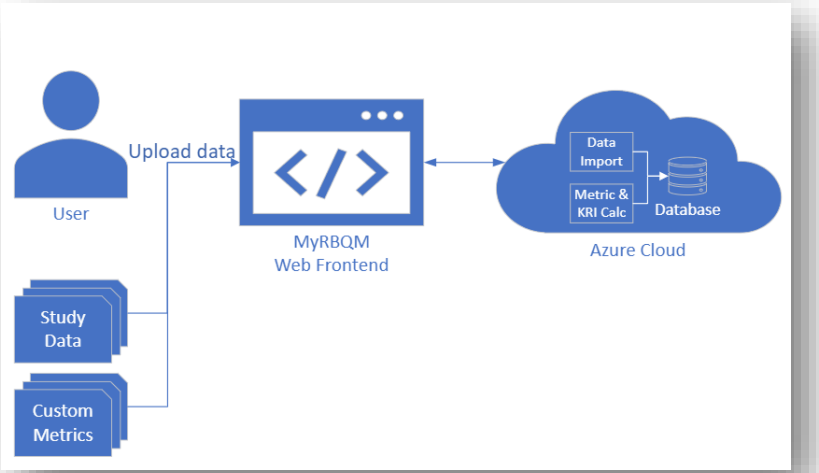
3. Choose on what level/entity you want to explore this metric, e.g. on site level.



4. Using the Search function, find the sites that are most interesting for you and click **Add to Details and Comparison**.
5. The metric for this site will appear below.
6. Toggle the presentation by selecting different modes  .
7. Click **Load Predictions** to get information on how a metric is expected to develop in the future.

Configuring Custom Metrics

Custom metric data can be a crucial part of your study data, allowing you to track various custom metrics over time. To ensure successful data management, follow the guidelines outlined below when uploading and structuring custom metric data files.

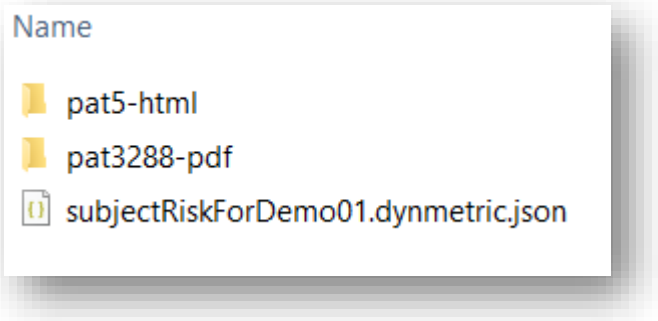


NOTE: It is important to follow specific guidelines when preparing and uploading these files.

File Naming Convention

- **Filename:** Each custom metric data file should have this format: <UniqueMetricName>.dynmetric.json.
- File Extension: The file extension must always be .dynmetric.json.

- **Unique Metric Name:** The <UniqueMetricName> must be a distinctive name for your metric and must not contain underscores. It should be unique across all custom metrics.
- **Zip Archive:** To upload your custom metric data, you must create a zip archive containing all the relevant .dynmetric.json files. This zip archive should also include other study data files, if applicable.



Example file structure of the zip archive

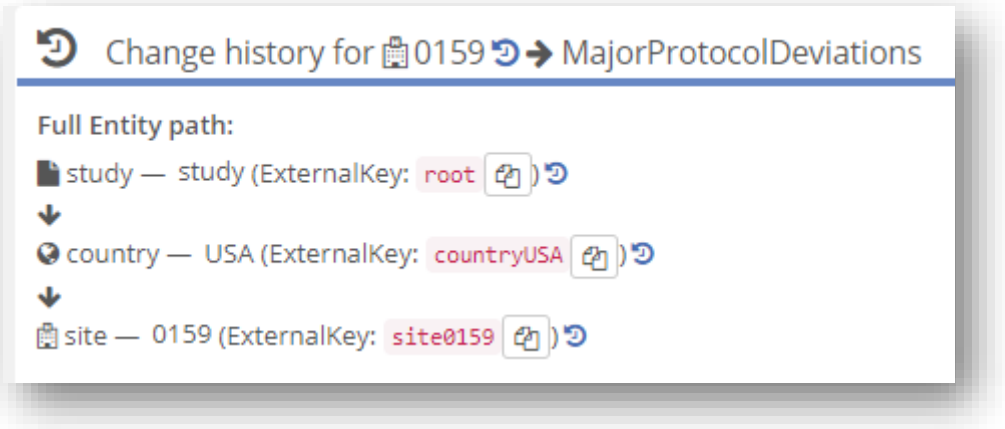
File Structure and Content

Each *.dynmetric.json file should adhere to the following structure:

```
{
   "Data": [
      {
          "ValueTime": "<Timestamp>",
          "EntityType": "<Entity>",
          "ExternalKey": "<Key>",
          "DataPoint": {
             "Value": <Value>,
             "Reports": [
                {
                  "RelativeFilePath": "<RelativeFilePath>",
                  "Name": "<Name>",
                  "Description": "<Description>",
                  "MimeType": "<MimeType>",
                  "IsRoot": <IsRoot>
                },
              // Additional reports can be added here
              ]
          }
      },
      // Additional data points can be added here
   ]
}
```

- The **root element** must be “Data” and is a list of metric data points.
- **<Timestamp>:** The timestamp represents the time of the metric value in ISO 8601 format (e.g., “2011-04-23T18:25:43.000Z”).

- **<Entity>:** The "EntityType" specifies the level of the metric data and can be one of the following: study, country, site, patient, or visit.
- **<Key>:** The "ExternalKey" should be in sync with the ExternalKey used in the study.



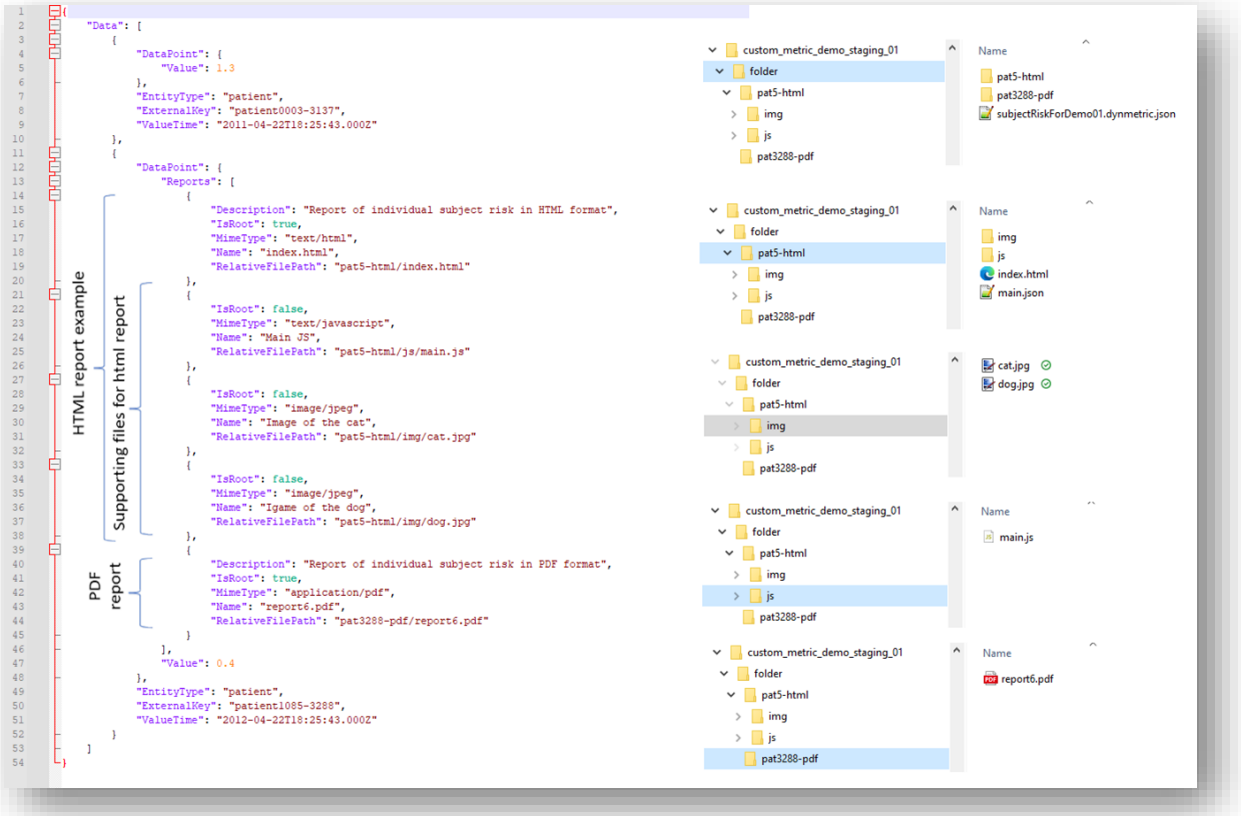
- **<Value>:** "Value" represents the actual metric value for the data point.

  ### Adding Reports

  You can include PDF and HTML reports associated with your custom metric data. These reports will be visible on the metric page. Each report should be structured as follows:

```
{
   "RelativeFilePath": "<RelativeFilePath>",
   "Name": "<Name>",
   "Description": "<Description>",
   "MimeType": "<MimeType>",
   "IsRoot": <IsRoot>
}
```

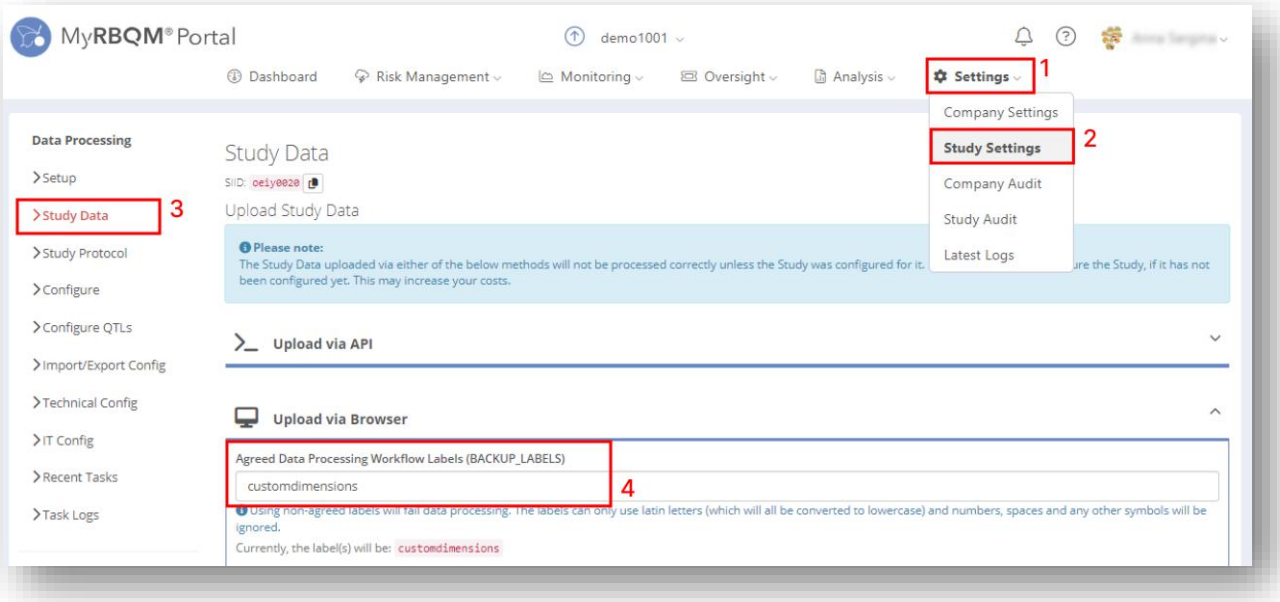
- **<RelativeFilePath> (mandatory):** The actual filename including the relative path of the report.
- **<Name> (optional):** The name of the report.
- **<Description> (optional):** A brief description of the report.
- **<MimeType> (mandatory):** The MIME type of the report (e.g., “text/html,” “application/pdf”).
- **<IsRoot> (mandatory):** Set to true if the report is the root report; otherwise, set it to false.
    - **IsRoot: true =>** core report file,
    - **IsRoot: false =>** supporting files for report (pics, scripts etc.)



Data Import

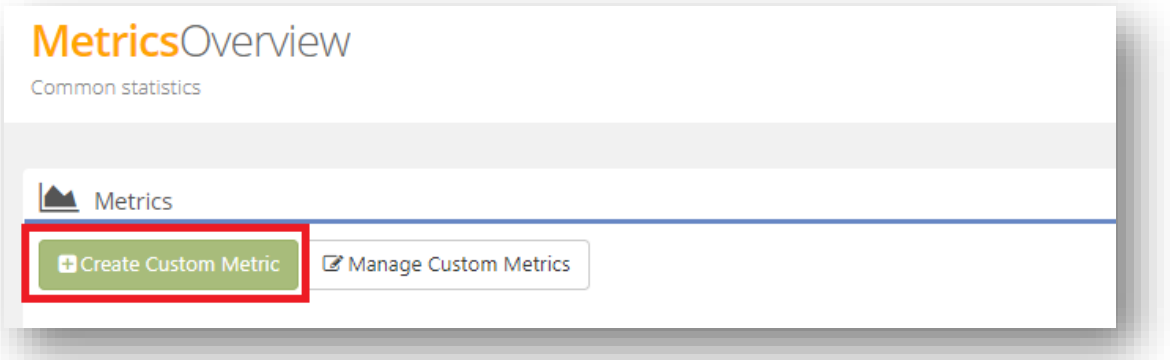
There are two ways to upload your zip archive containing all .dynmetric.json files and reports:

- Along with other study data through the regular data import process
- Separately, using **customdimensions** label in the data upload form field "Agreed Data Processing Workflow Labels" (as in the screenshot below). This will only import dynmetrics (and not other data) and will be quicker as the regular data import.

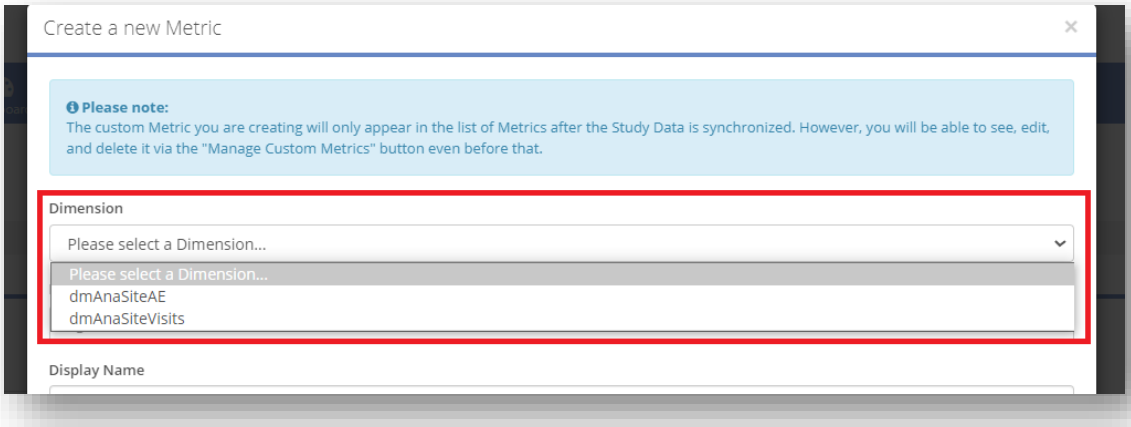


Create a Custom Metric

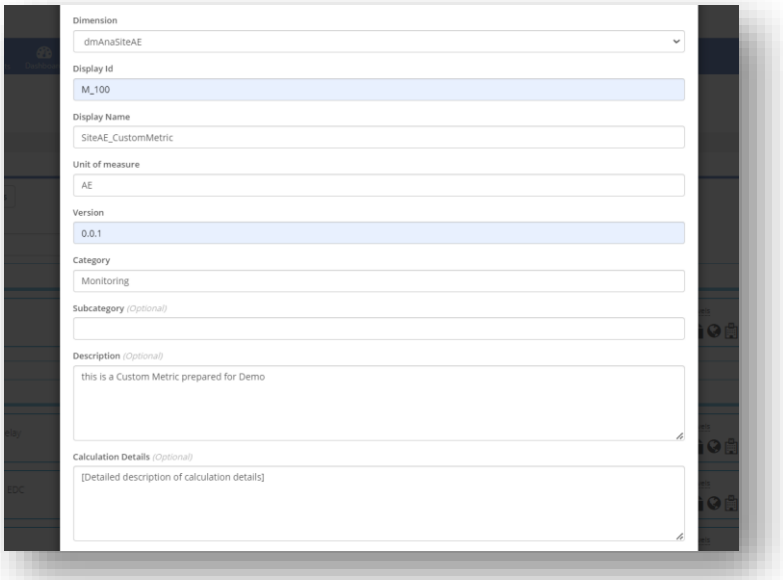
1. After a successful data import, navigate to the **Metrics** page and click **Create Custom Metric.**



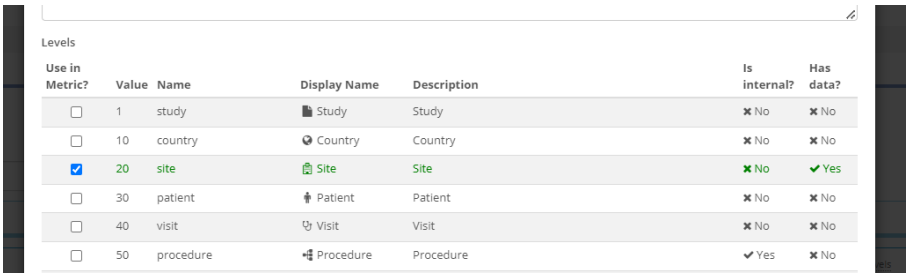
2. Select a Dimension among the ones that were uploaded as *.dynmetric.json* in the pop-up metric creation form.



3. Complete the rest of the fields. Some fields' placeholders suggest possible values as examples, but don't limit the users. Not mandatory fields are marked as *(Optional)*. **Unit of measure** and **Category** fields allow the user to select already existing values or create new ones:

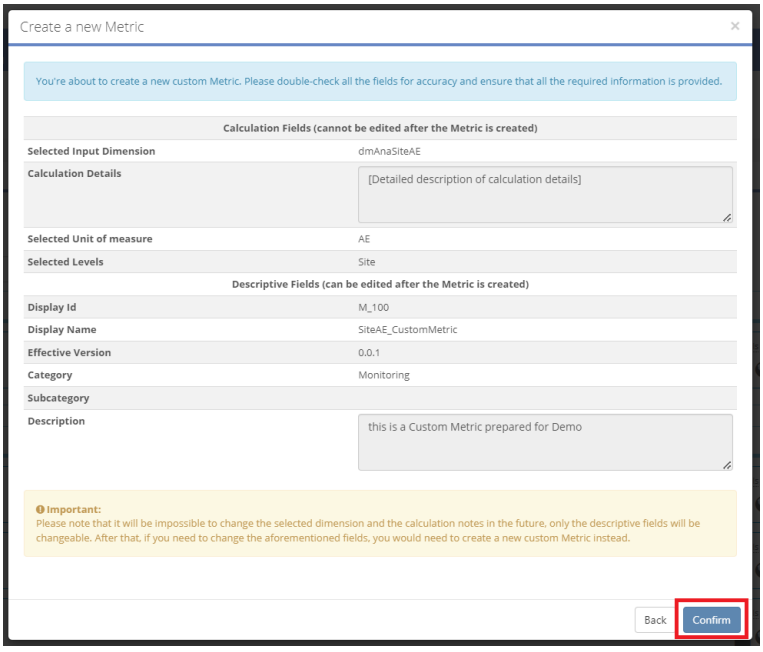


4. Select relevant levels from the list:



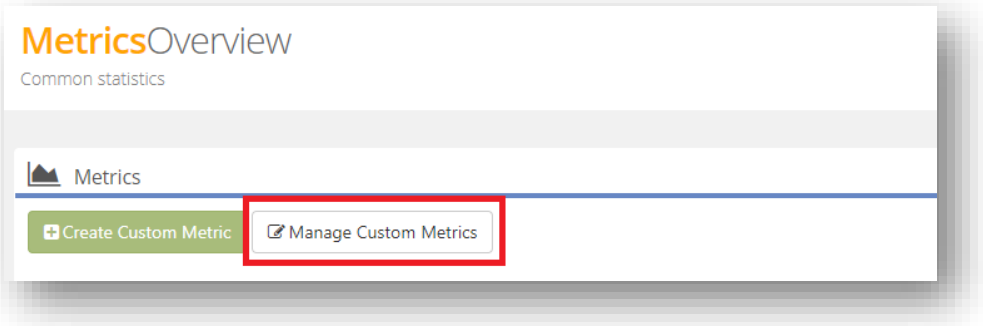
5. Once all mandatory fields are filled, click **Save**.
6. Double-check the new metric's details.
7. Click **Confirm**.

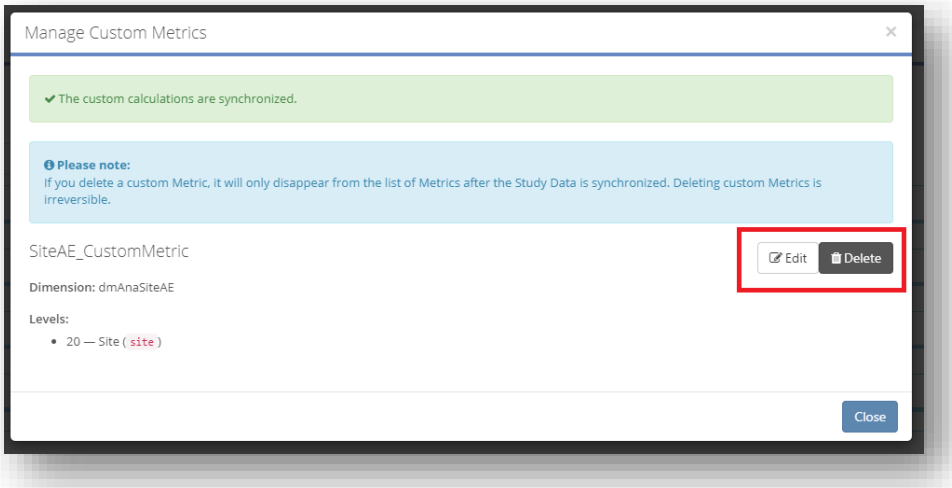
NOTE: selected dimension, calculation notes and levels can only be edited while creating a metric. If selected dimension, calculation notes and levels need to be changed after confirming metric's creation, the custom metric must be deleted and again created with the modified levels.



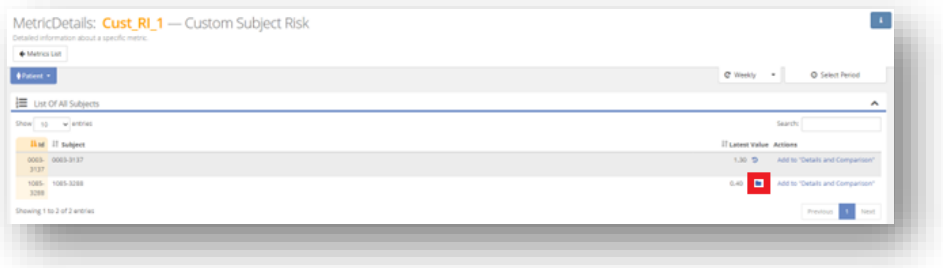
8. For the custom Metric you have created to appear in the list of Metrics, the study data needs to be synchronized first. To do so go to **Settings** → **Study Settings** → **Setup tab** and click **Send Synchronization Request** button.

However, you will be able to see, edit, and delete it via the **Manage Custom Metrics** button even before that:



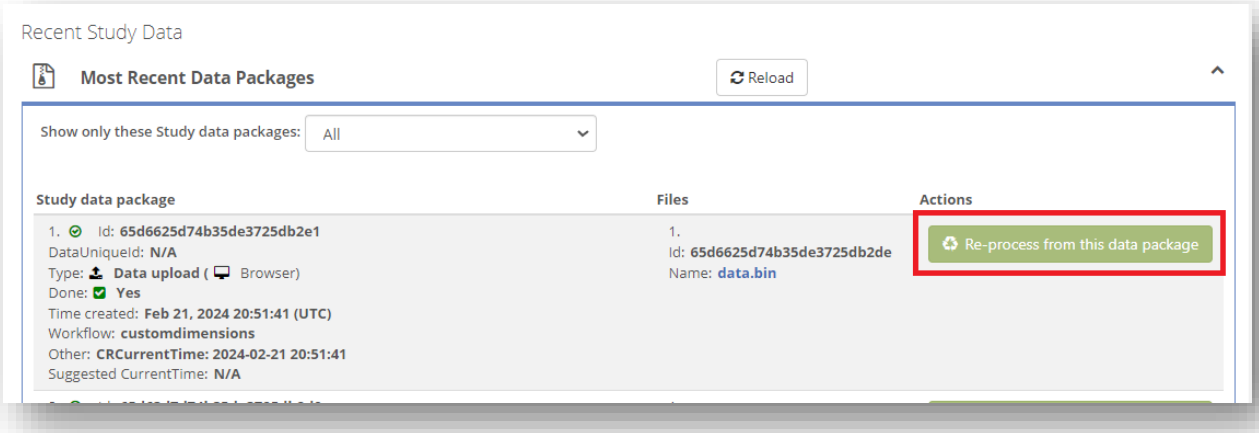


9. Inspect your custom metric in MyRBQM in the Metrics list under the selected Category. To find attached reports, navigate to the **Metric page** and click the **Folder** icon in the **Value** column:



Data Reprocessing

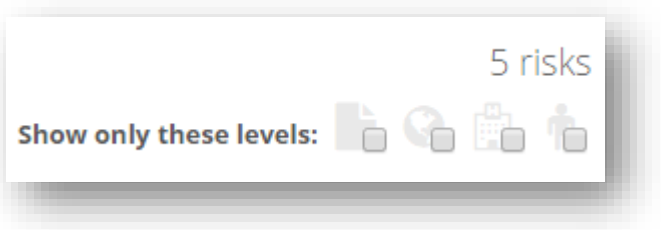
To ensure that your custom metric data is accurately reflected in your study data, it is important to reprocess the latest data import . You can initiate the reprocessing of the latest import by going to Study Settings -> Study Data page and selecting Re-process from this data package:



NOTE: Because of the intricacies of the software architecture, it is necessary for the Study Type to facilitate the import of custom metrics data (DynamicDataImport). If you're uncertain whether the Study Types deployed within your company support this feature, please contact Cyntegrity or refer to the Data Processing Specification in MyRBQM specific to your study and look up "DynamicDataImport". If you find this term, your study supports the data import of custom metrics.

KRI or QTL List

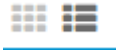
1. Select **Monitoring** → **KRI** or **QTL** from the menu bar.
2. You will see the KRI listed on the KRI page and QTLs on QTLs page.
3. You can group, sort and search within them.
4. Sorting by levels works similarly to sorting metrics:



NOTE: Cyntegrity doesn't recommend using more detailed levels than Study for QTLs.

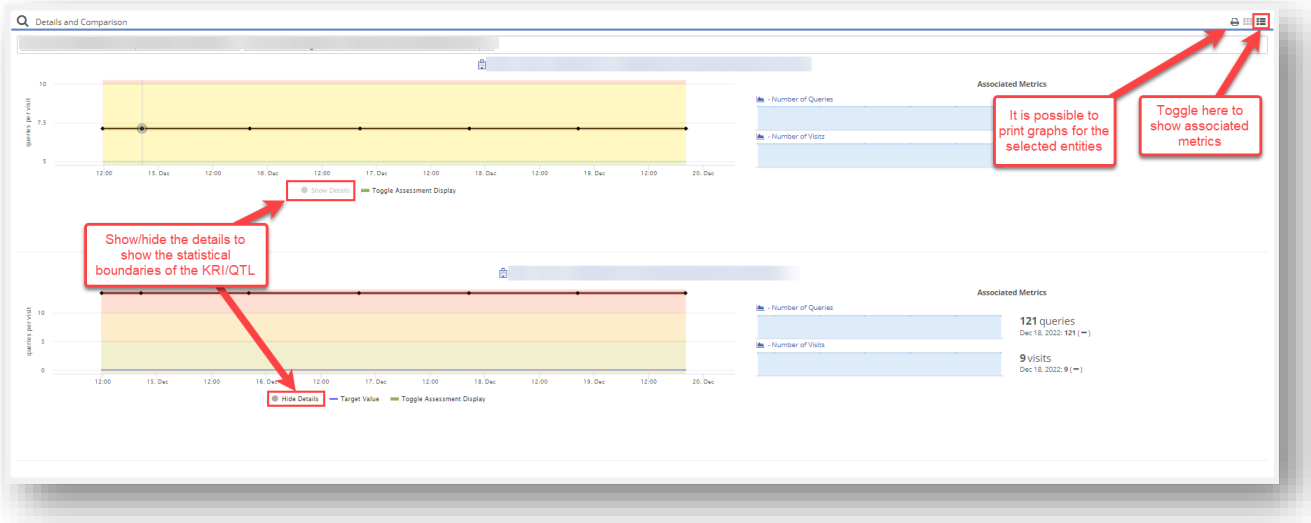
KRI (QTL) – Overview

1. Click chosen a KRI (QTL) from the list
2. The **Risk Indicator Details** page provides information about the KRI (QTL) version, the category the KRI (QTL) refers to, its levels and thresholds, calculation details and description, underlying metric and associated risks.
3. Below is the list of all sites/studies using the KRI (QTL), that provides the possibility to choose sites/studies for comparison.

4. Select sites (or other entities, depending on the level selected) by clicking **Add to Details and Comparison**. You will be able to explore them in the Details and Comparison view below.
5. Click **Show Details** of each KRI (QTL) to understand the boundaries of statistical significance and reference values.
6. Explore the associated metrics of a KRI (QTL) by clicking on the button in the upper right corner 

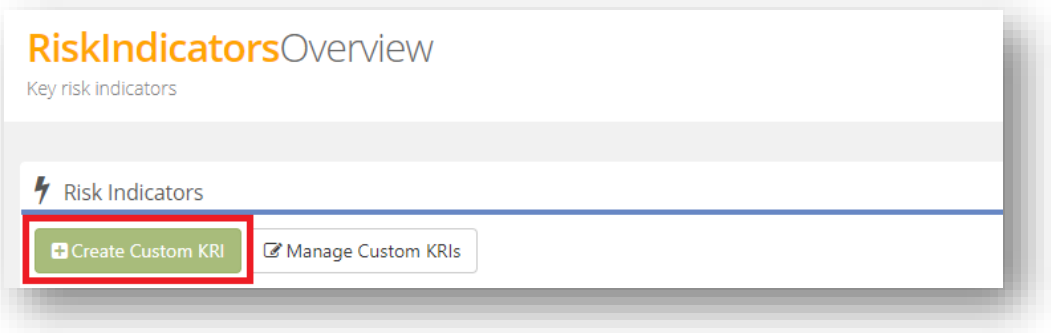
NOTE: Detailed information about the KRI (QTL) for the respective site/study is shown in the Tooltip that appears when hovering over the KRI (QTL) graph.

NOTE: RI-version changes and threshold changes are displayed on the KRI (QTL) plot.



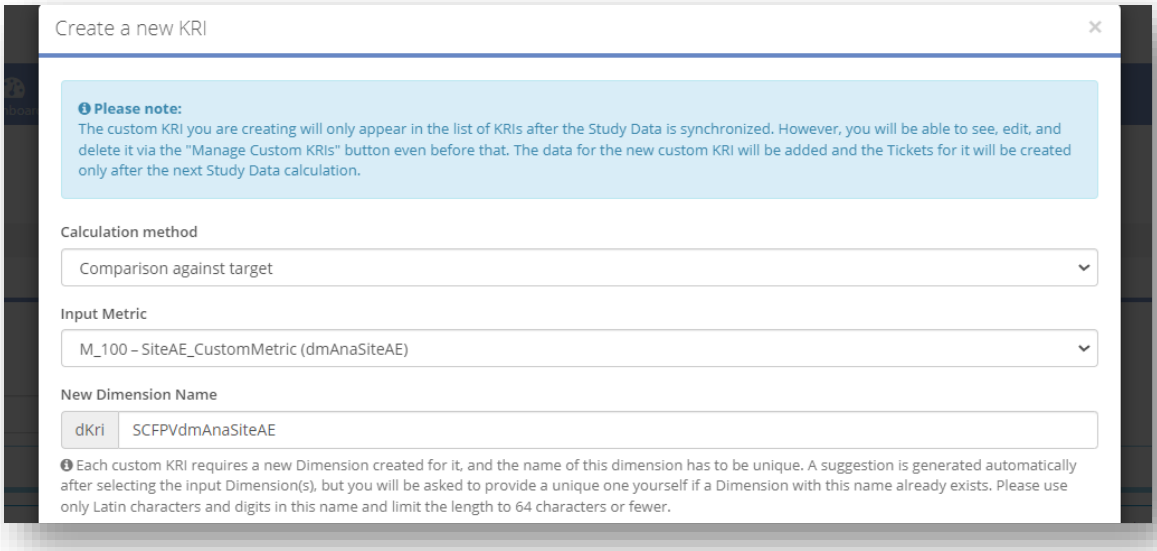
Custom KRI and QTL Creation

1. After creating your custom metric, navigate to KRI page and click Create Custom KRI. Custom KRI can only be based on the Custom Metrics.

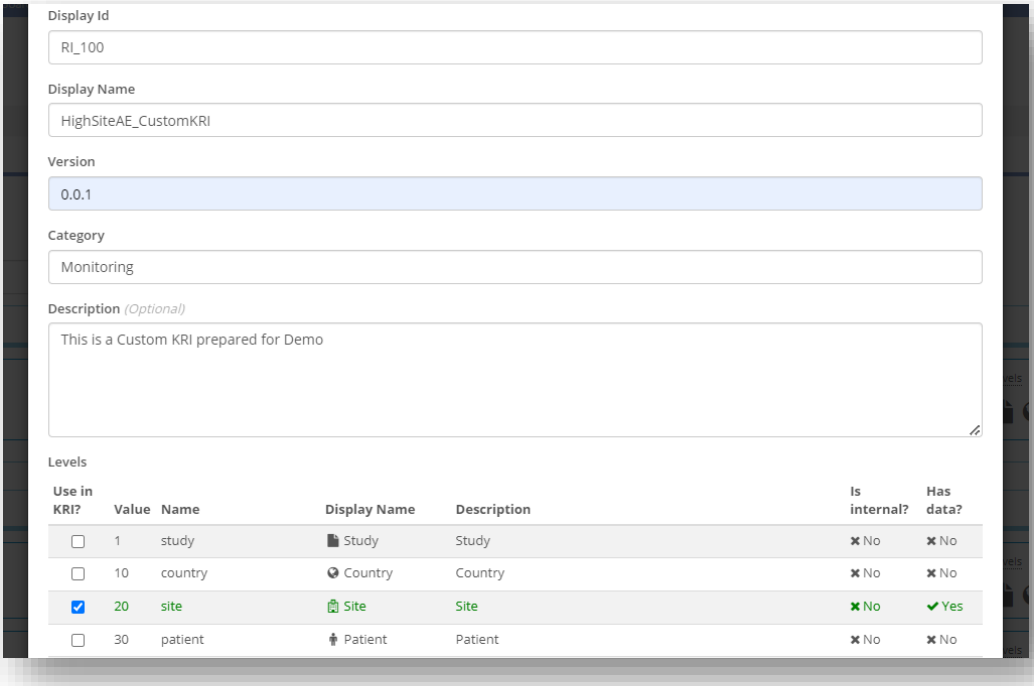


2. Select the Calculation method.
3. Select the Input Metric (one of the already created Custom Metrics).
4. Enter the New Dimension Name.

NOTE: Each custom KRI requires a new Dimension created for it, and the name of this dimension has to be unique. A suggestion is generated automatically after selecting the Input Dimension(s), but you will be asked to provide a unique one yourself if a Dimension with this name already exists. Please use only Latin characters and digits in this name and limit the length to 64 characters or fewer.



5. Similarly to the Metrics creation form, follow the wizard to fill in the rest of the fields and select the levels:



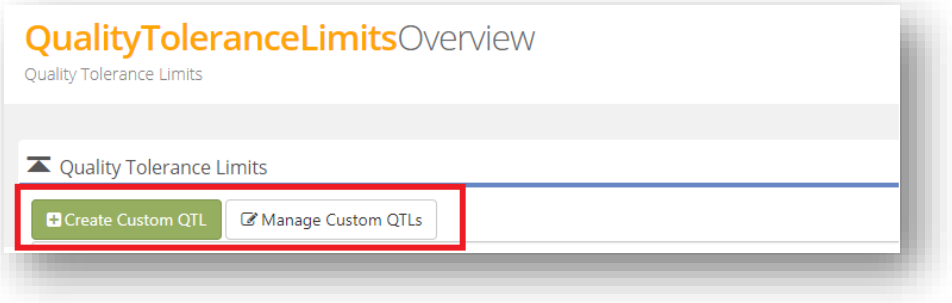
6. When all information entered, click **Save.**
7. Check all the details.
8. Click **Confirm** to create a KRI.

NOTE: *selected Calculation Method, Dimension(s) and Levels can only be edited while creating a KRI.* ***If Calculation Method, Dimension(s) and Levels need to be changed after confirming KRI's creation, the custom KRI must be deleted and again created with the modified levels.***

9. For the custom KRI you have created to appear in the list of KRI, the study data needs to be synchronized first. To do so go to **Settings** → **Study Settings** → **Setup tab** and click **Send Synchronization Request** button.

However, you will be able to see, edit, and delete it via the **Manage Custom KRI** button on the KRI page even before that.

NOTE: A custom QTL is created in the same way as a custom KRI. The Create and Manage Custom QTLs functions are located in the QTL tab:



KRI (QTL) Escalations – Tickets

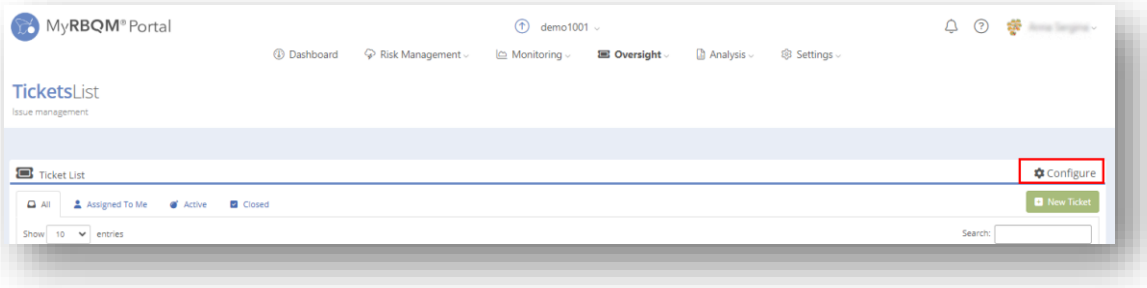
MyRBQM® Portal captures all escalations of KRI (QTLs) as "tickets". A ticket can have one responsible user or a Group (of users) as the designee. The designee can be re-assigned.

The System analyzes how systematic the issue is and sometimes does not create a ticket for minor issues that resolve themselves. This function is regulated by the Ticket Creation Timeout Parameter.

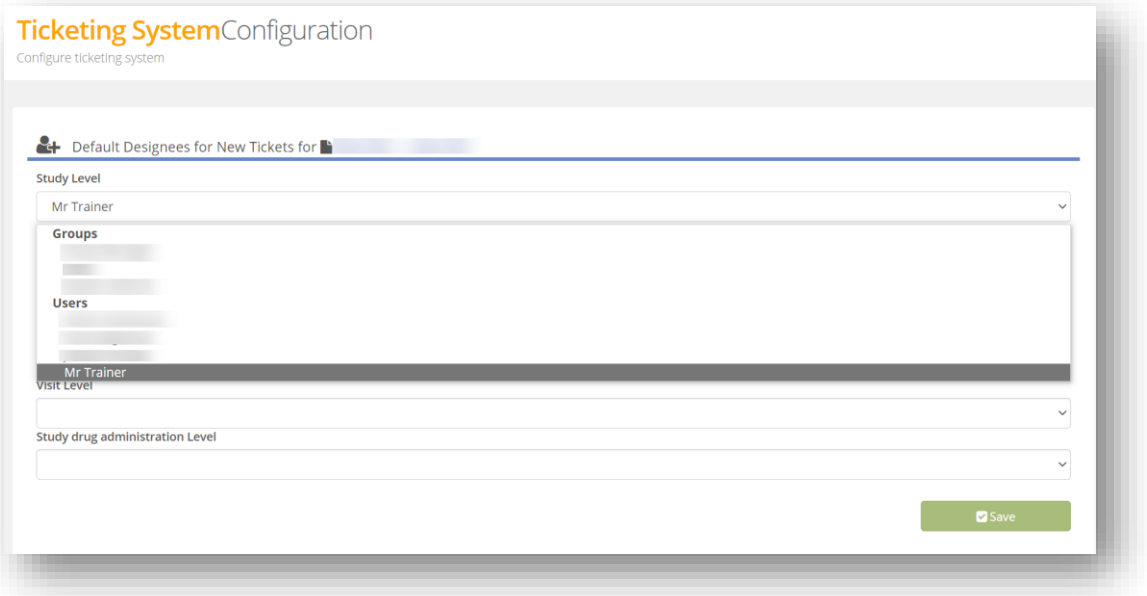
MyRBQM® Portal uses two types of Tickets: System-generated and Manually created Tickets, which are created by users.

To configure the designee for System-generated Tickets:

1. Go to **Oversight** → **Tickets**.
2. Click **Configure.**



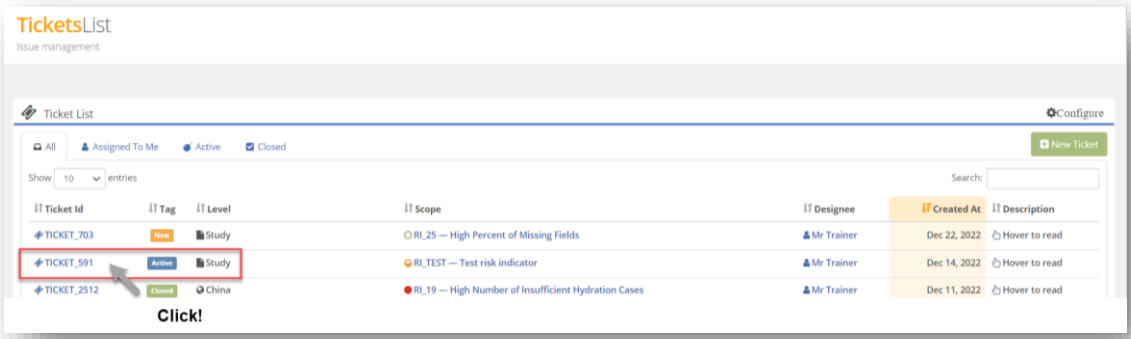
3. Select a person or a group from a drop-down list for every level:



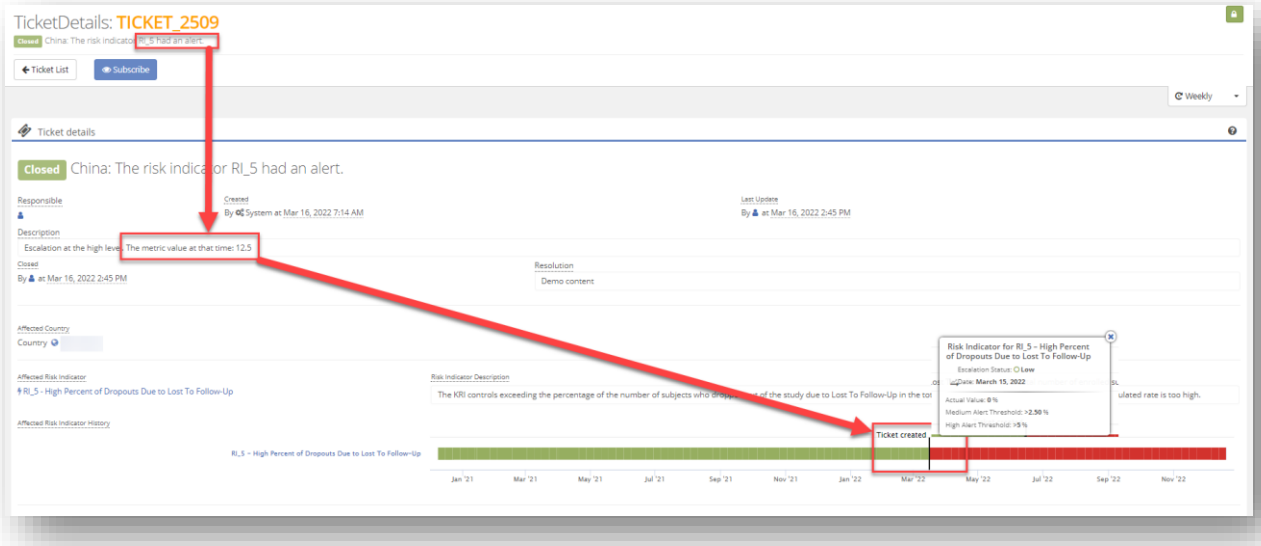
4. Save.

Similar to KRI (QTLs) or Metrics, a Ticket can be generated on different levels, e.g., subject, site, and study.

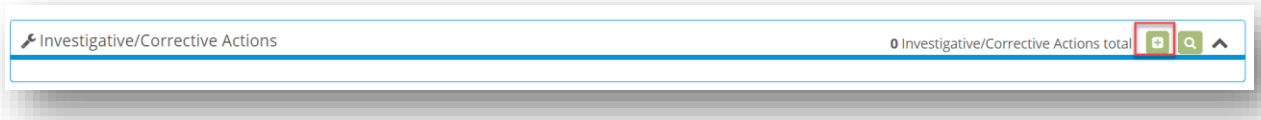
1. Click the **Ticket Id** to open a ticket and to explore its risk indicator history.



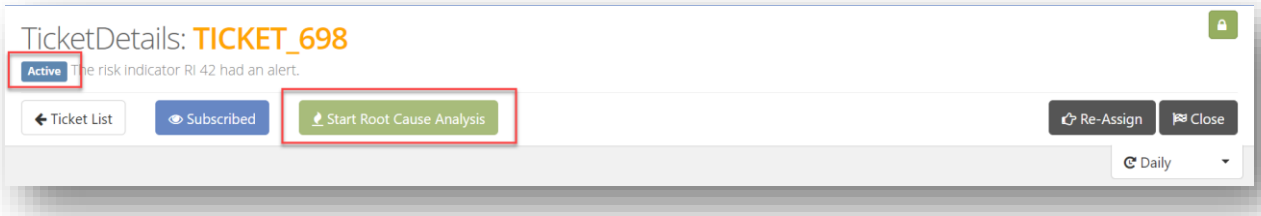
2. The vertical line on the risk indicator graph shows the time when a ticket was created by **MyRBQM® Portal**.



3. Assign investigative/corrective actions to the Ticket.



4. Perform a root cause analysis for the Active Ticket:



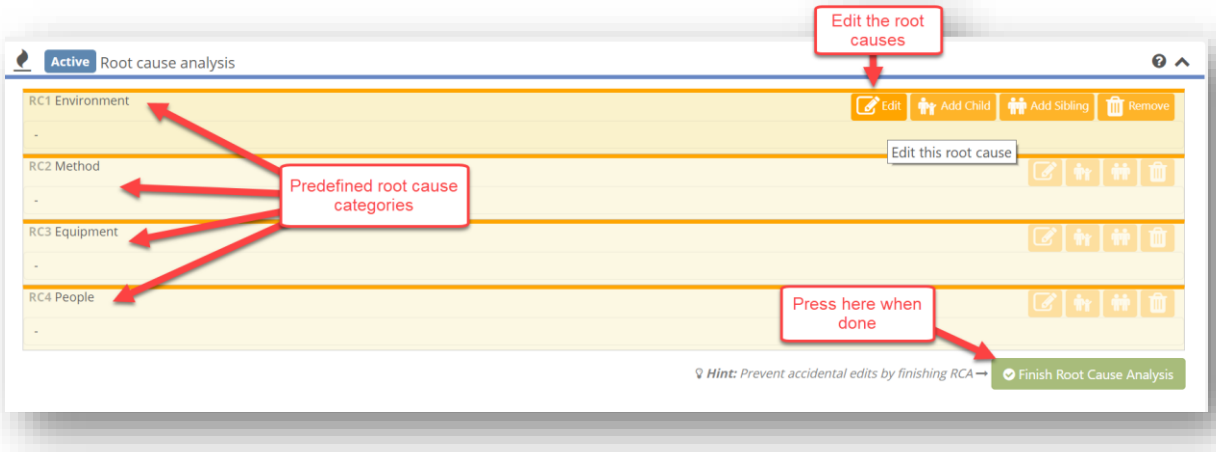
5. Attach a Mitigation Plan for each root cause and select the KRI (QTLs) for detecting the influence of the contingency actions on the data.

NOTE: Upon changes inside of a ticket, email notifications are sent to the Ticket Owner, Subscribers, and Designee. Ticket notifications can be aggregated by day, week, and month.

NOTE: Investigative/Corrective actions undergo the same lifecycle as all other mitigations/actions (e.g. create, activate, review, close, due date).

Root Cause Analysis

1. Click **Start a Root Cause Analysis (RCA)**.
2. Enter the root causes into the predefined categories or create new root cause categories.
3. Transfer all root causes into the tree structure, describing all the facets of the situation.
4. Click **Finish Root Cause Analysis** when done.

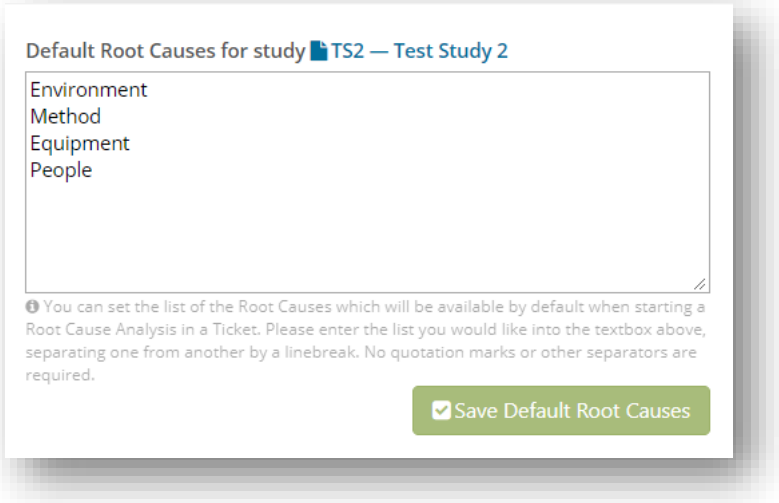


Manual Configuration of Default Root Cause Categories

The default root cause categories are configurable per study via the **Configuration Hub** by Company Admins.

To configure default root cause categories:

1. Open **Tickets** tab.
2. Go to **Configure.**
3. In the **Default Root Causes for study** section, add, remove or edit the default root cause categories by editing the text within the text box:

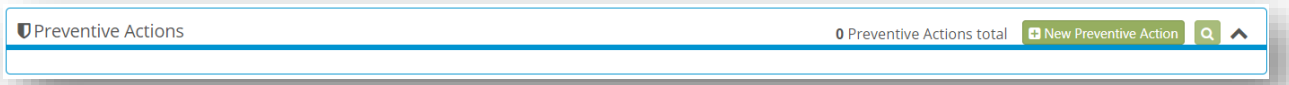


4. **Save Default Root Causes**.

NOTE: Every newly created root cause analysis will contain the new configurations. Root cause analyses started before the configuration will still contain the former categories.

Design a Preventive Actions Plan

1. After finishing the root cause analysis, hover over the + sign at the **Preventive Actions** section.
2. Click **New Preventive Action**.



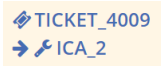
3. Select the **Root Cause** from the list that you want to prevent.
4. Select a **Responsible User**, who will take care of this plan.
5. Add an **Action** (text).
6. Add **Review Settings** – this defines how often the system reminds you of the action through email and/or an internal messaging system.

Actions List - Manage Ticket Actions

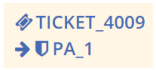
Analogous to risk mitigation actions, ticket actions (investigative/corrective and preventive actions) are managed via the Actions List, listed along with risk mitigation actions (see Actions List - Manage Risk Mitigation Actions section).

To Manage Actions:

1. Go to **Risk Management** → **Actions** from the menu bar.
2. Investigate the table of available actions. All created ticket actions must be listed, together with risk mitigation actions.

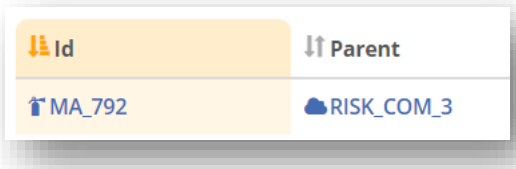
   Investigative/corrective actions are indicated with the corresponding Ticket Id together with a wrench icon and the action Id ICA_X, e.g. 

.

Preventive actions are indicated with the corresponding Ticket Id together with a shield icon and the action Id PA_X, e.g. 

.

3. Clicking the **Ticket/ Action Id** will redirect you to the corresponding Ticket Details page and auto-scroll to the Mitigation Action in question.
4. Manage (e.g., edit, activate, review, close) ticket mitigation actions here.
5. Clicking the parent Id (risk indicator) will redirect you to the Risk Indicator Details page.



Risk Review

Cyntegrity recommends extending/developing standard operating procedures (SOPs) for Risk Review:

For example, Cyntegrity recommends conducting regular team meetings to review and update @RACT+. The Risk and KRI Registers should be integrated into the risk management plan or a similar document. This document should define topics to be discussed between the project or

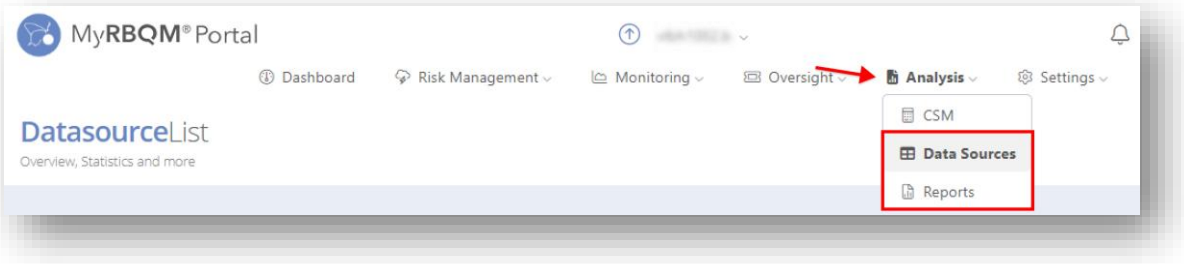
risk manager and team members during these team meetings, including, but not limited to:

- Identification of new risks since the last team meeting.
- Accuracy and reliability of risk Impact (I), Probability (P), and Detectability (D) levels (based on observed risk trends or occurrence).
- Successful avoidance or mitigation through effective planned risk responses and actions.
- The Occurrence of initially accepted risks; and if so, consideration of mitigation actions.
- Study deliverables and general study performance (achieved milestones, met timelines, data quality checks, data reviews, IT checks, etc.).
- Risk management process improvement.

If a deficiency in the risk-based quality management system (e.g., inadequate risk control) is detected, the project manager and team members should meet, discuss solutions and improve the affected processes, checking the efficacy of the agreed corrective actions after their implementation. Thereby, the project manager or designee must organize and direct an on-demand Risk Review and evaluate the need for conducting a formal CAPA.

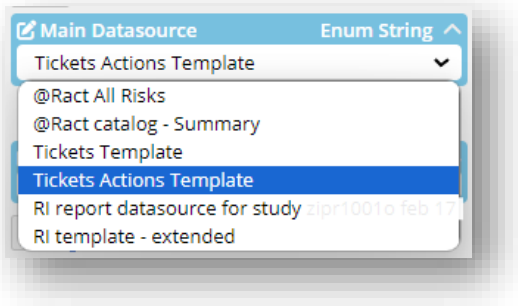
Risk Reporting

How Quality Assurance and Control (QA & QC) system deviations need to be reported depends on the complexity and duration of the trial. Thus, the ICH E3 guideline (Clinical Study Reports) states that the regulatory authorities should be consulted for agreeing with a format that will enable the overview of quality management compliance in situations where detailed reports are not practical due to their extent. In such cases, risk reporting would need to be simplified. Therefore, it is not possible to standardize the formats of risk reports.



The RBM System **MyRBQM® Portal** enables the export of summary tables summarizing the most relevant deviations from the quality control limits based on risk relevance. You can select deviations of low, medium or high risk to enable risk report adjustment and simplification. Thus, **MyRBQM® Portal** improves data visualization as well as communications with and reporting to the regulatory authorities.

Reports can be created based on the pre-defined report templates (e.g., Tickets, Risk Indicators). Moreover, **MyRBQM® Portal** allows the manual creation of report templates.



Efficacy and safety data should be briefly summarized and depicted in the relevant tables and figures, focusing on any new or unexpected findings. Thus, the KRI selected by Cyntegrity and its partners are based on key safety and study performance parameters directly related to critical issues such as serious adverse events (SAEs), events resulting in withdrawal and/or death, and lack of compliance (i.e., ratio of missing visits).[iv]

The Risk & Quality Management approach (risk-based QA & QC system) implemented in the trial should always be briefly described in the final Clinical Study Report (CSR). Any important deviation from the predefined quality tolerance limits must be reported together with the corrective actions taken for mitigating risk recurrence (ICH E3, Section 9.6 Data Quality Assurance).[iv]

Efforts towards quality assurance and standardization of the clinical study team and investigator performance have great relevance (i.e., audit procedures should be summarized).

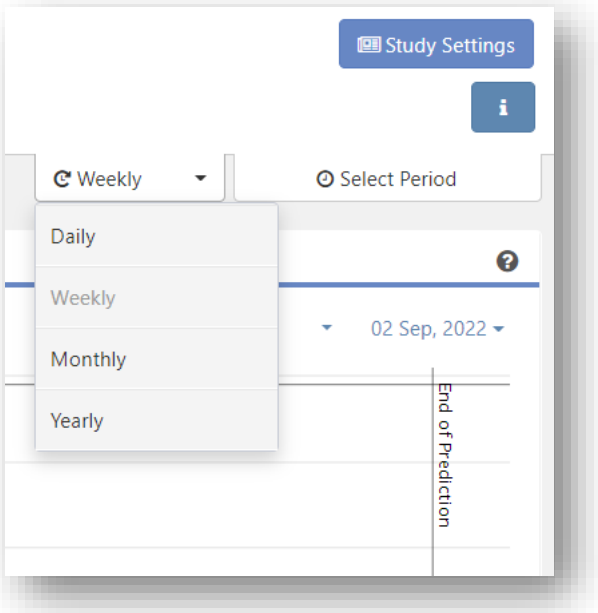
General Functions

In this chapter, available product features are described.

Change the Detail Grade of the Data Presentation

1. If you need a more detailed or a less detailed data presentation in the main dashboard, click the **i** button.
2. The data can be presented daily, weekly, monthly or yearly.

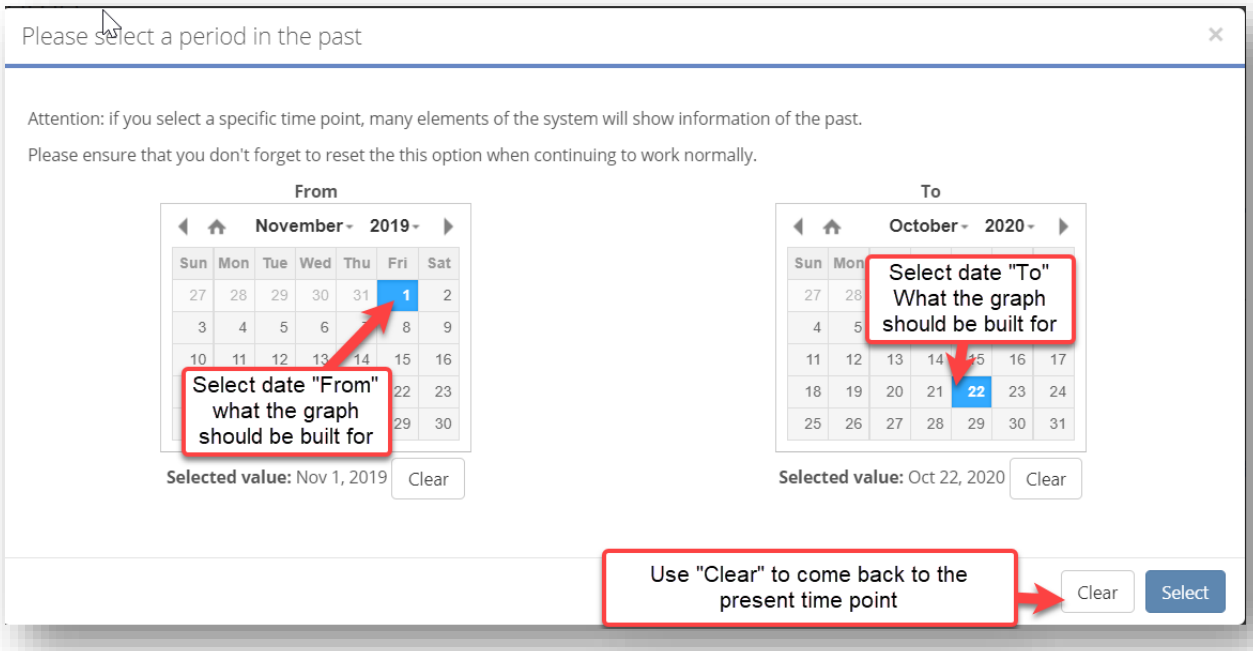
NOTE: The more detailed your choice (daily over monthly), the longer data upload take.



Jump to a Historical Time-Point

In order to see the risk situation at a certain time point, click **Select Period** in the main dashboard.

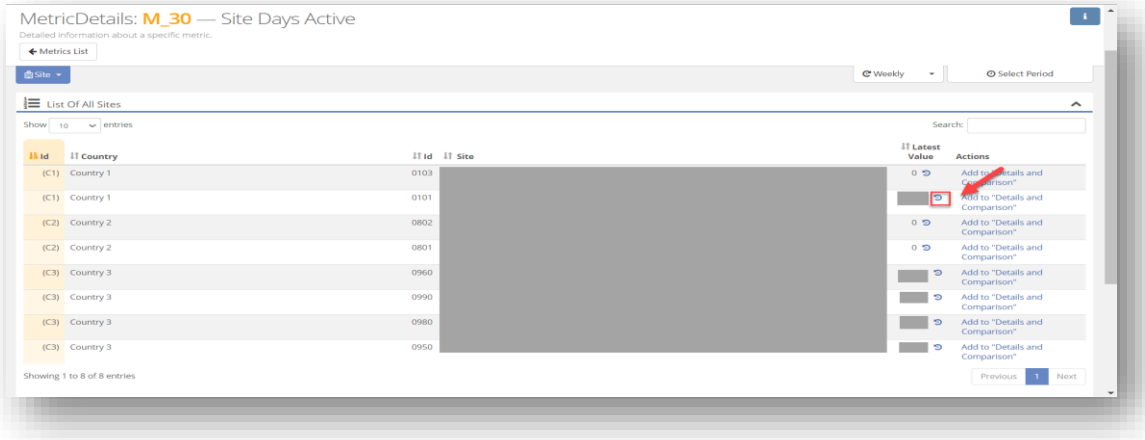
NOTE: Always clear the selected period after analysis.

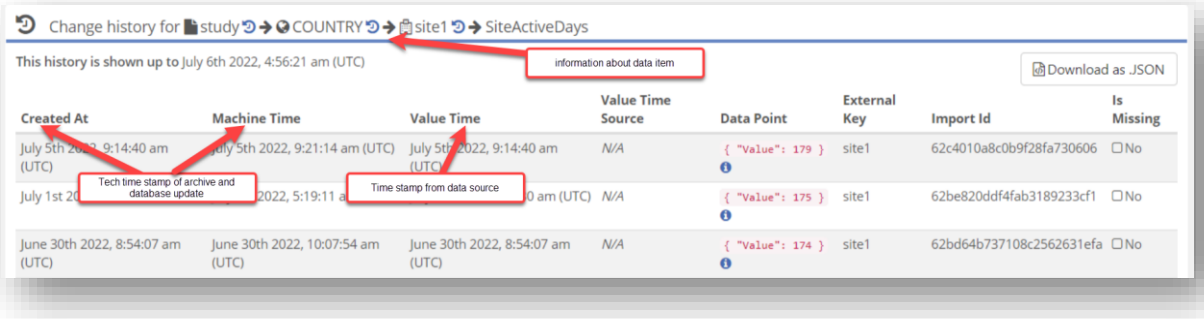


Check History of the Metric, KRI, QTL, FMEA and Subject information

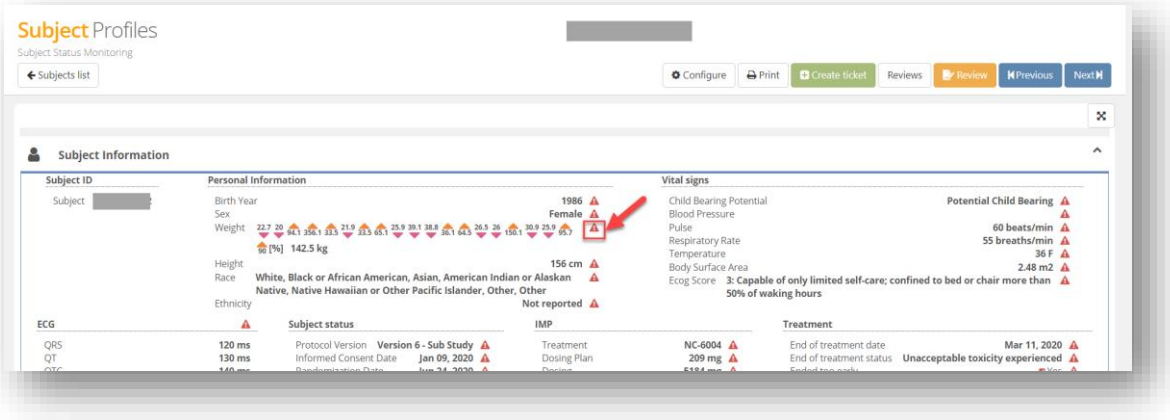
For Metrics, KRI/QTL, Subject Profile number characteristics, FMEA rating, etc., users can check the history of changes.

For example: Metrics.

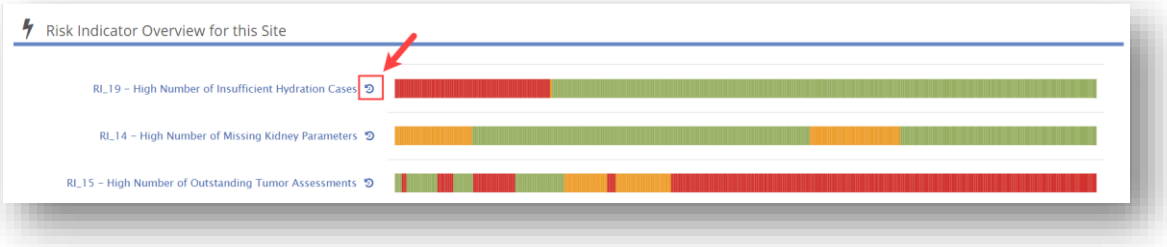




In Subject Profile Change, click the value status icon to see History.



View the History of RI values and an explanation of the RI value calculation from the **Study Details Page** (Site Heartbeat tab).

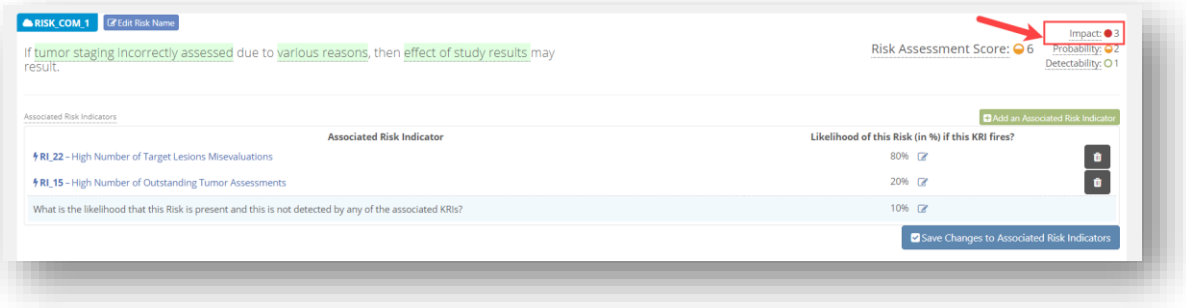


Calculation of Occurrence, Risk Rating Score

Risk rating scores are calculated based on **Risk Occurrence** and **Risk Impact**.

Risk Occurrence scores are calculated based on the number of times that a KRI breached its highest thresholds.

Risk Impact should be taken for the Risk from the Risk Tab and normalized.



Value from Risks Tab	Value for Risk Rating (normalized)
1	33%
2	66%
3	100%

The Calculation Algorithm for the Occurrence Score

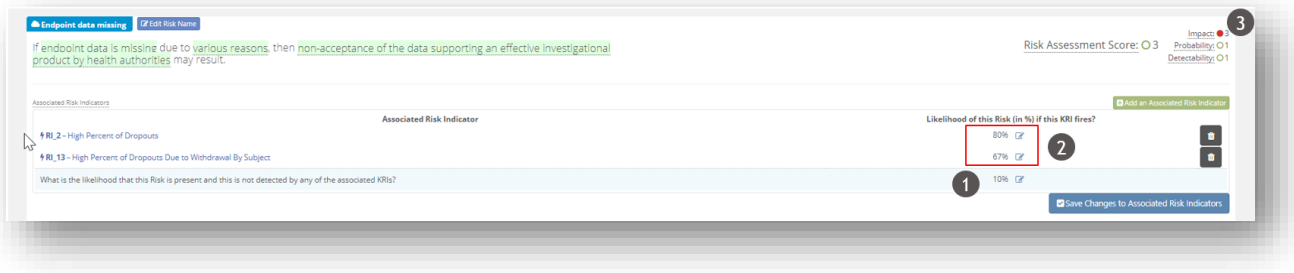
Occurrence at countries and study levels will be calculated from escalations of KRI at countries and study levels and **not** from averaging of Occurrences at sites.

The Occurrence should be calculated **at each level separately** because thresholds can be different at each level, as well as sample size, which is important for relative RI (High/Low Rate of …).

For the Occurrence calculation, we use a moving window of 4-8 weeks (depending on the study setting agreed with a customer).

$$\frac{Number\ of\ KRIi\ calculations\ that\ lead\ to\ escalations}{Number\ of\ total\ KRIi\ calculations} = \frac{Escalations}{Calculations}$$

The Calculation Algorithm for the Risk Rating



1. Risk rating is a result of Risk Occurrence x Risk Impact (3).
2. Risk Impact should be taken from Risk tab and normalized to 1.

→ Value from Risks Tab	→ Value for Risk Rating (norr
1	→ 33%
→ 2	→ 66%
→ 3	→ 100%

3. *Risk Occurrence= Probability of Risk Detection from KRI** $\sum_{i=1}^{n}(Weight\ KRIi\ (2) * Actualization\ KRIi)$**+** *Probability of Risk Detection w/o KRI (1), where*
   - n is number of KRI associated with this Risk
   - $Weight\ KRIi$ **should be normalized** to 1 if several KRI are associated with this Risk (can be found in Risk tab as associated Risk Indicators)

Example of normalization:

RI	Value from Risks Tab	Value for Risk Rating (normalized)
RI_2	80%	54% *80%/(80%+67%)*
RI_13	67%	46% *67%/(80%+67%)*

- $Actualization\ KRIi$ – number of times the KRI has breached the High Thresholds within determined period (discussed at the Study Set Up phase)

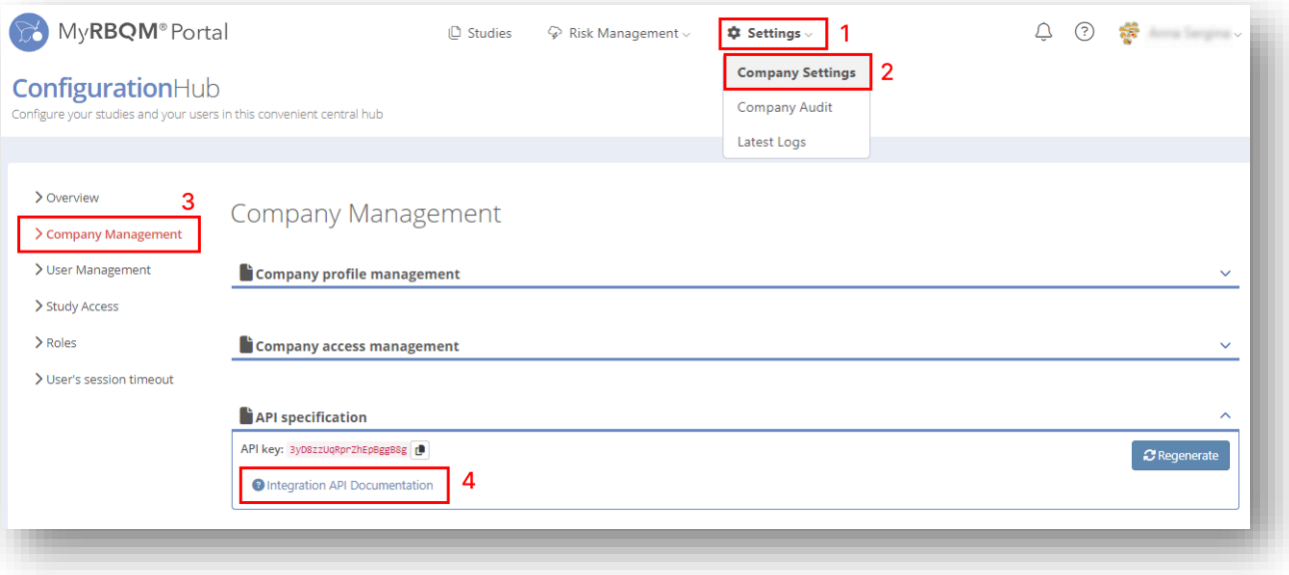
Probability of Risk Detection from KRI = 1-Probability of Risk Detection w/o KRI (2).

Integration with external systems

CTMS Integration

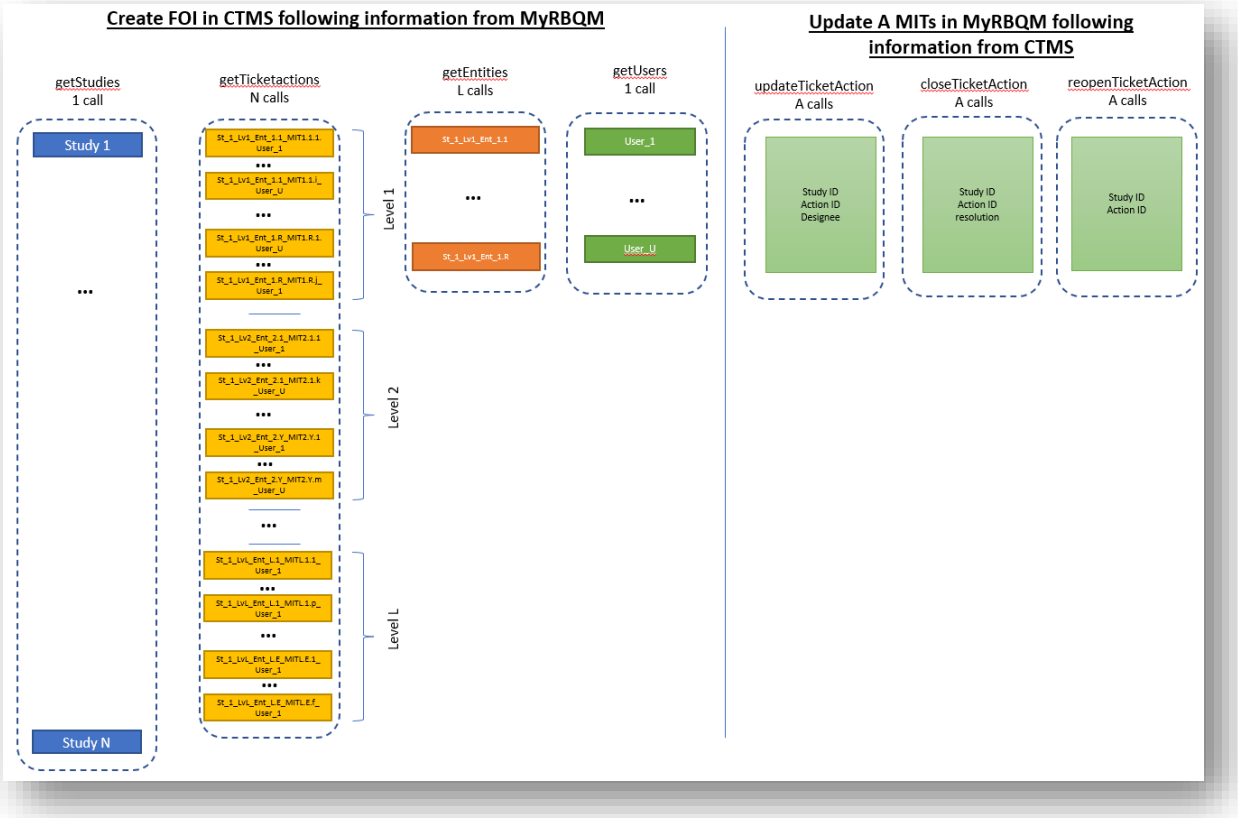
It is possible to extract ticket action information from MyRBQM using integration API to push it then into an external CTMS system (push step should be managed from the customer side).

Integration API information can be found via Settings → Company Settings → Company Management tab.



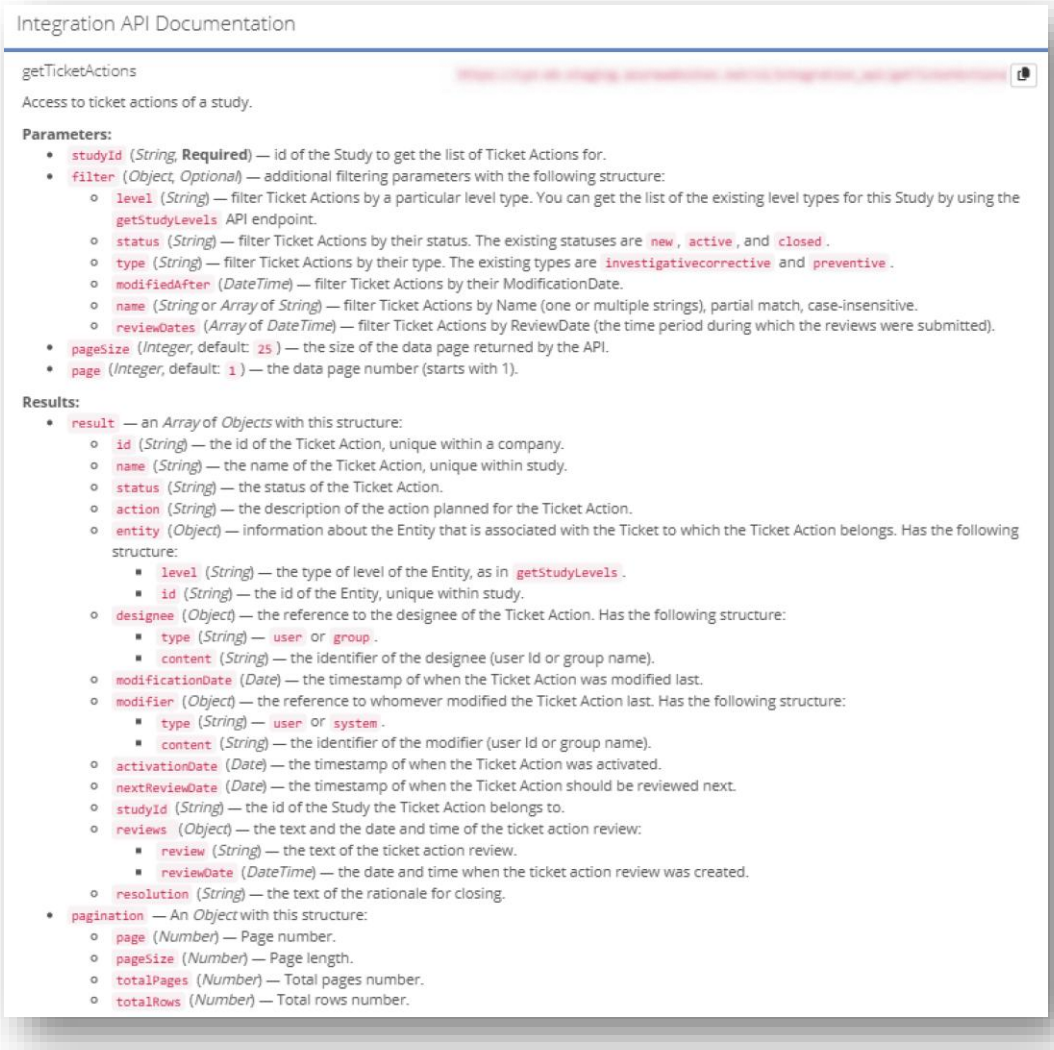
Proposed Way of Work

DISCLAIMER: MyRBQM offers the capability to extract the necessary information for creating an action item in an external CTMS system. However, any additional integration efforts, conflict management, data storage, and other related tasks that need to be handled on the customer's side should be managed by the customer's own team.



1. **Get all Studies** – to know Study ID
2. **Get Ticket Actions** from needed study-to create items in an external CTMS system.
3. **Get Entities Details** – to know Site or other entity credentials.
4. **Get Users** – to know who is assigned to an action execution.

Get Ticket Action information



Integration API Documentation

getTicketActions

Access to ticket actions of a study.

Parameters:

- `studyId` (*String*, **Required**) — id of the Study to get the list of Ticket Actions for.
- `filter` (*Object*, *Optional*) — additional filtering parameters with the following structure:
  - `level` (*String*) — filter Ticket Actions by a particular level type. You can get the list of the existing level types for this Study by using the `getStudyLevels` API endpoint.
  - `status` (*String*) — filter Ticket Actions by their status. The existing statuses are `new`, `active`, and `closed`.
  - `type` (*String*) — filter Ticket Actions by their type. The existing types are `investigativecorrective` and `preventive`.
  - `modifiedAfter` (*DateTime*) — filter Ticket Actions by their ModificationDate.
  - `name` (*String* or *Array* of *String*) — filter Ticket Actions by Name (one or multiple strings), partial match, case-insensitive.
  - `reviewDates` (*Array* of *DateTime*) — filter Ticket Actions by ReviewDate (the time period during which the reviews were submitted).
- `pageSize` (*Integer*, default: `25`) — the size of the data page returned by the API.
- `page` (*Integer*, default: `1`) — the data page number (starts with 1).

Results:

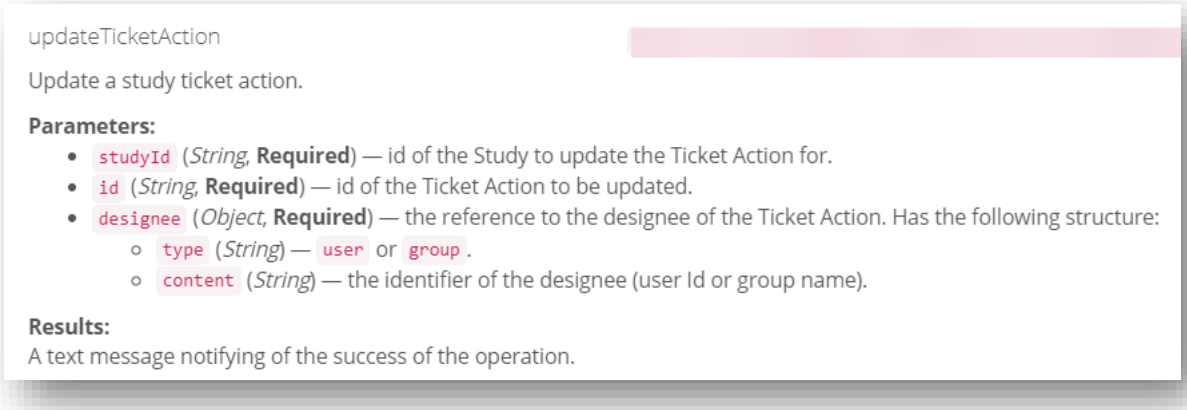
- `result` — an *Array* of *Objects* with this structure:
  - `id` (*String*) — the id of the Ticket Action, unique within a company.
  - `name` (*String*) — the name of the Ticket Action, unique within study.
  - `status` (*String*) — the status of the Ticket Action.
  - `action` (*String*) — the description of the action planned for the Ticket Action.
  - `entity` (*Object*) — information about the Entity that is associated with the Ticket to which the Ticket Action belongs. Has the following structure:
    - `level` (*String*) — the type of level of the Entity, as in `getStudyLevels`.
    - `id` (*String*) — the id of the Entity, unique within study.
  - `designee` (*Object*) — the reference to the designee of the Ticket Action. Has the following structure:
    - `type` (*String*) — `user` or `group`.
    - `content` (*String*) — the identifier of the designee (user Id or group name).
  - `modificationDate` (*Date*) — the timestamp of when the Ticket Action was modified last.
  - `modifier` (*Object*) — the reference to whomever modified the Ticket Action last. Has the following structure:
    - `type` (*String*) — `user` or `system`.
    - `content` (*String*) — the identifier of the modifier (user Id or group name).
  - `activationDate` (*Date*) — the timestamp of when the Ticket Action was activated.
  - `nextReviewDate` (*Date*) — the timestamp of when the Ticket Action should be reviewed next.
  - `studyId` (*String*) — the id of the Study the Ticket Action belongs to.
  - `reviews` (*Object*) — the text and the date and time of the ticket action review:
    - `review` (*String*) — the text of the ticket action review.
    - `reviewDate` (*DateTime*) — the date and time when the ticket action review was created.
  - `resolution` (*String*) — the text of the rationale for closing.
- `pagination` — An *Object* with this structure:
  - `page` (*Number*) — Page number.
  - `pageSize` (*Number*) — Page length.
  - `totalPages` (*Number*) — Total pages number.
  - `totalRows` (*Number*) — Total rows number.

getTicketActions will allow extraction of information:

1. MyRBQM Action ID
2. Ticket Action Name
3. Ticket Action Status
4. Information from the Action fields
5. Related entity (level, MyRBQM ID)
6. Action Designee (user or group, MyRBQM ID/group name)
7. Action Modification Date
8. Modifier information (system or user, MyRBQM ID/Group name)
9. Activation Date
10. Action Review Text and Date
11. Rationale for Action Closing
12. Next Review Date

NOTE: for detailed information (Required or optional field, syntaxis etc.) please refer to the Integration API Documentation.

Update Ticket Action



updateTicketAction

Update a study ticket action.

Parameters:

- `studyId` (*String*, **Required**) — id of the Study to update the Ticket Action for.
- `id` (*String*, **Required**) — id of the Ticket Action to be updated.
- `designee` (*Object*, **Required**) — the reference to the designee of the Ticket Action. Has the following structure:
  - `type` (*String*) — `user` or `group`.
  - `content` (*String*) — the identifier of the designee (user Id or group name).

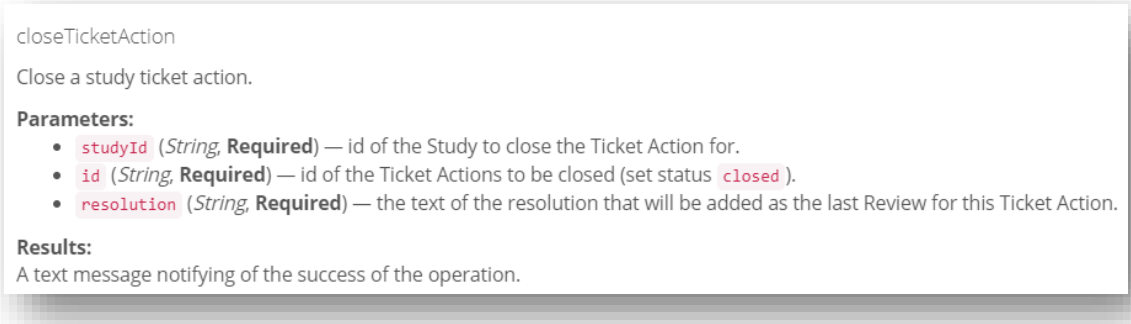
Results:

A text message notifying of the success of the operation.

If an Action Designee was updated in CTMS system, it is possible to update in Designee Name in MyRBQM using **updateTicketAction** API.

NOTE: Designee is the only field that can be updated from CTMS side. For all other fields (i.e., Action, Review Date, etc.) MyRBQM is source of truth for ICA and can be changed in MyRBQM and then imported again into CTMS.

Close Ticket Action



closeTicketAction

Close a study ticket action.

Parameters:

- `studyId` (*String*, **Required**) — id of the Study to close the Ticket Action for.
- `id` (*String*, **Required**) — id of the Ticket Actions to be closed (set status `closed`).
- `resolution` (*String*, **Required**) — the text of the resolution that will be added as the last Review for this Ticket Action.

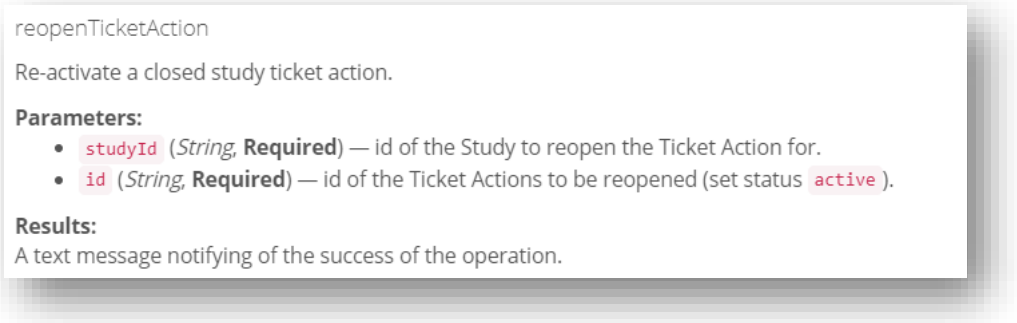
Results:

A text message notifying of the success of the operation.

If an action has been closed in an external CTMS system, the corresponding action in MyRBQM can be closed using the integration API **closeTicketAction**.

NOTE: The customer needs to decide whether the closure of Investigative Correction actions will be permitted in the user interface (UI) concurrently with the management of ICA actions in the external system.

Reopen Ticket Action


reopenTicketAction

Re-activate a closed study ticket action.

Parameters:

- `studyId` (*String*, **Required**) — id of the Study to reopen the Ticket Action for.
- `id` (*String*, **Required**) — id of the Ticket Actions to be reopened (set status `active`).

Results:
A text message notifying of the success of the operation.

NOTE: This function is not available in UI.

It is possible for an action item to be reopened in an external CTMS system. In such cases, the **reopenTicketAction** API can be utilized to reopen the corresponding Investigative Corrective Action (ICA) in MyRBQM, as well as the parent ticket, if necessary.

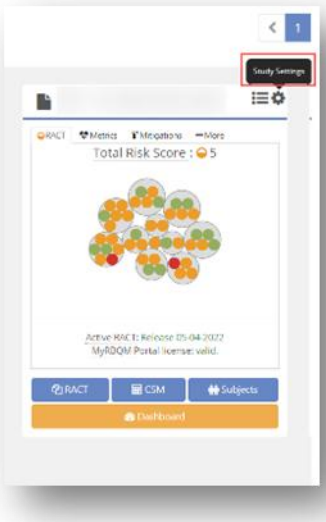
Administrator Functions

Study Settings

Study Settings can be found in **Settings** → **Study Settings** (upper menu).

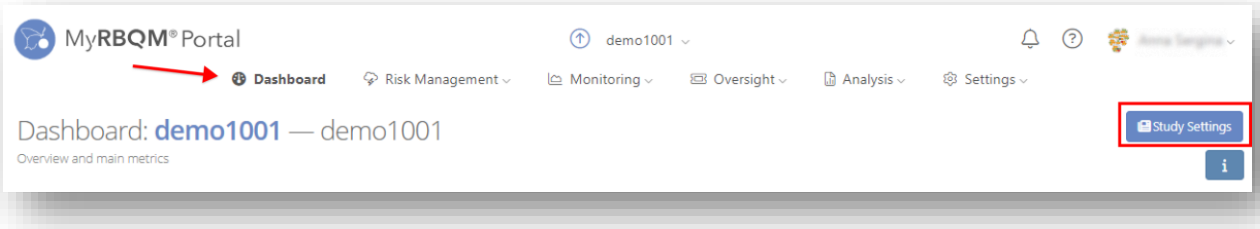
OR

From a Study tile:



OR

From Study Dashboard:



Setup

From here, users can:

- Disable/Enable Data Processing (If Data Processing is disabled, metrics and other calculations are stopped)
- Delete Pending Tasks
- Set Study Status to Live (it will prevent the Study retirement and Data deletion)
- Select Study type required for a particular study
- Set up sampling (how frequently calculation for the past period of Study (before the Study was created in **MyRBQM® Portal**) should be performed)
- Send Synchronization Request.

Study Data

Here, users can:

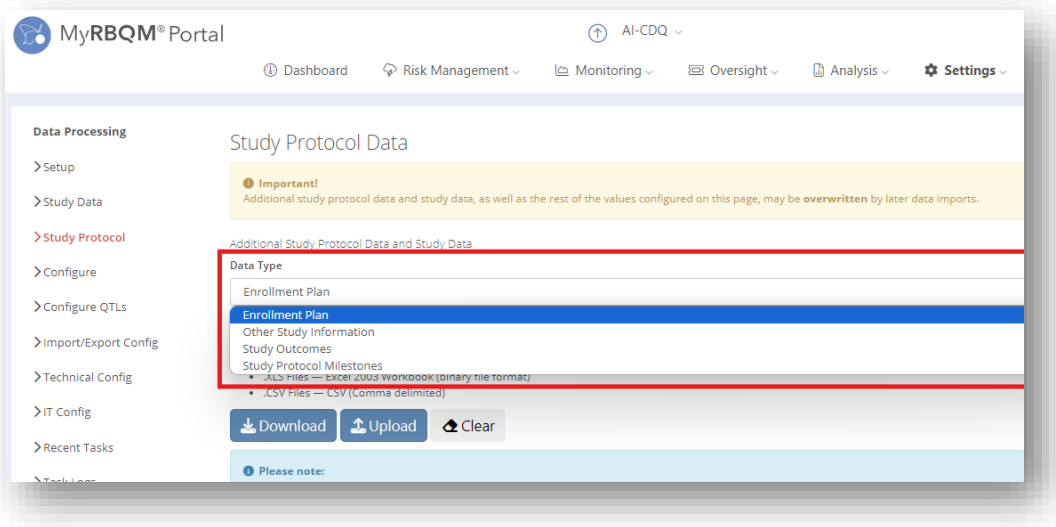
- Find API keys for data loading
- Upload data via Browser
- Delete Study Data (for Non-Live Studies, only)
- View information about the Recent Data Uploads

Study Protocol

In this tab of the Study Settings Menu, it is possible to:

1. Upload and download Enrollment plan, Study Outcomes, Study Protocol Milestones and other study information.

   NOTE: Files that should be set up in the Study protocol, their priorities, saving and update options depend on the study type. Please clarify requirements with your Project Manager.



2. Set up the Target Number of Subjects

NOTE: The Target Number of Subjects may be required for some Key Risk Indicators and Study

Predictions. The changes to this number will affect them after the next data import.

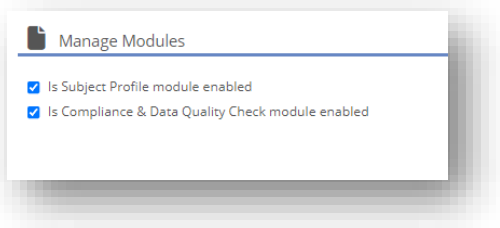
3. Set Vital Timelines

Vital Timeline reference information

- **Final protocol available prior to the first subject screened** - not frequently used, might be needed for some metrics (determined study to study)
- **Final CRF available prior to the first subject screened** - not frequently used, might be needed for some metrics (determined study to study)
- **All sites identified according to plan** - not frequently used, might be needed for some metrics (determined study to study)
- **IRB approval available prior to the first subject screened** - not frequently used, might be needed for some metrics (determined study to study)
- **Site staff GCP training completed prior to the first subject screened** - not frequently used, might be needed for some metrics (determined study to study)
- **Study drug supply prior to first subject randomized** - not frequently used, might be needed for some metrics (determined study to study)
- **Study Start date** - date on which we expect first data available in data import
- **First Subject First Visit (FSFV) according to plan** - previous name = Recruitment start date

- **Last Subject First Visit (LSFV) according to plan** - used as last date in Enrollment PI [Dashboard]
- **Database closure** – last date on which we expect any new data
- **Study stop date** - used as last date for metric predictions

4. Enable/Disable a Subject profile
5. Enable/Disable Compliance & Data Quality Check module



Configure/Configure QTL

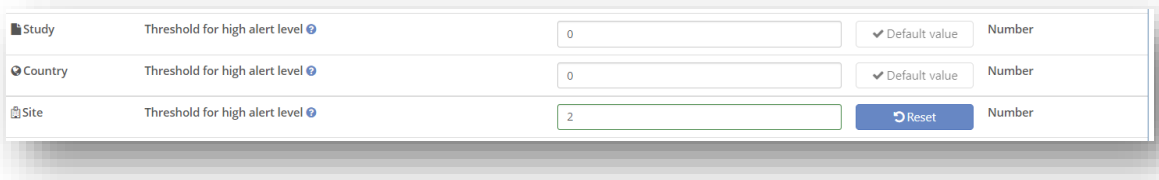
In this tab, a user can set up Metrics, RI, QTL and other groups' parameters one by one for configured levels separately.

Parameters might include:

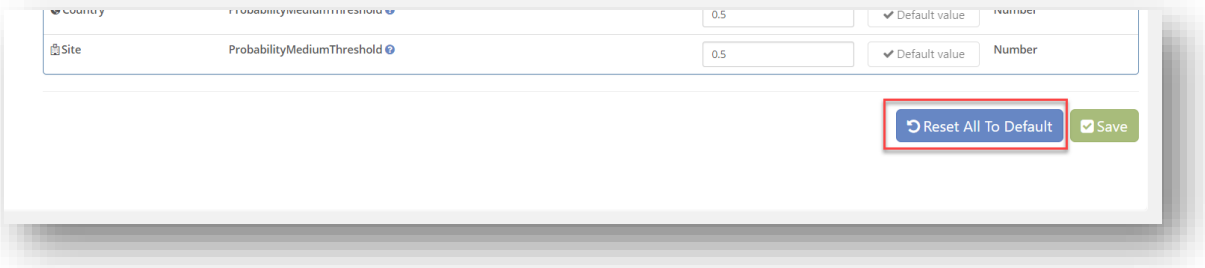
- Threshold for medium/high alert level
- Auto-closure of tickets: if KRI is de-escalated (returned to the yellow or green zone), it will auto-close the escalated tickets, auto-raised accordingly before

- Ticket creation timeout: KRI will not trigger tickets if a previous auto-created ticket was closed, despite the KRI remains escalated until that timeout, since the time of the previous ticket closure, has elapsed
- Muting
- Calculation disabled: disabling the calculation while keep displaying this KRI/QTL on UI
- Calculation parameters (scale)
- Others

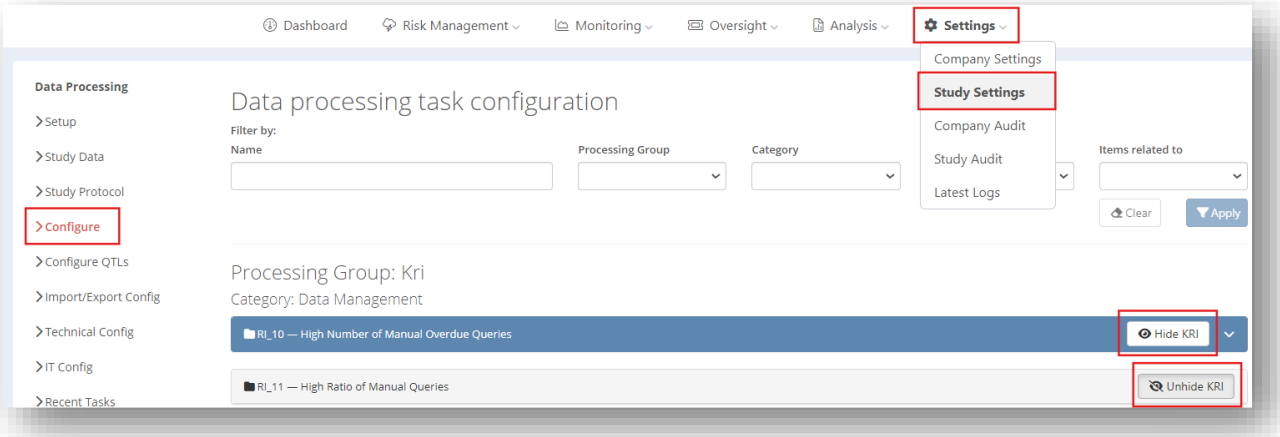
Clicking on the **Reset** button will return the parameter value or setting to default. (If a parameter has been changed, the user will see a **Reset** button in front of it.)



It is possible to **Reset All** [parameters] **to Default** at the bottom of the **Configure** tab.



For KRI there is a setting: **Hide KRI**, which stops the KRI calculation *and* tickets creation and hides the KRI from the UI.



There are several use cases for applying this functionality. For instance, to reuse a study type, KRI that are not relevant can be disabled and hidden from the interface to avoid developing separate study types for similar studies. Additionally, it is possible to hide KRI later during the study if they become irrelevant.

When KRI is hidden:

1. It will not be calculated; tickets will not be created.
2. It completely disappears from the related pages, where there was no important-to-be-recorded connection to this KRI (e.g., Sites List page, Sites Details page, KRI List page, Dashboard page: Risk Monitoring section (FMEA), Manage Custom KRI form, Create New Ticket form, Metric Information page, and others).
3. It gets replaced with "KRI was hidden [KRI ID - KRI Name]" (without a hyperlink) on the related pages, where there was an important-to-be-recorded connection to this KRI (e.g., Risks page: Associated RIs, Actions, Tickets and others).
4. On the Risks page, in the Associated Risk Indicators section, the hidden KRI remains displayed with the option: Adjust the Likelihood and Disconnect it from the Risk. We recommend checking and adjusting the likelihoods for all risks that were associated with the hidden KRI.
5. It stays on the Study Settings - Configure page, with the Unhide KRI button on the KRI bar.
6. It is not possible to change the KRI configuration while it is hidden.
7. If the only/last displayed KRI related to a particular metric is hidden, the metric gets hidden automatically.

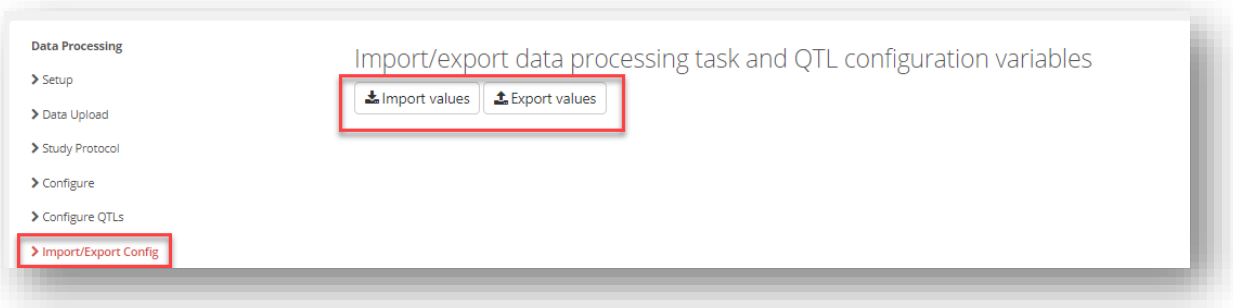
When KRI is unhidden:

1. It reappears on all relevant pages and sections where it was displayed before being hidden.
2. Its calculation restarts, tickets are created once it is unhidden.
3. Its configuration parameters are restored from the last saved version.

NOTE: Do not forget to click Save button and if requested, provide Rational for Change.

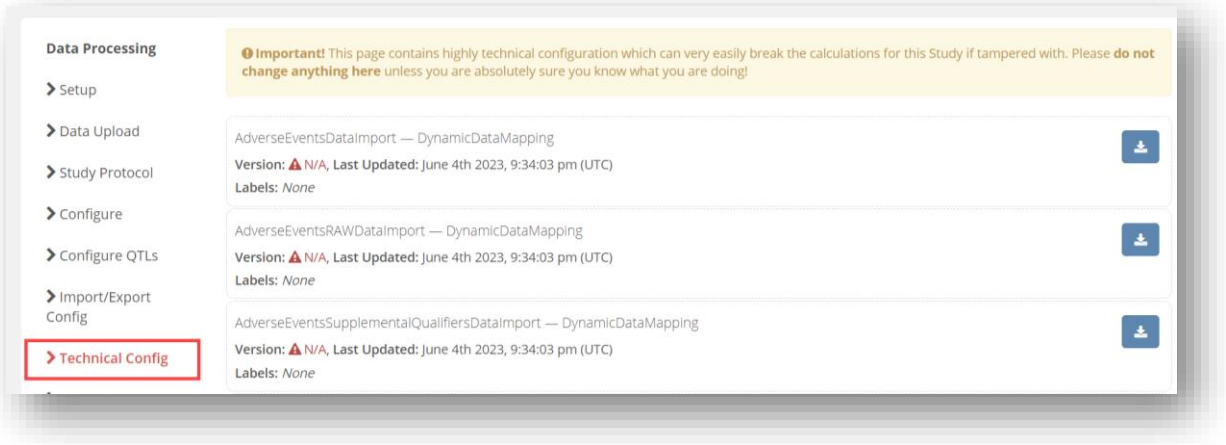
Import/Export Config

Users can upload and/or download KRI/QTL/Metrics and other items (available in Configure/ConfigureQTL) from a different study.



NOTE: Only those items' parameters that are configured in the study, where the configure file was imported, will be updated.

Technical Config



This page contains highly technical configuration, which can very easily break the calculations for this Study if tampered with.

Ideally all parameters under Technical Config should be set up before the study's status will set to "Live".

Due to the importance of these parameters, only Cyntegrity employees can make changes in Technical Config.

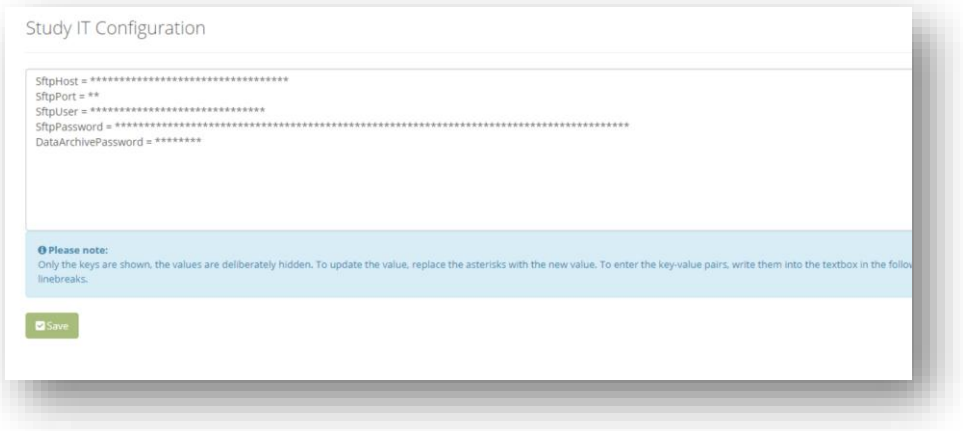
NOTE: It is not possible to change Technical Config for a "Live" Study.

IT Config

The IT configuration is utilized when retrieving study data from an external Data Lake.

An authorized user needs to input credentials into the designated text field. Each credential record should be displayed on a separate line, without any delimiters between the lines.

Example:



NOTE: Upon saving the IT configuration, the values (excluding parameter titles) will be concealed with "*" symbols for security.

User Groups

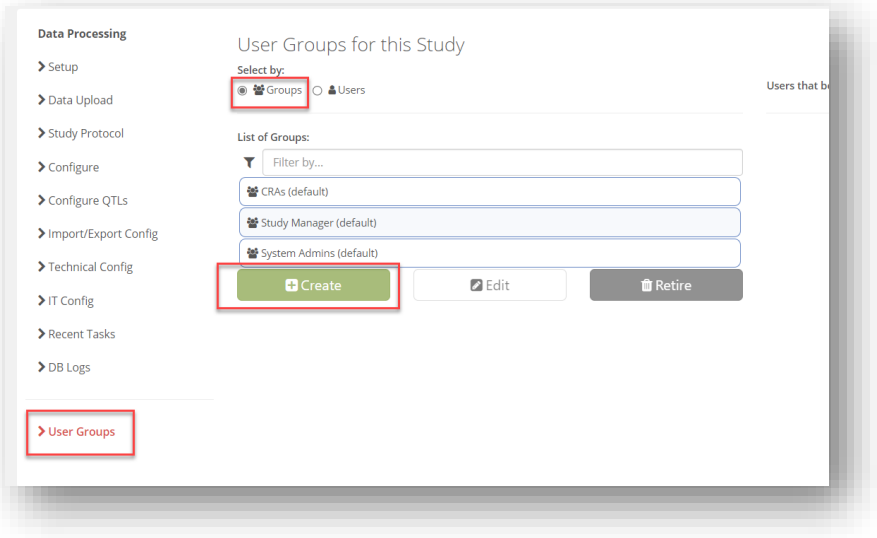
Groups contain users that should share the same set of preventive and mitigation actions. A group is **always assigned to a study**. Examples of predefined groups are: CRA, System Admins and Study Managers.

NOTE: Default groups can't be deleted.

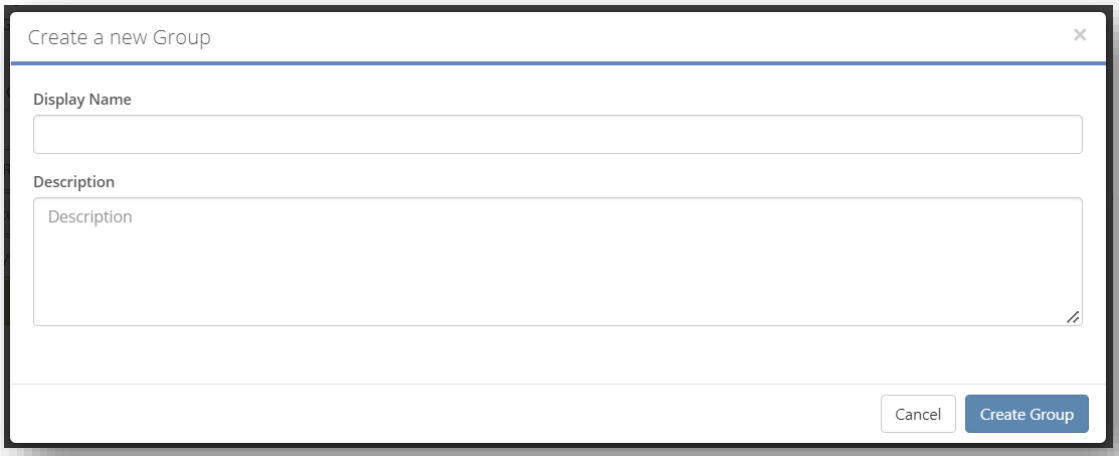
Create a New Group

To create a group:

1. Click **Settings** → **Study Settings** → **User Groups.**
2. In the opened tab, in the **Select by,** click **Groups.**
3. In the bottom of the existing groups list, click **Create**.



4. Enter a Display Name. Description is optional.



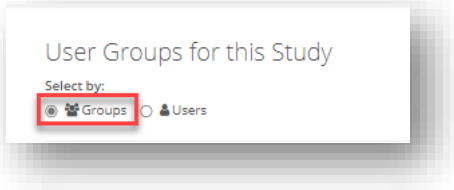
Users can:

- **Edit** the Group name and description
- **Retire** the Group.

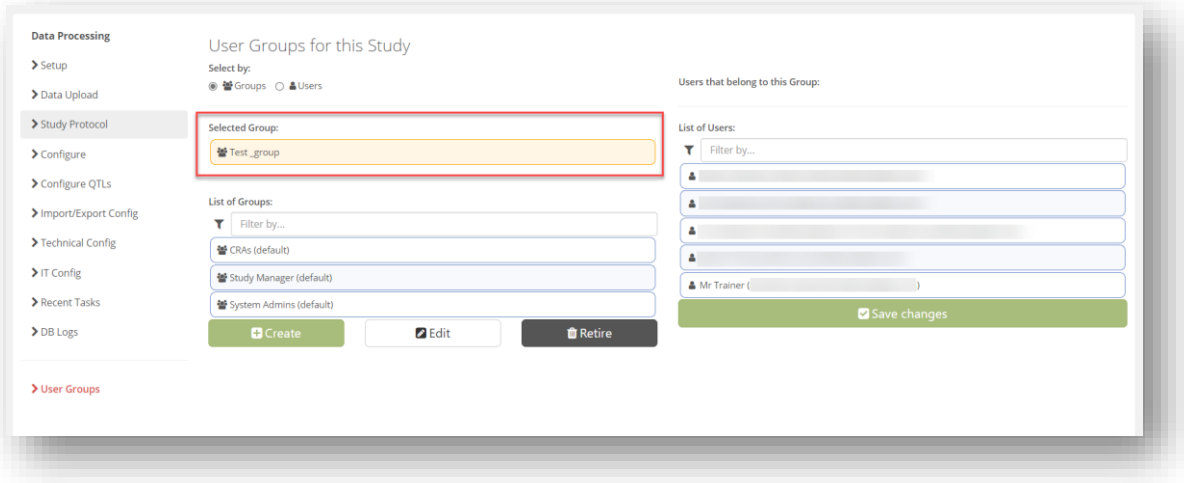
Assign a User to a Group

To assign a user to a predefined or a manually created group:

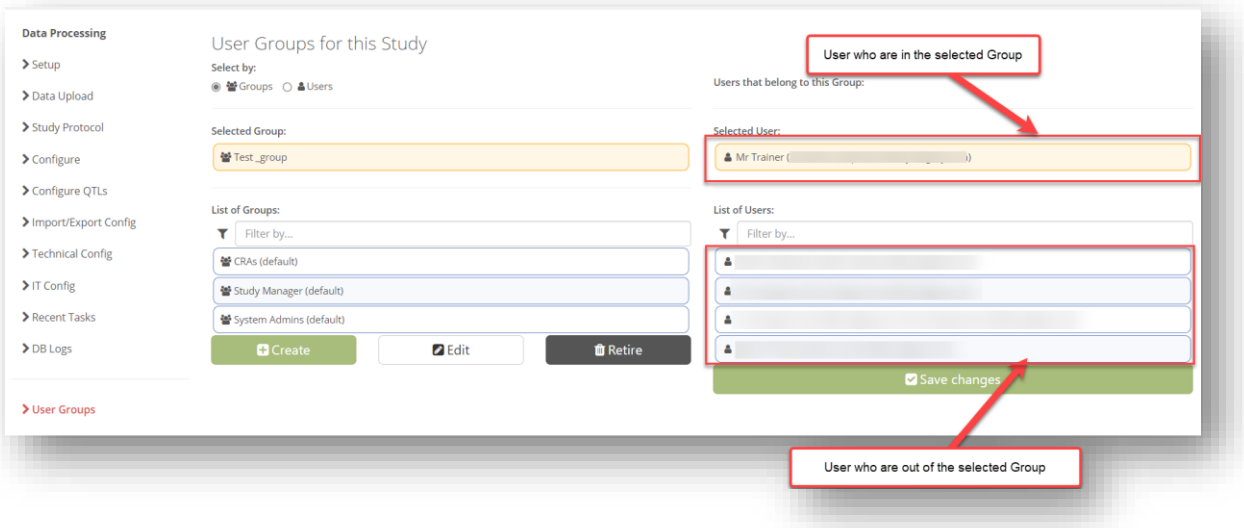
1. Click **Groups** in Select by switcher.



2. Click the Group name in the right-hand list.



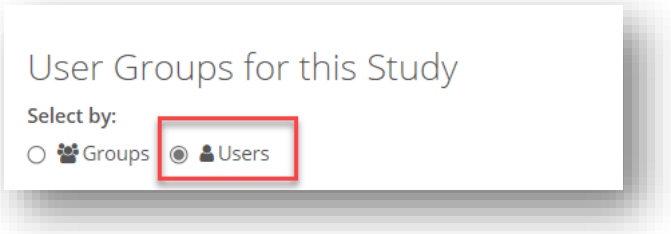
3. Select users who should be in the group by clicking on their names from the list on the left.



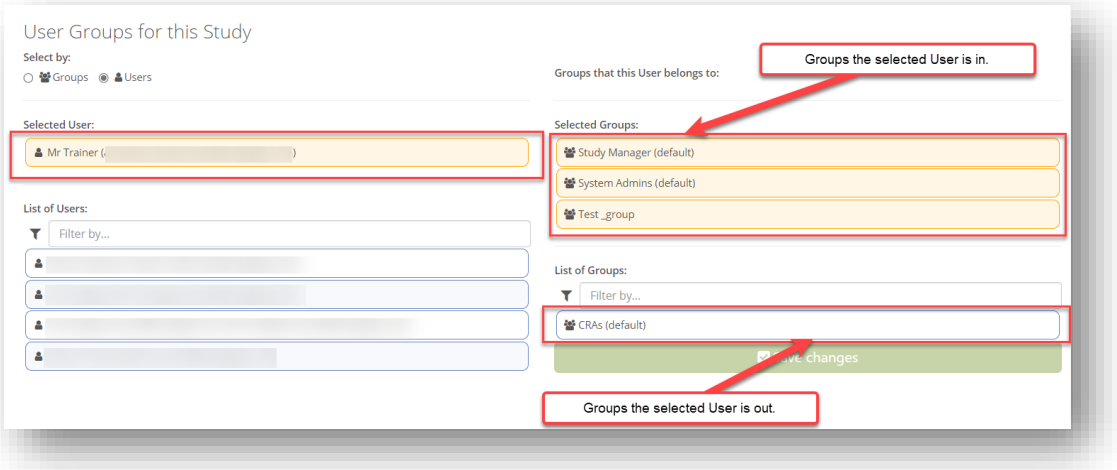
4. Click **Save Changes.**

Users can also manage groups from a user perspective:

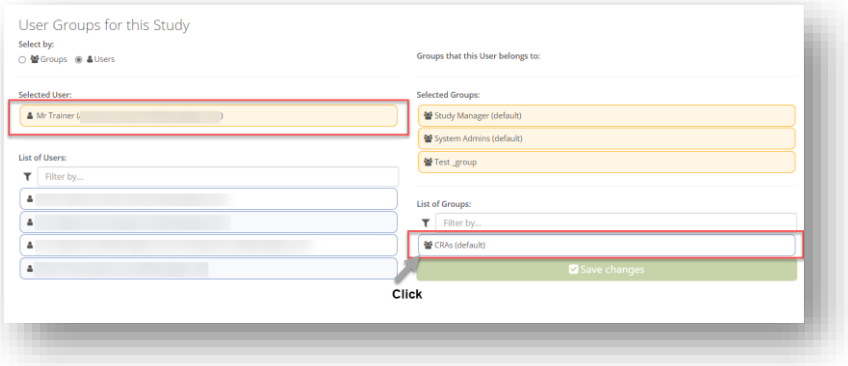
1. Select **Users** option in Select by.

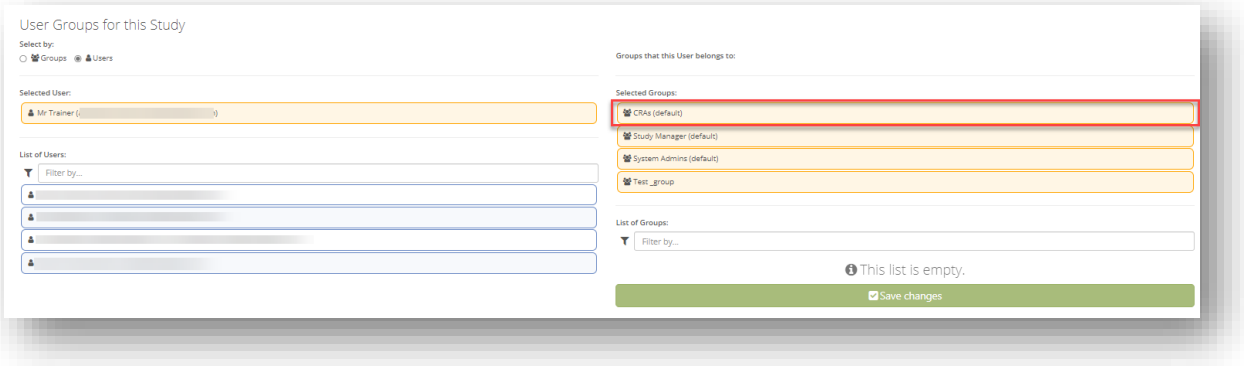


2. Select a user from right-hand list.



3. In the right-hand list, you'll see groups the user belongs to (highlighted in yellow) and groups the user is not part of (are shown in white icons).
4. Within the groups the user is not part of, (white icons) select those to which you want to add the user.





To remove a user from a Group:

1. Click **Users** in the **Select by** switcher.
2. Select the user whose membership of the Group you want to stop.
3. In the right-hand groups list, you will see all groups to which the user is member.
4. Click the Group from which you want to remove the user (it will be moved to the bottom list and will be shown as a white icon).
5. Click **Save Changes.**

Assign Groups to Mitigation Actions

To assign a group to a Mitigation Action:

For Risk Mitigation Actions:

1. Go to **Actions** in the menu bar.
2. Create a new mitigation action.
3. Select the user or group in the Responsible field.

For Ticket Investigative/Corrective Actions:

1. Go to **Tickets** in the menu bar.
2. Open the ticket for which you want to create an Action and add an Investigative/Corrective or Preventive Action.
3. Select the user or group in the **Responsible** field.

Action Settings

Default Action settings

- Manual closure of investigative corrective actions is allowed.
- "Every" and "Once at" review options are switched on for all actions.
- Study settings are inherited from Company level.

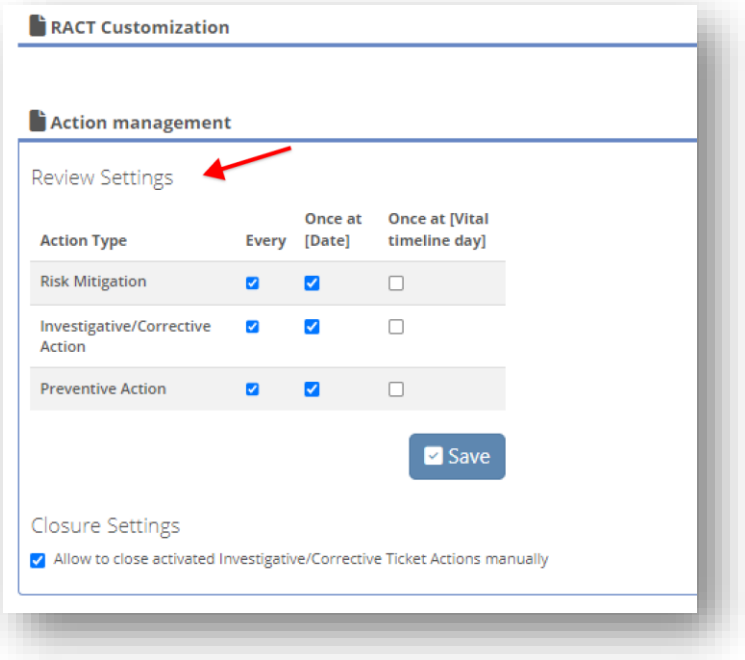
Review Settings.

It is possible to set Action Review Date options both at Study and Company Levels.

NOTE: The settings specified in the Study Settings hold priority over those in the Company Configuration.

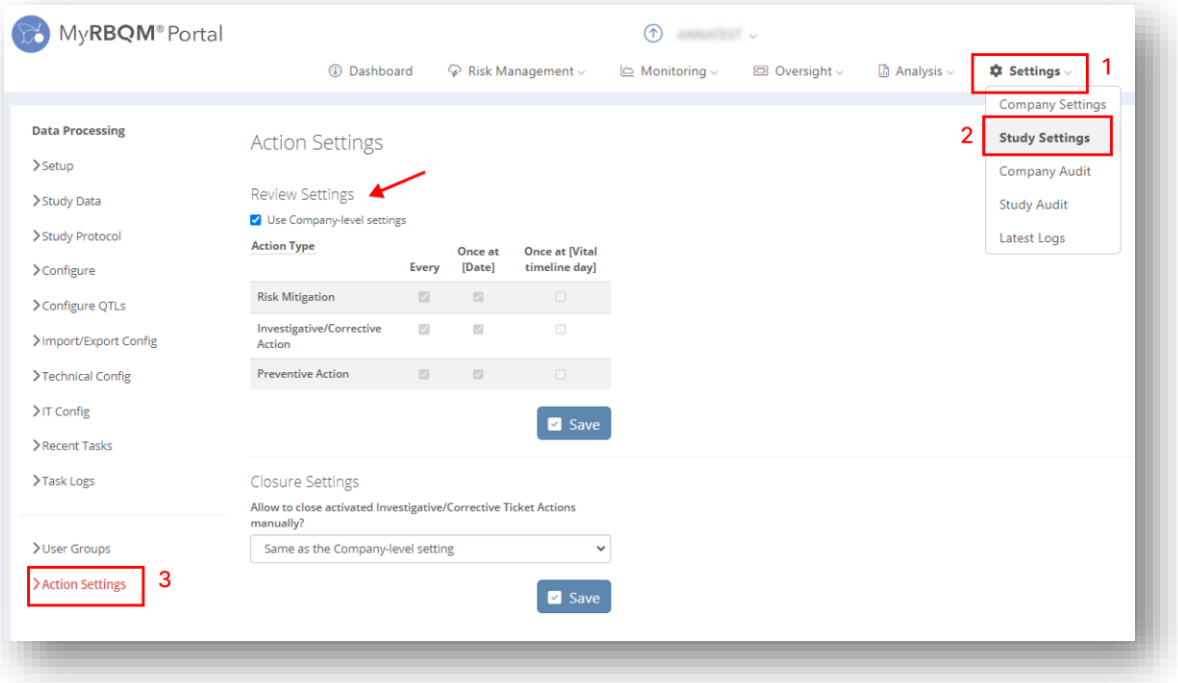
Company Configuration

Go to **Settings** → **Company Settings** → **Company Management tab**:



Study Settings

It is possible to set Action Review Date options at Study Level.



NOTE: At least one Date Setting should be selected for each Action Type.

Closure Settings

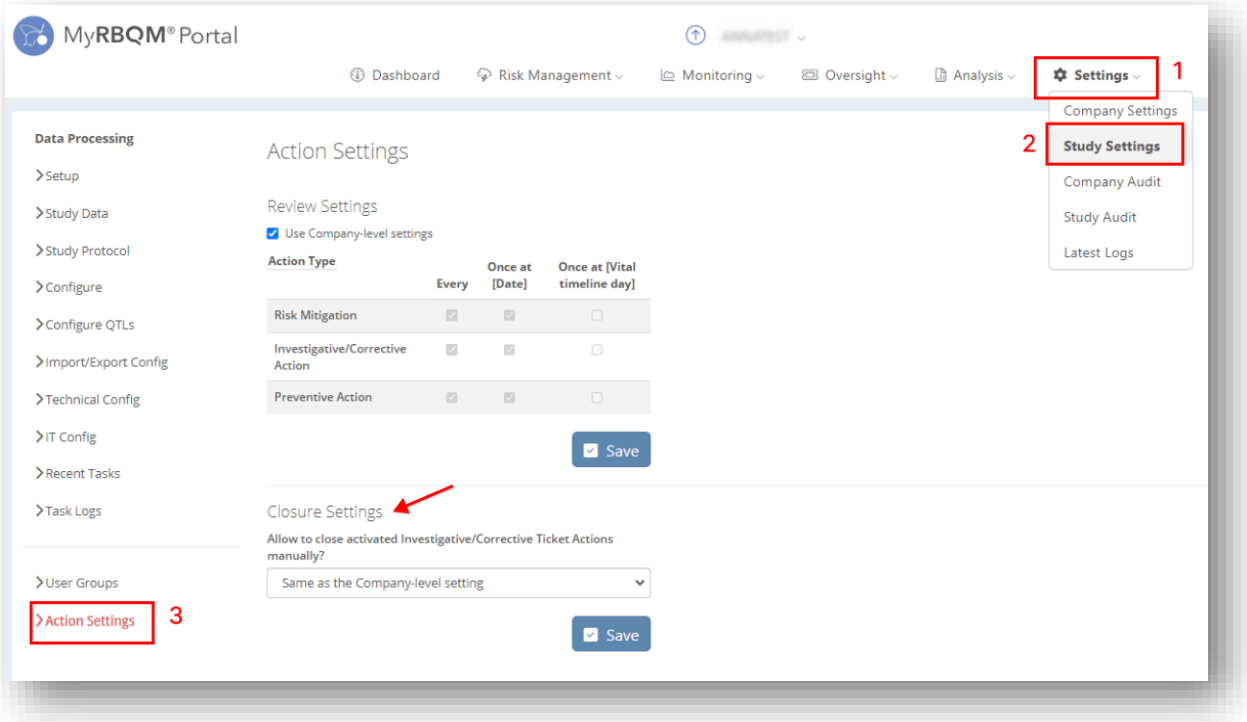
In the event of integration between the actions in MyRBQM and an external CTMS system, avoid manually closing actions in MyRBQM.

The closure of actions should only occur based on information received from the third-party system.

To facilitate this, the Investigative/Corrective Actions Closure settings were implemented in both the Study Settings and Company Configuration.

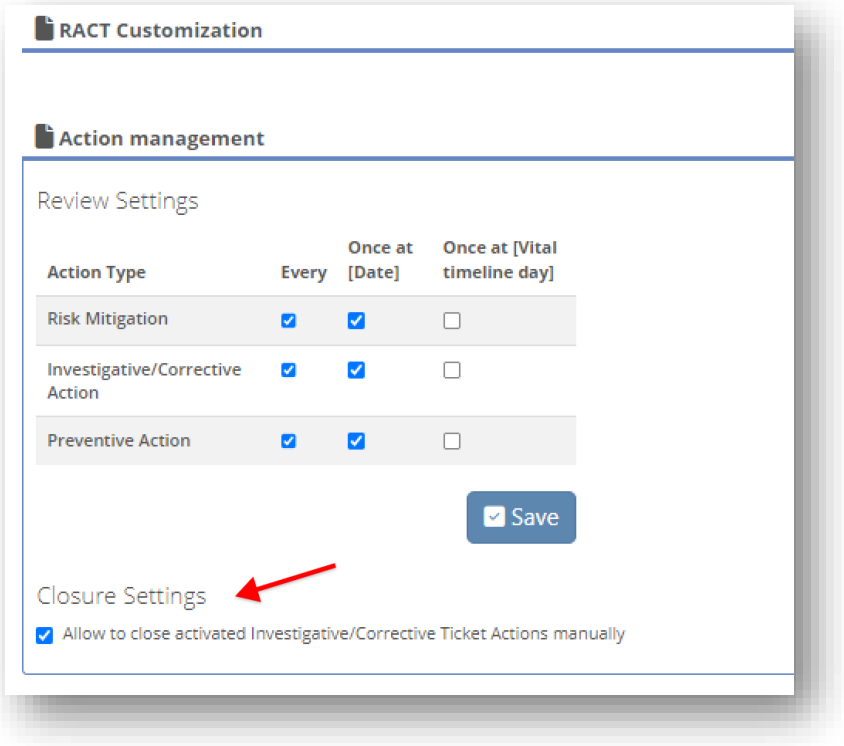
NOTE: The settings specified in the Study Settings hold priority over those in the Company Configuration.

Study Settings:



Company Configuration:

Go to **Settings → Company Settings → Company Management tab**:



Company Settings (Configuration)

To open the **Company Settings menu**, go to **Settings** in the upper menu and select **Company Settings** point from the drop-down list.

Company Management

Customize Your Company Account

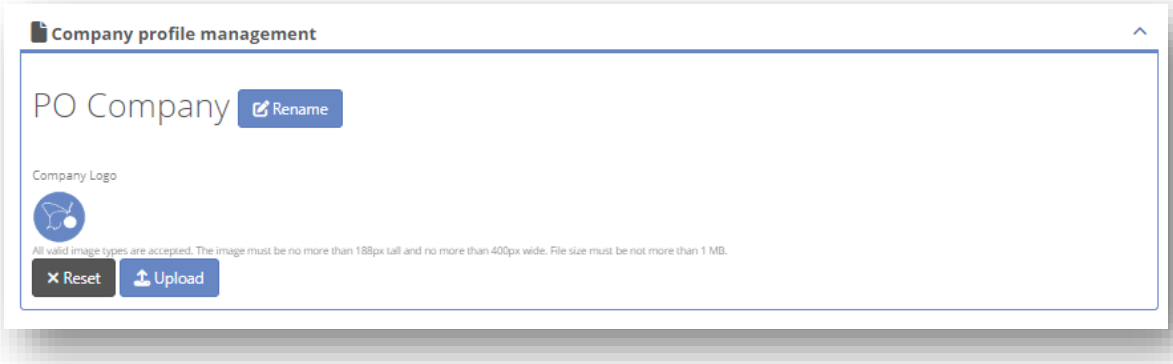
Just as users can customize their user accounts with detailed user information and pictures, **MyRBQM® Portal**, allows the same for companies.

To support the corporate identity of your company, you can customize the visual user experience for all users working in the company account. In this context, companies can customize the logo shown in the upper left corner on every site. To do so:

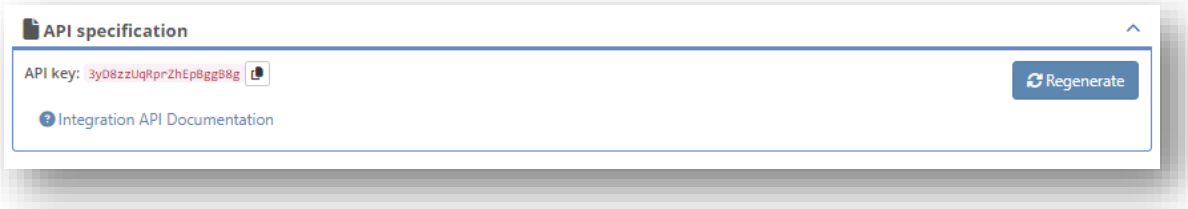
1. Go to **Settings** in the menu bar.
2. Select **Company Settings** from the drop-down menu.
3. In the **ConfigurationHub**, click **Company Management.**
4. Click **Upload** to choose a picture from your storage to replace the **MyRBQM® Portal** logo for all your users.

In the **Company Management** menu item, it is also possible to:

- Rename your Company and Change the Logo

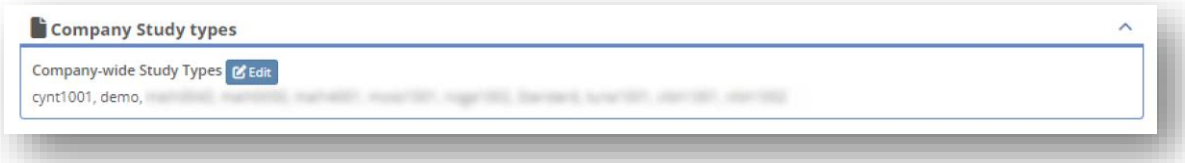


- Obtain Integration API keys and Documentation

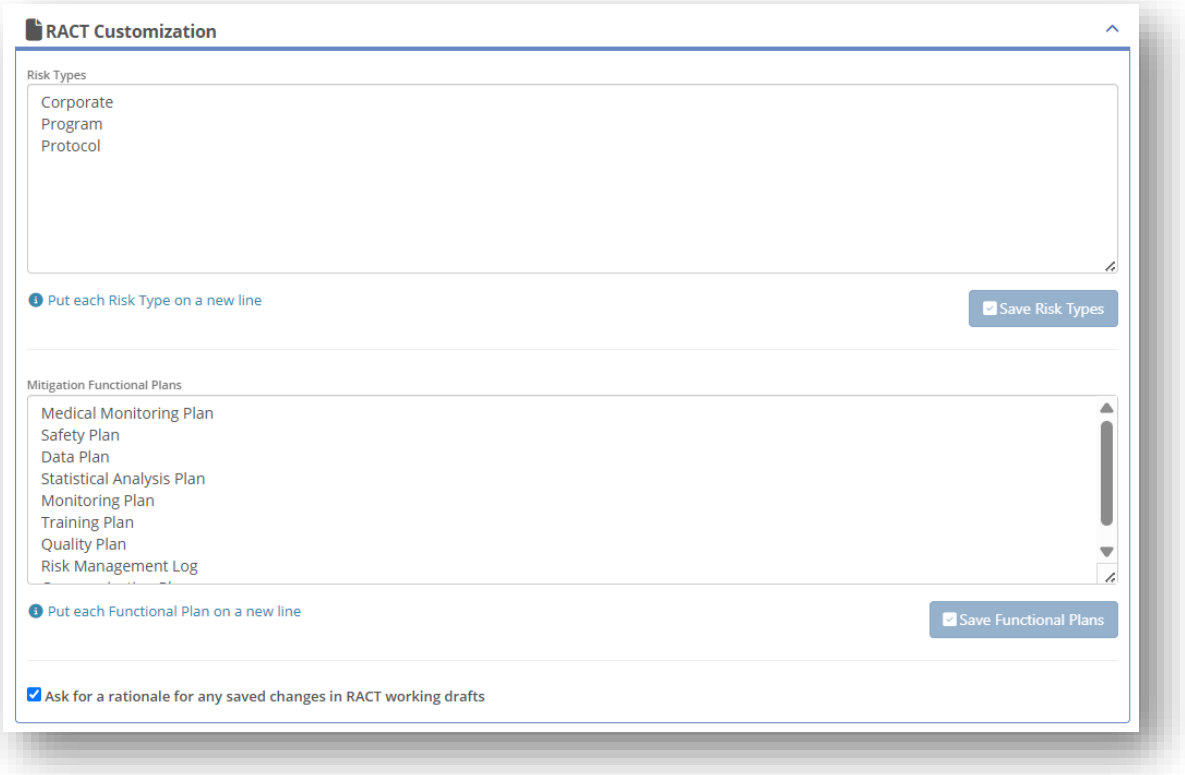


- Manage AI functionality (disabled by default)

- Change Company Study Types display names



- Set up Risk Types (RACT), Mitigation Functional Plans (for Mitigation Actions associated with a Risk) and Asking for a rationale for any saved changes in RACT working drafts

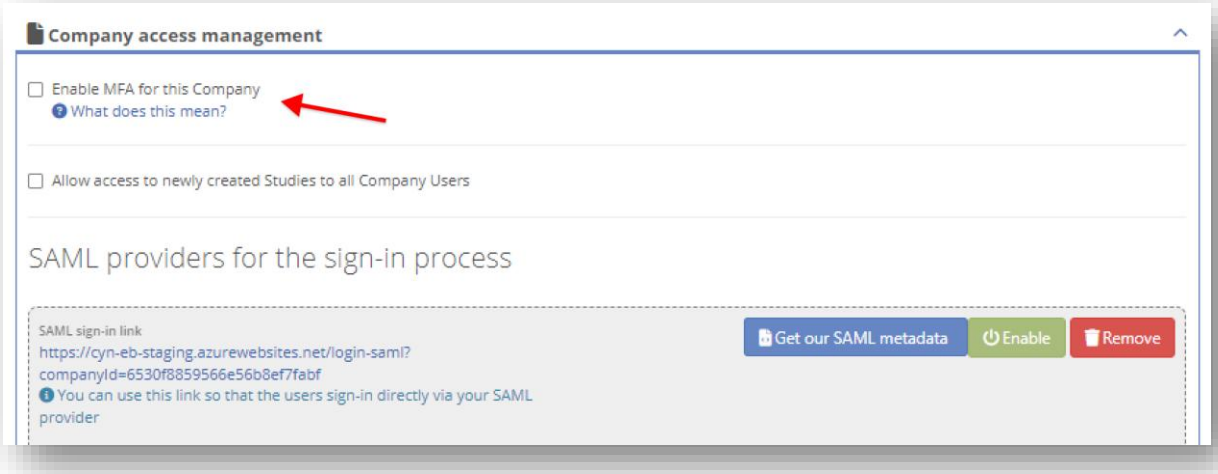


- Manage Actions review and closure settings.

Multi Factor Authorisation (MFA)

To enable MFA:

Go to **Settings** (upper menu) then **Company Settings** and **Company Management.**



NOTE: if the MFA is enabled, a user will not be able to change their password.

Enabled MFA function will cause these changes in the user management and login to the system:

- Users who cannot change their password should send a request to the Company/Business Administrator (C/BA).
- A new user will receive an email with a request to connect C/BA to generate a password.
- Verification code is required for Login. The code will be sent to the user email.

NOTE: The rules described in this paragraph are not valid if SSO is activated.

Single Sign-On (SSO)

Setting up SSO is a technical operation what should be performed by an IT specialist.

If you would like to implement SSO, please contact your Cyntegrity Project Manager or Customer Support.

Sometimes the email invitation is sorted as SPAM by the email.

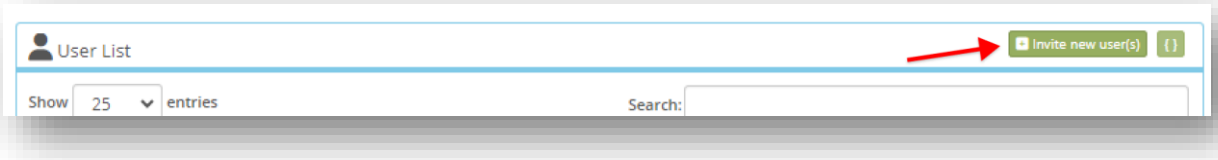
User Management

On this tab, the **Company Administrator** can:

- Invite a new user
- Block a user
- Add/Edit account details
- Send Password reset Email (if no SSO)
- Change subscription settings
- Assign existing Roles

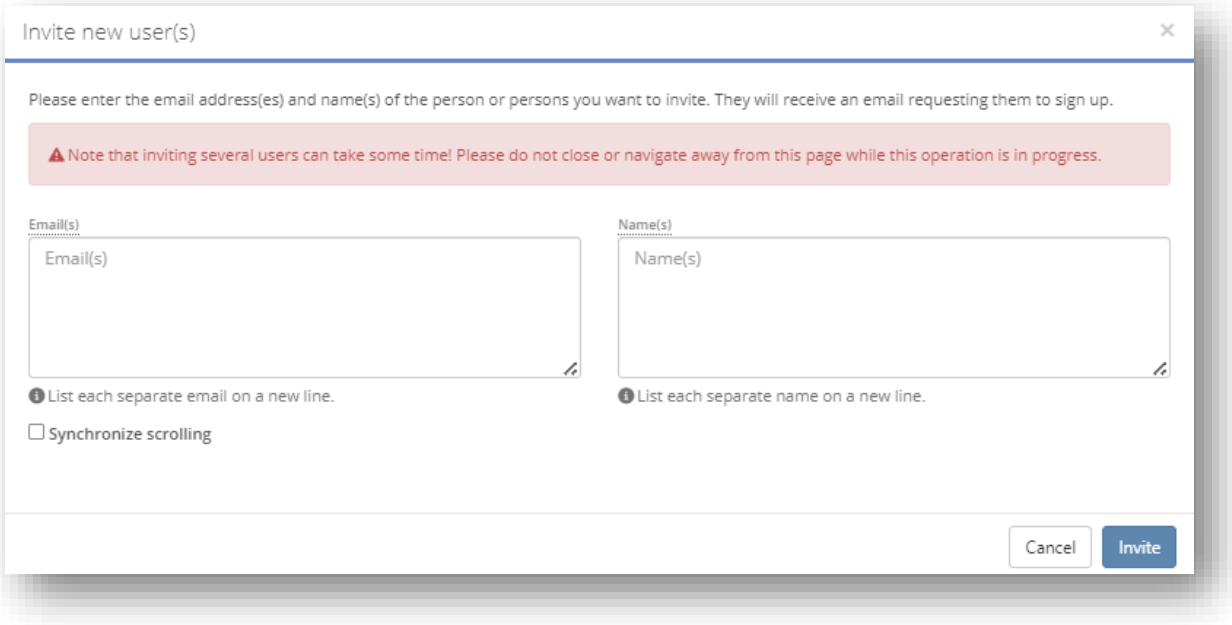
Invite a New User

1. Click the + sign and select **Invite a New User.**

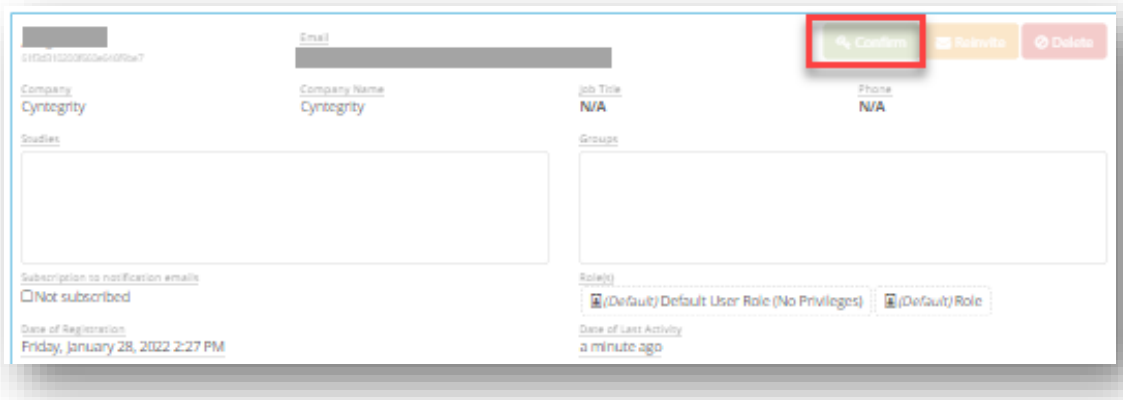


2. Enter the **email address(es)** and a **username(s)** for the new user(s).

3. Confirm by clicking **Invite**. An email invitation will be sent to the new user.
4. Users can invite several new users simultaneously. In this case, an administrator should check that user names order corelates with user emails.

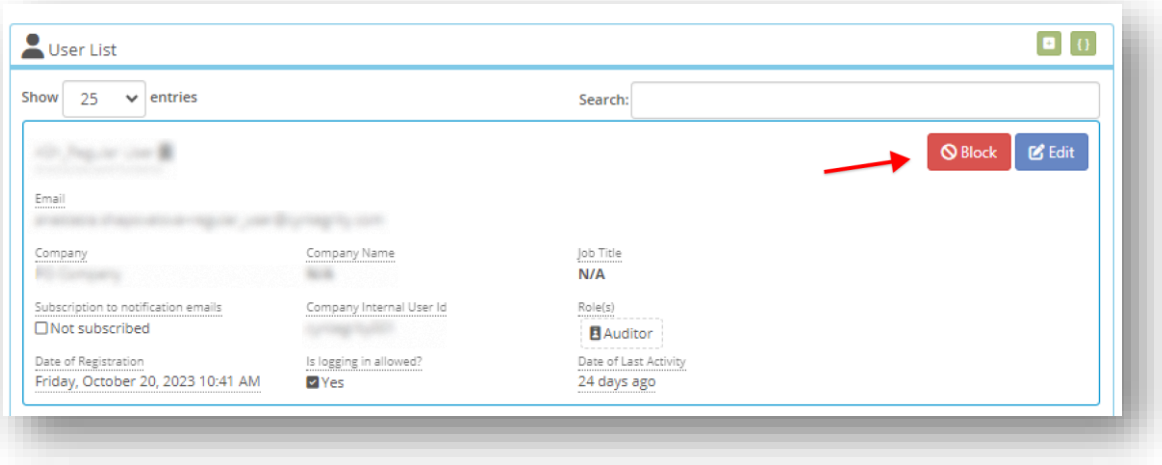


The administrator can confirm the user's account:



Block/Unblock a User

Click **Block** button.



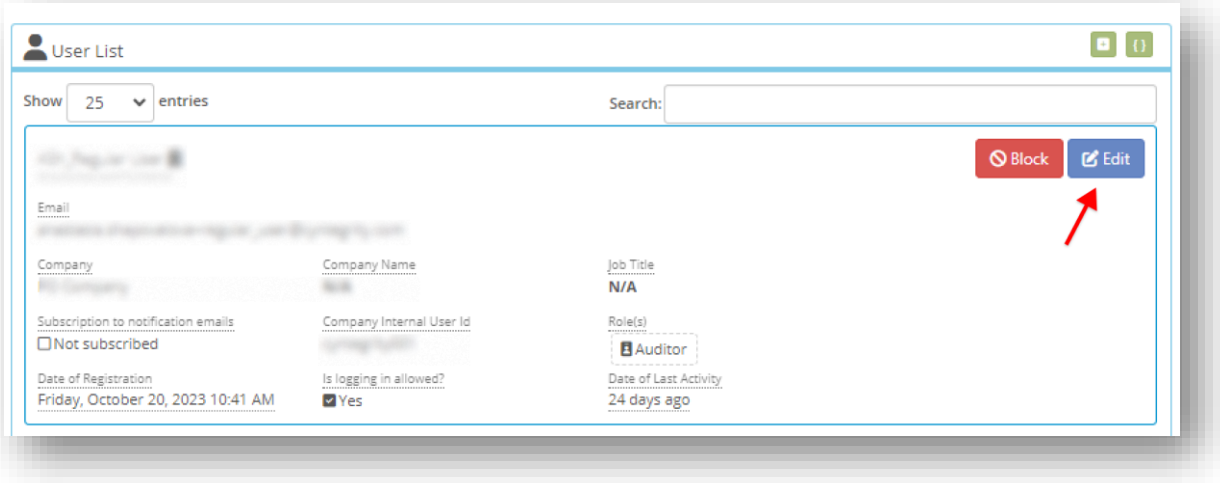
Blocked users can still log into their account but cannot use any functions of **MyRBQM® Portal**. Upon logging in, blocked users are informed about their account status.

Click **Unblock** to unblock a user. Immediately after unblocking, s/he can use **MyRBQM® Portal** again.

NOTE: A user cannot block her-/himself.

Edit a User

1. Click **Edit** to change any account details of the desired user.



2. Click **Save**.

Give Admin Privileges

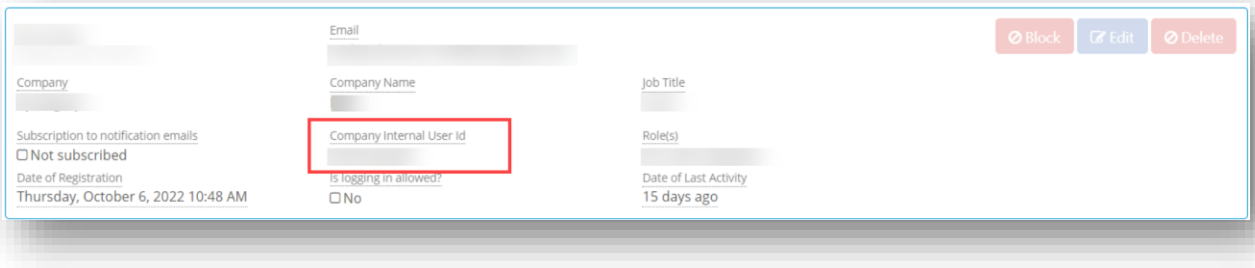
1. Click **Edit** to change any account details of the desired user.
2. Check the field under **Admin Privileges** that fits the privileges the user should have in your **MyRBQM® Portal** Environment. Choose between **No Admin rights** and **Company Admin rights**.
3. Confirm by clicking on **Save.**

NOTE: A user cannot elevate another user above his/her own administrative privileges.

Company [Customer] Internal ID

If the Customer Company chooses to integrate MyRBQM with another system, it may be necessary to include the Customer's internal ID. This ensures that user records can

be synchronized smoothly between the independent systems.



NOTE: it is not possible to add Customer Internal User ID through UI - only if the user record is created or updated through integration API.

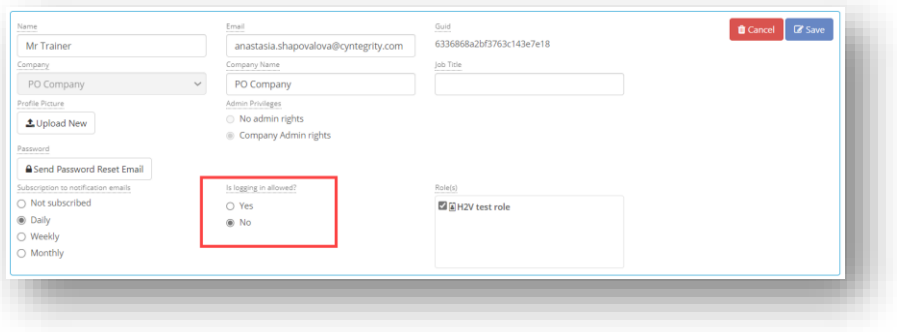
Allow Login

During the synchronization process of MyRBQM with an external system, the Customer Administrator may encounter a scenario where the external system is utilized by users who are not registered or authorized to use MyRBQM, meaning they have not undergone training or certification for MyRBQM usage. In such cases, a solution is available.

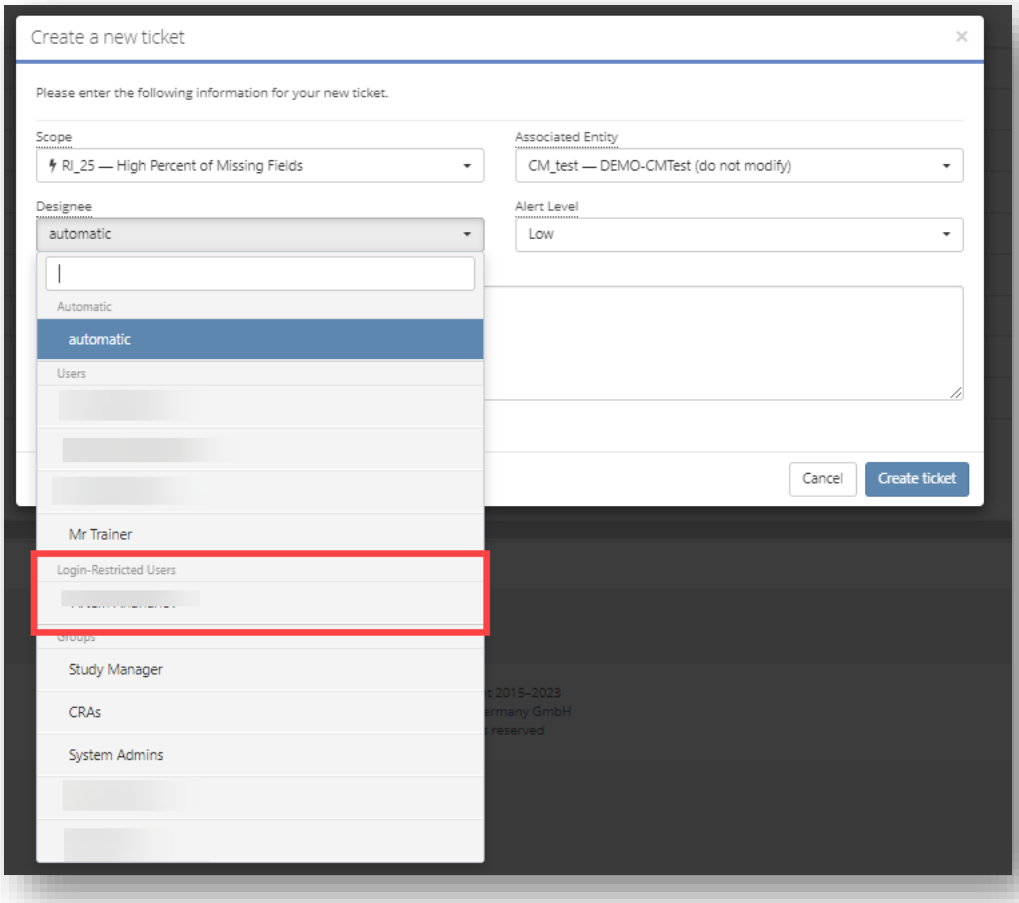
To address this situation, the option to create Login-Restricted users in MyRBQM is provided.

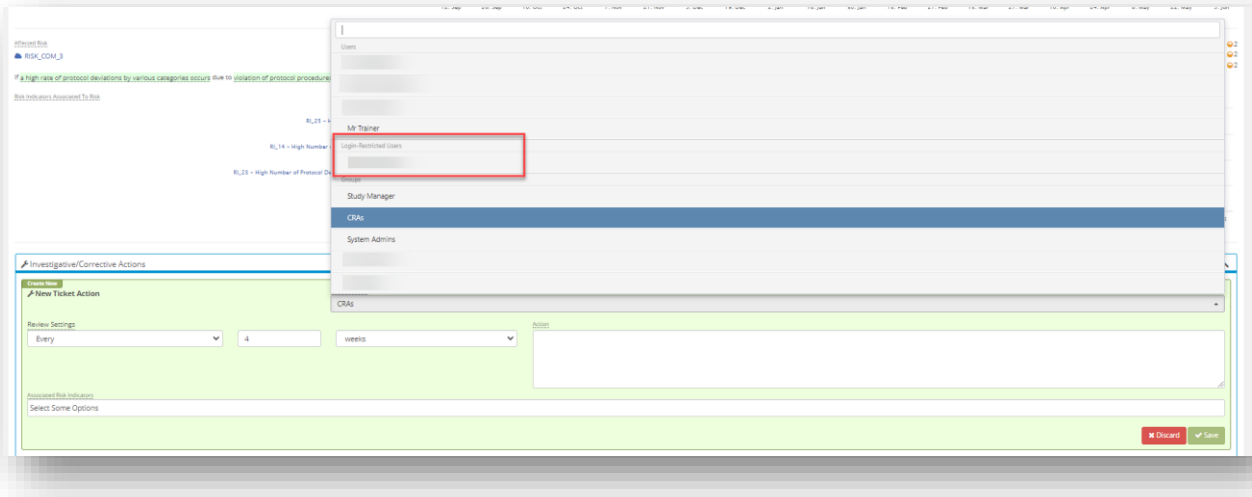
These users will have standard user profiles, but their "Is logging in allowed?" setting will be set to "No."

This configuration ensures that, while these users exist within MyRBQM, they are restricted from logging in and accessing the system.



In this scenario, users will be unable to log in to the system, but they can still be assigned to studies, tickets, or actions within the system. They can also be added to a group.


Create a new ticket
Please enter the following information for your new ticket.
Scope
RI_25 — High Percent of Missing Fields
Associated Entity
CM_test — DEMO-CMTest (do not modify)
Designee
automatic
Alert Level
Low
Automatic
automatic
Users
Mr Trainer
Login-Restricted Users
Groups
Study Manager
CRAs
System Admins
Cancel
Create ticket



The Designee drop-down lists are organized in next way:

- Users
- Login-Restricted Users
- Groups

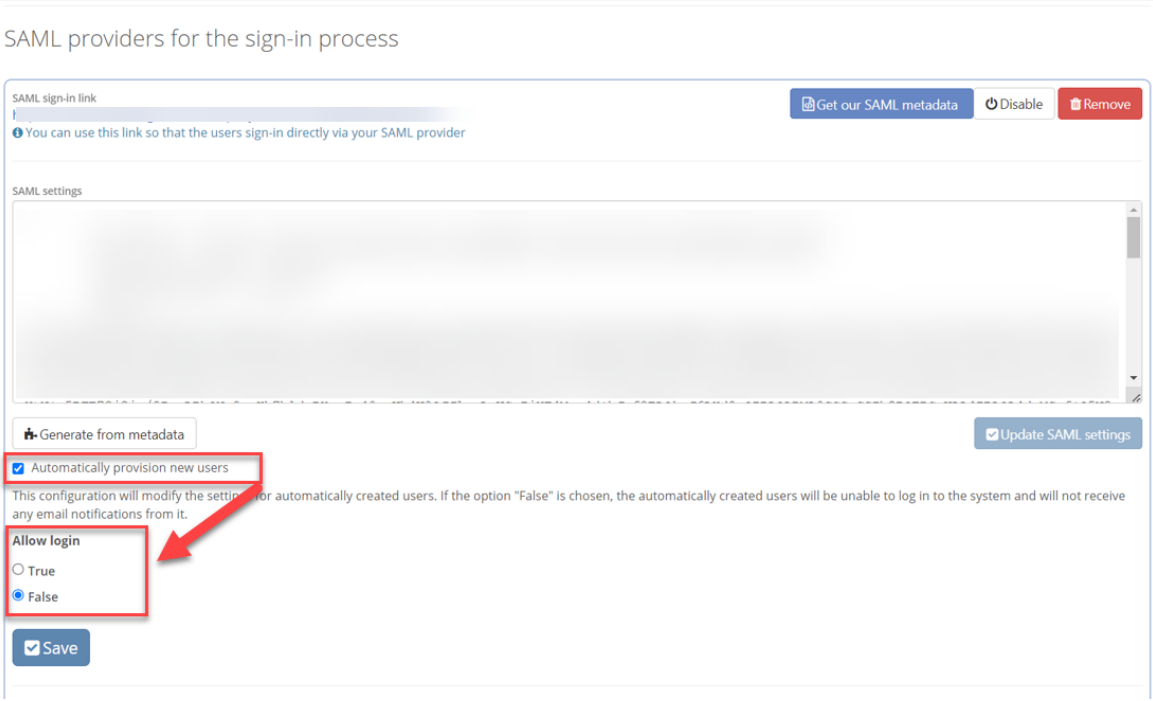
NOTE: Users who are not permitted to log in to MyRBQM will not receive any notifications, neither through the Notification List nor via email.

Allow Login and SSO

Allow Login settings are also presented in SSO "Automatically provision new users".

If "Automatically provision new users" is switched on (as shown in the picture below) the Company Administrator can set up the "Allow Login" parameter.

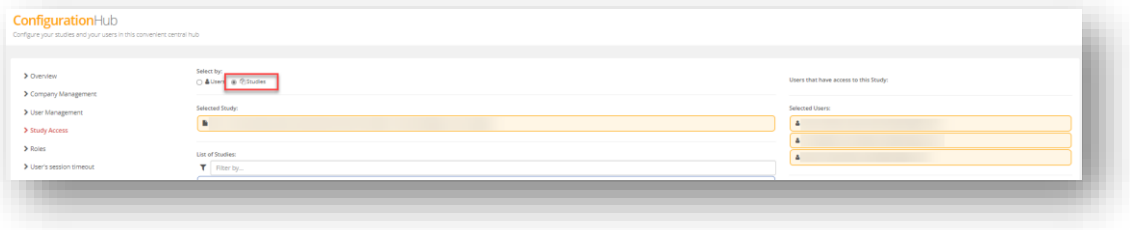
By default, "Allow Login" is False.



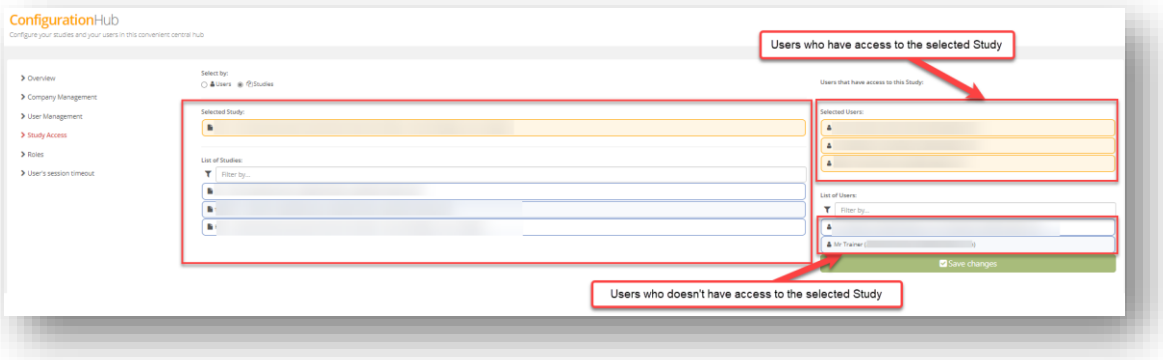
Study Access

To assign a user to one or more Studies:

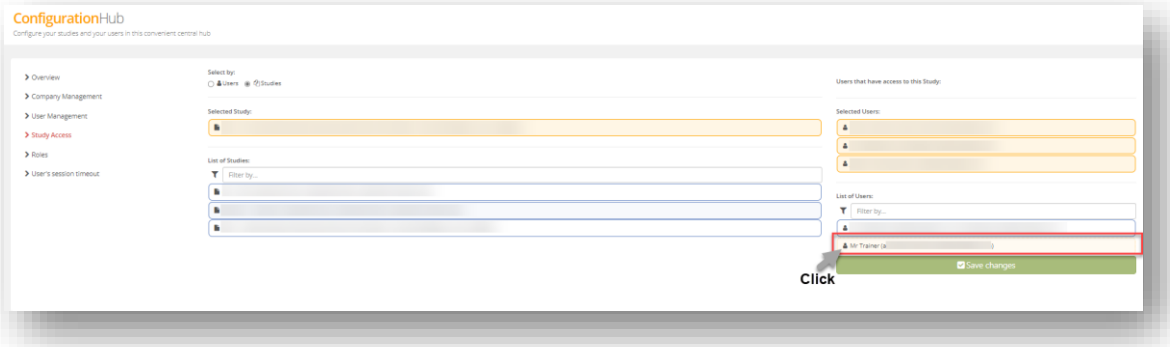
1. Switch **Select by:** switcher to **Studies.**

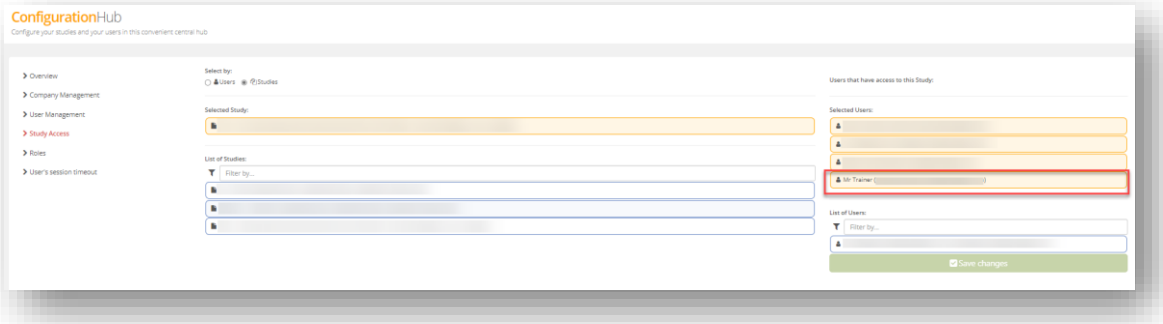


2. Select a Study (click the Study name in the list).



3. In the right-hand list, click on the name of users who should be assigned to the selected.

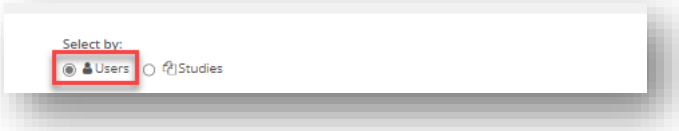




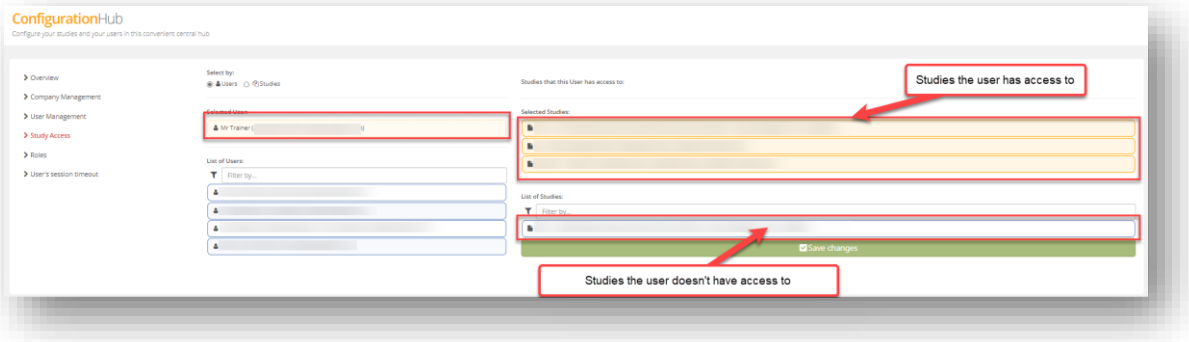
4. Click **Save Changes.**

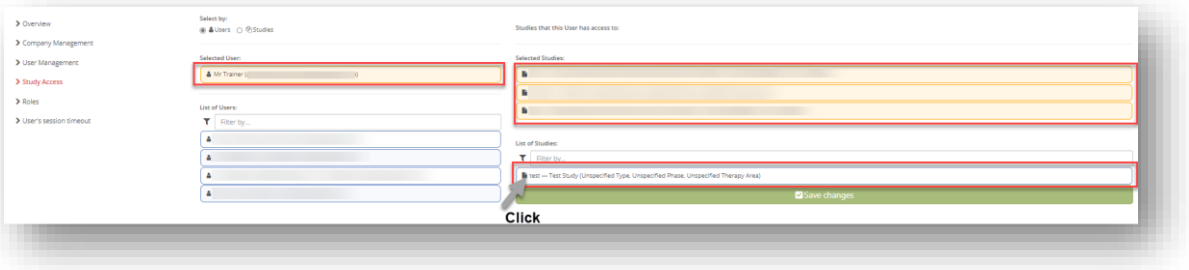
It is also possible to manage study access from the user perspective:

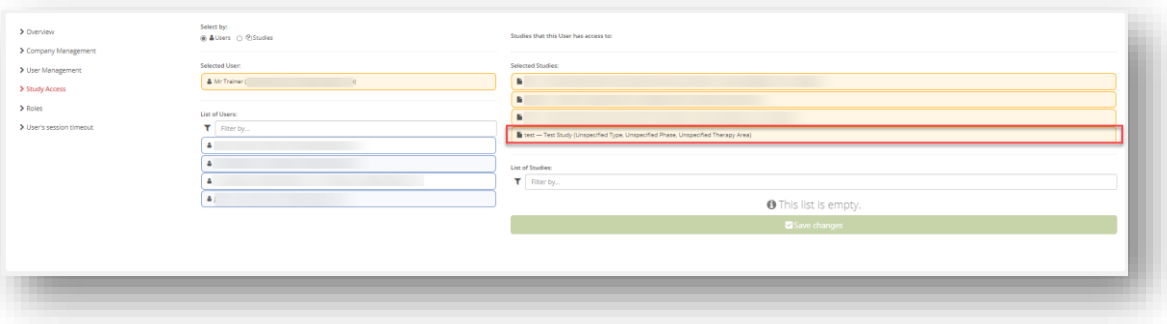
1. Select **Users** option in **Select by**.



2. Select a user from left-hand list.
3. In the right-hand, list you'll see studies the user has access to highlighted in yellow, and studies the user doesn't have access (white icons). Select the studies to which the user should be assigned.



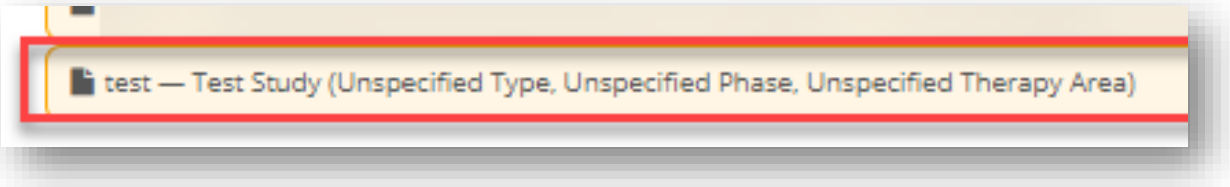




4. Click **Save Changes.**

NOTE: For your convenience, each study icon contains some information about studies:

- Name
- ID
- Type
- Phase
- Therapy Area



To remove the user assignment to a Study:

1. Click **Users** in the **Select by** switcher.
2. Select the intended user.
3. In the right-hand studies list, you will see all studies assigned to the user.

4. Click the study from which you would like to remove user access.
5. **Save Changes**.

Privileges and Roles

The system uses a role-based security model so that user permissions are tailored to the tasks the user needs to perform. Example roles are:

- Central Monitors
- Study Team Member
- Global Trial Manager
- Risk Management Lead
- Business Administrator
- Auditor

NOTE: MyRBQM® Portal does not have the capability to assign ownership.

Privileges

Your Business Administrator/Authorized user can create Roles combining the privileges below:

Privilege	Function
Accept Risks & Create Mitigations	Access the course of action for a Risk section:
	Accept Risks

	Create Mitigation Actions (including Suggestions and Ask AI)
	Edit the Risk's Acceptance Rationale
Access Audit Logs	Access Study Audit Trial and Company Audit Trial
Access Data Import Logs	Access Study Settings hub
	View Recent Tasks page (Latest imports, Latest data processing tasks)
Access Database Logs	Access Study Settings hub
	View Task Logs page
Assign & Edit Investigative Actions	Create, edit, activate, review, close and delete Investigative/Corrective Actions
	("View Tickets" privilege is required to access Tickets page)
Assign & Edit Preventive Actions	Create, edit, activate, review, close and delete Preventive Actions
	(To close: ticket should be active, Root Cause Analysis should be started)
	("View Tickets" privilege is required to access Tickets page)
	("Assign & Edit Tickets" privilege is required to access Preventive Actions section)
Assign & Edit Tickets	Activate, assign, re-assign, close Tickets
	Start and re-start (only for Active tickets), finish Root Cause Analysis
	Add, edit, remove root causes
	("View Tickets" privilege is required to access Tickets page)
CDQ - Access Compliance and Data Quality Check	Access Compliance and Data Quality Check module
CDQ - Configure Workflow	Access "Configure Workflow" page in the Compliance and Data Quality Check module Update the default designee for newly detected Compliance and Data Quality issues
CDQ - Status Change	Update status of the detected issues in the Compliance and Data Quality Check module
Company Administrator	All existing privileges are included in CA privilege by default. In addition CA privilege gives rights to:
	Manage Company Settings (including Invite, edit, block users, give Company Admin right, set user Session Timeout, configure SSO, access company integration API, Set

	Actions Review Settings Company LevelSet Investigative/Corrective Actions Closure settings at Company Level)
	See Retired Sites
	Manage Study Settings (including Set Study to Non-Live, Delete Study Data, Delete Pending Tasks, Manage Data Processing, Upload/download Additional Study Protocol Data and Study Data)
	Set Default Root Causes for Root Cause Analysis on a study level
	Cancel processing, delete, archive CSM Requests create by another user
Create CSM-related Tickets	Create a ticket from the CSM Request Results page and Request Summary page
	("View CSM" privilege is required to access CSM requests page)
Create Generic Tickets	Create a ticket from the Tickets page
	("View Tickets" privilege is required to access Tickets page)
Create KRI-related Tickets	Create a ticket from the Risk Indicator page
	("View KRIs" privilege is required to access KRIs page)
Create QTL-related Tickets	Create a ticket from the QTL page
	("View QTLs" privilege is required to access QTLs page)
Create Site-related Tickets	Create a ticket from the Site Details page
	("View Sites" privilege is required to access Sites page)
Create Subject Profile-related Tickets	Create a ticket from the Subject Profile page
	("View Subject Profiles Dashboard" privilege is required to access Subjects page)
Define Company Roles	Access Configuration hub (Company Settings)
	Access Roles page
	Create, edit, delete, import and export Roles, set a default role
Download IQRMP Reports	Download IQRMP Report from the Risk Management Overview page
Edit & Activate Mitigations	Edit, activate and delete (to delete, status should be "New") Mitigation Actions
Edit & Add Report Templates	Create, edit and delete Datasource templates on the Datasource page
	Create, edit and delete Reports on the Reports page
	("View Reports" privilege is required to access Reports and Data Sources pages)

Edit Automatic Ticket Assignment	Access Ticketing System Configuration from the Tickets page
	Configure default designees for new tickets on different levels
	("View Tickets" privilege is required to access Tickets page)
Edit QTL Configuration	Access Configure QTLs page in the Study Settings hub
	Manage settings in Configure QTLs page
Edit RACT Drafts	Edit RACT Working Draft (including Edit Risks)
Edit Study Details	Edit Study Details on the Study Details page
Generate AI Critical Processes and Data	Generate Study Critical Processes and Data on the AI-Enhanced Protocol Analysis tool page
	AI-Generated Study Critical Processes and Data: view, edit, delete, download
Generate AI Risk Assessment	Generate Risk Assessment on the AI-Enhanced Protocol Analysis tool page
	AI-Generated Risk Assessment: view, edit, delete
Import/Export Configuration Variables	Import or export KRI/QTL Values on the Import/Export Config page in the Study Settings hub
KRI Linkage to Risks	Add and remove an Associated Risk Indicator on the Risks Overview Page
	Edit Likelihood of a Risk if KRI fires
KRI Threshold Changes	Access Configure page in the Study Settings hub
	Manage settings in Configure page
Manage Action Settings	Access Actions Settings page in the Study Settings hub
	Set Actions Review Settings at Study level
	Set Investigative-Corrective Actions Closure settings at Study Level
	Choose to use Company-level settings for a study
Manage CSM	Create CSM request
	Edit, send for processing any CSM request
	Cancel processing, Delete, Archive only created by me CSM Requests
	("View CSM" privilege is required to access CSM requests page)
Manage Catalogs	Create, import, edit, edit details, copy and delete Catalogs
	("View Catalogs" privilege is required to access Catalogs page)
	Access Company Critical Processes and Data

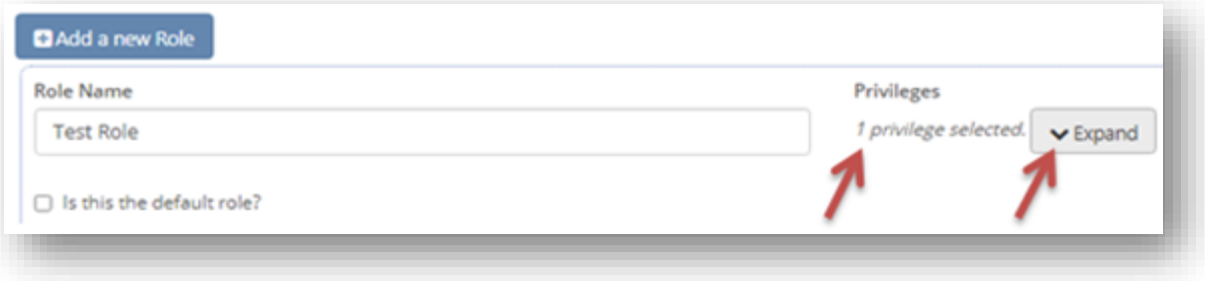
Manage Critical Processes and Data	Access Company Critical Processes and Data Edit, delete, import, mark as critical Company Critical Processes and Data Access Study Critical Processes and Data Edit, delete, import, mark as critical Study Critical Processes and Data
Manage Custom Calculations	Create, monitor and manage customer-provided metrics, KRIs and QTLs
	("View Metrics", "View KRIs" and "View QTLs" privileges are required to access relevant pages)
Manage Groups	Access User Groups page in the Study Settings hub
	Create, edit and delete User Groups
Manage Risks	Edit risk name (a short risk identifier e.g. RISK_XXX)
Manage Study Protocol	Upload and clear Study Protocol Data
	Change Vital Timelines
	Change Target Number of Patients
	Enable Subject Profile module
	("View Study Protocol" privilege is required to access Study Protocol page in the Study Settings hub)
Manual Study Data Upload	Upload study data via browser (one or multiple files) on the Study Data page in the Study Settings hub
Release RACT Drafts	Release RACT Working Draft
Retire Studies	Retire Studies
Review & Close Mitigations	Review, Close, Promote active Mitigation Actions
Review & Sign Subject Profiles	Leave a Review for a Subject
	("View Subject Profiles Dashboard" privilege is required to access Subjects page)
Save CSM Request Study Data for Download	Set up creation of .csv file with the Study Data that was fetched to a CSM Request
	(When creating a new CSM Request, a setting "Save Study Data for Download" is available. If selected, any User with access to the CSM Request will be able to download study data that was fetched to a CSM Request)
	("View CSM" privilege is required to access CSM requests page)
	("Manage CSM" privilege is required to create CSM requests)
Set up Studies	Create New Study on the Studies List page
	Access Studies Wizard page
Set up Study Access & Visibility	Access Configuration hub (Company Settings)
	Access Study Access page

	Assign existing studies to users
Unretire Studies	Unretire Study on the Study card
View CSM	Access Centralized Statistical Monitoring page
	Access CSM Request Details, CSM Request Results and CSM Request Summary pages
	Download data files from CSM Requests
View Catalogs	Access Catalogs List page
	Access Catalog details page
	Export Catalogs
View KRI Wiki	Access KRI Wiki in the Help dropdown
View KRIs	Access KRI page
	Access Risk Indicator Details page
View Metrics	Access Metrics page
	Access Metric Details page
View QTLs	Access QTL page
	Access QTL Details page
View Reports	Access Datasources and Reports pages
	View and download a Datasource template
	View and print a Report
View Retired Studies	Filter Retired studies on the Studies List page
	View Retired studies cards
View Retired Studies Data	View Retired Study Data in Read-Only Mode
	("View Retired Studies" privilege is required to access retired studies on the Studies List page)
View Sites	Access Sites page
	Access Site Details page
View Sites Data Inconsistency Report	Access Sites Data Inconsistency Report
	View Sites Inconsistency Score on the Sites List page
View Study Dashboard	Access Dashboard page
View Study Protocol	Access Study Protocol page in the Study Settings hub
View Subject Profiles Dashboard	Access Subjects page
	Access Subject Profile page
	Access Subject Profile reviews
View Tickets	Access Tickets page
	Access Ticket Details page
	Subscribe to or unsubscribe from a ticket
View User Management	Access Configuration hub (Company Settings)
	View User Management page

Roles

The Roles give the User access to different levels of functionality of the system. It presents the information according to the business needs.

1. Go to **Settings** in the menu bar (If you do not see this function, you do not have Administrator rights) and click **Company Settings** to enter the **ConfigurationHub.**
2. Click **Roles.** Here all roles are listed with privileges assigned.
3. Click the drop-down sign to expand and select privileges. The number of selected privileges is shown.



Add a New Role

1. Click **+ Add a New Role** (see the picture above.)
2. Enter a new role name, then select **Privileges**.

Export Roles

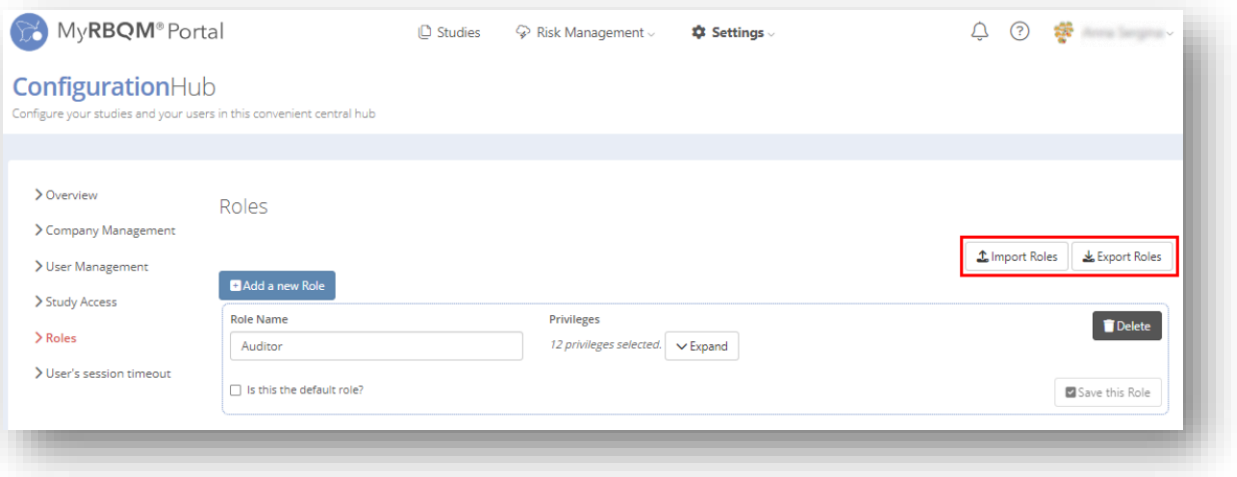
Click **Export Roles**, and a .csv file is created with MyRBQM User Role, Default and Privileges header. It also creates a row for each of the existing Roles for the company.

- The first column holds the Name of the Role.
- The second column holds a True/False, depending on whether the Role is default or not.
- The third has the comma-separated list of Privileges this Roles has (as they appear in the list of Privileges).

NOTE: Do not open exported file in Excel!

Import Roles

Click **Import Roles**, this imports an existing .csv file. If a Role in the .csv file and an already existing Role have the same name, the existing Role should be renamed.



Audit Trail

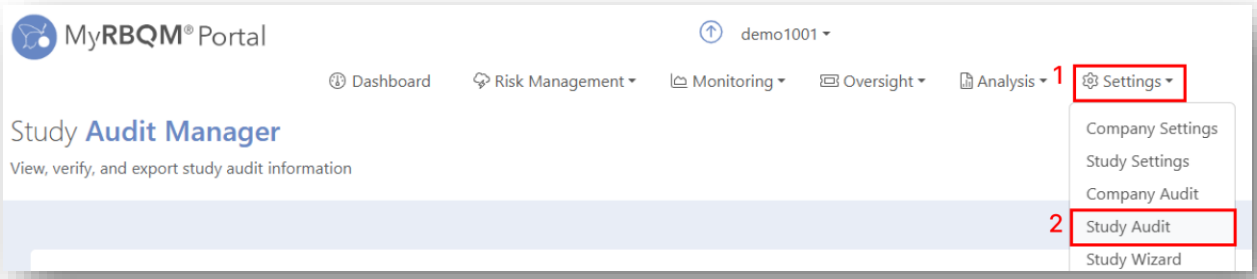
Auditors and inspectors may require full transparency of all actions taken during the management of a study. Additionally, users may need to track changes made within the **MyRBQM® Portal** throughout the study lifecycle.

For this purpose, the **MyRBQM® Portal** records all actions performed during the study in the form of an audit trail. The audit trail begins with the creation of a company and extends to the latest study working draft.

The audit trail in the **MyRBQM® Portal** is presented at two levels: **Company** and **Study**. Portal administrators can access both levels via the **Audit Manager**.

To access the **Company Audit Trail**, click **Settings** → **Company Audit** in the header menu.

To access the **Study Audit Trail**, navigate to the relevant study and select **Settings** → **Study Audit** (as shown below).



NOTE: The Study Audit can only be accessed from the Settings dropdown menu after a study has been opened.

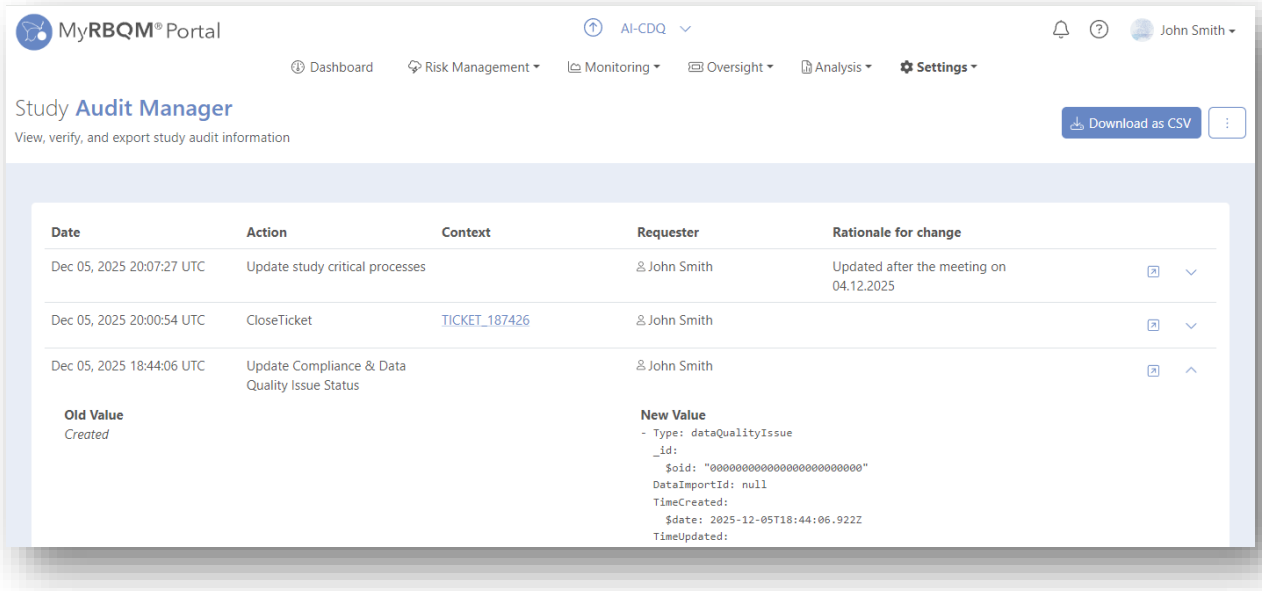
Each entry includes the following information:

- **Date**: the date and time when the change was requested
- **Action**: the type of change that was performed
- **Context**: a link to the item the change was performed with
- **Requester**: who triggered the action (user via the UI or API, or the system) - see details below
- **Rationale for change**
- **Old and New Values** (To view, expand a row by clicking on it.)

To export the Audit Trail for offline review in .csv format, click **Download as CSV**. The downloaded file includes all

existing audit entries. You can filter the entries by time period before downloading.

To navigate to the **Audit Entry page,** click the square arrow icon at the end of each row (as shown below).



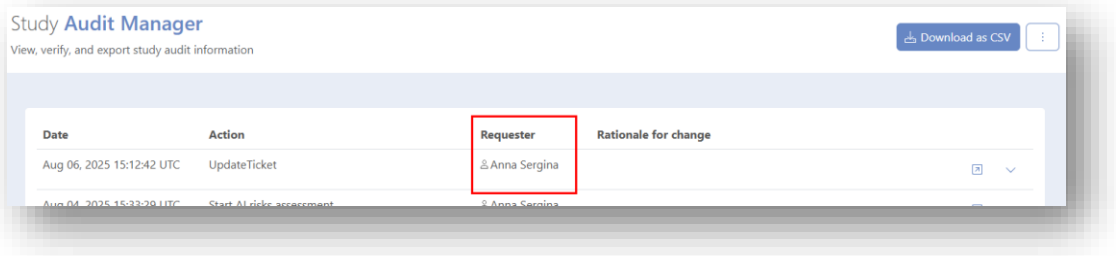
In addition to the fields listed above, the **Audit Entry** page includes a **Request** and **Response Details** section, where you can find:

- **Request Details**: Information about the specific action and its parameters that was requested by a user or in some other way (API Request)
- **System Response Details**: The system's reply to the request, including any returned data or error messages (API Response)

Each audit entry page has a unique ID and can be shared with other users by sharing the page link.

Types of Requesters in Audit Trial

Each audit entry in the Audit Trail includes a requester — a person or system that triggered the action.



Below are the definitions of each requester type:

Requester displayed in Audit Trail	**Meaning**
User name *(Global Administrator)*	Action performed by a Cyntegrity employee: initial company setup or editing of company configuration
User name	Action performed by a user from the company in MyRBQM
System	Action performed automatically by the system (e.g., ticket creation)
Company (via API)	Action performed via the Integration API
User Name *(blocked)* or *(deleted)*	Action performed by a user who is currently blocked or deleted
Internal user ID, if available *(user not found)*	User not found in the MyRBQM user database

The user name is displayed according to the following priority:

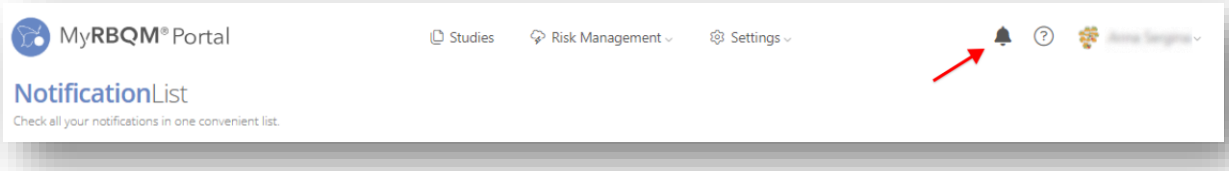
1. If the user's name is defined in the portal, it is displayed.
2. If the user's name is not available, the email address is displayed (if available).
3. If neither the user's name nor email address is available, the GUID (user's internal ID) is displayed, followed by "(user not found)".
4. If none of the above information is available, "User not found" is displayed.

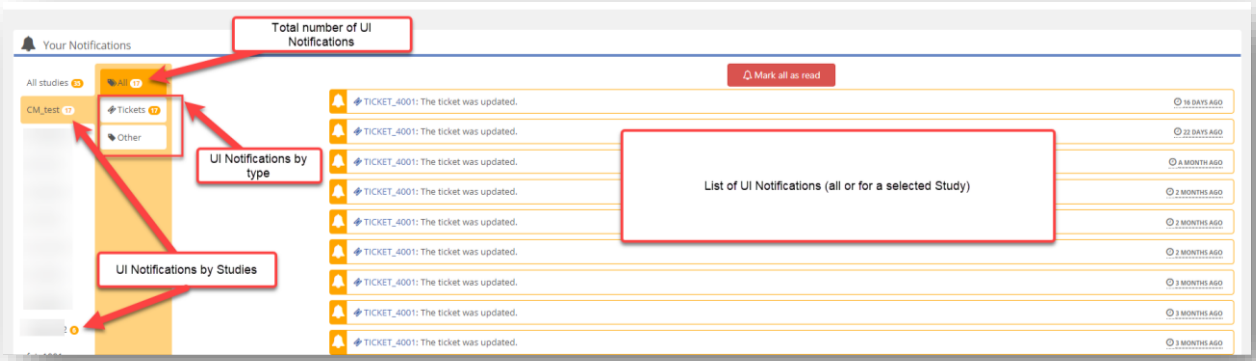
Notifications

There are two types of Notifications in MyRBQM:

- UI Notifications are records visible in the list in the User Interface.
- Some periodic emails (they are missed notification emails of different periodicity) contain information about notifications, but they don't appear at the same time as UI Notifications. They are sent much later and contain information only about unseen (not browsed) UI Notifications.

UI Notifications:





Emails:

List of all emails in the MyRBQM® Portal:

The **Daily Missed Notifications** email is sent every day at *__Daily__. Parameters: “threshold”: 20, “cap”: 40. That means:

If a number of missed notifications is less than “threshold”, the email template used is "**MissedNotificationsMail**".

If a number of missed notifications is less than “cap”, more than “threshold”, the email template used is "**MissedNotificationsShortMail**".

If a number of missed notifications is more than “cap”, the email template used is “**Capped Missed Notifications Email**” and then there is just “cap” number notifications in the email.

NOTE: Missed Notifications emails are sent to a user who is subscribed to notification emails in their user profile and is the recipient of a certain notification.

Threshold and cap details:

- **The Weekly** Missed Notifications Email is sent at *Weekly. Parameters: threshold: 40, cap: 60.
- **The Monthly** Missed Notifications Email is sent at *Monthly. Parameters: threshold: 60, cap: 80.

Other special emails:

- **The Notifications Email about unconfirmed users** is sent every Week.
- **The periodic New Users Email** is sent every Week**.**
- **There are also Fatal Logs, Log Collection Overview, and Error Queue** emails for Admins**.**
- **User Account Emails** sent immediately to a user owning an account (or invited person)**.**

On user confirmation:

- Onset user password by somebody else than the user
- On reset user password
- On update user profile by somebody else than the user
- On new user invited to the company
- On new user invited to MyRBQM® Portal
- On new user reinvited to MyRBQM® Portal

NOTE: Emails configured at study level are changed for that concrete study, only.

Warning emails about due mitigations are sent *Weekly. It is sent to the mitigation designee (which is user or group) and CC (only for overdue): to the notified group, which is by default, System Administrators.

Mitigation is considered due if it is marked **due in the next 7 days.**

Warning emails about overdue mitigations are sent every day (Daily). Recipients are the same as for due mitigations. Mitigation is considered overdue **if it is marked due more than 24 hours ago**. Due/overdue mitigation emails include the mitigations which are

respectively due/overdue right **at the moment of sending**.

UI Notifications lifecycle:

Notification is **marked as seen** only if a recipient opens the list of notifications containing that notification in MyRBQM® Portal User Interface.

Designee can be a user or a group (all users in that group). Ticket subscribers by default include a ticket designee and a ticket creator (if that creator is a user and not the system). They also may include users who subscribed after the ticket was created.

UI Notification is **created immediately** if:

- A mitigation is activated/reviewed/closed - for its designee & associated ticket subscribers
- A mitigation is created/deleted - for subscribers of the associated ticket
- A user is subscribed/unsubscribed to a ticket - to the subscribed user
- A ticket is created - for a designee
- A ticket is activated/closed - for subscribers of the ticket
- For a ticket's Root Cause Analysis is created/closed/reopened - for subscribers of the ticket

- A ticket is assigned - to a new assignee (another name - a new designee & ticket subscribers)

About Us

Cyntegrity is a leading Risk-Based Quality Management (RBQM) company, which offers specialized services with proprietary software for efficient RB(Q)M of clinical trials. Cyntegrity's mission is to offer high quality analytics that is more predictive than retrospective and provides the ability to integrate knowledge from previous trials with contextual, real-world data to reduce patient risk and to optimize preventive care.

Cyntegrity offers expertise, technology and experience to make the transition to data-driven RBM fast and comfortable. We are happy to work closely together with our customers through this transformation.

Contact Details

Cyntegrity Germany GmbH
Headquarters:
Altenhöferallee 3 D- 60438 Frankfurt (Main), Germany

Operations Office:
Münstererstr. 49
D-65719 Hofheim, Germany
Email: post@cyntegrity.com
Phone: +49 6192 47 01 13 50
Web: cyntegrity.com

References

i See TransCelerate's RACT tool available at:
http://www.transceleratebiopharmainc.com/assets/rbm-assets/
(Consulted online on 7 March 2017).

ii ICH Harmonised Tripartite Guideline: Quality Risk Management Q9. International Council for Harmonization (ICH), 9 November 2005, 11.

iii Moe Alsumidaie et al. Data from Global RACT Analysis Reveals Subjectivity. Applied Clinical Trials, 11 May 2016. Consulted online on 03-Mar-2017: http://www.appliedclinicaltrialsonline.com/data-global-ract-analysis-reveals-subjectivity.

iv ICH Harmonised Tripartite Guideline: Structure and Content of Clinical Study Reports E3. International Council for Harmonization (ICH), 30 November 1995.