User Groups in Security Risk Management

Last Modified on 04/05/2022 11:41 am EDT

User groups determine the applications and fields users can access within the Security Risk Management app. The app has five default user groups:

- Security Risk Team: Users in this group are the primary users of the app and have full access to all profiling and risk functionality, issues, corrective actions, findings, and the library. The security risk team can also create new internal locations for profiling and has access to profiling details of locations and assets. They can also be named as Location Owners.
- Security Assessment Team: These users are responsible for designing, creating, and launching security audits. This includes creating and scoping security frameworks and questionnaires. They can also be named as Location Owners.
- Security Audit Fieldwork (Limited User): These users are responsible for carrying security audits once they have been moved to the **Fieldwork** state, as well as documenting issues discovered during an audit and assigning them to Issue Owners. They also have full access to issues and corrective actions within their assessments.
- Security Assigned Actions (Limited User): Users in this group can be assigned to issues and corrective actions to address concerns that arose from the audit.
- Administrator (Incident Management): These users monitor the application and have access to view all data.