SimpleRisk

SimpleRisk Release Notes

(20210930-001)

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 a new Control Type field. When the Control Type is Enterprise you will be able to track a status of pass fail that stays with that control, whereas before you could only review the state of a control by reviewing its most recent audit tests. This also feeds into new additions you will see on the mitigation page for Control Validation when a control is attached to a mitigation. This includes the ability to attach a control artifact.
- Added a new feature that allows users to create a risk based on a control failure when submitting the failed control test during an audit. When users save an audit test with a test result of "Fail" the user will be prompted with the ability to submit a risk based on this failure or attaching this failed control to an existing risk. Users can select "No" to not associate the failed test with a risk.
- Added the ability for users to configure the max subject length of risks. (Configure → Settings)

Usability

- Added all customization fields to Dynamic Risk Report regardless of if they appear in an active template.
- Added audit logging for documentation reviews.
- Added the ability to select jquery CDN or local for restricted environments.
- Updated to a lower resource costing version of the font system in place.
- Added filters to the Risks and Controls Report.
- Added filters to the Risks and Assets Report.
- Added Reporting for Risk Mapping to the Dynamic Risk Report
- Added the ability to edit asset names in the Asset Management menu.
- Added several improvements and details to the Risks and Assets report including new fields for highest residual risk, average residual risk, highest inherent risk, and average inherent risk.
- Added a filter for projects to the Risks and Assets report.
- Risks and Controls report now displays the color of the highest risk score in the table header for each control.
- Added the ability to edit asset names directly through the "Edit Assets" menu in the "Asset Management" section.
- Added the ability to edit Project names in the "Plan Project" menu.

- Added additional details associated with projects. (Due Date, Consultant, Business Owner, Data Classification.)
- Added additional debugging to the Upgrade Extra.
- Added a Healthcheck to ensure php max_var_char is set properly.
- Added a Healthcheck to ensure php-gd and php-zip are present.

Security

- Integrated CSRF Magic to allow for newer versions to be included with SimpleRisk.
- Fixed XSS when adding an attack vector with a script in the name.
- Fixed XSS when adding an IM playbook with script in the name.
- Fixed an issue where a user could view all Asset Valuations without permission to do so.
- Fixed an SQLi when retrieving risks from the database.

Bug Fixes

- Fixed an issue where changing date format would result in the Document Program next review date not automatically populating.
- Updated the display method for active audits to support high volumes of active audits.
- Fixed an issue where users could configure the risk scoring levels into a state that was not functional and could not be corrected through the UI.
- Fixed an issue where custom fields continued to not be exported unless currently assigned to a template.
- Updated jquery CDN to use google instead of jquery's CDN.
- Fixed a bug where asset management using team-based separation would not block the view of assets properly.
- Fixed an issue where sorting by Next Review Date in the Dynamic Risk Report would cause the report to indefinitely say "Processing".
- Fixed an issue where submitting a risk with any template outside of the default would cause affected assets to not poll correctly.
- Fixed a bug where users were unable to upgrade the Upgrade Extra unless they were on the newest release.
- Fixed an issue where the link generated for Management Review yes/no in All Open Risks Assigned to me incorrectly adds 1000 to the url for the risk ID.
- Fixed an issue where All Risks Assigned to Me report did not function as intended with team-based separation turned off.
- Fixed a bug where admin users could add users with invalid e-mail addresses.
- Fixed an issue where using the SimpleRisk API would create a session for the user that could be used to gain access to the UI.
- Fixed a bug where removing the Risk Scoring Method field would result in the risk being unable to be scored or displayed properly.

SimpleRisk Extras

Risk Assessment Extra

- Fixed a bug where Risk Submission via the Risk Analysis did not function.

- Fixed a bug where not entering certain fields during risk submission of a pending risk would prevent the confirmation messages from displaying.
- Fixed an issue where Risk Analysis did not use the correct submission date format.
- Fixed an issue where fill in the blank questions could not be edited.

Import/Export Extra

- Updated the extra to function with multiple templates and export the template associated with a risk and it may now be declared during import as well.

Customization Extra

- Fixed a bug where removing the Risk Scoring Method field would result in the risk being unable to be scored or displayed properly.
- Fixed an issue where removing the Supporting Documentation field would break the ability to submit risks.

Notification Extra

- Fixed a bug where the middle date range for sending a notification for the Document Program would not send as intended.
- Fixed an issue where the 3rd and furthest out date e-mail notification for Document Program would display $due_date instead of the number of days until due.

Team-Based Separation Extra

- Added an asset permission for “Allow all users to see assets not assigned to a team” which is checked by default. When unchecked only admins will see assets that are not currently assigned to a team.

Incident Management Extra

- Fixed a bug in Incident Management where the related risks subject was encrypted when the Encrypted Database Extra was enabled.
- Fixed a bug where the Fontawesome icon name changed and the disk "save" icon wasn't displaying.

Custom Authentication Extra

- Added the ability to manage and map Roles and Teams to users using LDAP or SAML. A new claim/assertion may be required to make those values available to SimpleRisk.

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.