Analytics Suite

System Configuration Module

Why OCA did this project

System configuration involves assigning who can access the financial system and what they can do once they gain access. Roles, permissions and workflow management are all a part of configuration management. Appropriate configuration management can control access to sensitive data and limit the ability to make unauthorized transactions and system changes. This analytics module provides a broad system overview making monitoring easier.

How OCA did this project

System Configuration is the 13th module in an audit analytics suite. Similar to previous modules, the project team began with a discovery phase, which included researching common system configuration risks and controls, exploring and mapping the City's Munis environment, and interviewing staff to document processes and priorities for analysis. The team used this information to develop the data analytics in this module.

Project Deliverables

Nineteen data analytics seamlessly integrate with Munis and run continuously to monitor and pinpoint risks. These data analytics will be available to financial system administrators to monitor risk. Auditors will use this data to focus projects on areas where risk is highest.

Example Analytics

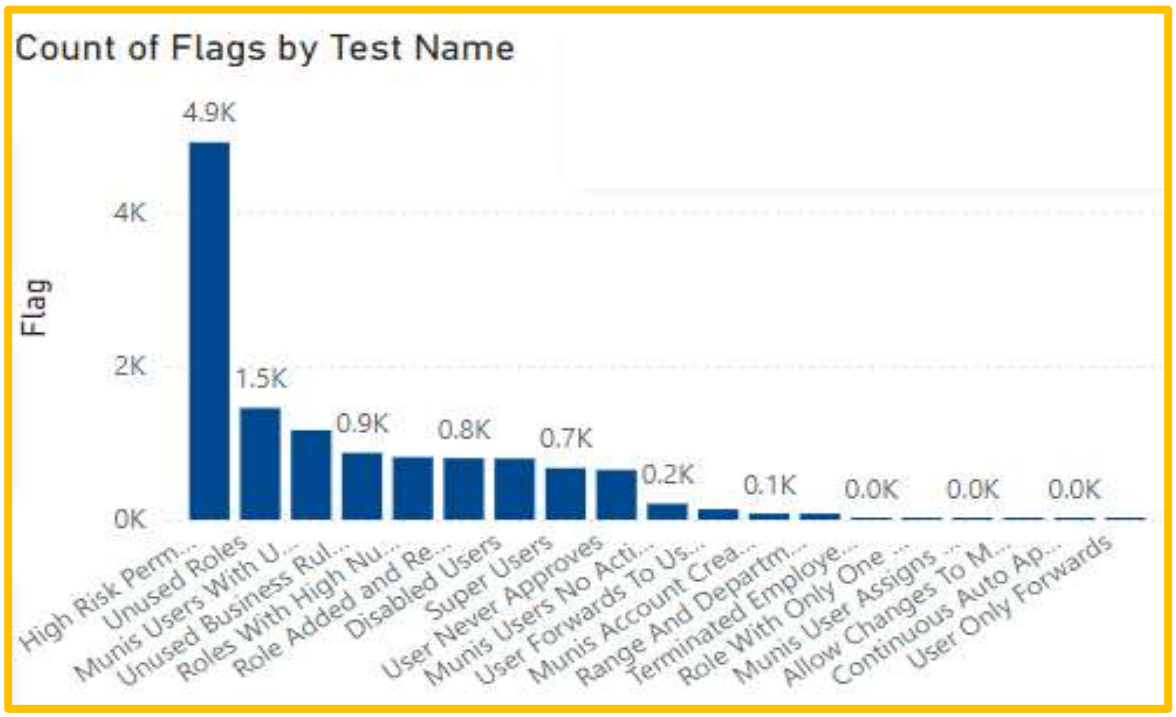
The table below shows 10 examples of the 13 System Configuration analytics. Data analytics track transactions in Munis as they move through workflow. Each analytic tests a transaction. If the transaction meets the criteria, the analytic will flag the transaction.

Analytic	**Description**
Unused roles	Flags if a role exists but has no users assigned.
Terminated employee-Enabled account	Flags if a user is no longer an employee but access is still enabled.
Munis Users-No activity	Flags user accounts with no records in the activity log.
Munis Users-Unused roles	Flags roles assigned to a user that have no access activity with the role.
Disabled Users	Flags a user if the account status is disabled.
Super Users	Flags a user if they are assigned a super user role.
Munis account created then removed	Flags if an account was created and then removed in less than 8 days.
Munis user assigns own roles	Flags if the user assigning a role matches the user approving the role.
High risk permissions–Many users	Flags a high-risk permission if the number of users assigned is one standard deviation above the average of all other permissions.
User only forwards	Flags a user if they only forward in a workflow

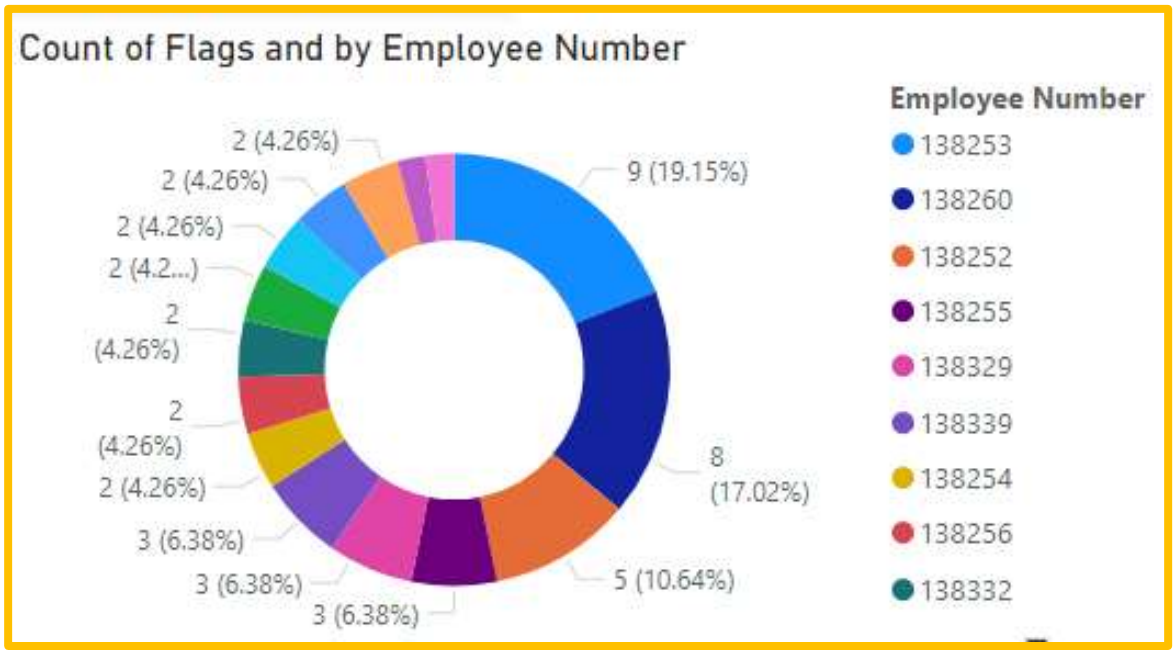
Dashboard

The images below illustrate the System Configuration dashboard.

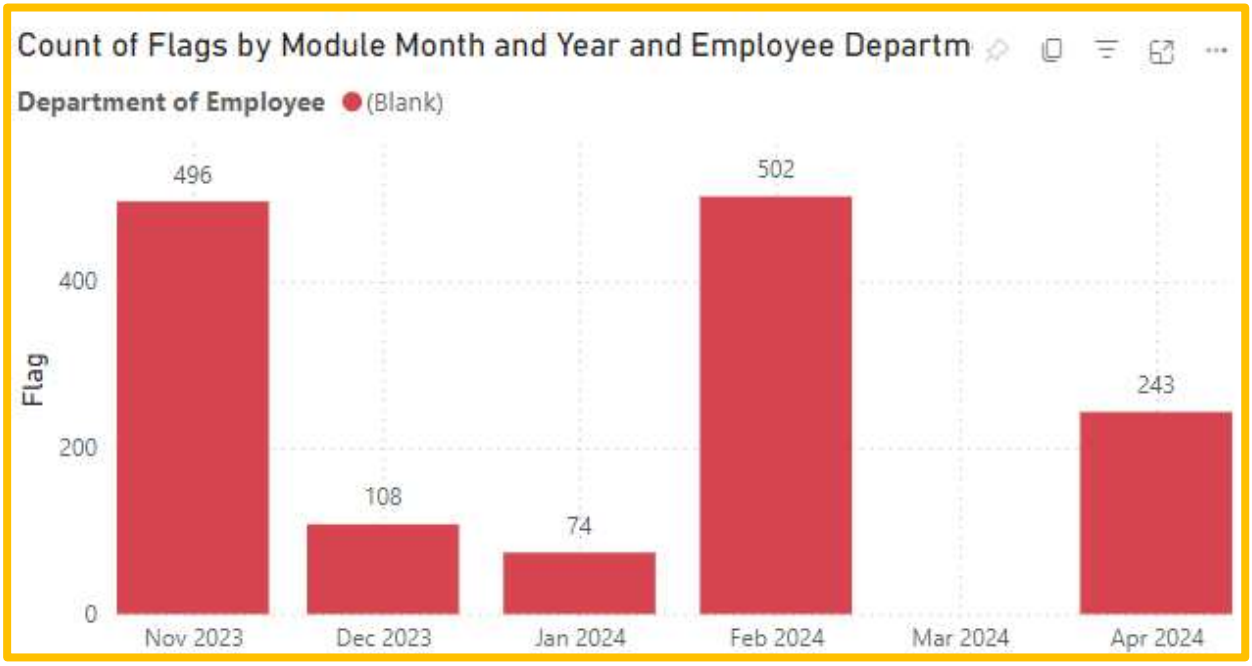
Count of Flags by Test Name
This visual allows users to easily determine which data analytics have accumulated the most risk flags.



Count of Flags and by Employee Number
This visual allows users to easily determine which financial system users have accumulated the most risk flags.



Count of Flags by Module Month and Year and Employee Department
This visual allows users to easily monitor the change in system configuration flags over time.



The data analytics dashboard allows users to drill down to details to learn more information about risk flags.

Analytics Suite

As of June 2024

All modules of the analytics suite were complete in June 2024.