MICHIGAN STATE
UNIVERSITY

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

From Students…
…to Professionals

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
    - Records stored
    - Records requiring review determined
  - User notified via email of their pending reviews

Functional Specifications

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

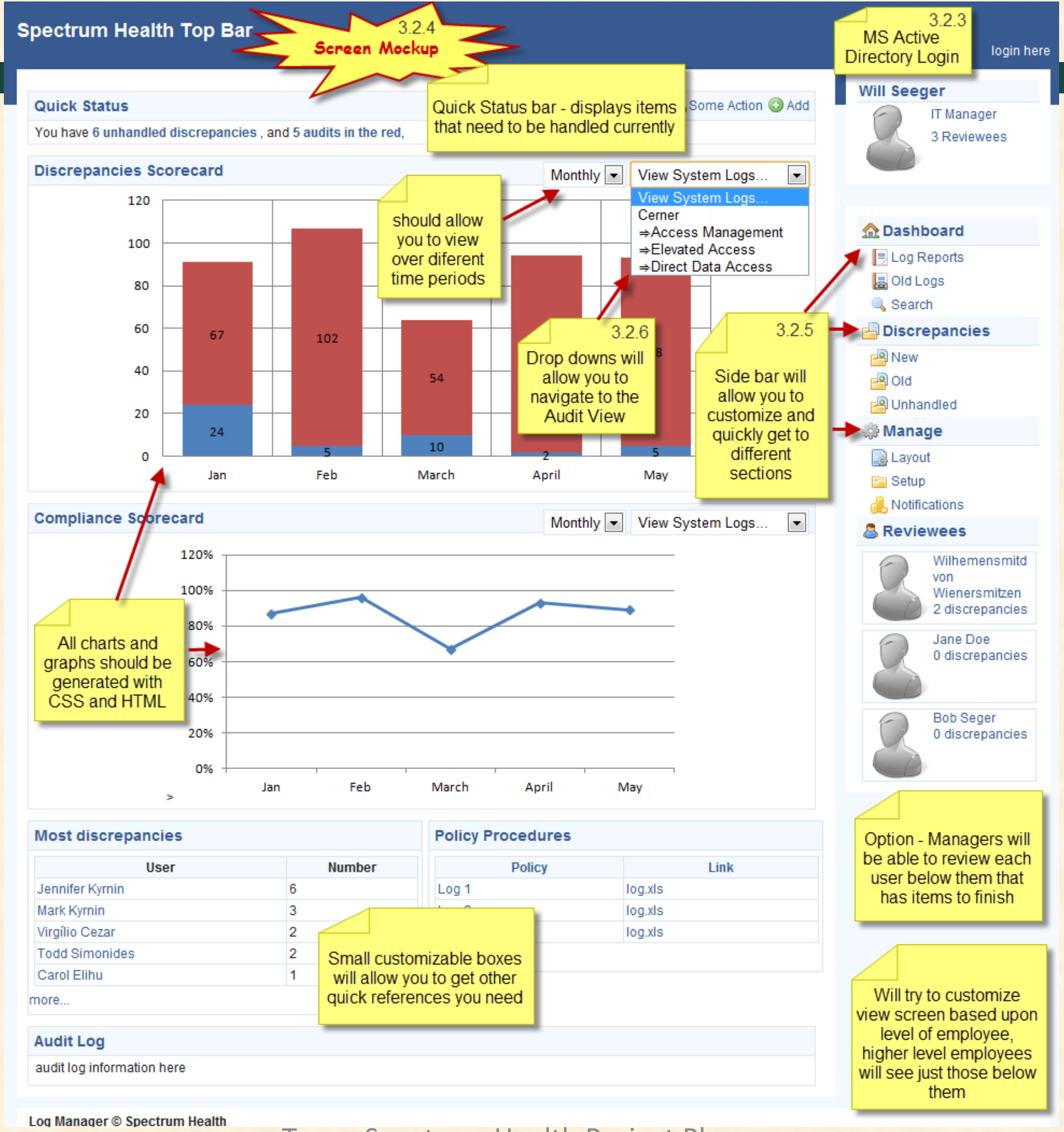
Design Specifications

- 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



Spectrum Health Top Bar

3.2.4
Screen Mockup

3.2.3
MS Active Directory Login

login here

Quick Status

You have **6 unhandled discrepancies** , and **5 audits in the red**,

Quick Status bar - displays items that need to be handled currently

Some Action   Add

Will Seeger
IT Manager
3 Reviewees

Discrepancies Scorecard

Monthly ▾   View System Logs… ▾

View System Logs…
Cerner
⇒Access Management
⇒Elevated Access
⇒Direct Data Access

should allow you to view over diferent time periods

3.2.6
Drop downs will allow you to navigate to the Audit View

3.2.5
Side bar will allow you to customize and quickly get to different sections

Compliance Scorecard

Monthly ▾   View System Logs… ▾

All charts and graphs should be generated with CSS and HTML

Dashboard
Log Reports
Old Logs
Search

Discrepancies
New
Old
Unhandled

Manage
Layout
Setup
Notifications

Reviewees

Wilhemensmitd von Wienersmitzen
2 discrepancies

Jane Doe
0 discrepancies

Bob Seger
0 discrepancies

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

Most discrepancies

User	Number
Jennifer Kyrnin	6
Mark Kyrnin	3
Virgílio Cezar	2
Todd Simonides	2
Carol Elihu	1

more...

Policy Procedures

Policy	Link
Log 1	log.xls
	log.xls
	log.xls

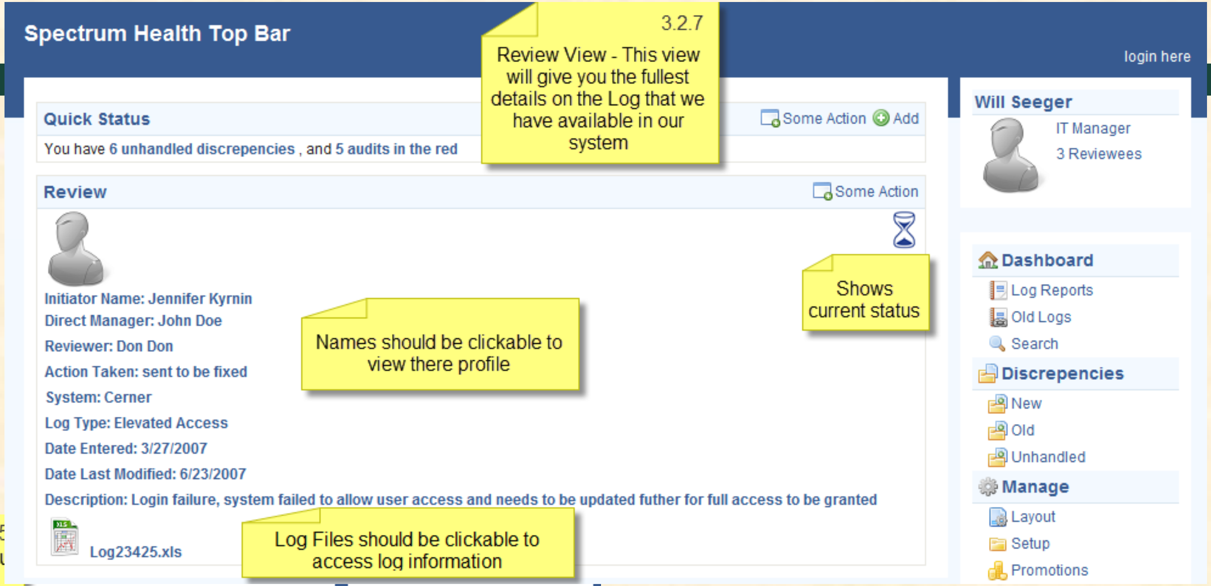
Small customizable boxes will allow you to get other quick references you need

Audit Log

audit log information here

Log Manager © Spectrum Health

Screen Mockups



Spectrum Health Top Bar

login here

3.2.7

Review View - This view will give you the fullest details on the Log that we have available in our system

Quick Status Some Action Add

You have 6 unhandled discrepencies , and 5 audits in the red

Review Some Action

Shows current status

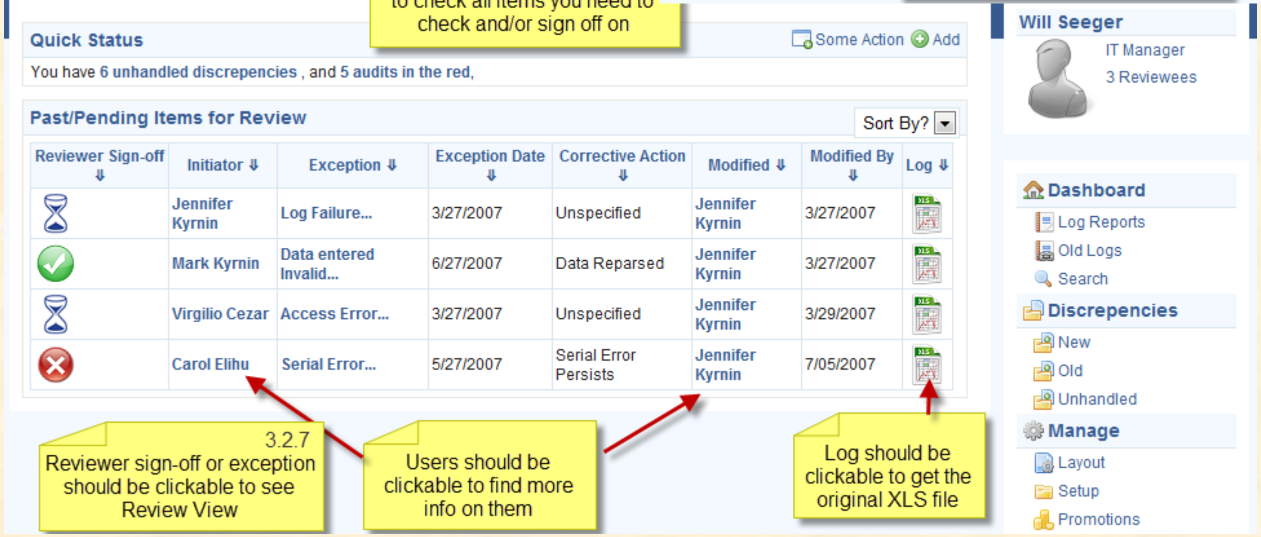
Initiator Name: Jennifer Kyrnin
Direct Manager: John Doe
Reviewer: Don Don
Action Taken: sent to be fixed
System: Cerner
Log Type: Elevated Access
Date Entered: 3/27/2007
Date Last Modified: 6/23/2007
Description: Login failure, system failed to allow user access and needs to be updated futher for full access to be granted

Log23425.xls

Names should be clickable to view there profile

Log Files should be clickable to access log information

Will Seeger
IT Manager
3 Reviewees



Spectrum Health Top Bar

3.2.5

Past/Pending Items - Allows you to check all items you need to check and/or sign off on

Quick Status Some Action Add

You have 6 unhandled discrepencies , and 5 audits in the red,

Past/Pending Items for Review Sort By?

Reviewer Sign-off ⇓	Initiator ⇓	Exception ⇓	Exception Date ⇓	Corrective Action ⇓	Modified ⇓	Modified By ⇓	Log ⇓
⌛	Jennifer Kyrnin	Log Failure...	3/27/2007	Unspecified	Jennifer Kyrnin	3/27/2007	XLS
✓	Mark Kyrnin	Data entered Invalid...	6/27/2007	Data Reparsed	Jennifer Kyrnin	3/27/2007	XLS
⌛	Virgilio Cezar	Access Error...	3/27/2007	Unspecified	Jennifer Kyrnin	3/29/2007	XLS
✗	Carol Elihu	Serial Error...	5/27/2007	Serial Error Persists	Jennifer Kyrnin	7/05/2007	XLS

3.2.7

Reviewer sign-off or exception should be clickable to see Review View

Users should be clickable to find more info on them

Log should be clickable to get the original XLS file

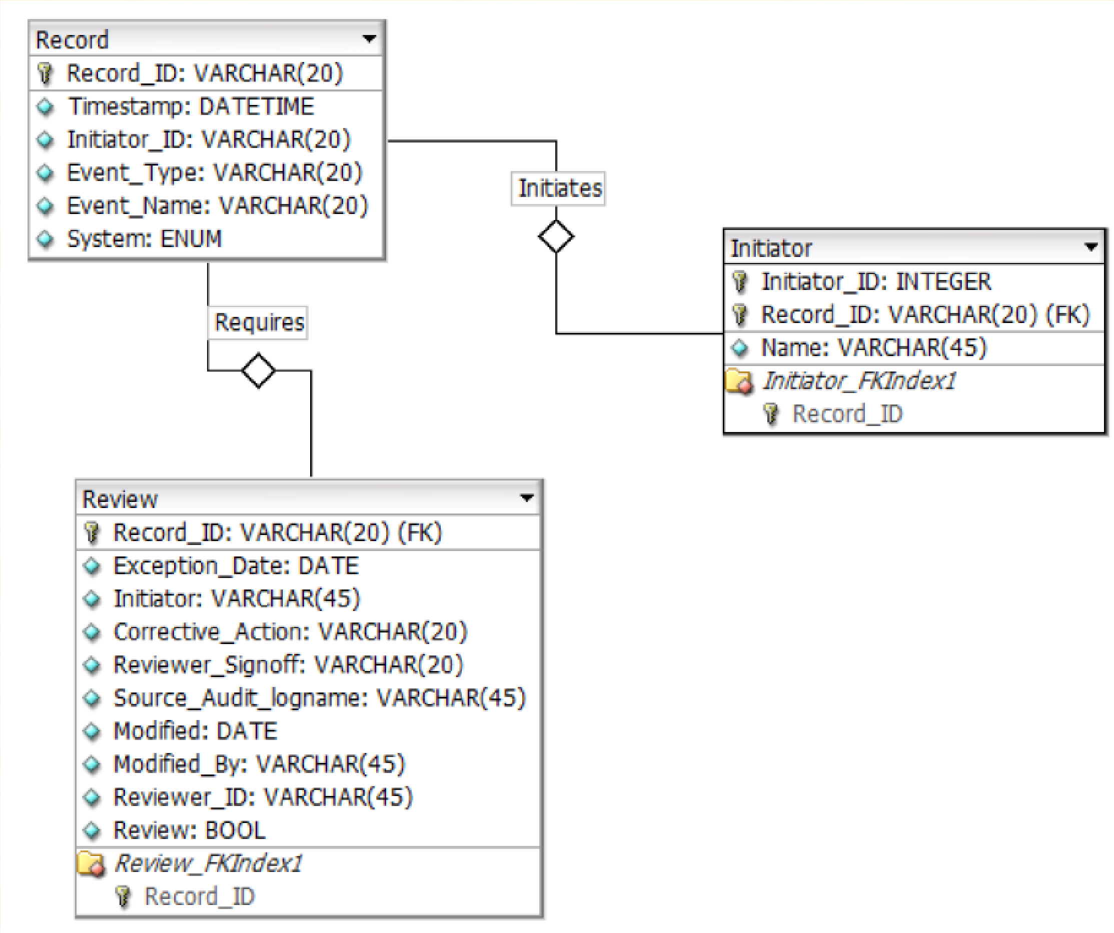
Will Seeger
IT Manager
3 Reviewees

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**



Record
- Record_ID: VARCHAR(20)
- Timestamp: DATETIME
- Initiator_ID: VARCHAR(20)
- Event_Type: VARCHAR(20)
- Event_Name: VARCHAR(20)
- System: ENUM

Initiates

Initiator
- Initiator_ID: INTEGER
- Record_ID: VARCHAR(20) (FK)
- Name: VARCHAR(45)
- *Initiator_FKIndex1*
  - Record_ID

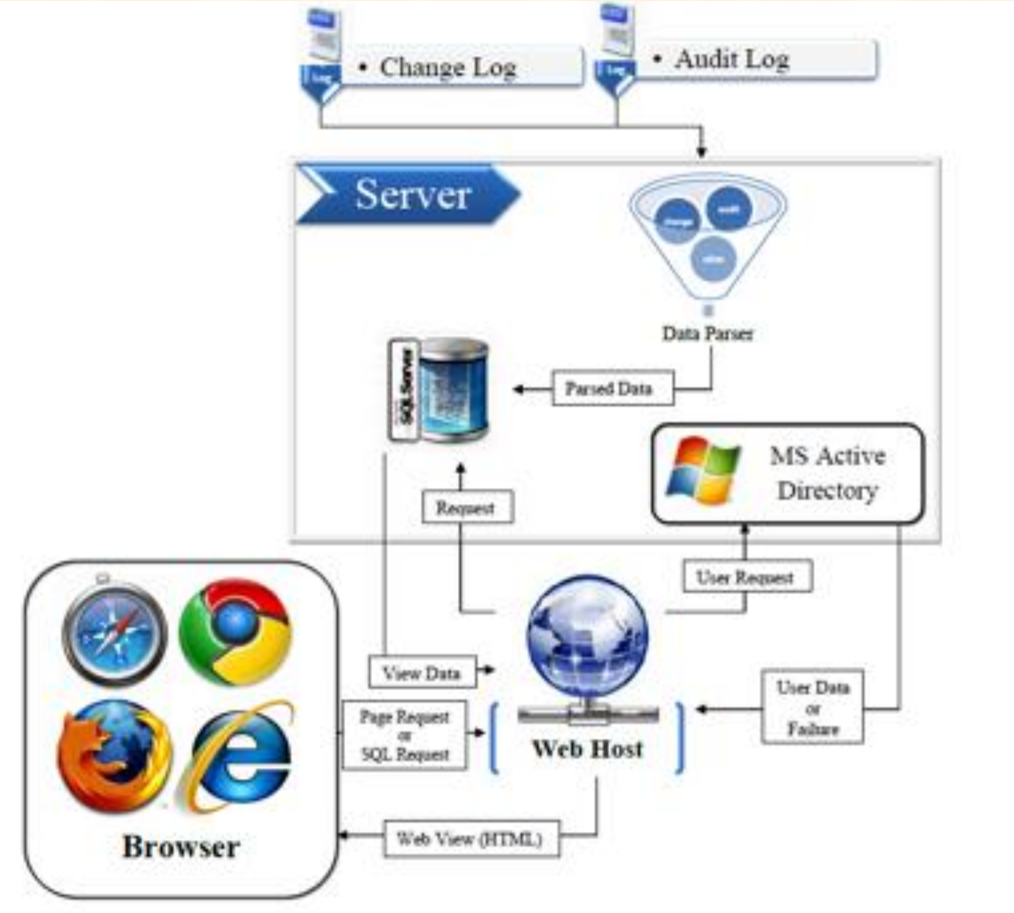
Requires

Review
- Record_ID: VARCHAR(20) (FK)
- Exception_Date: DATE
- Initiator: VARCHAR(45)
- Corrective_Action: VARCHAR(20)
- Reviewer_Signoff: VARCHAR(20)
- Source_Audit_logname: VARCHAR(45)
- Modified: DATE
- Modified_By: VARCHAR(45)
- Reviewer_ID: VARCHAR(45)
- Review: BOOL
- *Review_FKIndex1*
  - Record_ID

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
  - Windows Server 2008, SQL Server 2008, Active Directory
- 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