SimpleRisk

SimpleRisk Release Notes

(20220306-001)

If you are not already running SimpleRisk, then you will need to DOWNLOAD it and follow the instructions for your chosen installation method. If you are currently running a previous release of SimpleRisk, then you will need to go to your Configure menu, select Register & Upgrade, and then click the "Upgrade the Application" button. This will run both the application and database upgrades to move you to the most recent release.

The complete list of changes for this release is below:

SimpleRisk Core

New Features

- Added the ability to use the Controls "Filter by Text" field to find control numbers associated with mapped frameworks.
- Updated the Control Gap Analysis report to use the Reference Name rather than the Control Number so it displays the number for the selected framework.
- Added a new error message for instances where SimpleRisk cannot communicate with the database.

Security

- Fixed several SQL injection vulnerabilities through the SimpleRisk Extras in a new initiative to ensure we are taking every precaution to secure SimpleRisk.
- Fixed an XSS vulnerability in the Risk Assessments module.

Bug Fixes

- Fixed an issue where Project Due Date does not respect the selected date format. Users were required to use 0000-00-00. This is no longer the case and the date format selected for the account will now work for saved due dates.
- Fixed an issue where saving a review and assigning a new project would not create the new project or assign the risk to it.
- Fixed an issue where controls would display with the word "top" in front of the control short name.
- Fixed an issue where the Review Regularly page in the Risk Management module risk ID field could not be filtered or searched properly.
- Fixed an issue where the "Control Status" field displayed when you go to Governance and select the "Controls" tab shows a value of 0 or 1 instead of "Pass" or "Fail".

SimpleRisk Extras

Vulnerability Management Extra

- Fixed a number of issues in the tenable.io implementation.
- Fixed a bug in the tenable.io connectivity test.
- Updated the tenable.io integration to ignore scans that are older than 35 days and have been archived.
- Updated tenable.io to only pull active sites.
- Updated the "Triage Vulnerabilities" page to display the number of vulnerabilities to triage.
- Updated the "View Risks" page to display the number of vulnerabilities that have been triaged into risks.
- Updated the "Triage Vulnerabilities" and "View Risks" pages to limit the initial description displayed to 500 characters and provide a "Read More" option to expand.
- Added a "platform" tag to risks created from Tenable.io.
- Added a log to show when the last run of Vulnerability Management was.

Customization Extra

- Fixed an issue where custom fields would not be displayed when editing a risk.

Team-Based Separation Extra

- Added a suite of new permissions controls for different situations regarding the Document Program. You can now specify what attributes will give a user access to a given document including: User, Team, Stakeholders.
- Fixed an issue where non-admin users could not edit documents when the Team-Based Separation extra was active.

Email Notification Extra

- Added an Action notification to send an email when a new document is added.
- Added an Action notification to send an email when a document has been edited.

Incident Management Extra

- Fixed an XSS present in the IM Extra.
- Fixed an issue where users could not delete a newly added playbook.
- Fixed an issue where older versions of MySQL and MariaDB could not enable the extra successfully due to a renamed field.

Import-Export Extra

- Fixed an issue where the Next Review Date column is not populated when exporting the Dynamic Risk Report.
- Fixed an issue where the characters “‘“ and “&” would not be exported properly.

Compliance Forge SCF Extra

- Fixed an issue where the following Frameworks did not associate with their controls successfully:ISO__27018 v2014 MPA__Content Security Program v4.07 NIST__800-161 [partial] NIST__800-171 rev 2 US__IRS 1075 US SSA__EIESR v8.0.

Encryption Extra

- Add a configuration to enable the Encrypted Database Extra debug logging so it does not fill up the debug log file by default.

Other Notes

- A SimpleRisk user noted that they were having difficulty logging in with the default username of “admin” with password of “admin”. Upon investigation, it was discovered that PHP was enforcing secure cookies, but the application was not using SSL, so the session values were not set. This may be an isolated instance, but if you experience this issue, try installing a SSL certificate and run SimpleRisk over HTTPS to fix it.