

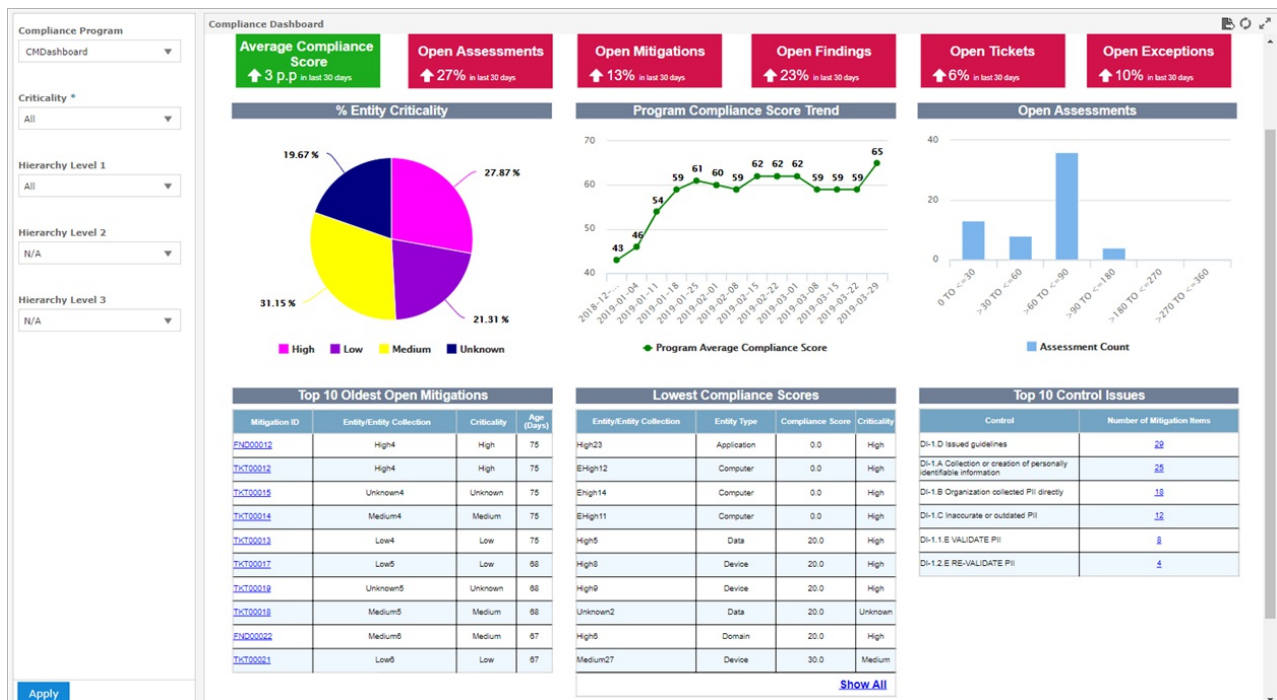
Version 9.2 Release Notes

Risk & Compliance Reporting

Compliance Dashboard

The new [Compliance Dashboard](#) allows executives, information security officers, and security and compliance teams to easily monitor, track, and review compliance and remediation statuses and scorecards within a relevant program, all in one place. Charts include average, lowest, and trending compliance scores, the number of open assessments and mitigations, and more.

Dashboard filters are saved for the currently logged in user, so they don't need to be applied each time the dashboard is accessed. Filters include Program, Criticality, and Hierarchy Levels 1 through 3. The Compliance Dashboard is highly flexible and can be used to report on business units at various levels, including an entire organization, a division, and a department.



Risk-Related Enhancements to Assessments Domain

Recent enhancements to the [Assessments domain](#) now makes it possible to create a number of new risk-related reports using new fields, including Risk Score, Compliance Score, Overall Impact, Overall Likelihood and more.

Choose Data

To move items in or out of selected fields, double-click them, drag them, or use the direction buttons.

The screenshot displays a user interface for selecting data fields. It is divided into two main sections: 'Source' and 'Selected Fields'. The 'Source' section on the left contains a list of data categories and their associated fields. The 'Assessment Risk details' category is currently selected and highlighted in blue. The 'Selected Fields' section on the right is currently empty. Between the two sections are five directional buttons: a right-pointing arrow, a left-pointing arrow, a double right-pointing arrow, and a double left-pointing arrow. The 'Source' list includes the following items:

- Control Groups
 - Control Groups/Controls
 - Control Type
 - Compliance Score
 - % Answered
 - Risk Score
- Assessment Risk details** (highlighted)
 - Risk Permanent ID
 - Risk Title
 - Risk Categories
 - Risk Description
 - Assessment Risk Owner
 - Overall Likelihood
 - Overall Impact
 - Inherent Risk Score
 - Residual Risk Score
 - Current Risk Score
- Controls and Subcontrols Mapped To Risks
- References Mapped To Risks

Remediation-Related Features

Batch Workflow Transition

The new [Batch Workflow Transition](#) action allows users to move up to 50 objects to another workflow stage in bulk, making it quick and easy to transition tickets, findings, exceptions, or incidents that are in the same stage through a single action.

New Findings

1-47 of 47 Show 100 rows

New Details Delete More Actions...

<input type="checkbox"/>	Finding Id	Title	Subcontrol	Owner	Awaiting Action By	Team
<input checked="" type="checkbox"/>	FND00075	Ftest2		CMDashboarduserk	CMDashboarduserk	N/A
<input checked="" type="checkbox"/>	FND00074	FTest1		CMDashboarduserk	CMDashboarduserk	N/A
<input checked="" type="checkbox"/>	FND00073	Ftest3	Medium20 (of Program Test CMDashboard)	CMDashboarduserk	CMDashboarduserk	N/A
<input checked="" type="checkbox"/>	FND00072	Ftest2	Medium20 (of Program Test CMDashboard)	CMDashboarduserk	CMDashboarduserk	N/A
<input type="checkbox"/>	FND00071	Ftest1	Medium20 (of Program Test CMDashboard)	CMDashboarduserk	CMDashboarduserk	N/A

More Actions...
 More Actions...
 Import Audit Findings
 Add Finding Response
 Show Finding Responses
 New Exception
 New Ticket
 Synchronize Workflow
 Delegate
 Batch Workflow Transition
 Save as CSV
 Customize

Batch Edit Tickets

Users can now edit the modifiable fields of up to 50 tickets at once with the [Batch Edit Tickets](#) action.

Open Tickets

1-56 of 56 Show 100 rows

New Details Delete More Actions...

<input type="checkbox"/>	Ticket ID	Title	Type	Owner
<input checked="" type="checkbox"/>	TKT00069	TKT1	Entity Control Resolution	CMDashboarduserk
<input checked="" type="checkbox"/>	TKT00068	Tkt 12	Entity Control Resolution	CMDashboarduserk
<input checked="" type="checkbox"/>	TKT00067	Tkt 18	Entity Control Resolution	CMDashboarduserk
<input type="checkbox"/>	TKT00066	Ticket42	Entity Control Resolution	CMDashboarduserk
<input type="checkbox"/>	TKT00065	Ticket41	Entity Control Resolution	CMDashboarduserk

More Actions...
 More Actions...
 Synchronize Workflow
 Batch Edit Tickets
 Delegate
 Save as CSV
 Customize

Hide Action & Comment Required Workflow Options

With the new Hide Action and Comment Required [options](#), actions can be hidden in the Workflow section of an object (when a transition is automated and doesn't require any action from end-users) and comments can be marked as either mandatory or optional.

Actions						
	Label	Next Stage	Email Template	Status	Hide Action	Comment Required
<input checked="" type="checkbox"/>	Close	Closed	Exception Signoff [Default]	Sign Off Approved	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Reject	Requested	Exception Signoff Rejected	Sign Off Rejected	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>

Workflow Stage Notification for Owner

Notify requester use Email Template

Allow Delegation

Delegation Label: Delegate To use Email Template Exception Delegation [De] Preview

Allow additional stakeholders to be added Comment required

Additional Threat & Exploit Data Fields

Exploit Date Fields

Exploits now show the dates the exploit was added and last updated via the new Date Added and Last Updated Date fields.

Threat Intelligence Fields

The General tab in a Threat object page has three additional read-only fields from the FireEye connector: Risk Rating, Exploit Rating, and Exploitation inTheWild, all three of which provide important information about the risk of a vulnerability.

Threat: Google Devices qdsp6v2 Unspecified Vulnerability Edit

General

Report

Vulnerabilities

Targeted Entities

Tickets

Incidents

Threat Information

Type Vulnerability

Source FireEye

Title Google Devices qdsp6v2 Unspecified Vulnerability

Description An unspecified vulnerability exists within the qdsp6v2 component in Google devices that, when exploited, allows an attacker to locally gain elevated privileges. Exploit code is not publicly available. Mitigation options include a vendor fix. Exploitation Rating: No Known

FireEye iSIGHT Intelligence considers this a Low-risk vulnerability due to the local access and interaction with a malicious application required for exploitation. Customers with specific questions regarding this vulnerability can contact the Vulnerability & Exploitation Team at analystaccess@fireeye.com.

Published 2018-02-06

Date

Last N/A

Updated

Owner N/A

Severity N/A

Likelihood N/A

Risk N/A

Risk Rating LOW

Exploit No Known Rating

Exploitation No InTheWild

Mitigation Status

Status N/A

Comment N/A

Change History

Results as of 2019-04-09 14:44:19

[Save as CSV](#) Filter by - Show all - [Refresh](#)

Changed Attribute	Old Value	New Value	Who	When

Enterprise Risk Manager Usability Enhancements

Program Name

The grid on the Risk Register page has a new Program column that displays the program name. Additionally, clicking on a risk will open the Risk Details page in a new tab in your browser, where the program and assessment name are also displayed.

RISK VISION Enterprise Risk Manager User Settings Configure UI Help Log Out

Home Entities Assessments Risks Analytics Configuration

Welcome Risk Register Risk Responses Message Center Questionnaires Submitted Questionnaires Tickets Exception Requests

1-20 of 21 Show 20 rows Page 1 2 Go to 1 Go

[Edit](#) [More Actions...](#) Hide Non-Applicable Items Filter by - Show all - [Refresh](#)

Assessment	Program	Risk	Owner	Description	Inherent Risk	Overall Impact	Overall Likelihood	Responses	Controls	Residual Risk
E-testRRV-3185	RV-131	Sabotage, Lack of monitoring of non employee access points		Non-employee physical premise access is controlled and monitored.	Low	Medium	Medium	None	No Control	N/A
E-testRRV-3185	RV-131	<code><img/src=x onerror=alert('Fuser')></code>		<code><img/src=x onerror=alert('Fuser')></code>	Low	Medium	Medium	None	No Control	N/A
E-testRRV-3185	RV-131	Gas leaks, Lack of disaster recovery process		Organizational premise where business information processing or storage is performed and analyzed for environmental hazards including exposure to hazardous manufacturing facilities, natural gas, petroleum or other pipelines, natural disasters such as flooding, tornadoes or earthquakes, etc.	Low	Medium	High	None	No Control	N/A
E-testRRV-3185	RV-131	Sabotage, No Testing of data center security		Penetration tests are performed to verify the data center physical security	Medium	High	High	None	No Control	N/A
EntityExceptionImprovements0016	RV-131	DNS failure, Lack of network redundancy		Network redundancy or diverse network routing is maintained.	Medium	High	Medium	None	No Control	N/A
EntityExceptionImprovements0016	RV-131	DNS failure, Lack of business recovery procedures		A comprehensive business continuity plan, including technology solutions is in place to address recovery of service during a time of business interruption.	Low	Medium	Medium	None	No Control	N/A
EntityExceptionImprovements0016	RV-131	Floods, Lack of disaster recovery		Copies of system and data back-ups are taken and stored off-site at locations with an adequate distance from the production site and for an adequate period of time	Medium	High	Medium	None	No Control	N/A

Additional Fields on the Risk Details Page

To provide greater context when looking at the Risk Details page, we have added fields for both program name and assessment name.

The screenshot shows a web interface for risk management. At the top, it displays "Risk 1 of 5" with navigation links for "Previous Risk" and "Next Risk", and a "Back" button. Below this, the risk title is "Risk: Application software failure, No logging at application level". To the right, there are two buttons: "Medium Inherent Risk" and "Low Residual Risk".

The main content area is titled "Summary" and includes a dropdown menu for "Actions" set to "--Select--". The "Summary" section contains the following details:

- Program ERM Always On Program 2-21-17
- Assessment 10.10.16.101
- Risk Title Application software failure, No logging at application level
- Category Application software failure
- Permanent Id BR0454
- Owner Herb Hancock
- Description Security events are logged at the application level. ABC.
- Applicable Yes
- Custom String 1 N/A

Below the summary, there are several expandable sections:

- Controls
- Risk Responses
- Risk Assessment Questionnaires
- Comments
- Inherent Risk Analysis
- Residual Risk Analysis
- Risk Auto-Identification

Minor Version Upgrade Installer

This [new installer](#) allows users to perform minor upgrades of the the third-party software needed to run the latest version of RiskVision, preventing the need to download and install updates individually.



Minor Version Upgrade Completed

Installation process completed.

- 1)Apache Web Server to version 2.4.37
- 2)Apache Tomcat to version 8.5.35
- 3)Oracle MySQL to version 5.7.24
- 4)Java to version 1.8.0_202

Cancel

< Back

Finish