Project Plan
Log Monitoring Compliance

The Capstone Experience

Team Spectrum Health
Kathryn Bonnen
Collin Lotus
Will Seeger
Wayne Stiles

Department of Computer Science and Engineering
Michigan State University
Fall 2011
Project Overview

• Problem:
  - Existing process requires user to check lists manually searching for audit records they need to review.
  - Several systems with lists of records
    - Very easy to miss necessary reviews
    - These users have better uses for their time

• Solution:
  - Unified Log Monitoring Compliance system
    - Integrates systems and lists
    - Displays personalized information to each user
Functional Specifications

• Automating Cerner system
  ▪ Audit log types to be automated: CCL Monitoring, Elevated Access Monitoring and Access Management

• Analysis and Central Data Store
  ▪ Log files parsed daily
    o Records stored
    o Records requiring review determined
  ▪ User notified via email of their pending reviews
Functional Specifications

• Multi-level User Interface
  ▪ Display based on role
    o Reviewer: Lists of pending records.
    o Manager: Summary of reviews
    o Executive: Scorecard overview of Compliance Health
Design Specifications

• Log-in
  ▪ User authentication
    ○ Query Active Directory

• Scorecard Display
  ▪ Shows trends of discrepancies across systems and audit types
  ▪ Two views: TIS Audit Discrepancy Scorecard, TIS Audit Logging Compliance Scorecard
  ▪ Default display for Senior Executives

• Compliance Summary Display
  ▪ Shows history of review actions taken for oversight
  ▪ Default display for Managers

• Pending Reviews Display
  ▪ Shows records which need to be reviewed by the user
  ▪ Links to displays of individual records from which actions can be taken
  ▪ Default display for Reviewers
Design Specifications

• Automated Analysis and Notifications
  ▪ Server consumes log files and determines whether records need to be reviewed.
  ▪ Server decides which user should review the record.
  ▪ Notifies users daily via email what reviews are due within 2 days

• Audit Exports
  ▪ Script accessible from web application to export the reviews in a .csv format by system, log type, and date
Screen Mockups

Quick Status bar - displays items that need to be handled currently should allow you to view over different time periods Drop downs will allow you to navigate to the Audit View Side bar will allow you to customize and quickly get to different sections

All charts and graphics should be generated with CSS and HTML

Small customizable boxes will allow you to get other quick references you need Option - Managers will be able to review each user below them that has items to finish Will try to customize view screen based upon level of employee, higher level employees will see just those below them
Technical Specifications

• **System/Audit Types**
  - Cerner/ Access Management, Elevated Access activity, Direct Data Access Activity

• **Data Parser**
  - Consume and input log data into SQL database daily
  - Different parser per system and audit type
  - Identical output
  - C#
Technical Specifications

• Database Schema
Technical Specifications

• **User Interface**
  - Users registered in Active Directory
    - Will handle authentication for system access
  - Views
    - Default view determined by job code
    - Requests to SQL database for content
    - Ability to enter reviews (outside of automated system)

• **Notifications**
  - Automated daily email notifications (by server) of pending reviews

• **Audit Export**
  - Server job to export records into CSV file by system, log type, and date
System Architecture
System Components

• Server Specifications

• Software Platforms/Technologies
  ▪ Browsers: Internet Explorer 6,7,8; Mozilla Firefox 3,4,5; Google Chrome; Safari
  ▪ ASP.NET MVC 3.0 framework with Razor engine, .NET framework 4.0, C#
  ▪ HTML, CSS, JavaScript and jQuerys
Testing

- Will use cleansed data while testing system
- Proof of concept / prototypes
  - Server configuration
  - Email notification
  - Automated testing of browser use
  - Audit export
  - Active Directory
- Debugging
  - Start quality assurance after Alpha presentation
  - Continue for remainder of project timetable
Risks

• Active Directory
  ▪ Roles, accessing upline manager
  ▪ Configured
  ▪ Simulate set of users with hierarchy; test necessary information accesses

• Automated email notifications
  ▪ 1. Server execute script to send hello world email
  ▪ 2. Server execute script to send dynamic template

• MVC Razor Framework
  ▪ Can use framework to make queries and display information
  ▪ More complex examples; Implement SQL database to proceed with MVC Razor