Version 9.5 Release Notes

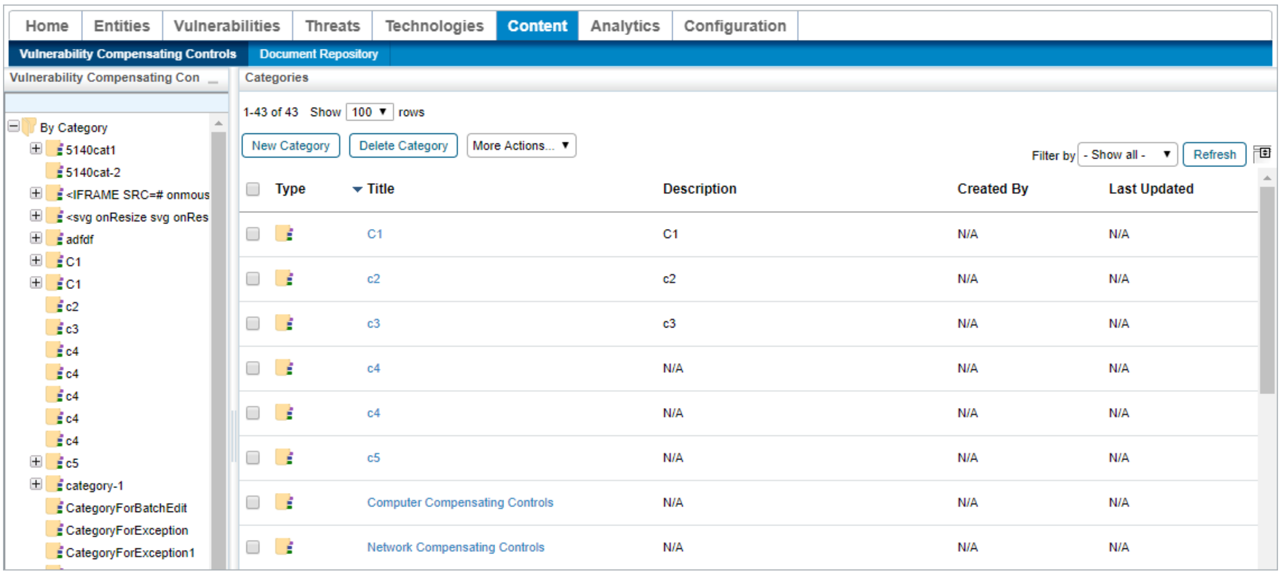
The following describe the new features and improvements introduced in RiskVision version 9.5 released on August 26, 2020.

Vulnerability Compensating Controls

Users of the **Threat & Vulnerability Manager** application can now use vulnerability compensating controls to track a vulnerability's risk mitigations. There are two primary use cases addressed by this feature:

- Adding new compensating controls to assets; and
- Reflecting existing compensating controls that are already in place.

Vulnerability compensating controls can be created by users and attached to vulnerabilities, entities, exceptions, and tickets. Attaching the compensating controls to tickets will help track the implementation of the compensating controls while attaching the compensating controls to exceptions will help justify the exception.



1-43 of 43 Show 100 rows

Type	Title	Description	Created By	Last Updated
	C1	C1	N/A	N/A
	c2	c2	N/A	N/A
	c3	c3	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c5	N/A	N/A	N/A
	Computer Compensating Controls	N/A	N/A	N/A
	Network Compensating Controls	N/A	N/A	N/A

Exception Enhancements

Multiple improvements have been made to the exception object across all Riskvision applications. These improvements include:

- Risk reductions from exceptions are now tied to the Status value rather than the workflow stage. This affords the flexibility to take approved exceptions to either an intermediate or terminal stage.
- Exception status values are now mapped to **Approved** so they can be named anything the user chooses.
- Users can now take risk reductions against multiple status values.
- Exceptions can now be set to expire, causing risk reductions to be reversed. Expired exceptions can be routed to whichever workflow stage the user chooses. For example, they can be moved to a review stage or a terminal stage.

The following improvements relate specifically to vulnerability exceptions:

- There can be multiple exceptions on an individual vulnerability instance.
- When an exception scope is defined as **Vulnerability Definition(s)**, **Common Platform Enumeration(s)**, or **Apply to All Vulnerability Definitions for Selected Entities**, it will automatically apply to all current vulnerability instances under the selected scope, as well as all vulnerability instances that are discovered within the scope in the future.
- Exceptions can now be created for Common Platform Enumerations (CPEs). When exceptions are created against a CPE, the exception will automatically apply to all the Common Vulnerability Enumerations (CVEs) linked to the CPEs. This can be useful, for example, if there is a technology you know you won't be able to patch for a given asset scope. Instead of having to create an exception for each vulnerability related to the CPE, you now only need to create a single exception for the entire CPE.

NOTE: After upgrading to RiskVision version 9.5 or higher, each RiskVision instance must have at least one approved status mapped before performing any action in RiskVision. To view this new page the user must have the Exception Manage permission. New installations at version 9.5 or higher will have a default mapping already provided that can be overridden.

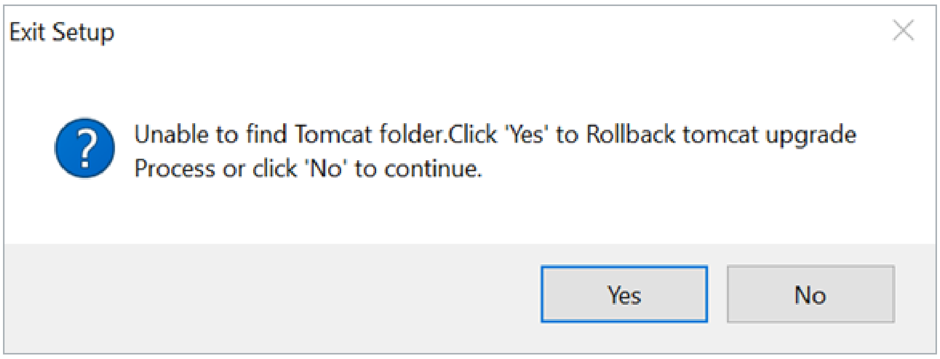
NOTE: After upgrading to RiskVision version 9.5 or higher, the user must run the **Rebuild Grouping Cache** job. Otherwise the risk scores in a vulnerability's Affected Entities tab will not display properly.

Attachment Encryption

Users can now re-enable or disable their RiskVision server's automatic encryption of attachments.

Upgrade Rollback Feature

RiskVision's Minor Version Upgrade Installer has a new rollback feature that allows the user to roll a component back to its previous version in the event that the upgrade fails.



Unable to find Tomcat folder.Click 'Yes' to Rollback tomcat upgrade Process or click 'No' to continue.

Restricted Entities Error Message

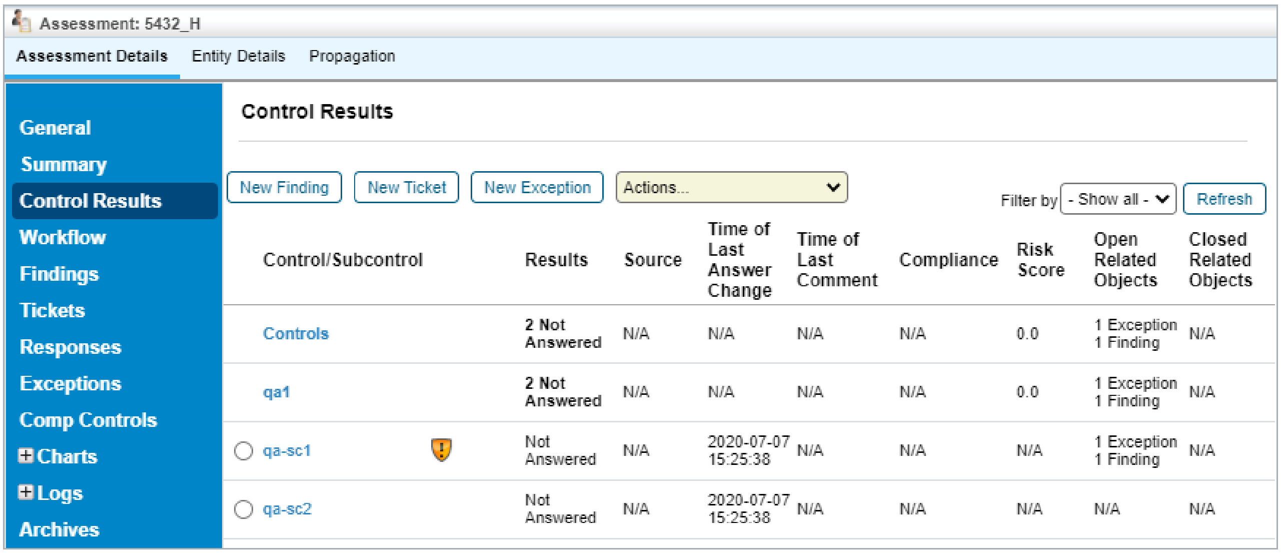
When a user who does not have permission to view all entities attempts to view a page that shows all the entities attached to a vulnerability or threat, he or she will see the following message: **You are not able to see all the entities on this page because you are restricted from seeing [quantity of hidden entities] entities**. This will make RiskVision's behavior clear when customers apply filters that restrict the data a user can view.

Classification Assessment Enhancements

RiskVision can now handle even more complex dependent questions on classification assessments by taking the latest timestamp for a given Confidentiality, Integrity, and Availability value. This allows for multiple layers of dependent questions, and allows users to implement detailed classification requirements like those detailed in NIST 800-60.

Control Results Grid Enhancements:

The Control Results grid has new **Time of Last Comment** and **Closed Related Objects** columns. In addition, the **Time** and **Related Objects** columns have been renamed to the **Time of Last Answer Change** and **Open Related Objects** columns respectively. These changes make it easier to see if a recent comment was made on a subcontrol question and whether there are any closed remediation objects associated with the subcontrol.

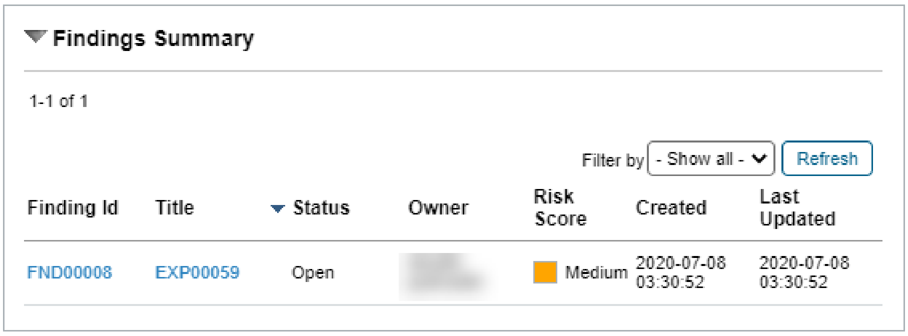


Control Results

Control/Subcontrol	Results	Source	Time of Last Answer Change	Time of Last Comment	Compliance	Risk Score	Open Related Objects	Closed Related Objects
Controls	2 Not Answered	N/A	N/A	N/A	N/A	0.0	1 Exception 1 Finding	N/A
qa1	2 Not Answered	N/A	N/A	N/A	N/A	0.0	1 Exception 1 Finding	N/A
○ qa-sc1	Not Answered	N/A	2020-07-07 15:25:38	N/A	N/A	N/A	1 Exception 1 Finding	N/A
○ qa-sc2	Not Answered	N/A	2020-07-07 15:25:38	N/A	N/A	N/A	N/A	N/A

Furthermore, the Control/Test Details pages for controls or sub controls in the grid now have a **Status** column for the **Findings Summary**, **Tickets**

Summary, and **Exception Summary** grids.



▼ Findings Summary

1-1 of 1

Filter by - Show all - Refresh

Finding Id	Title	▼ Status	Owner	Risk Score	Created	Last Updated
FND00008	EXP00059	Open	[redacted]	🟧 Medium	2020-07-08 03:30:52	2020-07-08 03:30:52

Health Report Auto-Send Format Change

The Health Report will now be auto-sent in a .ZIP format instead of a .HTML format for customers who have the Health Report Auto-Send feature enabled. If your organization has not enabled this feature, it is recommended that you enable it to help Resolver better serve your organization.

Zombie Attachment Retrieval

RiskVision now offers a way of retrieving zombie attachments. This allows users to identify and delete unwanted files, and may improve the performance of your RiskVision instance.