SimpleRisk

SimpleRisk Release Notes

(20210625-001)

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 automated database backup scheduling system under Configure → Settings → Backups.
- Increased granularity in the audit log regarding risks.
- Increased the information retained for the audit log regarding audit tests.
- Added the ability to add custom impact descriptions for the Contributing Risk scoring methodology.
- Added an "About This Page" link in the help menu to provide additional context and help for the different pages in SimpleRisk. This feature is still under construction and only available for the Risk Management module at this time.

Usability

- When no mitigating control is available for a mitigation the system will now report "No Control Available"
- Updated mouseover descriptions for User Permissions.
- The control short name is now displayed with audit tests.
- Removed the ability for admins to remove their own admin rights.
- Admins can no longer change what teams they belong to as they have access to all risks.
- Updated the Dynamic Risk Report so that when you group by a value that can have multiple checked for a single risk (ie. "teams"), it only shows that group once with all associated risks. In previous releases, it splits it out so if you assign a risk to multiple teams, that shows as a separate grouping.
- Added Project Status (Active, On Hold, ect.) to the Dynamic Risk Report.
- Filters on the Define Tests page are now kept after editing a test.
- Filters on the Define Control Frameworks page are now kept after editing a control.
- The Management Review filter found on Plan Mitigations and Perform Reviews isi now a dropdown to be in line with mitigation planned.
- Added a "Back" button to the Manage Users tab in User Management when editing a user.
- Updated from unsupported Zend Escaper to the newer Laminas Escaper.
- Added Risk Scoring to the dynamic risk report to allow users to display a column of the current risk scoring methods in use for risks listed in the table.

- Added a field to display the Inherent Risk score from 30/60/90 days ago in the Dynamic Risk Report.
- Added the ability to view the contributing risk likelihood and impact values in the Dynamic Risk Report.
- Increased control_number field size to 50 characters.
- Added a healthcheck to determine what the memory_limit value is set to in the php.ini file.
- Added a healthcheck to determine what USE_DATABASE_FOR_SESSIONS is set to in the config.php file.

Bug Fixes

- Fixed an issue where "Current Control Maturity" and "Desired Control Maturity" values are not copied when cloning a control.
- Fixed an issue where browser zoom would cause the Governance → Define Control Framework page would not display properly.
- Fixed an issue where users could receive a notice in the PHP log when viewing the Document Program page.
- Fixed an issue where an Asset Group's name would be escaped when editing and would save with unintended characters in the group name.
- Fixed an issue where not setting a compliance test result and leaving null would result in being unable to see that test in the past audits.
- Fixed an issue where long control names would not display properly in Compliance → Past Audits.
- Fixed a bug where approximate time was not saved when editing a compliance test.
- Fixed an issue with double encoding pop up menus on the Governance → Define Exceptions page.
- Fixed an issue where submitting a risk the displayed pop confirmation would not be escaped properly.
- Fixed an issue where returning the test audits last test date and next date were incorrect.
- Fixed an issue experienced when using Internet Explorer where the page doctype would be improperly set causing display and submission issues.
- Fixed an issue with the Connectivity Visualizer not showing assets when the Encrypted Database Extra is not enabled.
- Added a Default Desired Maturity value to Settings.
- Added a Default Current Maturity value to Settings.
- Fixed a Fatal Error when trying to communicate with SimpleRisk services when they are unavailable.

Security

- Fixed a potential XSS vulnerability on the Control Gap Analysis report.
- Fixed a potential XSS vulnerability with Control Exceptions.
- Fixed a potential XSS vulnerability on the Dynamic Risk Report.
- Fixed a potential XSS vulnerability on the View Risk page.
- Fixed a potential XSS vulnerability on the Custom Authentication Settings tab when mapping LDAP groups.
- Fixed a potential XSS vulnerability on the Plan Mitigation

- Fixed a potential XSS vulnerability in the Connectivity Visualizer.
- Fixed an issue where Team-Based Separation could be circumvented.
- Fixed an issue where a username matching a UID could be used to login as that username.
- Fixed a potential XSS vulnerability on the Add and Delete Assets page
- Fixed a potential XSS vulnerability on the Manage Asset Groups page
- Limited platform to one password reset for a given user every ten minutes to prevent 'Email Bomb' attacks.

SimpleRisk Extras

Customization

- Added the ability to create multiple templates for use with Organizational Hierarchy.
- Fixed an issue where User Multi-Select dropdowns would cause a risk to be unable to save.
- Fixed an issue where the Risk Mapping field could not be restored.
- User Multi Dropdowns will now respect organization hierarchy.

Custom Authentication

- Added a check that prevents users from manually creating duplicate users using LDAP/SAML.

Risk Assessment

- Added sharing functionality for Risk Assessments allowing you to give access to the results to a person who does not have a SimpleRisk login.
- Import/Export capabilities have been updated to be more in line with how Risk imports work. Question IDs are now absolute values and no longer only relative to the import. Mapping question ID will update the question in the line and leaving it unmapped imports the question as a new question.
- Fixed an issue where mapped controls were not saved if Compliance Assessment was not checked.
- We now display the Question ID in various places to help with the new changes to import/export
- When an Import is done that includes an answer that has Submit Risk set to "1" and no "Subject" defined we now set submit risk to "0" and give the user a warning that questions lacking a subject were edited to not attempt to submit a blank risk subject.
- Imports can now be used to remove answers to a question. Only answers imported with a given question will remain on the imported question even if others already exist in the system for that question.

Import-Export

- Added the Current and Desired Control Maturity fields to Control Import.
- Added the Current and Desired Control Maturity fields to Control Export.
- Filters on the Dynamic Risk report will now be respected when exporting.

Notification

- Added a new feature allowing users to customize their notifications layout and text.
- Fixed an issue where certain configurations in the Notification Extra Configuration page would not be saved.

- Fixed an issue where Automated Notifications of Unreviewed / Past Due Risks fails to complete if there's a user with no review permissions and only the notify reviewer option is selected.
- Fixed an issue where mitigation related e-mails would not decrypt properly with encryption turned on.
- Fixed an issue where unreviewed risks did not appear in the unreviewed/past due risk scheduled e-mail
- Added Notify Approver to the notify section for Document Reviews.
- When a review rejects and closes a risk the close notification will now send as expected.

Organizational Hierarchy

- Fixed an issue where Org Hierarchy would not function properly with admin users who did not belong to all teams.
- Added the ability for users to now assign individual templates based on the active Business Unit they are currently working with.
- Fixed a potential XSS vulnerability associated with the use of Organizational Hierarchy

Incident Management

- Added permissions for Incident Management.

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.