

Reasonable **Risk**[™]



Training Module

Focus Area: Risks and Risk Register

Agenda

Topic – Risks and Risk Register

Modules

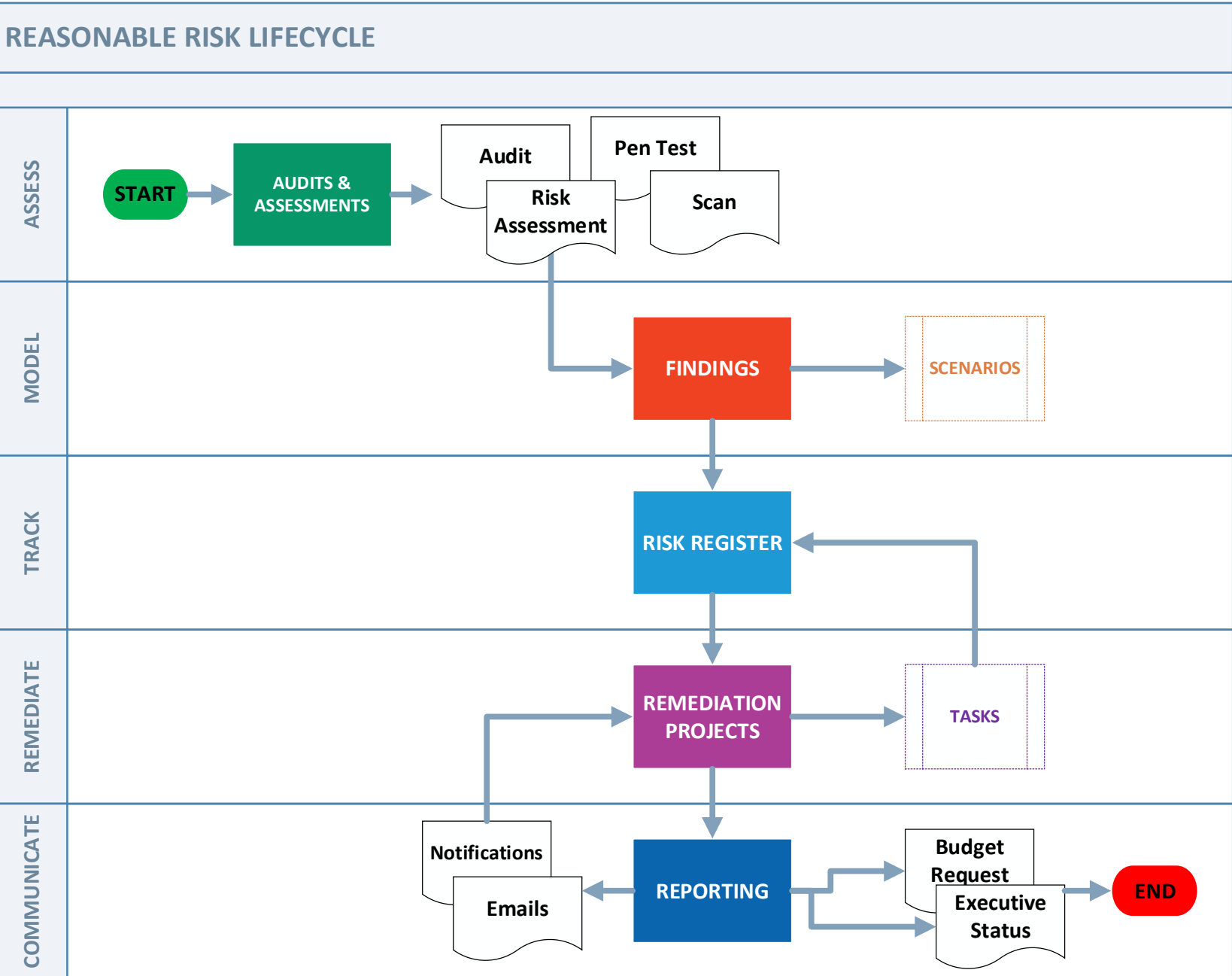
Audits & Assessments allow you to plan and monitor the periodic activities and assessments normally associated with a security program.

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 input or imported from an external source.

The **Risk Register** tracks identified risks, recording the initial and safeguard risk score and associated details. Risks are created by promoting a **Finding** or **Scenario**, they may be also be manually input or imported from an external source.

Remediation Projects are created to group and manage implementation of safeguard controls for **Risks**. **Tasks** are time bound activities or milestones required to reduce Risks to an acceptable level.

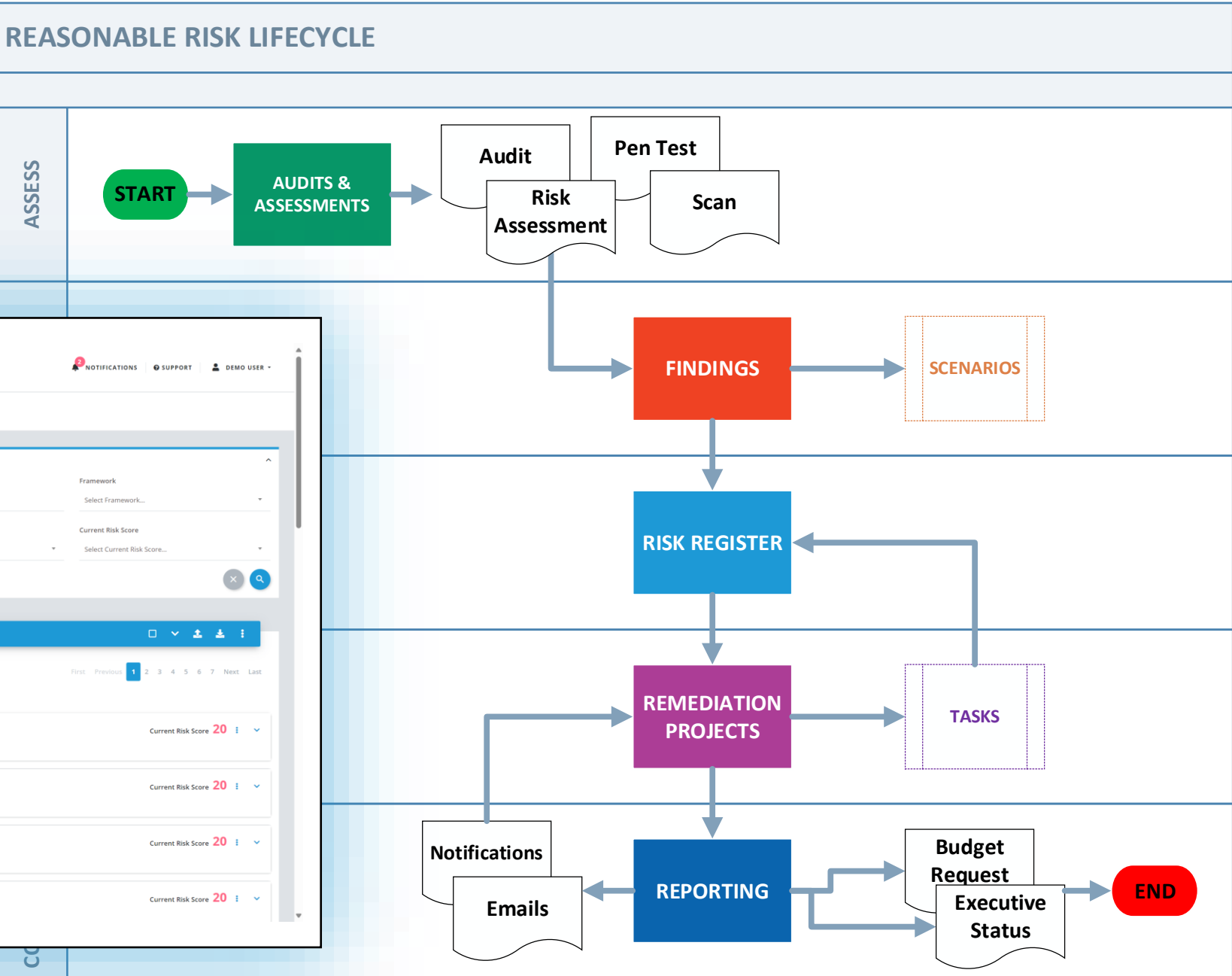
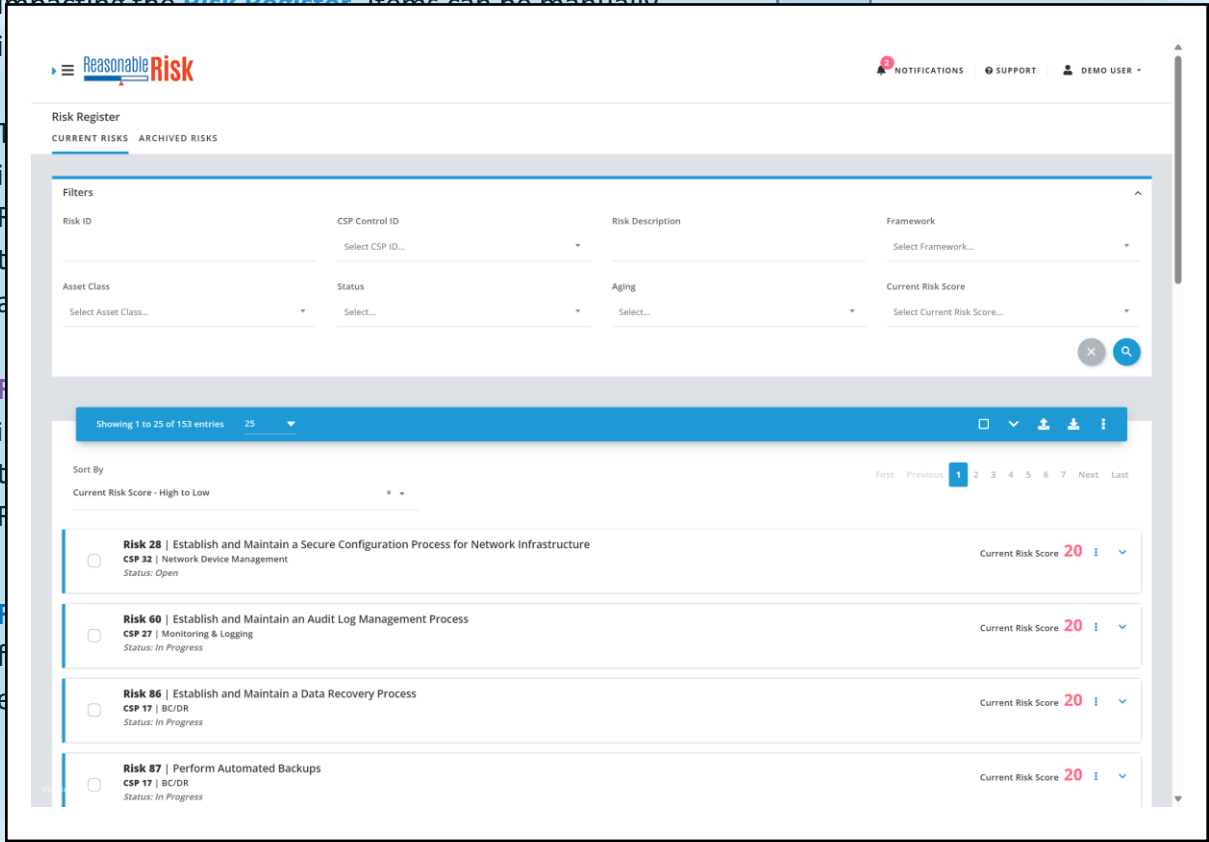
Reporting provides a consistent and efficient process for generating executive level communications in an editable PowerPoint deck.



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



Risk Register

- Objectives:
 - Review and understand risks list/search bar
 - Review and understand the risk register
 - Update risks information and risk score
 - Add comments to risks
 - Understand the complete risk lifecycle
 - Understand the reasons why a risk would be in each state of the risk lifecycle

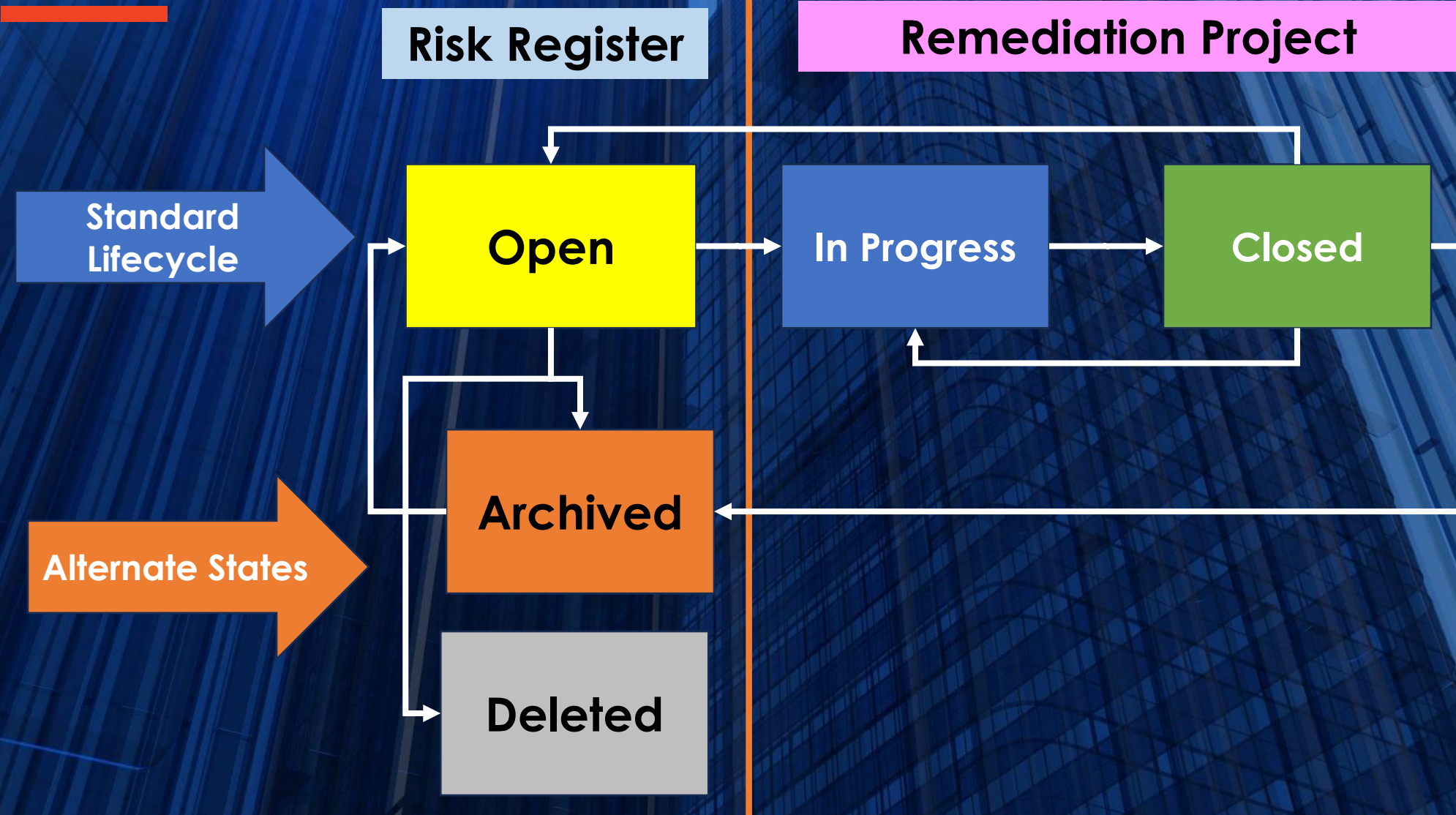
Risk Register: Overview

- The Risk Register is the main core of Reasonable Risk – as the main purpose is to remediate risks.
- Risks can be placed into Risk Register only 2 ways:
 - Promoted from Findings
 - Directly imported from a spreadsheet
- The key driver for all risks in the Risk Register is to remediate those risks that are not tolerable/above the acceptable level of risk – these need to be mapped to a project.
- All risks also appear in the various Key Performance Indicator graphs as applicable, as well as within the Budget Request Report, and the Executive Status Report.

Risk Register: Risk Status Workflow

Status	Described	Movement to other status
Open	This is the default risk status. This means it is NOT mapped to a project.	Map to Project → In Progress Risk Register → Archive Risk Register → Delete
In Progress	When a risk IS mapped to a project, it is considered to be IN PROGRESS.	Disassociate From Project → Open Close Within Project → Closed Close Project → Closed
Closed	A Risk can be closed only when it is mapped to a project and then closed within it individually. All risks within a project can also be closed at once if a project is closed.	Project must be Open Closed Risks within Projects → In Progress Risk Register (project the closed risk is mapped to must also be closed) → Archive Risk Register → Delete
Archived	When a risk is archived, it no longer will “count” on any KPI, but it is still available for review. Can only archive Open risks, or Closed Risks that are also part of Closed projects. This can only be done from the Risk Register.	Promote to Risk Register → Open (if risk was closed in a closed project, and then archived, and then promoted back to the risk register, it will be removed from the previous project)
Deleted	This is a physical delete of the risk record.	Once a risk is deleted, it is no longer recoverable.

Risk Status Lifecycle



Screen Narrative: Risks

Item	Narrative
Purpose(s)	<ul style="list-style-type: none">• Maintain Risks in a risk register.• View Risks• Edit, delete & archive risks as necessary.• Map risks to remediation projects.
High Level Description	<ul style="list-style-type: none">• Risks are brought into the risk register and are reviewed, edited, and most importantly are mapped to remediation projects for purposes of remediation.• All reports and key performance indicators are based on the risks that are in the risk register.
Detailed Description/Workflow	<ul style="list-style-type: none">• Risks may be created by promoting a Finding or Scenario to the Risk Register, or they may be directly imported from an existing risk register.• Risks include an overall description, the current mitigating control as well as a possible vulnerability• Risks can be mapped to one or many frameworks• Risks include an Initial Risk Score, Current Risk Score, and Safeguard Risk Score. The Initial Risk Score may be modified within the Risk Register. The Current Risk Score is automatically generated, based on the status of remediation, and the Safeguard Risk is managed within a Remediation Project.• Risks are mapped to Remediation Projects so they may be remediated as necessary.• Not all risks that are in the risk register are non-acceptable, some may be initially acceptable.• You can also add comments to every risk, and those comments can be attributed to individual users and are non-editable once submitted.• Each risk is fully auditable where the history of each risk can be reviewed at any time.
How this screen fits into the overall risk lifecycle	<ul style="list-style-type: none">• Risks can be imported from an external source or promoted from a finding to get into the risk register. The first status is considered to be “open”.• A risk can be associated to or remediation project, at that point it is considered to be “in progress.”• If a risk is in the risk register it could also be archived or deleted.• A risk can only be closed when it is within a remediation project.

Screen Review: Risk (1 of 3)

Screen: Individual Risk Blue Action Bar

Menu Selection: Risk Register\Individual Risk

Navigation Notes: Individual Risk → Blue Action Bar on Top of Risk

Field/Action/Selection	Description	Req?	Best Practice
CSP Control ID	Common Security Program Number – which relates to a category.	Y	All security controls can map to one or more of 30 common security program categories.
Mapped Framework Controls	These are the mapped framework controls that are possible based on the CSP that was selected.	N	Select as many as appropriate.
Risk Description	Long description of the risk.	Y	This can be the risk itself, or it can be the control from a control framework.
Vulnerability	The vulnerability that needs to be corrected.	Y	If using a framework, this can be the gap between the framework and what is the current mitigating control. Generally the “gap” – or the “thing that needs to be fixed.”
Asset Class	A pull-down selection of asset classes that align to the risk.	Y	There are many to choose from. This is later available to be filtered upon from the risk filter or the risk filter.
Asset	A free text description of the asset related to the risk.	Y	Could be a specific name of an asset, such as a server name as necessary, or type of servers where the vulnerability applies.
Threat Type	Pull down selection of the most relevant threat type.	Y	The list comes from the Veris Community database.
Threat Description	Free text description of the threat.	Y	Sometimes this comes from framework materials.
Industry	Pull down selection of the industry of the organization you are in.	Y	This is something that is generally selected one time during setup.
Origin	Pull down selection of various origins (e.g. risk assessment, penetration test, etc.)	Y	There are many to choose from.
Origin Description	Free text description of origin.	Y	Describe the origin, this is useful in filtering, such as “Risk Assessment 2025”
Origin Score	A text field for an origin score, if applicable. If not applicable, put a “0”.	Y	If the risk is based on a scan where an actual score can be provided, such as a CVSS score, please provide it here.

Screen Review: Risk (2 of 3)

Field/Action/Selection	Description	Req?	Best Practice
Mitigating Control – Text Formatting	When typing in the Mitigating control, the text can be rich text formatted using the menu for italics, bold, bullet points,	N	Rich text can be very descriptive where you can put bullet points etc.
Mitigating Control – Rich Text Area	This is the control that is in place right now.	Y	If reviewing a framework, this is how the framework control is being met currently (to whatever level it is being met).
Safeguard Description – Text Formatting	When typing in the Safeguard Description, the text can be rich text formatted using the menu for italics, bold, bullet points,	N	Rich text can be very descriptive where you can put bullet points etc.
Safeguard Description - Rich Text Area	This is what needs to be done in order to fully remediate the risk.	N	IF there is a vulnerability, the safeguard should fill the gap and fix what is “broken.”
Score Information: Threat Cluster	Select the threat cluster for this particular risk from the list provided.	Y	There are nine threat clusters in all.
Score Information: Maturity Level	Select the maturity level that the current mitigating control is at, on a scale of one to 5.	Y	There are five maturity levels that can be selected from 5 being the highest maturity level.
Score Information: Likelihood	Based on threat cluster and maturity level and industry, a likelihood will be suggested, this can be overridden.	Y	On a scale of 1 to 5, a 1 being least likely, and five being most likely, this is derived from information provided.
Score Information: Mission	Based on your calculated acceptable risk definition, select your mission impact, on a scale of 1 to 5.	Y	Non-tolerable is generally a 3 of 5.

Screen Review: Risk (3 of 3)

Field/Action/Selection	Description	Req?	Best Practice
Score Information: Objectives	Based on your calculated acceptable risk definition, select your objectives impact, on a scale of one to 5.	Y	Non-tolerable is generally a 3 of 5.
Score Information: Obligations	Based on your calculated acceptable risk definition, select your obligations impact, on a scale of 1 to 5.	Y	Non-tolerable is generally a 3 of 5.
ACTION: RECALCULATE LIKELIHOOD	If you change The threat cluster or the maturity level and you would like to see what the likelihood change is, click recalculate likelihood. The words “recalculate likelihood” is actually a clickable button in this area.	ACTION	The recalculate likelihood doesn’t look like a button, you can press it and change things and press it as many times as you need to see what the scores end up looking like.
SCORE	This is the score that is presented to you.	N	It is read only, it can only be changed by changing the score information and a recalculate likelihood link press.

Screen Visual: Risk

Risk 3 | Utilize an Active Discovery Tool
⋮ ^

☐ CSP 23 | Asset Management
Status: *In Progress*

CIS CSC v8 | -- | 1.3 | Inventory and Control of Enterprise Assets | Utilize an Active Discovery Tool (Detect) (IG2, IG3)

CIS CSC v8 | -- | 1.1 | Inventory and Control of Enterprise Assets | Establish and Maintain Detailed Enterprise Asset Inventory (Identify) (IG1, IG2, IG3)

Vulnerability Applications, systems, and data may be unsecured and unmonitored and may permit errors and attacks to expose data, or cause system failure.	Asset Class Process	Asset Enterprise
Threat Type Personnel Error	Threat Description Uncontrolled or compromised systems may attack neighboring information assets within the network.	Industry Information Services
Origin Other	Origin Description External Assessment	Origin Score N/A
Mapped Remediation Project Asset Management Program (2025)	Aging 28 Days	Associated Scenario ID ---

Mitigating Control & Safeguard Description ^

Mitigating Control Description of existing controls	Safeguard Description Safeguard Description
--	--

Initial Risk 	Threat Cluster Personnel Error	Maturity Level 2	Likelihood 5	Mission 3	Objectives 4	Obligations 4	20
Current Risk	Threat Cluster Personnel Error	Maturity Level 2	Likelihood 5	Mission 3	Objectives 4	Obligations 4	20
Safeguard Risk	Threat Cluster Hacking System	Maturity Level 4	Likelihood 2	Mission 3	Objectives 4	Obligations 4	8

Created On: 03/26/2025	Created By: tbecker@halock.com	Modified On: 04/23/2025	Modified By: gstout@reasonablerisk.com	Closed On: ---
------------------------	--------------------------------	-------------------------	--	----------------

Screen Review: Risk Register Filter

Screen: Risk Register - Filter

Menu Selection: Risk Register

Navigation Notes: Filter on top of Risk Register Screen

Field/Action/Selection	Description	Best Practice
Action: Carat Upper Right	Expands and collapses entire filter panel	If not needed, you can collapse to provide more screen real estate.
Risk ID	This is automatically assigned to each risk. It is the only unique identifier for the risk.	This is a really easy way to find a particular risk.
CSP Control ID	Pull down selection of all common security programs.	This is a really easy way to find risks that are in a particular common security program, such as "Access Control" – For purposes of seeing which ones would fit into a project.
Risk Description	Free text Description	If you are looking for a particular risk that has certain words in the description, use this.
Framework	Pull down selection of all available frameworks within the scope	If you want to want to see risks that are mapped to a particular framework, use this filter.
Asset Class	Pull down selection of all asset classes	If you want to see certain risks that are associated to a particular asset class, use this filter
Status	Open – In Progress - Closed	If you want to see certain risks of certain status, you can choose this filter.
Aging	Pull down selection of various age ranges	Use this filter to see risks of a certain age.
Current Risk Score	Pull down selection of various risk score categories	Use this filter to see risks of certain score category ranges. This would be unacceptable, high, whatever your range you set was in your CARD.
Action: Magnifying Glass	This is the button you press to execute the filter search.	Press this button and your resultant to list appears below.
Action: Circle with X	Cancel and clears all filters	Use when you want to reset to default

Screen Review: Risk List Blue Action Bar

Screen: Risk List Blue Action Bar

Menu Selection: Risk Register

Navigation Notes: Blue List Action Bar

Field/Action/Selection	Description	Best Practice
Action: Showing X to X entries	This is a selectable showing how many entries you can show on a page.	The default is 25.
Action: Square Box	When you see risks and you click the square box, the square box will select all of the risks that are on that page, allowing you to take action on all the selected risks.	Expand and collapse, as well as Map to Project will execute on selected risks.
Action: Carat	The carat expands all of the risk details or collapses them.	The carat changes depending on the whether things are currently expanded or collapsed.
Action: Upload Arrow	This is the import feature, when selected it will provide a screen that allows you to browse and select a file for import	It will also provide you a downloadable template to be completed for import.
Action: Download Arrow	This exports the entire risk register, whether any risks are selected or not.	If there are more than one frameworks mapped to a risk, it will only provide 1 in the export, and if the risk is mapped to more than 1 project, it will only provide 1 in the export.
Action: Three Dot Menu\Map to Project	Any selected risks will be shown in an additional pop-up menu and you'll be provided the opportunity to map these to a single project.	This is a good way Filter risks select them and then map them to projects.
Action: Sort By	Pulldown selection of how the risks should be sorted.	This is a very valuable sort, especially by risk score high to low.
Page Breadcrumbs: <ul style="list-style-type: none">• First/Previous• Page Number• Next/Last	Standard page navigation breadcrumbs going from next page or to a particular page number	Standard page navigation.

Screen Visual: Risk Register Filter & List Action Bar

Risk Register

CURRENT RISKS ARCHIVED RISKS

Filters

Risk ID	CSP Control ID	Risk Description	Framework
	Select CSP ID...		Select Framework...
Asset Class	Status	Aging	Current Risk Score
Select Asset Class...	Select...	Select...	Select Current Risk Score...

✕ 🔍

Showing 1 to 25 of 154 entries 25

🗨️ ⌵ ⬆️ ⬇️ ⋮

Sort By

Current Risk Score - High to Low ✕

First Previous 1 2 3 4 5 6 7 Next Last

Screen Review: Risk Blue Action Bar Three Dot Menu

Screen: Risk Action Bar Three Dot Menu

Menu Selection: Risk Action

Navigation Notes: Review a Risk → Blue Bar on Top

Field/Action/Selection	Description	Best Practice
Action: Edit Risk	Use this to edit the risk.	You can only edit the main information you cannot edit the risk scores
Action: Archive Risk	Use this to archive the risk. Once you archive the risk it will not appear on any reports.	You can always unarchive a risk. See the archived risks in the menu item right next to the regular risk register. You can only archive one risk at a time.
Action: Comments	Click here to make a comment about the risk.	You can make multiple comments, once the comment is made and submitted it cannot be edited, comments can be made about why you closed a risk, or made edits to it, or changed the risk score, or anything at all.
Action: Risk Audit	Click here to see a full risk audit of the history of the risk elements.	From risk creation to any edits that have been made to anything at all, this is a full risk audit.
Action: Delete Risk	Use this to delete a risk Once a risk is deleted, it cannot be undeleted.	You can only delete one risk at a time, of course this is a very powerful command and should not be done lightly.
Action: Carat	This is used to expand or collapse the wrist detail so you can see them.	The carrot changes from up to down depending on if the risk is expanded or collapsed.

Screen Visual: Individual Risk Blue Action Bar

Risk 13 | Establish and Maintain a Data Management Process
CSP 14 | Data Classification & Handling
Status: In Progress

CIS CSC v8 | --- | 3.1 | Data Protection | Establish and Maintain a Data Management Process (Identify) (IG1, IG2, IG3)

Vulnerability Management may not understand expectations for personnel to handle information and information assets in a secure manner.	Asset Class Process	Asset Enterprise
Threat Type Personnel Error	Threat Description Errors while handling confidential information, such as by sending, storing, sharing, printing, disposing of information may lead to information breaches.	Industry Information Services
Origin	Origin Description	Origin Score

- Edit Risk
- Archive Risk
- Comments
- Risk Audit
- Delete Risk

Demonstrate

- Filter Risks
- Edit Risk
- Archive Risk (and bring back to risk register)
- Delete Risk
- Add Comments to Risk

Exercise

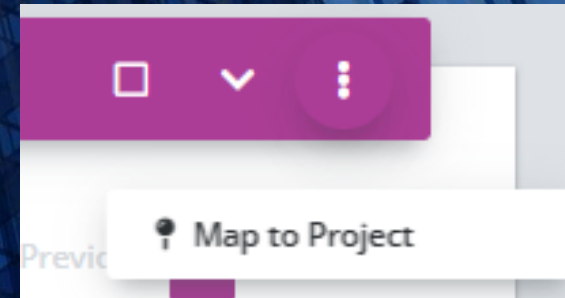
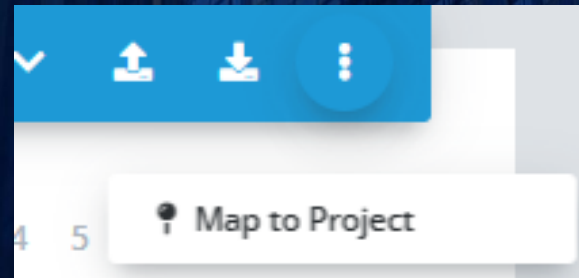
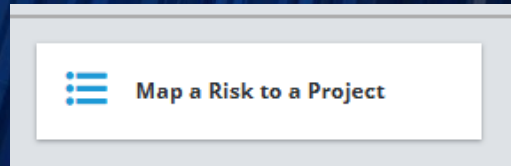
- In the production environment:
 - Filter Risks
 - Edit Risk
 - Identify where to Archive Risk (do not execute)
 - Identify where to Delete Risk (do not execute)
- Add Comments to Risk

Screen Narrative: Map Risks to Project

Item	Narrative
Purpose(s)	<ul style="list-style-type: none">• To map an open risk to remediation project for purposes of remediation
High Level Description	<ul style="list-style-type: none">• In order for a risk to ultimately be closed, it must be mapped to a project. Generally speaking risks that have a common Theme, or if a particular action or series of tasks will close a number of risks, they are generally assigned the same project.
Detailed Description/Workflow	<ul style="list-style-type: none">• Risks need to be assigned to projects in order to be closed, whether they are already at an acceptable level or not .• An example could be a number of access control risks, or data classification risks, or software development risks. These all would be created and assigned to a particular project and then that project is managed as its own entity. It can get its own budget, its own resources, and it could be shown how the overall risk score of all of those risks can go from its now high level down to its safeguard risk level.• Risks can be mapped to multiple projects if appropriate where it's possible that multiple projects might have to be executed for a particular risk to be closed.• Risks can be mapped from the risk register, which is shown in this particular part of the training, or they also can be mapped from within the project itself, which is a similar approach.
How this screen fits into the overall risk lifecycle	<ul style="list-style-type: none">• This is the first step after the risk is in the risk register, they need to be mapped to a project in order to be remediated.• One best practice is that if there are a number of risks that you wish to close but are already at an acceptable level sometimes a special project is created which is simply named "acceptable risks" and all of those acceptable risks are placed into that project, and then the risks are closed.

Map Risks to Project: Overview

- Risks must be mapped to a project in order to be remediated or closed.
- There are three different paths that can be taken to map risks to projects:
 1. From the Action Items tiles:
 2. From the Risk Register, Blue Action Three Dot Menu
 3. From within a Remediation Project, within the risks area, Purple Action Three Dot Menu



- The effort is generally the same – map risks to existing projects, or users can create new projects on the fly as they are mapping.

Screen Visual: Map Risks to a Remediation Project

This approach is taken when one or more risk(s) is/are selected, and then “Map to Project” menu section is chosen from the from “three dot menu” on the blue action bar.

Map Risk(s) to a Remediation Project

Select Remediation Project

Remediation Project
Select Remediation Project... ▾

New Remediation Project Name

Selected Risks

	Risk Name and Description
<input checked="" type="checkbox"/>	Risk 5 Use a Passive Asset Discovery Tool
<input checked="" type="checkbox"/>	Risk 14 Establish and Maintain a Data Inventory
<input checked="" type="checkbox"/>	Risk 15 Configure Data Access Control Lists

CANCEL **SAVE & CLOSE**

Screen Visual: Map Risk to Project (1 of 2)

 Map a Risk to a Project

This approach is taken when using the main Action Items “Map a Risk to a Project” tile. A user can filter on risks, select them, and then map to a project on bottom of screen (see 2 of 2).

Map Risk(s) to a Remediation Project

Filters

Risk ID CSP Control ID

Asset Class Status Aging

Select Risks

Showing 1 to 25 of 154 entries 25

Risk ID	Risk Description	Project Name	CSP Control ID	CSP Control Description	Framework	Framework Control ID	Framework Control Description
<input type="checkbox"/> Risk 1	Establish and Maintain Detailed Enterprise Asset Inventory	Asset Management Program (2025)	23	Asset Management	CIS CSC v8	1.1	Inventory and Control of Enterprise Assets Establish and Maintain Detailed Enterprise Asset Inventory (Identify) (IG1, IG2, IG3)
<input type="checkbox"/> Risk 10	Allowlist Authorized Software	Accepted Risks	23	Asset Management	CIS CSC v8	2.5	Inventory and Control of Software Assets Allowlist Authorized Software (Protect) (IG2, IG3)
<input type="checkbox"/> Risk 100	Deploy a Host-Based Intrusion Detection Solution	Vulnerability Management program (2025)	28	Vulnerability Management	CIS CSC v8	13.2	Network Monitoring and Defense Deploy a Host-Based Intrusion Detection Solution (Detect) (IG2, IG3)
<input type="checkbox"/> Risk 101	Deploy a Network Intrusion Detection Solution	Vulnerability Management program (2025)	28	Vulnerability Management	CIS CSC v8	13.3	Network Monitoring and Defense Deploy a Network Intrusion Detection Solution (Detect) (IG2, IG3)
<input type="checkbox"/> Risk		Network Device program		Network Device			Network Monitoring and Defense Perform Traffic Filtering Between Network Segments

Screen Visual: Map Risk to Project (2 of 2)

First Previous **1** 2 3 4 5 6 7 Next Last

Select Remediation Project

Remediation Project

Select Remediation Project...

New Remediation Project Name

CANCEL SAVE & CLOSE

At the bottom of the screen, the user can select an existing project to map to or choose “Create new project” and type in a name of a new project. Then Save & Close.

Select Remediation Project

Remediation Project

Select Remediation Project...

- Create New Project
- Access Control program (2025)
- Asset Management Program (2025)
- BC/DR Program (2025)

Screen Review: Map Risk to Project (1 of 2)

Screen: Map Risk to Project

Menu Selection: Risk Register -> Risk Three Dot Menu

Navigation Notes: Action Items → Map a Risk to a Project

Field/Action/Selection	Description	Best Practice
ACTION: Close Window	Closes pop up mapping window	There are 3 ways to map risks – this way, by selecting a risk and using the three dot menu, and from within a project.
Action: Carat Upper Right	Expands and collapses entire filter panel	If not needed, you can collapse to provide more screen real estate.
Filter: Risk ID	This is automatically assigned to each risk. It is the only unique identifier for the risk.	This is a really easy way to find a particular risk.
Filter: CSP Control ID	Pull down selection of all common security programs.	This is a really easy way to find risks that are in a particular common security program, such as “Access Control” – For purposes of seeing which ones would fit into a project.
Filter: Risk Description	Free text Description	If you are looking for a particular risk that has certain words in the description, use this.
Filter: Framework	Pull down selection of all available frameworks within the scope	If you want to want to see wrists that are mapped to a particular framework, use this filter.
Filter: Asset Class	Pull down selection of all asset classes	If you want to see certain risks that are associated to a particular asset class, use this filter
Filter: Status	Open – In Progress - Closed	If you want to see certain risks of certain status, you can choose this filter.
Filter: Aging	Pull down selection of various age ranges	Use this filter to see risks of a certain age.

Screen Review: Map Risk to Project (2 of 2)

Field/Action/Selection	Description	Best Practice
Filter: ACTION: Circle with X (cancel)	This is the button you press to execute the filter search.	Press this button and your resultant to list appears below.
Filter: ACTION: Magnifying Glass (Search/Filter)	Cancel and clears all filters	Use when you want to reset to default
Select Remediation Project:	Allows you to select an existing project to map the risks to. You can also select "New Project."	You can only select one project, but multiple risks.
New Remediation Project Name:	When you select "New Project" above, you can type in the new project name here.	When you do this, the Remediation Project Overview page opens up for you to edit. There are several required fields within Remediation Project Overview so be ready to complete those fields. If an existing project, the Project Overview page will still be opened, but with existing information for review.
ACTION: Cancel	Cancel the mapping	No mapping will be executed.
ACTION: Save and Close	This will execute the mapping	If this is a new project, the Remediation Project Overview page opens up for you to edit. There are several required fields within Remediation Project Overview so be ready to complete those fields. If an existing project, the Project Overview page will still be opened, but with existing information for review.

Demonstrate

- Mapping from Risk Register
- Mapping from Action Items Tiles
- Mapping from within a project

Exercise

Simulate in the production environment:

- Mapping from Risk Register
 - Mapping from Action Items Tiles
 - Mapping from within a project
-
- Do everything except save and close

Overview: Edit Initial Risk Score

- When a risk has been imported or promoted to the risk register from a finding, at times the initial risk score could be incorrect or based on additional information it needs to be adjusted.
- If this is the case the initial risk score needs to be edited.
- This can ONLY be done starting from within the Risk Register (Note: Even if you Edit the Risk from within a project, you will not be able to edit the current risk score)

Screen Narrative: Edit Initial Risk Score

Item	Narrative
Purpose(s)	<ul style="list-style-type: none">To edit the initial risk score of a risk
High Level Description	<ul style="list-style-type: none">When a risk has been imported or promoted to the risk register from a finding, at times the initial risk score could be incorrect or based on additional information it needs to be adjusted in this case the initial risk score needs to be edited.
Detailed Description/Workflow	<ul style="list-style-type: none">When you are editing the initial risk score, the entire risk does not have to be edited, it simply needs to be expanded and when you review all of the 3 risk scores, such as initial risk score, current risk score, and safeguard risk score, when you are in the risk register, the only editable risk score is the initial risk score.Your ability to edit the initial risk score is the depiction of a pencil icon next to the words initial risk score.When you click the pencil icon, the pop up menu to edit the initial risk score is displayed.Please note that even though the initial risk is changed, the current risk will not change automatically, so if you need to also change the current risk that must be done only if the risk is mapped to a project. The only way to change a current risk is via the project area that lists the risks.
How this screen fits into the overall risk lifecycle	<ul style="list-style-type: none">This fits into the overall risk life cycle in the beginning, because if we are editing the initial risk score that means we are just getting started in the risk life cycle process.

Screen Visual: Edit Initial Risk Score

Mitigating Control &

Initial Risk



Current Risk

Safeguard Risk

When a user reviews a risk, there is a pencil on the Initial Risk (only) and therefore it can be edited from within the risk register. When this is selected, the window on the right appears.

Once changes to selections are made – the “Recalculate Likelihood” link needs to be clicked. The score will change.

Edit Initial Risk Score

Risk 3 | Utilize an Active Discovery Tool
CSP 23 | Asset Management
Status: In Progress

CIS CSC v8 | --- | 1.3 | Inventory and Control of Enterprise Assets | Utilize an Active Discovery Tool (Detect) (IG2, IG3)
CIS CSC v8 | --- | 1.1 | Inventory and Control of Enterprise Assets | Establish and Maintain Detailed Enterprise Asset Inventory (Identify) (IG1, IG2, IG3)

	Threat Cluster	Maturity Level	Likelihood	Mission	Objectives	Obligations	Score
Current Risk	Personnel Error	2	5	3.00	4.00	4.00	20
Safeguard Risk		4	2	3.00	4.00	4.00	8

Initial Threat Cluster: Personnel Error × ▾

Initial Maturity Level: 2 - Safeguard is implemented ful... × ▾

Initial Likelihood: 5 - Continuous × ▾

Mission: 3.0 (3) × ▾

Objectives: 4.0 (4) × ▾

Obligations: 4.0 (4) × ▾

Score: **20**

[RECALCULATE LIKELIHOOD](#)

CANCEL **SAVE & CLOSE**

Screen Review: Edit Initial Risk Score

Screen: Edit Initial Risk Score

Menu Selection: Risk Register

Navigation Notes: Risk Register → Select Risk → Click Pencil to Edit Initial Risk

Field/Action/Selection	Description	Req?	Best Practice
Risk ID	Displays current risk ID	N/A	Review only.
Risk Description	Displays current risk description	N/A	Review, this is not editable on this screen.
CSP	Displays common security program ID and description	N/A	Review, this is not editable on this screen.
Status	Displays risk status	N/A	Review, this is not editable on this screen.
Mapped Framework(s)	Displays mapped framework controls	N/A	Review, this is not editable on this screen.
Current Risk Information and Score	Displays current risk information and score	N/A	Review, this is not editable on this screen.
Safeguard Risk Information and Score	Displays current safeguard information and score	N/A	Review, this is not editable on this screen.
Initial Threat Cluster	Select the threat cluster for this particular risk from the list provided.	Y	There are nine threat clusters in all.
Initial Maturity Level	Select the maturity level that the current mitigating control is at, on a scale of one to 5.	Y	There are five maturity levels that can be selected from 5 being the highest maturity level.
Initial Likelihood	Based on threat cluster and maturity level and industry, a likelihood will be suggested, this can be overridden.	Y	On a scale of 1 to 5, a 1 being least likely, and five being most likely, this is derived from information provided.

Screen Review: Edit Initial Risk Score

Screen: Edit Initial Risk Score

Menu Selection: Risk Register

Navigation Notes: Risk Register → Select Risk → Click Pencil to Edit Initial Risk

Field/Action/Selection	Description	Req?	Best Practice
Mission	Based on your calculated acceptable risk definition, select your mission impact, on a scale of 1 to 5.	Y	Non-tolerable is generally a 3 of 5.
Objectives	Based on your calculated acceptable risk definition, select your objectives impact, on a scale of one to 5.	Y	Non-tolerable is generally a 3 of 5.
Obligations	Based on your calculated acceptable risk definition, select your obligations impact, on a scale of 1 to 5.	Y	Non-tolerable is generally a 3 of 5.
ACTION: RECALCULATE LIKELIHOOD	If you change The threat cluster or the maturity level and you would like to see what the likelihood change is, click recalculate likelihood. The words “recalculate likelihood” is actually a clickable button in this area.	ACTION	The recalculate likelihood doesn't look like a button, you can press it and change things and press it as many times as you need to see what the scores end up looking like.
SCORE	This is the score that is presented to you.	N	It is read only, it can only be changed by changing the score information and a recalculate likelihood link press.
ACTION: Cancel	Cancels all changes without saving	ACTION	Use when you don't want to save.
ACTION: Save & Close	Saves all changes and closes the window	ACTION	Saves and closes.
ACTION: Circle with X (Upper Right)	Cancels all changes without saving	ACTION	Use when you don't want to save.

Demonstrate

- Demonstrate the changing of the initial risk score

Risk Audit: Overview

- To see the history of a risk, users can use the RISK AUDIT feature that is within the risk register.
- A risk audit is part of the Three Dot Menu for each individual risk.
- When selected, an entire page appears, showing the history of the risk, including when a risk was edited, when status changed, etc.