Reasonable Risk™

Training Module
Focus Area: Remediation Projects

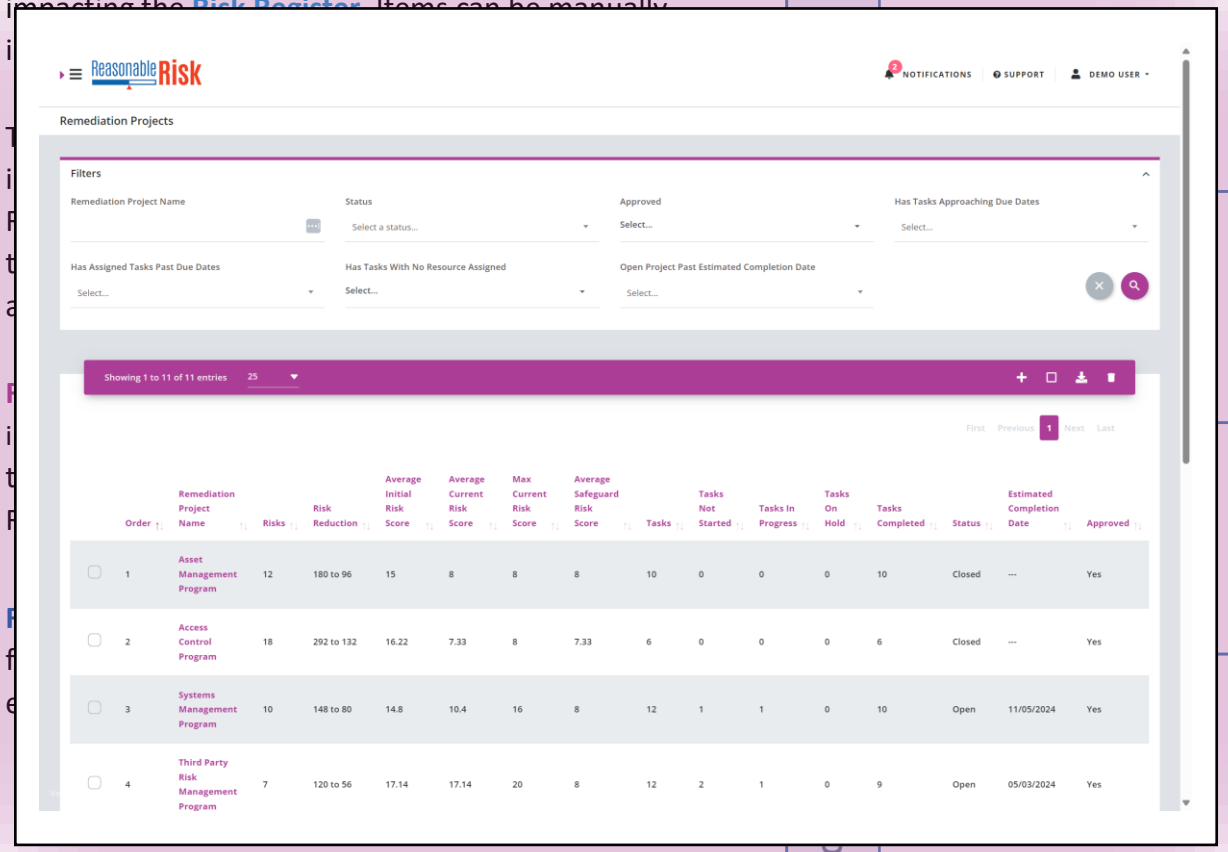
Agenda

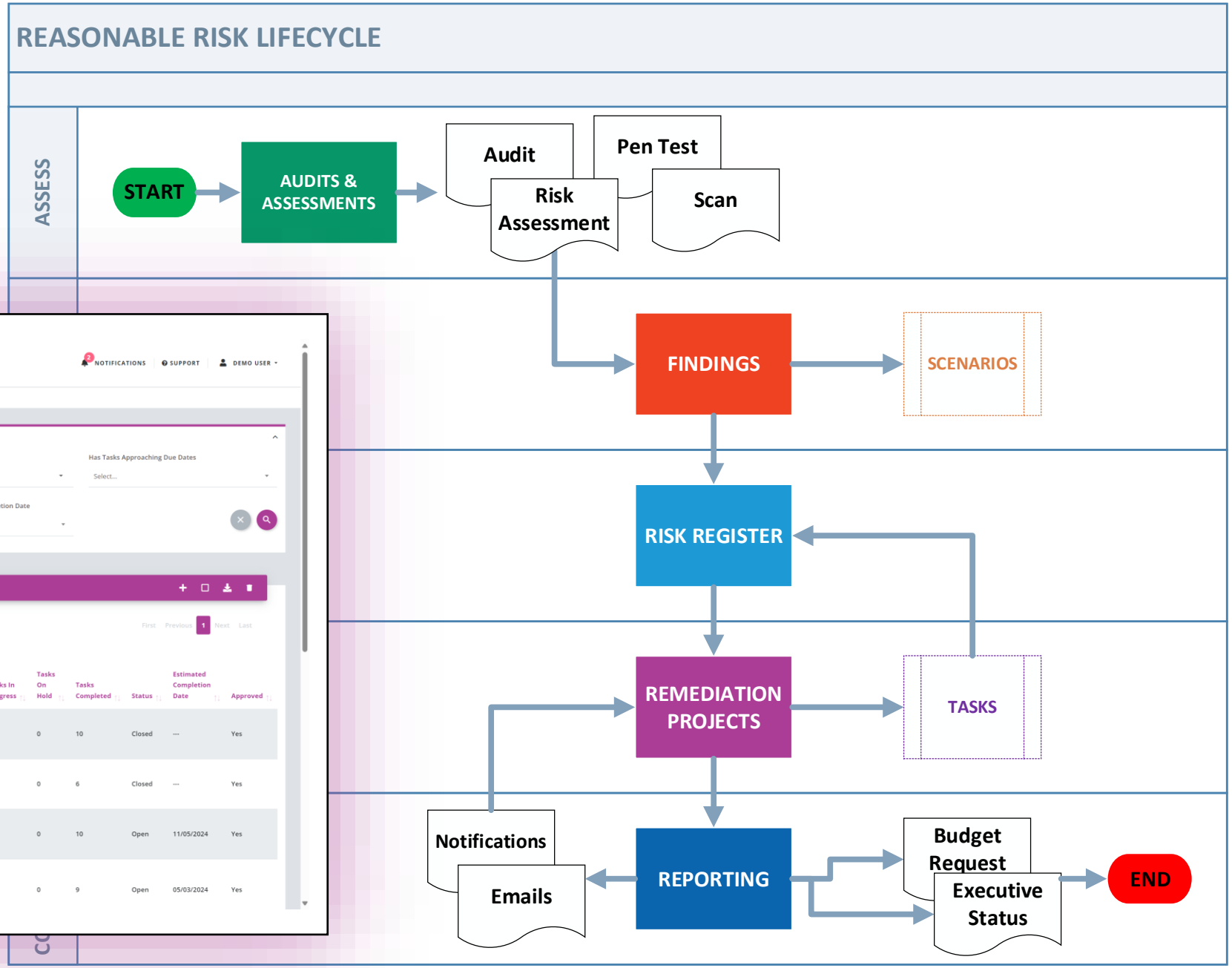
Topic – Remediation Projects

Modules

Audits & Assessments allow you to plan and monitor the periodic activities and assessments normally associated with a security program.

Findings & Scenarios provide a safe place to allow for the modeling of safeguard control use cases without impacting the Risk Register. Items can be manually





Reasonable Risk

Remediation Projects

- Objectives:
  - Review and understand projects listing/search bar
  - Review and understand Project Overview
  - Understand Project Task Dates
  - Understand Project Costs
  - Approve Projects with Approved Project Date
  - Create new project
  - Understand how to Close Project

Remediation Projects - Overview

In order to remediate risks – they must be mapped to a project. This topic was already covered in the Risk Register module.

The remediation project is a collection of risks and tasks that drive the risks to an acceptable level using project management.

The remediation project information is also important material on the executive status presentation regarding status.

The dates that are on tasks which are also associated to risks also drive the roadmap graph indicating when the overall risk level will be “acceptable.”

Remediation Projects – Overview (Continued)

To start – when a team has a number of risks – they tend to categorize them into groups that make sense for remediation such as Common Security Program (i.e. Access Control, Third Party, etc.).

Alternatively, teams may collect risks into projects based on risk levels (i.e. Pen Test High Risks).

Another option is to create projects based on timing – such as goals based on a quarter or a “sprint” (i.e. Q4 2025 Risks, Q3-Sprint 2 Risks).

There are many options, in fact, there are 3 slides of 10 different project type options later in this deck that describe the pros and cons of each type.

The bottom line – projects need to be created, and risks need to be associated to those projects.

Remediation Projects – Workflow Discussion

Projects are created when risks are initially mapped to them.

When projects are created, the idea is that tasks should be created to support those projects, so that time duration and budget numbers can be determined for each project.

These time durations and costs are then rolled up to an overall project summary level.

A best practice once this is done is to run the Presentation: Budget Request – which is designed to review projects for purposes of budget review and project approval.

Therefore, once this is done, 2 key fields can change, as well as status:

- Approved (Yes/No) – would get changed accordingly
- Approved Completion Date – would get changed to the approved completion date
- The overall SCHEDULE, SCOPE and STATUS can also get the initial status as well, most likely "Good" (green) – but it is possible that an approved project may have issues, so select accordingly.

As a default – the Project State is OPEN - when a project is complete – it should be changed to CLOSED. When it is changed to CLOSED – all of the associated risks automatically are closed as well.

Remediation Projects – Workflow Graphic

1 - Create Project

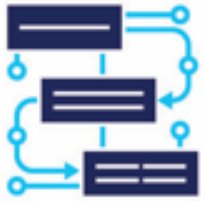
First, the projects is created

2 - Map Risks

Next, risks are mapped to the project. However, sometimes the project is created at the same time as a mapping.

3 – Create Tasks

Create tasks and associate them to the risks within the project. Ensure that every risk has at least one task associated to it.



4 – Run Budget Request Presentation

Run Budget Request Presentation and have a meeting with stakeholders to get projects approved, with budget and timelines as appropriate.

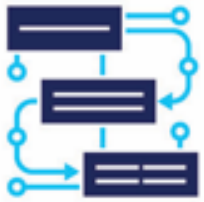
5 – Update Project Info and Status

Update Project Approved Yes/No and Approved Completion Date in Project Overview Area

Remediation Projects – Workflow Graphic

6 – Work on/ Close Tasks

The various tasks that are associated to the projects are worked on and closed.



When tasks are completed, risks can also be closed. This will then reflect the safeguard risk score.

7 – Close Risks

8 – Update Project Info and Status

Update Project status continually with updated Schedule, Scope and Resources when they change

Run Executive Status Presentation to show status of project at ANY TIME on demand. As risks are closed, the roadmap and other graphs will change showing progress!

8 – Run Executive Status Presentation

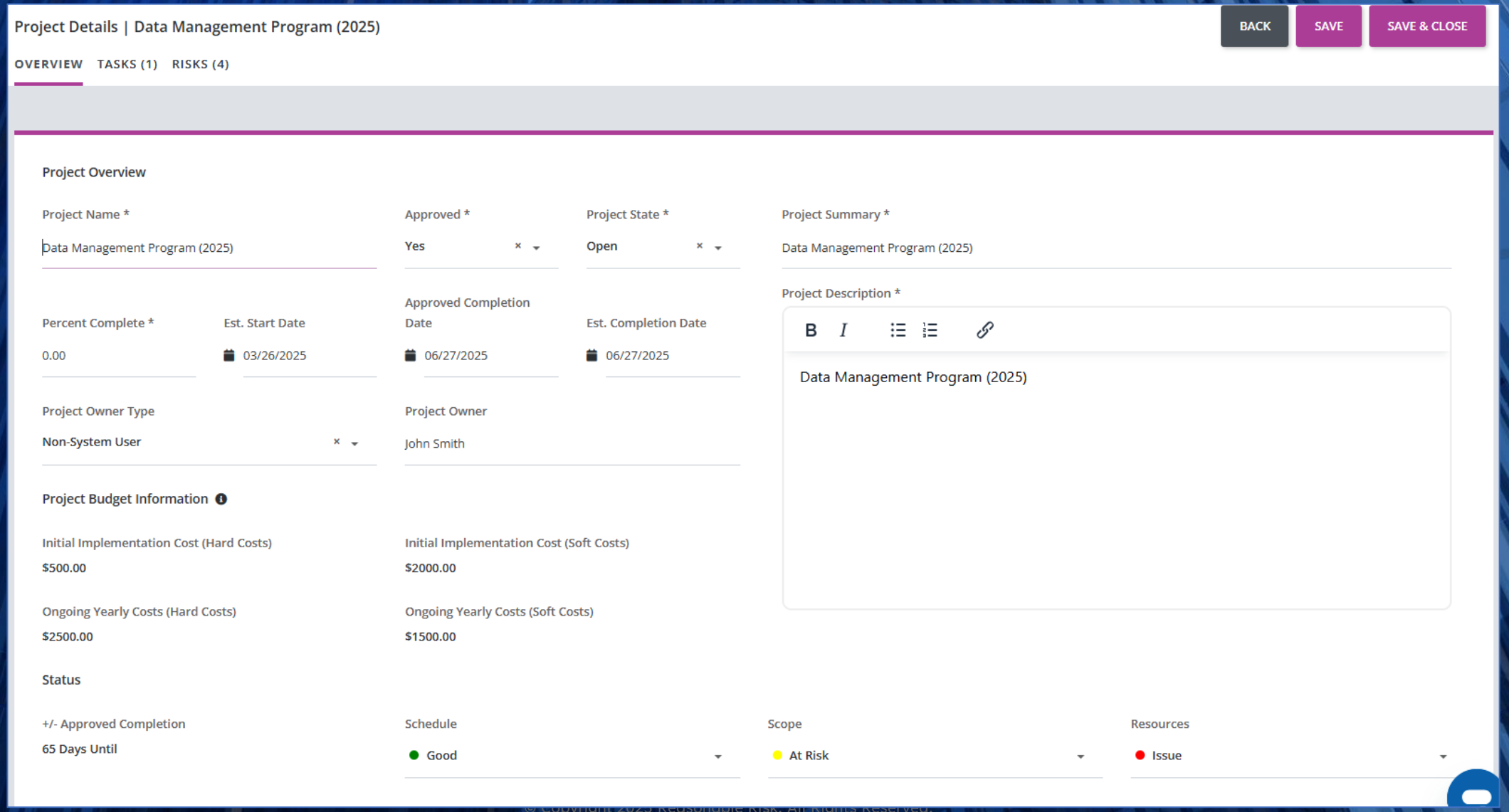
9 – Close Project

When Project is complete, change Project State to CLOSED. When this is done – all risks are automatically closed as well.

Screen Narrative: Remediation Projects

Item	Narrative
Purpose(s)	• Maintain Remediation Projects • Associate risks and tasks with projects • Work on tasks to remediate risks • Close risks
High Level Description	Associate risks to a common group of effort (project) where tasks can be executed and risks will thereby be closed. Apply costs to tasks and assign dates and resources to tasks in order to provide summary costs, dates, overall risk reduction and status for the overall project.
Detailed Description/Workflow	Risks are mapped projects from within the risk register, where a project can be created at that time. Additionally, risks can be mapped to projects after they are created. Risks can be mapped to multiple projects if necessary. Within a project overview, a user can see: • The Project Name, Summary, and description • The project approval status • The estimated completion date range – which is aggregated from individual tasks • Overall project budget details are aggregated from individual Tasks. • Access to associated Tasks and Risks • Aggregation of Project Risk scores • Count of Risks by Acceptance Level Lastly, it also allows for project managers to provide a “Green/Yellow/Red” status for three main indicators of Schedule, Scope and Resources – this is important because this appears on the Executive Status PowerPoint.
How this screen fits into the overall risk lifecycle	Risks are associated to projects, and can be EDITED, or CLOSED from a project. They can also be moved from CLOSED back to IN PROCESS while they are associated to a project. Additionally, you can “de-associate” a risk from a project, which moves it back to the risk register into the status of OPEN, where you would need to re-map it to another project in order to work on it and close it.

Screen Visual: Remediation Project Overview



Screen Review: Project Overview (1 of 2)

Screen: Project Overview
Menu Selection: Remediation Projects
Navigation Notes: Left Menu Remediation

Field/Action/Selection	Description	Req?	Best Practice
Project Name	Name of the Project	Y	Try to choose a name that best describes the project, such as a project that has a few Access Control risks – try to have "access control" in the project name.
Approved	Yes/No on whether the project is approved or not	Y	Projects do not have to be approved, but it is a best practice to have them be approved, along with setting the approved Completion Date (below) as this appears on the Executive Status PowerPoint deck.
Project State	Open/Closed on whether the project is still actively open or closed	Y	Closed projects can no longer be edited in any way.
Project Summary	A short summary of the project	Y	This is what will be on the Executive Slide Deck PowerPoint
Project Description	A detailed description of the project	Y	This more detailed, and can include rich text, bullet points, etc.
Percent Complete	The percentage complete the project is estimated to be.	Y	This is a MANUAL estimation done by the project manager.
Est. Start Date	Calculated start date of the project based on the earliest start date of the tasks that are currently within project.	N/A	This is a calculated field, non-editable.
Approved Completion Date	This is an entered date that is the approved completion date. This is to be used in conjunction with the APPROVED YES/NO field.	N	The best sequence should be: 1) Approved should be No 2) Change this date to approved date – hit Save 3) Change approved to Yes – hit save
Est. Completion Date	Latest end date of the project based on the latest end date of the tasks that are currently within project.	N/A	This is a calculated field, non-editable.

Screen Review: Project Overview (2 of 2)

Field/Action/Selection	Description	Req?	Best Practice
Project Budget Information: Initial Implementation Cost (Hard Cost)	This is an aggregate hard cost of all of the costs that are indicated within the tasks within this project (initial implementation).	N/A	This is a calculated field, non-editable.
Project Budget Information: Initial Implementation Cost (Soft Cost)	This is an aggregate soft cost of all of the costs that are indicated within the tasks within this project (initial implementation).	N/A	This is a calculated field, non-editable.
Project Budget Information: Ongoing Yearly Costs (Hard Costs)	This is an aggregate hard cost of all of the costs that are indicated within the tasks within this project (ongoing yearly costs).	N/A	This is a calculated field, non-editable.
Project Budget Information: Ongoing Yearly Costs (Soft Costs)	This is an aggregate hard cost of all of the costs that are indicated within the tasks within this project (ongoing yearly costs).	N/A	This is a calculated field, non-editable.
+/- Approved Completion	A calculated field indicating how many days it is until the approved completion date.	N/A	This is a calculated field, non-editable.
Schedule	This is a project management indicator that is manually set based on the project status of the SCHEDULE: Good (Green)/At Risk (Yellow)/Issue (Red).	N	While not required, it is key, because this appears on the project status slide on the Executive Status PowerPoint.
Scope	This is a project management indicator that is manually set based on the project status of the SCOPE (is it clear, understood?): Good (Green)/At Risk (Yellow)/Issue (Red).	N	While not required, it is key, because this appears on the project status slide on the Executive Status PowerPoint.
Resources	This is a project management indicator that is manually set based on the project status of the RESOURCES (are they available to work on this project?): Good (Green)/At Risk (Yellow)/Issue (Red).	N	While not required, it is key, because this appears on the project status slide on the Executive Status PowerPoint.

Advanced Topic: Project Types

There are many ways to create projects, this table reviews the many ways that it can be done, with the pros and cons of each.

Project Approach	Defined	Example Project Name	Risks	Tasks	Pros	Cons
Common Security Program	A project where all of the risks are in the same overall domain (e.g. Access Control, Security Awareness Training) - you would include acceptable and non-acceptable risks.	Access Control Logging and Monitoring	All related to the domain - you would close acceptable risks.	One or more tasks associated to risks in project. No tasks for acceptable risks as they are immediately closed.	All risks and tasks are in the same domain - allowing for synergies of solutions - one solution solving multiple risks. Most likely fewer projects, or a known maximum.	Timing could be extended. This project may be a year or more - which impacts the overall Board Deck slide that indicates the current plan vs baseline plan.
Framework or Standard Category	Based on a Standard such as NIST or ISO, or some Framework such as CMMC - this may inform risk collections (NIST Family, ISO Chapter, CMMC area) you would include acceptable and non-acceptable risks.	NIST AC - Access Control NIST AU - Audit and Accountability ISO - Asset Management CMMC - Level 1	All related to a framework area or section - you would close acceptable risks.	One or more tasks associated to risks in project. No tasks for acceptable risks as they are immediately closed.	Same as CSP	Same as CSP
Any combo - but contains risks that are CLOSED	If there are many risks that are imported into RR, and they are acceptable - to close them, they need to be placed into a project - and then closed.	2022 Risk Assessment - Closed Risks Access Control - Closed Risks	Generally acceptable risks that are immediately closed.	No tasks are generally created for projects like this.	Risks have an opportunity to be closed, and associated to one project.	Cannot close risks any other way. When risks are in this one project, they lose any categorization.
Organization Project "Driven"	The client organization may already have a project process and named a larger project - and the risks identified are part of that project.	Project YXZ	Risks associated to the org project.	Tasks can be associated to risks - or additional tasks can be added that those external to the team are doing and perhaps not associated to a risk.	Assists with adoption of RR to the organization if the client - and algins to the project management approach of the client.	Outside team members may not provide updates or have incentive to do so.
Specific Tool or process implementation	One or more risks are resolved by the implementation of a tool or technology	Mimecast implémentation VPN Implémentation SIEM Implémentation	Risks associated to a particular tool or technology.	Tasks can be associated to risks - or additional tasks can be added that those external to the team are doing and perhaps not associated to a risk.	Aligns to an internal project.	Outside team members may not provide updates or have incentive to do so.

Reasonable Risk

Advanced Topic: Project Types

Project Approach	Defined	Example Project Name	Risks	Tasks	Pros	Cons
<Some timing> Sprint	Based on some timing - generally quarterly - create a project based on timing of completion.	2025 Q1 - Quarterly Sprint 2025 Q2 - Quarterly Sprint 2025 MARCH - Monthly Sprint	Will be a various collection of unrelated risks in most cases. But some could be similar so that one action could cover multiple risks. Risks are selected based on timing to be able to remediate during the selected timeframe.	Be sure to associate a risk to EVERY task to ensure what task is associated to what risk - and order them so they are together.	Positive impact on the board deck current plan graph. Allows the team to be more focused on risks when given a concrete timetable.	Risks and tasks are generally unrelated, possibly causing confusion.
"Few" risks	A small number of related risks (not a whole CSP, framework or standard category) there could be additional similar risks in other projects.	Access Control - Admin Access SAT - Training Update	Small number of risks (3 or 4) that are related - perhaps on main effort will remediate all of them (such as "train all users in SAT" will close many risks)	All tasks should have one to many risks within project.	Small number of risks focuses team on completion - generally with one "implementation" covering all risks.	Could lead to a lot of projects if used a lot.
1 risk - 1 project	Create a project per a single risk. Generally used when non-risk team users are going to be using RR and not fully familiar - or many tasks for lots of risks where the tasks are getting jumbled or confusing to non-frequent users.	AC-02 - Access Control ISO 7.1 - HR	1 Risk	Generally used when there are many tasks required to resolve risk. Associate risk to final task.	Easy to manage - especially for non-frequent users that want to know "where to go" to update things.	Will generate many projects if used frequently.

Advanced Topic: Project Types

Project Approach	Defined	Example Project Name	Risks	Tasks	Pros	Cons
"Tickets" (mostly for pen testing)	Create a project that is based on tickets created in the internal ticket system. Generally used for pen testing remediation. Can create different projects (Pen Tests - Critical, Pen Tests - High, etc.)	Pen Test Risks - Critical Pen Test Risks - High	Pen tests generally are promoted from findings. Full information is not necessarily needed. Risk score can be standardized based on Critical - High - Med - Low.	Generally 1 task per risk - the task name can be the ticket number. Also, the comments can contain a link to the ticket system ticket.	Good compromise to use ticket system of organization, minimizing IT team members that would need to log into RR. Keeps RR system of record, and leverage ticket system capabilities, workflow, etc.	Reliant on external system to drive work. Need to review other system to update task status.
Risks based on risk Score	Generally post risk assessment - if an organization wants to close "high scored risks quickly" - create projects that are risk score based "Critical risks Project" - etc.	Critical Risks High Risks Risks Scored 16 and greater	Collection of risks that are of like risk level (e.g. Critical, high)	Tasks created to best resolve risks - can be many or few, based on situation.	Allows a team to zero in on critical or high risks as a priority.	Risks may be unrelated and therefore possibly confusing to track.
Risks based on owner or department	Where risks are focused on a particular team or department	Third party Audit Team Privacy				

Screen Narrative: Remediation Project Filter and List

Item	Narrative
Purpose(s)	• Review project list • Filter projects listing
High Level Description	This is the projects listing and filter, which allows us to filter on our overall projects list. The projects list shows all projects, both open and closed. The filter selections will search out and display on those projects that meet the search criteria. Additionally, some of the column headers within the project listing also serve as alphabetic sorts when clicked, the list is sorted alphabetically one way or the other when clicked again.
Detailed Description/Workflow	Most of the time, organizations place active projects near the top of their list, they use the “move project” function to do this. However, if a filter or search is required, the filter\search bar is used when a particular project is needed to be found quicky. There is a great deal of criteria available for the filter, from project name, to details about tasks approaching the due date. Additionally, project list features in the maroon action bar include the ability to download the entire project list as well as delete a project, if certain conditions are in place. The columns in the project list are very descriptive, and most allow for an alphabetic sort when clicked one way or another.
How this screen fits into the overall risk lifecycle	Risks are associated to projects, and can be EDITED, or CLOSED from a project. They can also be moved from CLOSED back to IN PROCESS while they are associated to a project. Additionally, you can “de-associate” a risk from a project, which moves it back to the risk register into the status of OPEN, where you would need to re-map it to another project in order to work on it and close it.

Screen Review: Remediation Project Filter

Screen: Project Filter
Menu Selection: Remediation Projects
Navigation Notes: Remediation Projects

Field/Action/Selection	Description	Best Practice
Remediation Project Name	Filter on project name	Search for the project name.
Status	Select OPEN or CLOSED	There are only 2 project status.
Approved	Select YES or NO	There are only 2 choices.
Has Tasks Approaching Due Date	Select YES or NO	The criteria for this is that if it is YES, that means that the tasks are past the due date or are within a week of the due date.
Has Assigned Tasks Past Due Dates	Select YES or NO	The criteria for this is that if it is YES, that means that the tasks are past the due date.
Has Tasks with No Resource Assigned	Select YES or NO	If YES, shows projects where there are tasks with no resources assigned.
Open Project Past Estimated Completion Date	Select YES or NO	If YES, shows projects that are open and past the estimated completion date.
ACTION: Cancel	Will Clear filter	Resets everything to the default
ACTION: Magnifying Glass	Will execute the search/filter	Will show results of filter in the list below.

Screen Review: Project Action Bar/List

Screen: Project Action Bar/List
Menu Selection: Remediation Projects
Navigation Notes: Remediation Projects

Field/Action/Selection	Description	Best Practice
Showing X of Y Entries	Shows a number of entries on the page. Shows the number of entries out of the total number of possible entries in the series.	The default is 25.
ACTION: "+" Sign (add)	Click the plus sign to add a new project.	This is another way to add.
ACTION: Square	Select this box to select "all" in the current view.	This will only select those that are currently displayed.
ACTION: Download Symbol	Will download all, whether selected or not.	They do not have to be selected to be downloaded, they will be downloaded into a .csv file.
ACTION: Garbage Can Symbol (Delete)	Need to select a project first to delete it.	There are only certain conditions where a project may be deleted, for example, if there are non-completed tasks, a project cannot be deleted.
Header: Selection Box	Check this box to select the row.	If you select multiple boxes, you can take actions on multiple items at once, if allowed, such as delete.
Header: Order	This is the order that the element is in, shows a number. This column has an arrow by is and is sortable.	You can click this and sort it back and forth.
Header: Remediation Project Name	Project Name	Sortable
Header: Risks	Number of risks associated to the project	Sortable – this is sometimes used to prioritize projects.
Header: Risk Reduction	The total risk score of all of the risks that are associated to the project is the first number – and the second number is the total safeguard risk scores of all associated risks.	Sortable – this is sometimes used to prioritize projects.

Screen Review: Project Action Bar/List (1 of 2)

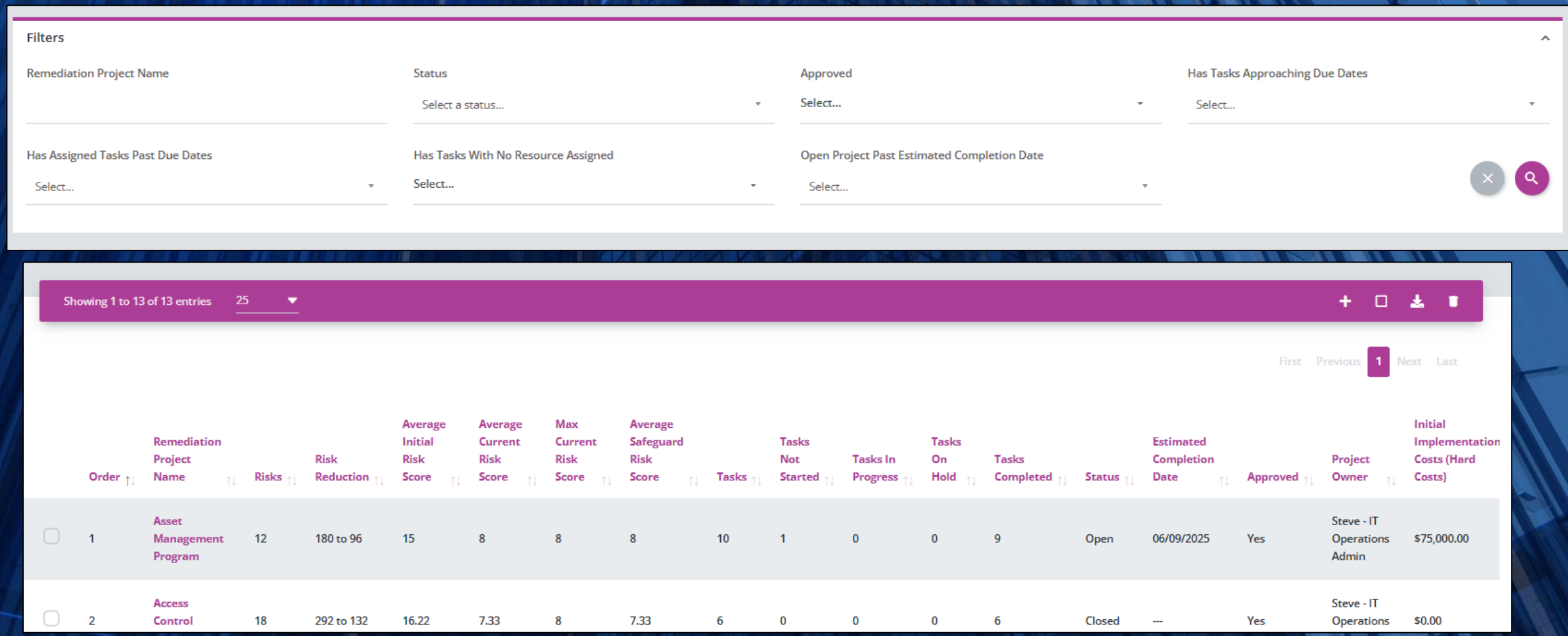
Screen: Project Action Bar/List
Menu Selection: Remediation Projects
Navigation Notes:

Field/Action/Selection	Description	Best Practice
Header: Average Initial Risk Score	Average Initial Risk Score of all risks associated with the project.	Sortable – this is sometimes used to prioritize projects.
Header: Average Current Risk Score	Average Current Risk Score of all risks associated with the project.	Sortable – this is sometimes used to prioritize projects.
Header: Average Safeguard Risk Score	Average Safeguard Risk Score of all risks associated with the project.	Sortable – this is sometimes used to prioritize projects.
Header: Tasks	Number of tasks within the project.	Sortable - Easy to spot what projects have no tasks, or what ones are more complex.
Header: Tasks Not Started	Number of Tasks Not Started	Sortable – Can quickly review the tasks that are not started.
Header: Tasks In Progress	Number of Tasks In Progress	Sortable - Can quickly review the tasks that are in progress.
Header: Tasks on Hold	Number of Tasks on Hold	Sortable - Can quickly review the tasks that are on hold.
Header: Tasks Completed	Number of Tasks Completed	Sortable - Can quickly review the tasks that are completed.
Header: Status	Project status of open and closed	Sortable – organizations place closed at the end of the list.
Header: Estimated Completion Date	Estimated Completion Date of the project	Sortable - this may or may not be filled in for each project yet
Header: Approved	Approved – yes or no	Sortable – Makes it easy to see approved projects or not
Header: Project Owner	Project Owner	Sortable – can see if there are many projects for the same person. This also may or may not be filled in for projects.

Screen Review: Project Action Bar/List (2 of 2)

Field/Action/Selection	Description	Best Practice
Header: Initial Implementation Costs (Hard Costs)	Rolled up costs for this category by adding it up from all the tasks in the project.	Sortable – Sometimes used to prioritize projects.
Header: Initial Implementation Costs (Soft Costs)	Rolled up costs for this category by adding it up from all the tasks in the project.	Sortable – Sometimes used to prioritize projects.
Header: Ongoing Yearly Costs (Hard Costs)	Rolled up costs for this category by adding it up from all the tasks in the project.	Sortable – Sometimes used to prioritize projects.
Header: Ongoing Yearly Costs (Soft Costs)	Rolled up costs for this category by adding it up from all the tasks in the project.	Sortable – Sometimes used to prioritize projects.
Header: Total Costs	Rolled up costs total costs for this category by adding it up from all the tasks in the project.	Sortable – Sometimes used to prioritize projects.
Project Action – “3 dot Menu” Move to Position	Pop up menu indicating a range of project numbers with the current project order number in place. You can edit it to be the new order number.	This is often used to put closed risks at the end of the list.

Screen Visuals: Project Filter – Project List



Order	Remediation Project Name	Risks	Risk Reduction	Average Initial Risk Score	Average Current Risk Score	Max Current Risk Score	Average Safeguard Risk Score	Tasks	Tasks Not Started	Tasks In Progress	Tasks On Hold	Tasks Completed	Status	Estimated Completion Date	Approved	Project Owner	Initial Implementation Costs (Hard Costs)
1	Asset Management Program	12	180 to 96	15	8	8	8	10	1	0	0	9	Open	06/09/2025	Yes	Steve - IT Operations Admin	$75,000.00
2	Access Control	18	292 to 132	16.22	7.33	8	7.33	6	0	0	0	6	Closed	---	Yes	Steve - IT Operations	$0.00

Demonstrate

- Project Filter Features
- Project List Features
- Project Creation – Field Discussion
- Project Overview
  - Project Approval
  - Project Completion Date
  - Project Schedule, Scope, Resources