# Overview

The FEDEBOM System is classified as Secret and the Segregation of Duties (SOD) Standard found in the Information Security Policy (ISP) applies.

This system has a complex Client Server landscape. The complexity takes the form of a large Java based client that utilizes Web Services to make calls to servers while maintaining local synchronized JSON files. This system leverages the Ford Infrastructure Team and has several home-grown applications that have become the one source of truth. These applications include QlikView, Alteryx, and SPLUNK. Several features depend on batch jobs run on a scheduler.

There are multiple environments to support production, Quality Assurance(QA), Training, and Development. The source code is in a CMDB called AccuRev where code promotions take place and multiple Eclipse Add-Ins are used to manage builds including Gradle, Jenkins, and GitHub.

The SOD will be applied to AccuRev, the DEV environment, the Scheduler, the Servers, and all Generic ID’s used for different development functions.

# Problem

The SOD that exists for FEDEBOM Development Team has not been aligned to the ISP SOD.

# Scope

Leverage the GCH Segregation of Duties changing all GCH references to FEDEBOM then pasting in the list of PDO developers that have access to DEV. Finally, identifying those CDSID’s with conflicts and displaying their roles. This report will be used as an action item list for select owners. A potentially in scope item will be a proposal of an automated system run on a schedule a pre-determined frequency that sends out notices to select owners as conflicts appear.

# Out of Scope

## Business Team within PDO

# Goals

## Identify developers with edit access to DEV and edit access to PROD by Aug 31

## Transfer enough knowledge to get internal team on the same page by Aug 31

## Identify conflicts with DBA and infrastructure users by end of Sep

## Provide action items for teams by end of Sep

## Create OICs as needed by end of Nov

# Objectives

## To be prepare for an audit

## To complete all OIC’s as needed

# Constraints

## This system is rated as secret

# Assumptions

## All supporting teams will be available as needed

## The template from GCH will be used

## LL6 CDSID’s will be excluded from all conflicts

## Select CDSID’s will be excluded from all conflicts

## The entire GENERIC\_3008.log covering the SOD time period will be available

### This log may be broken up into smaller logs

## The Secret rating does, however, enforce that only restricted temporary access can be provided to allow developers to be setup with Production access

### Production viewer access is temporarily allowed for developers so they can troubleshoot procedures.

### Temporary access is defined as a day or two.

# Stories

## This plan and risks

## Prototype of automated tool

## Potentially create a Monitoring process

### The source of truth will be validated on each execution

## Potentially Development and proposal of measurable metrics

## Identification of conflicts, categories, owner, and lead

### Ensure only select developers with edit access to the development environment will have the capability of requesting a temporary generic ID to view Production data.

### Ensure developers with AccuRev LEAD role, which is used to promote code, do not have edit access to the development environment.

### Ensure developers with Scheduler update access to the development environment cannot access the production Scheduler and vice versa.

### Ensure development DBA’s have access only to the databases in then development environment.

### Ensure production DBA’s have access only to the databases in the production environment.

### Ensure Team’s supporting the development environment network have access to only the development environment.

### Ensure Team’s supporting the production environment network have access to only the production environment.

### Ensure Team’s updating generic ID passwords for the development environment have access to only the development environment

### Ensure Team’s updating generic ID passwords for the production environment have access to only the production environment

## Potentially a List of internal procedures needing improvement

## Setup meeting with Stakeholders

## Setup meeting with Business

## Creation of OIC’s if needed

## Potentially Testing of monitoring process

## Potentially Monitoring of corrective actions

## Potentially Review of metrics at pre-determined frequencies

# Milestones

## Review and approval of this plan and risks

## Potentially Review of the Monitoring process

## Potentially Review and approval of measurable metrics

## Discussion with key conflict owner

## Discussion with key conflict owner and leader

## Review of corrective action items

## Potentially Review of internal procedures needing improvement

## Sign-off from Stakeholders

## Sign-off from Business

## Review of OIC’s if needed

## Potentially Starting of monitoring process

## Execution of corrective action monitoring

## Potentially Review of metrics at pre-determined frequencies

# Risks

## If source of truth data that comes from other groups within PDO is not accompanied by the scripts or query used to obtain the data then the risk is high that future process executions will not be consistent.

## If developers, when they are helping end users, adjust either local JSON or cache files, then there is a risk that they can indirectly update production data under the end users CDSID.

## If resources on other PDO Teams do not create Stories to allow Rally dependencies, then work can potentially be stopped without Rally be capable of stating why. To mitigate, each story will utilize Risks to cover this.