SimpleRisk Release Notes

Version 20180527-001

This version includes a XSS vulnerability fix, several bug fixes, the introduction of the role-based access control functionality, enhancements to the risk over time chart, the ability to change risk level names, and a new ComplianceForge SCF Extra available for free on registered SimpleRisk instances. If you are not already running SimpleRisk, then follow the standard installation instructions. If you are currently running the 20180301-001 release of SimpleRisk, then you will need to extract the new files over the old ones (back up your config.php first) and then run the /admin/upgrade.php script to upgrade your database.

The complete list of changes for this release is below:

- New Features
  - Added the ability to associate multiple technologies with a single risk.
  - Added more granular roles for the Governance section of permissions.
  - Created a new role-based access control functionality that allows you to map one or more user responsibilities to a role. Adds the ability for a user to be assigned to a role, which will automatically grant them those responsibilities.
  - Created a role for "Administrator" that, when assigned to a user, will grant the user all available responsibilities as well as assign them to all teams (including newly created teams).
  - Created a new Risk Management permission for "Able to accept mitigation". If a user has that permission enabled, they will be presented with a button called "Accept Mitigation" on the risk mitigation tab. When clicked, SimpleRisk will capture the username and timestamp of the acceptance and then add a checkbox showing "Mitigation accepted by <username> on <date> at <time>". Users with this role will then have a new button for "Reject Mitigation" which would revert that activity.
  - Created a new setting under Configure -> Settings for "Default User Role". This will be set to null by default, but provides a list of all of the roles that are available. Whichever role is selected will make it so that role and those options are automatically selected when going to create a new user under Configure -> User Management.
  - Added a new "Default Initiated Audit Status" before "Default Closed Audit Status" under Configure -> Settings. This value defaults to "--", but can be set to something else to affect the default status of an audit when it is initiated.
  - Added a dropdown for "Default Date Format" under Default Timezone in the Configure -> Settings menu. All existing date and datetime values DISPLAYED in SimpleRisk will use this format.
  - Added the ability to change the names of the different Risk Levels (Insignificant, Low, Medium, High, and Very High) to something defined by the user.

    - Added a new table to track the residual risk over time. It will be updated any time a control is added or removed for a risk, the mitigation percent value is changed for a control, the mitigation percent value is changed for a risk mitigation, or the risk score is updated for a risk.
    - Added the ComplianceForge SCF controls available for download and activation free with SimpleRisk registration.
- Security
    - Fixed a XSS vulnerability in the password reset page.
    - Added the "X-Content-Type-Options: nosniff" header.
- Usability
    - Added the “Planned Mitigation Date” column before the “Mitigation Effort” Column in the Dynamic Risk Report.
    - Added a Health Check to verify that SimpleRisk is running on PHP 5.x.
    - Automatically assign “Able to Accept Mitigations” responsibility to all users with access to the “Configure” menu as part of the upgrade process.
    - Automatically assign administrator role to all users with access to configure menu as part of the upgrade process.
    - When viewing the Active and Inactive frameworks tables under Governance, rows will now expand in order to accommodate description content that is larger than the row width allows.
    - Created a “TEST” functionality to verify that email is configured properly.
    - Added the Control information to the printable view for a risk.
    - Added the risk mitigation date to the Dynamic Risk Report.
    - Colored the header for the "Risks by Asset" view of the "Risks and Assets" report the same color as the highest level of risk associated with that asset. Added an "Asset Risk" value underneath the "Asset Value" for whatever the max risk value is.
    - Added the residual risk score to the printable view of a risk and renamed the current risk to inherent risk.
    - Added a button between the edit and delete buttons to duplicate a control. Clicking it will pop up a window to add a new control with the same values from the control that was copied.
    - Created functionality to track scoring history for residual risk over time.
    - Updated the risk scoring history chart to reflect the current line as "Inherent Risk". Create a new line labeled "Residual Risk" that shows the residual risk score over time on the same chart.
    - Sorted the Control Priority on the Governance Controls page alphanumerically.
    - Changed the label "Risk Score" on Risk Over Time graph to reflect "Inherent Risk" instead.
- Bug Fixes
    - Made the Inherent Risk on Risk Over Time always draw a line even if the Inherent Risk Score only has one data point.

  - Fixed an issue where changing the color for high risks in configure risk formula would change the color for medium risk in the risk dashboard.
  - Fixed an issue where sort by Residual Risk was not working on the Dynamic Risk report.
  - Fixed an issue where audit trail reports scoring method updated instead of risk score updated when changing the score of a risk.
  - Fixed an issue where risk submission would hang when supporting documentation file attachment was greater than the max size allowed. Will now report an error message instead.
  - Fixed an issue where Current Impact/Likelihood didn't match from an export to an import.
  - Fixed an issue where user created teams did not show up in the list of teams dropdown in Reporting -> Risk Dashboard.
  - Fixed an issue when viewing the printable version of a risk the risk score background color did not show.
  - Fixed an issue when clicking on a "Review Column" to view on the All Open Risks by Team by Risk Level Report, the screen refreshes and the columns displayed seem to be reset to the default and can't display any of the "Review Column" columns.
  - Fixed an issue where sorting on the Residual Risk column in the Dynamic Risk Report did not work.
  - Updated the risk score in the risk advice recommendations to be rounded to two decimal places.

- Notes
  - Beginning with the 20170102-001 release, SimpleRisk utilizes a new API for the Risk Management section as well as several of the reports. In order for it to work properly, you will need to enable the API by setting "AllowOverride all" in your Apache configuration file. This tells Apache to utilize the newly included .htaccess file in the /api directory.
  - As of the 20151219-001 release, we will no longer provide the SQL files for the various languages. Instead, users should use the Installer Script to perform their SimpleRisk MySQL database installation. If you would like to inspect the MySQL database schema before installing, the files can still be found under the "db" directory included with the Installer Script.
  - In performing some testing with a newer version of PHP, it appears that PHP has removed the standard JSON extension as of PHP 5.5rc2 due to a license conflict. This functionality is used in SimpleRisk's graphing library. If you notice that your pie charts are not displaying properly, you may need to install the "php5-json" package for these charts to work as expected.
  - 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.