

# Security Management And Risk Tracking (SMART)

Web-based application to manage information risk

# Current Features

- Web-based interface for managing projects and submitting new project request
- Roles-based access for team lead, administrators, manager, and security consultants
- Online submission of new information security policy exception requests
- Workflow for submission of projects and exceptions
  - Route new requests to team leads
  - Allow team leads to assign the projects to security consultants
- Issue management for different projects
- Contact management and associating contacts to SC&A projects
- Reporting (new enhancements in progress)
- Searching
- Copying issues to current project after searching (to avoid duplication of effort)
- Delegation of duties and trust relationships
- File library to share documents to all visitors of the web site and allow administrator to maintain the library

# Current Features (cont)

- Policy management
  - Add/modify/update policies, rules, and standards
  - Manage policy domains and link each policy item to a domain
  - Attach policy to exceptions
- Third party link management
  - Telecom service provider management
  - Link types management
  - Linking third party connections to business units
- Asset management
  - Managing types of assets
  - Linking assets to exceptions
  - Asset vendors
  - Asset out of service date management
- File attachments
  - Upload and download files
  - Attach files to projects
- Knowledgebase of standard issues

# Asset Management

- Assets are considered “Objects” and play central role in risk tracking.
- Attributes related to assets are:
  - Asset types (router, server, etc.)
  - Asset groups (to link many assets to a complete system)
  - Location
  - Vendor
  - MAC and IP addresses, if available
  - Asset end-of-life date to ensure any outdated systems are not present on company network.
  - Sarbanes-Oxley (SOX) flag
  - HIPAA covered flag
  - Criticality of an asset
- Linking assets to:
  - Policy exceptions
  - Risk assessment
  - Incidents
  - Audits
- Using the “Real Time Assessment”, periodic scans can be done on assets (e.g. If a new open port is detected, the owner will be alerted)

# New Features (In Progress)

- Enhanced reports, PDF reports
- Export to other formats (MS Word, OpenOffice, etc)
- Enabling interface for security audit issues
- Creating more roles in the application to allow new types of users
- LDAP integration and password hashing using strong hash algorithms
- Support of additional databases
- Email notifications for:
  - After a new project is submitted for review
  - When a project is assigned to a security consultant
  - Getting signatures for draft and final reports
  - Notifications for overdue issues
  - Reminders and notifications for security exceptions
- Logging and auditing

# User Interface

- Consistent user interface
- Intuitive navigation features
- User of Cascading Style Sheets to allow quick change in interface
- Popup calendars to select dates
- Use of drop down menus to eliminate errors in data entry
- Pagination to avoid too long pages and too much data download during navigation
- Intuitive search capability
- Graphical representation for risk posture for manager role
  - Graphs showing projects risk distribution
  - Graphs showing exception risk distribution
  - Issue risk graphs will be integrated shortly
- User interface layout consistent across different roles, although capabilities are different

# Product Roadmap

- Q1-2006
  - Request Submission (New SC&A project, New Policy Exception Request, New Firewall change request) (Completed, except firewall)
  - Standard Issue submission and insertion into existing projects (Completed)
- Q2-2006
  - WYSIWYG Editor for HTML based editing
  - LDAP Integration, LDAP based access for project submission
  - Upgrade to MySQL 5.0 for enhanced features (Views, Transaction, etc.)
  - Better reporting tools, PDF reports
- Q3-2006
  - Basic Risk Assessment integration to issue management
  - New roles, including report generators
  - File attachment (already complete)
- Q4-2006
  - Enabling Contact feed from different resources
  - Data import and export
- 2007
  - Support of additional database (PostgreSQL, Oracle, DB2)
  - Move to J2EE platform
  - Incident management
  - Security audit management

# Roadmap: Miscellaneous Features

- Announcements (e.g. changes in security policy)
  - On the first page (home page)
  - Enable users to have email subscription to announcements
- Library, that will contain reference documents related to information security (e.g. PDF version of security policy, different forms etc.) (Completed)
- Links to related web sites (e.g. if there are any internal web site to request firewall changes)
- Addition of third party link questionnaire and risk assessment
- Policy printing
- Risk identification, ISO-17799 checklists
- Creating roles on-the-fly and page-based access

# Logging and Monitoring

- Logging events
  - Successful login
  - Unsuccessful login
  - Last login time for users
  - File attachment upload
  - File attachment download
  - ID switching (if IDs are delegated)
- Logging parameters
  - Timestamps
  - Event category
  - Event description
  - User
- Logs will be viewable to the application administrator
- Accounts may be locked for specified number of unsuccessful attempts

# Miscellaneous

- Migration
  - Depending upon existing systems, data migration strategy will be developed
  - Most probably all data from any existing application should be migrated with some effort
  - The application will allow data import in future releases
- Support
  - Arrangement will be made for annual support contracts (with free feature enhancements and free software upgrades)
  - Estimated cost will be 15K to 20k per year with free updates
- Licensing and intellectual property rights
  - Some software components are covered by GPL or other open source licenses (e.g. similar to Linux)
  - The software will be licensed like any other software ***without licensing intellectual property rights or any right to resell***
  - Licensing may also be on per user basis

# Features needed

- LDAP integration (table to hold LDAP parameters like server, usernam/password for server access, etc.)
- Email (Add functions to conformix.php)
- PDF files (integration of htmldoc)
- Graphics (JP Graph)
- Export to Excel
- Search for any word in any field of an issue or project
- Database encryption for everything
- Linking assets to each issue (Object based risk management)