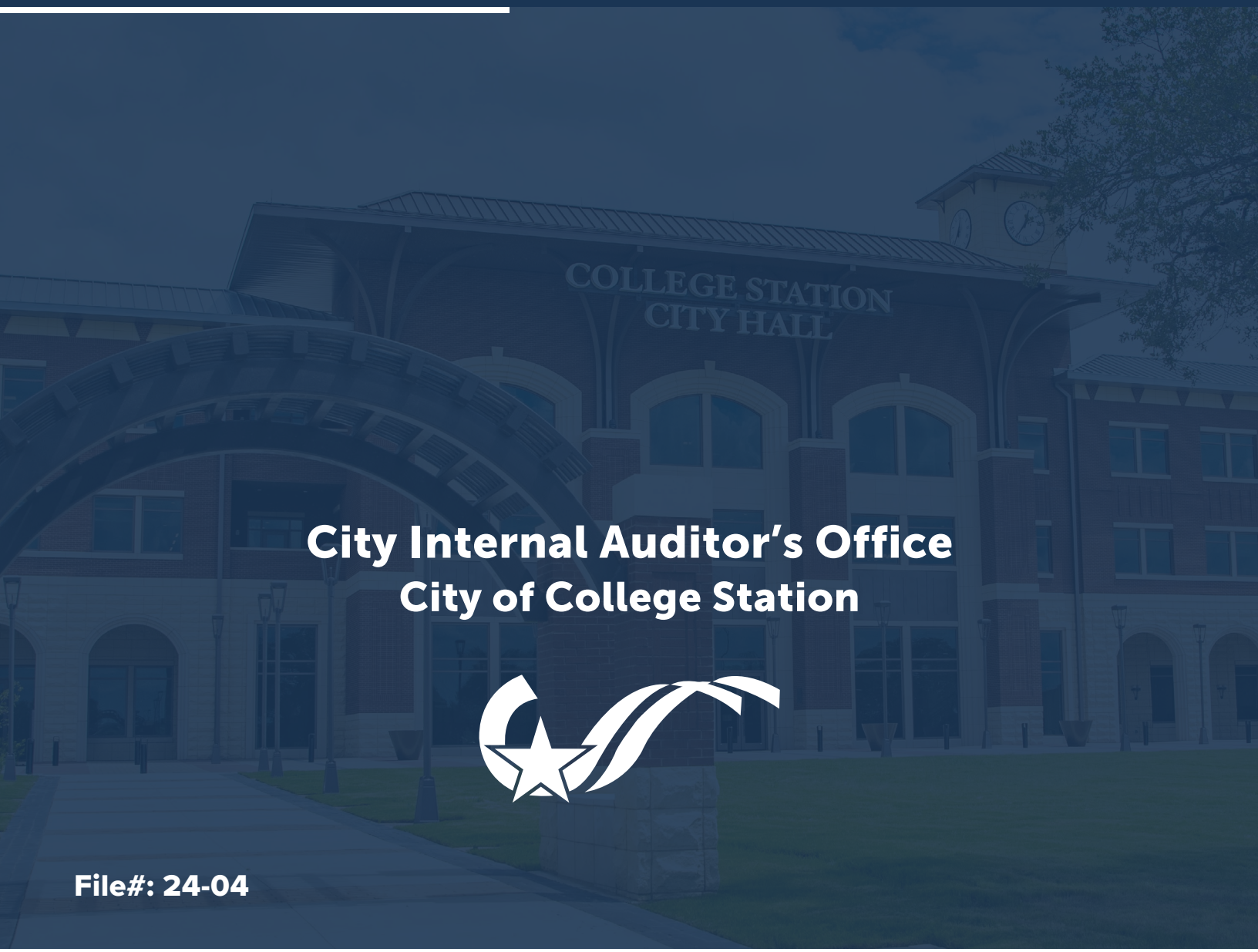
AUDIT OF
Segregation of Duties
within ERP Role-Based Access

September 2024



City Internal Auditor's Office
City of College Station

File#: 24-04

Intentionally Left Blank

Executive Summary

Effective Segregation of Duties (SoD), can ensure that no single individual can perform conflicting tasks, which is crucial for maintaining a robust system of internal controls that mitigates the risk of errors or fraud. One method of implementing SoD is through system controls, which can be an efficient method to enforce user responsibilities since it utilizes automated processes to manage access and duties. Despite the importance of functioning SoD, there has not been an audit of user privileges since the implementation of the City's Enterprise Resource Planning (ERP) system, Tyler Munis. Based on the direction given by the Audit Committee, an audit of SoD within ERP Role-Based Access was included in the Fiscal Year 2024 Audit Plan.

What We Found

We reviewed the City's role-based access policies, procedures, and practices to determine the effectiveness of the controls in place for ensuring system SoD that assigns access based on an employee's role within the City. After careful analysis, we identified areas for improvement in the City's role-based access control:

Employees have access to privileges that meet the criteria of an ISACA conflicting task.

Standards set by the Information Systems Audit and Control Association (ISACA) highlight functions that, when combined, pose a risk to an organization and possibly allow users to forgo the typical SoD for a task. In total, 128 users and 44 roles have at least one ISACA conflict.

Privilege creep should be addressed by enforcing the principle of least privilege.

Over time, employees have accumulated access rights exceeding their current job responsibilities, increasing the risk of unauthorized access. This privilege creep contradicts the principle of least privilege, which dictates that users should only be granted the minimum level of access necessary to perform their job functions. For example, we found that a Compensation Analyst in Human Resources had access to the Budget Manager role, which is typically reserved for Budget staff.

The process for removing user access could benefit from efficiency improvements.

Deactivating user access for terminated employees relies on department notifications, which often results in delays. The average time to deactivate access was 32 days from the termination date. However, Information Technology (IT) can typically deactivate an account within one business day if they are informed of the termination. Implementing automated notifications from Human Resources to IT could reduce delays and enhance security.

Naming conventions need revision to alleviate audit log ambiguity.

The current naming conventions used in the Active Directory allow the recycling of user IDs after 12 weeks, creating ambiguity in the audit logs. This practice could complicate efforts to trace user activities and undermine the accountability and transparency of the system's audit log.

System configurations allow for self-approval in some business processes.

The configurations for the four levels of system controls allow certain Finance users to self-approve changes to vendor records and general ledger entries. This SoD condition increases fraud risk as it enables users to perform actions without independent oversight, increasing the potential for misuse to go unnoticed.

Superuser permissions should be restricted to positions that require them.

There are currently more superusers than necessary, which goes against the principle of least privilege. For instance, only two employees outside of IT should have superuser access to the approval workflow. However, a total of 14 users had access to maintain pending actions in the workflow. One item that presents a concerning level of privilege is the Payroll Superuser permission, which allows users to perform both personnel and payroll functions, thereby creating opportunities for fraudulent activities, such as the creation of ghost employees. However, removing this permission without impacting the current payroll process is challenging due to system limitations.

Recommendations

To address the audit findings, there are improvements the City could make to better manage the system controls in the City's ERP system. They are encompassed in the following audit recommendations:

1 Enforce Least Privilege

To enhance the effectiveness of the City's system controls, management should enforce the least privilege principle by conducting a review of current user privileges, disabling unnecessary access at the permission, menu, data, and/or approval level, granting inquiry only access, and/or reassigning privileges to other roles. Additionally, temporary roles can be created to award privileges for nonroutine and emergency situations.

2 Automate Terminated User Notifications

The key control in notifying IT of a user's termination is a department submitting an IT support ticket requesting the deactivation of the ERP account. However, departments are not always timely in notifying IT, allowing terminated users to maintain access. IT should coordinate with Human Resources a trigger point that signifies an employee's termination. Once this trigger point has been identified, IT should develop reporting controls to automatically notify the business systems team of an employee's termination.

3 Reassess Approval Processes for Users with Permission Access

Management should reassess permission access for workflow processes where self-approvals can occur. Due to the current system configurations, some employees can enter and self-approve vendor modifications, including banking changes and General Ledger entries. To mitigate this risk, management could ensure that anyone who is an approver for vendors does not have access to edit or enter any changes. Additionally, they could change workflow steps that are high risk of self-approval to require approvals from multiple users in a step. Another option is to add a step with more refined criteria, directing specific vendor changes to an additional approval step. It is important to note that while these changes might help enhance segregation of duties, it may come at the cost of staff efficiency.

4 Investigate Changes to Naming Conventions

Currently, the naming conventions utilized by the City allow for user IDs to be recycled, which creates ambiguity in the audit log. Best practices indicate that organizations must ensure the unique identification of users and maintain accurate audit records to support accountability. Therefore, IT should investigate system or process changes that would grant each user a unique identifier in the ERP system, even after their employment with the City has ended.

5 Develop and Document Policies and Procedures for Superuser Privileges

The City should establish policies and procedures for role-based access tailored to organizational needs and job functionality. These policies should define superuser responsibilities and set conditions for granting and revoking superuser privileges, including specifying which positions are eligible for such access. Regular reviews of access rights and continuous monitoring of superuser activities should be conducted to ensure compliance and mitigate security risks. Moreover, options should be investigated to prevent instances of end users being setup as superusers.

6 Respond to Privilege Access Reviews

The Audit Office plans to conduct periodic privilege audits. In response to the results of these audits, management should take the appropriate corrective actions to ensure that the risks of fraud, misuse, or abuse are reduced. This includes verifying that superusers require their high-risk access, ensuring all users have the appropriate level of access for their position, and confirming that terminated employees do not retain active access to the system.

Table of Contents

Introduction

The Office of the City Internal Auditor conducted this performance audit of the City of College Station's (the City) Role-Based Access Control (RBAC) framework pursuant to Article III Section 30 of the College Station City Charter, which outlines the City Internal Auditor's primary duties.[1]

A performance audit is an objective, systematic examination of evidence to assess independently the performance of an organization, program, activity, or function. The purpose of a performance audit is to provide information to improve public accountability and facilitate decision-making[2]. Performance audits encompass a wide variety of objectives, including those related to assessing program effectiveness and results; economy and efficiency; internal control; compliance with legal or other requirements; and objectives related to providing prospective analyses, guidance, or summary information. A performance audit of the City's RBAC Framework was included in the Fiscal Year 2024 Audit Plan based on the direction given by the Audit Committee. We investigated whether instances of fraud, misuse, or abuse were occurring in the City's system controls for the RBAC framework.

Definitions

Fraud

Intentional acts that involve the use of deception, misrepresentation, or other unethical means to obtain a financial or personal gain or to cause a loss to an organization.

Misuse

The inappropriate use of an organization's systems, either accidentally due to lack of knowledge or intentionally by disregarding established protocols, leading to authorized system activity.

Abuse

Behavior that is inconsistent with acceptable business and ethical standards, leading to the improper or excessive use of an organization's resources.

[1] City of College Station, TX, "Code of Ordinances," § 30 (2017), 12.
[2] U. S. Government Accountability Office, "Government Auditing Standards 2018 Revision (GAO-18-568G)" (2018), 10–17.

Importance of Segregations of Duties

Segregation of duties (SoD) is a fundamental principle in maintaining an effective control environment within any organization. Its primary aim is to safeguard resources entrusted to the government by ensuring no single individual controls all aspects of any critical business process. This approach minimizes opportunities for undetected errors or misuse. In instances where a business operation has limited staff, achieving proper SoD can be challenging, as employees often have to manage multiple roles. However, compensating controls, such as additional monitoring and oversight by independent reviewers or external parties, can mitigate the risks associated with overlapping duties. Effective SoD involves the strategic distribution of responsibilities, such as custody, recording, reconciliation, and authorization, among different individuals. For example, an employee responsible for purchasing should not also be responsible for receiving goods. One method to implementing SoD is through system controls, such as the ones utilized in the RBAC framework, or process controls that can restrict an employee's access to performing certain functions.

SoD ensures no single individual controls all aspects of any critical business process.

Implementing SoD through system and process controls helps establish an effective control environment. System controls, automated and embedded within software applications, offer consistency, efficiency, and timely information. They are less prone to circumvention compared to manual controls and enforce SoD by electronically limiting access and segregating duties. However, their effectiveness depends on the configurations of a system, which can limit their scope and introduce risks such as system inaccuracies and unauthorized access.

Conversely, process controls rely on human intervention, allowing for professional judgment and skepticism. This adds a nuanced evaluation that automated systems might lack. Despite this, manual controls are inherently less consistent, more susceptible to human error, and easier to override, making them vulnerable to collusion and fraud. An optimal control environment combines both system and process controls, leveraging automated processes for consistency and efficiency while applying manual controls where human judgment is needed.

An ideal environment would use a combination of manual controls and automated processes.

Segregation of Duties in Practice: Control Activities

Role Based Access Control Framework Background

A RBAC framework involves several complex components, each working together to manage user access. Understanding these components helps in effectively auditing user privileges within an ERP system. **Table 1** provides definitions for key terms that will be referenced in this audit.

Table 1: Roles and Permissions Terminology

System Control	A control embedded within software applications designed to enforce rules and restrictions on user access and actions.
Process Control	A control relying on human intervention and judgment to oversee and manage business processes, ensuring that activities are conducted according to policies and procedures, often complementing system controls.
Detective Control	A type of control that is reactive and that detects undesirable events that have occurred.
Privilege	The system rights granted to a user, allowing them to perform particular actions within an ERP system, such as accessing data, executing transactions, or generating reports.
Least Privilege	A security principle dictating that users should only be granted the minimum level of access necessary to perform their job functions, thereby reducing the risk of unauthorized access and potential security breaches.
Role Based Access Control (RBAC)	An access control mechanism where privilege is assigned to predefined roles rather than individual users.
Role	Privileges are granted to users through an assigned role(s). Roles may contain multiple levels of access.
Enterprise Resource Planning (ERP)	Enterprise Resource Planning (ERP) systems are software platforms that organizations employ to effectively manage various day-to-day business activities, including accounting and procurement. These systems integrate and connect a myriad of business processes, facilitating the seamless flow of data between them. The City utilizes Tyler Munis (the Munis system) for our ERP system.
Active Directory	A directory service developed by Microsoft for Windows domain networks. ERP access cannot be granted without Active Directory access.
Business Workflow	Automates the flow of approvals, notifications, and tasks within an organization using tailored business rules. Administrators can monitor workflows in real-time and track progress.
Permission Access	A specific authorization that allows a user to perform certain actions within an ERP system, such as updating/adding/deleting/data, printing AP checks, or running payroll.
Menu Access	The level of control that dictates which applications a user can access within an ERP system.
Data Access	Restricts which data a user can view and interact with within an ERP system.
Approval Access	A control mechanism that determines who can approve transactions and activities within an ERP system and is linked to predefined business workflows.
ISACA	The Information Systems Audit and Control Association (ISACA) is a professional organization that serves to provide guidance and standards for the governance, control, and security of information systems.
Conflict	A pair of permissions that provide an individual user control over two or more parts of a process and/or function within a system, creating a potential SoD issue as defined by ISACA.
Internal Conflict	A conflict caused by the internal configurations of a role, where the permissions assigned to a single role create a potential SoD issue.
External Conflict	A conflict that arises when a role is matched with another role, and the combination of their permissions creates a potential SoD issue.
User	An individual who has been granted access to an ERP system, with specific roles and permissions assigned to perform their job functions.
Disabled User	A user whose access to the ERP system has been suspended, preventing them from logging in and performing any actions within the system.
Terminated User	A user whose employment status has been terminated, but still has ERP system access.

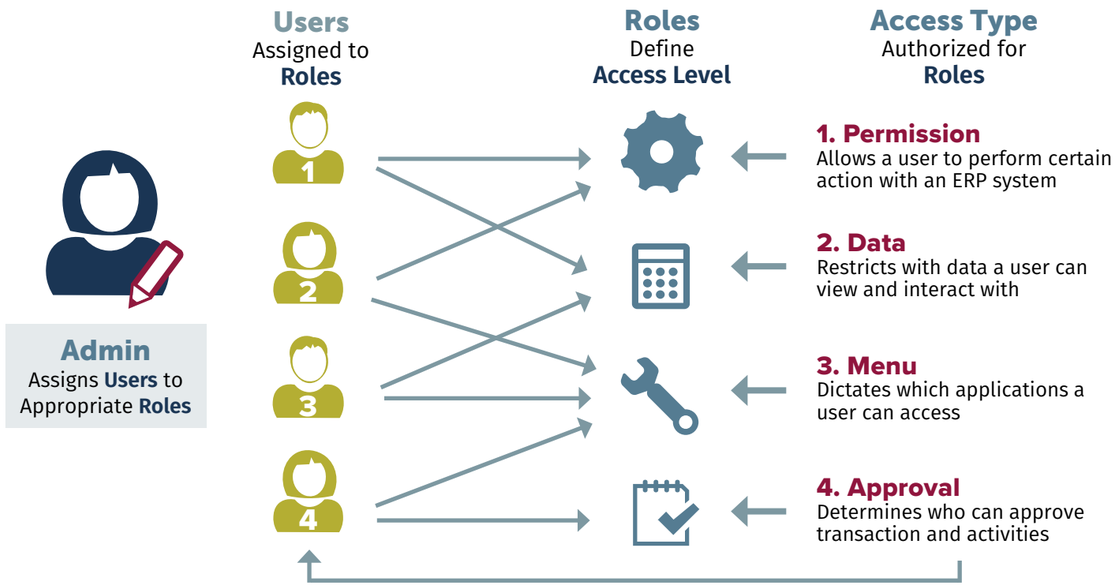
The City utilizes Tyler Munis for its ERP system, which was implemented in 2015. During the initial setup, roles were designed with input from employees to determine the privileges necessary for maintaining operations. This collaborative approach aimed to ensure access controls aligned with the functional needs of various departments. However, since the implementation, there have not been subsequent privilege audits to assess if the initially granted privileges align with current business processes. This has led to **privilege creep**[3], where employees accumulate access rights over time that are no longer relevant to their job functions, thereby increasing the risk of unauthorized access and potential SoD violations. Auditing this area is challenging for several reasons. Firstly, the dynamic nature of access means that what may be appropriate at one moment can quickly become outdated, making it difficult to assess privileges accurately. Secondly, other access controls may determine if employees can effectively use their privileges, such as permission, menu, data, and approval access.

RBAC is an adaptable access control system that revolves around roles and the privileges linked to them (see **Figure 1**). By utilizing elements such as role-access levels, user-role assignments, and multiple role relationships, RBAC can streamline the management of user access within an organization.

The process begins with an administrator who can assign users to appropriate roles based on their job responsibilities. Each role is configured to grant a certain level of access, which includes permissions, data, menu, and approval types.

In an ERP system, multiple levels of system access controls ensure SoD and mitigate risks of unauthorized access and misuse. Menu access dictates which applications a user can access, preventing interaction with critical processes if access is restricted. Permission access further restricts user actions within an application, though not all applications allow fine-grained control. Our audit focused on evaluating the permission access for users, and reviewed other levels of control when necessary. Data access limits what data a user can view and interact with, ensuring relevance to their roles. Approval access controls determine who can approve system transactions, tied to predefined workflows, and resembles process control due to its susceptibility to human error. In the business workflow, approval access is tied manually to users for financial processes, while in human resource management processes, the approval access is tied to roles.

Figure 1: Role-Based Access Control



[3] ISACA. (2011). Data Integrity—Information Security's Poor Relation. ISACA Journal, Volume 5.

In **Figure 1** on the previous page, User 1, representing a Limited User, demonstrates how a role's configuration can function as a control to prevent misuse. For example, this user has permission and data access but lacks menu access, effectively preventing them from accessing the application. This scenario illustrates how different access types can work together to maintain proper SoD, ensuring that if one control level fails, another can still enforce SoD. User 2, the End User, has the ability to prepare transactions within Munis, but their changes are subject to approval for higher-risk activities. This user lacks approval access, which helps maintain the separation between the roles of preparer and approver, further supporting SoD.

User 3, an Inquiry User, has inquiry-only access allowing them to view data across the entire system without the ability to alter it. This confines their role to observation rather than action, thanks to having only menu and data access. Finally, User 4, the Approver, is responsible for approving transactions but is restricted from making any system transactions they could approve by not having permission access. This setup helps in maintaining SoD, as it prevents self-approvals within the system. While the examples listed elaborate on how user-role-access relationships can help ensure proper SoD, the highest risk occurs when a user has privileges across all access types.

Audit Objective

The purpose of the audit is to evaluate the effectiveness of the system controls in preventing unauthorized access within the RBAC framework. The City's controls are intended to provide reasonable assurance but cannot guarantee that fraud and errors will not occur. We assessed the effectiveness of system controls within the RBAC framework by answering the following:

- **How many users and roles have conflicting permissions that could possibly lead to instances of fraud, misuse, or abuse?**
- **What are the root causes of SoD conflicts in the RBAC framework?**
- **Are there system control weaknesses that allow the opportunity for fraud, misuse, and abuse?**

In total, there are 913 user accounts set up in Tyler Munis, of which 470 are active and 443 are deactivated. These users can be assigned any combination of the 258 roles that are actively being used. When setting up a new ERP user account, the IT business systems team assigns roles to the new user based on the roles held by their predecessor or someone in a similar position. This situation poses a risk, as it not only allows current users to possibly exploit outdated privileges for fraud, misuse, or abuse but also exposes future users to similar risks.

If a user requires access to a new role for new responsibilities, they will submit a ticket to the business systems team requesting access. While the business systems team adds/updates/removes roles given a request, they do not authorize access to those roles. Instead, they defer to employees designated with sufficient approval authority. For example, the role of J_AUDITOR[4], which is the job role of a staff auditor and has inquiry access to the Munis system, would require approval from the City Auditor. The impacts of how user-role assignments have been done in the past will be evaluated in the Findings and Analysis section of this report.

[4] Munis role naming conventions use prefixes to denote the role type (e.g., data, functional, job), followed by the associated department (e.g., Finance, Human Resources, IT) and the specific function (e.g., system audit, budget management, accounts payable). For clarity in this report, we will refer to these roles in simplified terms (e.g., the J_AUDITOR role becomes the Auditor role).

Scope

The City Internal Auditor's Office conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the audit team plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit focuses on the policies and procedures used in the governance, management, control, and oversight of SoD within the roles-based access control framework. Audit fieldwork was conducted from February 2024 through July 2024. The audit scope encompassed the roles-based access control framework as of July 31, 2024. Since roles-based access is a dynamic process, the scope of our review covered the privileges and access granted to users from February 2024 through July 2024.

Methodology

The Internal Audit team has reviewed the City's ERP user access and permissions for fraud, misuse, and abuse risks. With the assistance of the City IT Department personnel, we used software from a vendor, ThirdLine (thirdline.io), to extract and evaluate all roles and permissions for each user for conflicts related to the segregation of duties, practices, and the principle of least privilege. While the ThirdLine methodology focused on the permission access level of control, we reviewed the menu, data, and approval access in instances where a user was flagged as having the possible opportunity to violate the SoD principle.

Using the "Implementing Segregation of Duties: A Practical Experience Based on Best Practices,"[5] ThirdLine software evaluates every ERP user's permissions within and across each role assigned to that user. It identifies conflicts when a pair of permissions provide an employee too much control within the ERP system when considering the principle of segregation of duties, as outlined by ISACA, the leading association focused on IT governance matters. Using the number of conflicts identified, ThirdLine identifies the potential risks in the ERP system by calculating the most conflicting roles and permissions for individuals and within departments. In addition, ThirdLine also provides the ability to review whether terminated employees still have ERP access and which users have permissions that are considered high-risk because of the system impact they could have.

In addition to using ThirdLine, evidence of current practices through data requests, interviews, and observations was gathered. We presented our findings of ThirdLine conflicts to Finance, Human Resources, and IT staff to gather feedback on whether the privileges awarded to particular users and roles accurately reflected job requirements. In response to these discussions, Finance and IT have developed a corrective action plan to adjust flagged users' current roles (see **Appendix B**).

Finally, our office validated the ThirdLine results to ensure accuracy and interviewed IT personnel on the process for creating, modifying, and assigning a role and creating and disabling a user. In instances where there appeared to be a control weakness, or permission granted significant privileges, the audit team, with the support of IT, tested the permission in the Munis testing environment to document the risk that the control weakness presented.

Noteworthy Accomplishment

We would like to acknowledge the IT business systems team for managing the City's ERP system's role-based access control framework, Tyler Munis. IT's work in modifying roles, overseeing ERP users' system onboarding and offboarding processes, and maintaining user access has been crucial in ensuring system security. Acknowledgment also goes to the Finance Department for ensuring user privileges reflect current business processes and their role in designing the SoD for workflow approvals. The collaborative efforts of these teams have significantly enhanced the effectiveness and security of the City's ERP system controls.

[5] Ferroni, Stefano. "Implementing Segregation of Duties: A Practical Experience Based on Best Practices." ISACA Journal, Volume 3, May 19, 2016.

Findings and Analysis

Privilege audits, which assess whether access rights are appropriately assigned and maintained, are rarely conducted in our city and other municipalities. This infrequency can lead to privilege creep, unawareness of the opportunities granted to many users by the system, and instances where terminated users still have access. We analyzed the effectiveness of the current access controls in preventing unauthorized access and ensuring compliance with SoD principles. Our findings identify areas where privilege creep has occurred, highlight specific instances of conflicting permissions, and evaluate the impact of these conflicts on the system's integrity. Additionally, procedures for managing user access, weaknesses in system controls, and the alignment of user privileges with current job responsibilities, were examined.

Figure 2: SoD System Conflict Example

Task: AP Payment

Permission	Role
Generate EFT File[6]	Finance Operations Assistant
Print AP Checks	Finance Operations Assistant; Accounts Receivable

Task: Vendor Master Maintenance

Permission	Role
View/Maintain vendor banking information	Finance Operations Assistant

For this audit, we tested for system SoD conflicts at the permission level, as illustrated in **Figure 2**. These conflicts arise when two sets of business processes, referred to as tasks, overlap. In the example provided, a user has permissions from their roles that allow them to process AP payments and perform maintenance on the vendor master file. Conflicts can occur internally due to role configurations or externally when a user is assigned multiple roles that collectively grant conflicting permissions. For instance, a user with the Finance Operations Assistant role can print AP checks and view/maintain vendor banking information. Even if the print AP checks permission is deactivated in the Finance Operations Assistant role, the user would still have access through the Accounts Receivable role. While job responsibilities may require a user to have conflicting tasks, there should be awareness of the associated risks along with proper oversight.

Risk of Privilege Creep Violating Least Privilege Principle

The accumulation of unnecessary access rights over time, known as privilege creep, has undermined the principle of least privilege in the RBAC framework. Over time, employees have accumulated access rights that exceed their current job responsibilities, increasing the opportunity for unauthorized access. Many of these conflicts are due to the internal design of roles, which has not been regularly reviewed or updated.

After reviewing the permission access data, it was found that conflicts exist within the ERP system, impacting various departments. These conflicts, primarily rooted in role-based access configurations, have led to instances where employees possess access rights beyond their current job responsibilities. This situation appears to be caused by privilege creep, which violates the principle of least privilege. The conflicts arising from role configurations constituted a substantial portion of the conflicts.

[6] Although a user may have permission access to generate an EFT file, the system only allows the inclusion of approved invoices using pre-approved remit information. However, the risk escalates significantly when a user also possesses permissions for vendor master maintenance and the authority to approve invoices and system changes.

Our testing searched for 49 unique conflicts that, according to ISACA, allowed users to perform conflicting tasks (see **Appendix C**), each of which tested positive at least once. The majority of these conflicts were found in the Finance, Information Technology (IT), and Human Resources (HR) departments. Specifically, the Finance department was flagged for 49 conflicts, IT for 44, and HR for 11 (see **Table 2**). On average, 128 users had 6.2 conflicts each. However, within the Finance department, 28 users had an average of 13.7 conflicts per user. In IT, 10 users had an average of 27.2 conflicts per user, while in HR, 12 users had an average of 1.8 conflicts per user, contributing to the 11 unique conflicts identified. These findings prompted further testing to determine the causes of conflicts in the remaining departments, particularly examining if roles were assigned to a high number of employees.

Table 2: Conflict Analysis by Department

Department	Users	Average Conflicts	Unique Conflicts
Capital improvement Projects	10	1.1	3
City Manager's Office	4	1.3	3
Community Services	4	1.8	3
City Secretary's Office	1	2.0	3
Economic Development	3	1.3	3
Electric	11	1.6	4
Fire Department	2	2.0	3
Finance	**28**	**13.7**	**49**
Human Resources	**12**	**1.8**	**11**
Information Technology	**10**	**27.2**	**44**
Legal	3	1.3	3
Municipal Court	4	2.0	2
Public Communication	2	1.0	3
Planning and Development	3	2.0	3
Parks and Recreation	7	1.4	3
Police	3	1.7	3
Public Works	11	1.2	4
Utility Customer Service	4	2.0	2
Water	6	1.5	3
Total:	**128**	**6.2**	**49**

For employees outside of Finance, Human Resources, and Information Technology, many SoD conflicts arise due to outdated roles that no longer align with current business processes. Historically, contract entry was managed by city engineers and CIP, but now it is solely handled by the Purchasing department. Similarly, timekeepers currently have access to merge and move timesheets, a task that should be completed exclusively by Finance. Reworking these roles to reflect current responsibilities will help eliminate SoD conflicts for several users, specifically reducing the conflicts for 50 users who have the "Maintain Time Data - Process Payroll" conflict and for 66 users with the "Create Contracts - Approve Contracts" conflict (see **Appendix D**). While there are users with privileges to access historical business processes their job responsibilities once entailed, there are also employees with access to roles that grant privileges outside their current job responsibilities.

Some users have been assigned roles that grant privileges far beyond their responsibilities. For instance, a compensation analyst in Human Resources had access to the Budget Manager role, typically used by Budget staff. This role granted the compensation analyst privileges related to Finance's operations, including the ability to manage accounts, process customer invoices, post journal entries, and handle cash applications. Such extensive access is beyond the scope of the compensation analyst's job responsibilities and poses a risk of unauthorized system activity by users outside of Finance. Management concurred that this access should be removed immediately to mitigate the risk of unauthorized activities (see **Appendix B**). This issue highlights a broader concern that, throughout the City, it is difficult to assess the level of privileges some employees may have in Munis.

Users that have been assigned roles with privileges far beyond their responsibilities pose as a risk.

Risk of Over-Privileged Roles & Self-Approval

How a role-based access control is configured can assist in maintaining SoD within an ERP system. However, the assignment of specific access within roles must be carefully managed. If the roles themselves are not correctly configured, they may grant users access to multiple functions that should be separated to prevent possible unauthorized system activity. Effective system controls ensure that each role has clearly defined and limited permissions, restricting users to only the functions necessary for their job responsibilities. However, there are several roles with extensive privileges.

There are particular roles that present a higher risk of SoD violations than others. Upon review of the current role configurations, we identified that 44 out of the 258 active roles are generating SoD conflicts either internally within the role or externally between other roles that are assigned to a single user (See **Appendix E**). These roles predominantly encompass functional or job-specific roles assigned to users within HR, Finance, and IT departments. Notably, the IT System Administration and Finance System Manager roles are responsible for the highest number of internal conflicts, each accounting for 44 conflicts. These roles, which are superuser roles within IT and Finance, respectively, are assigned to a total of 8 users. Although these users are not directly involved in operational tasks, their extensive level of access poses the highest risk for potential SoD violations. In other cases, while a role may not create as many conflicts, it is assigned to more users.

It was observed that while some roles, such as the Contract Manager role, generate only one conflict, they are assigned to a more extensive user base, in this case, 67 users. This disparity indicates that even roles with fewer conflicts can pose substantive risks due to the high number of users with access, necessitating a detailed review of the privileges granted to such roles. Furthermore, 38.64% of roles are found to create conflicts exclusively due to their internal configurations, contributing to 69.79% of all identified conflicts. Conversely, 30.21% of conflicts arise from the interaction between different roles, emphasizing that many conflicts could be effectively resolved by reassessing and refining the internal configurations of roles. Addressing external conflicts, however, would require an awareness of the impact of assigning multiple roles to a user. However, one item that can be easily assessed is the superuser permissions assigned to a role.

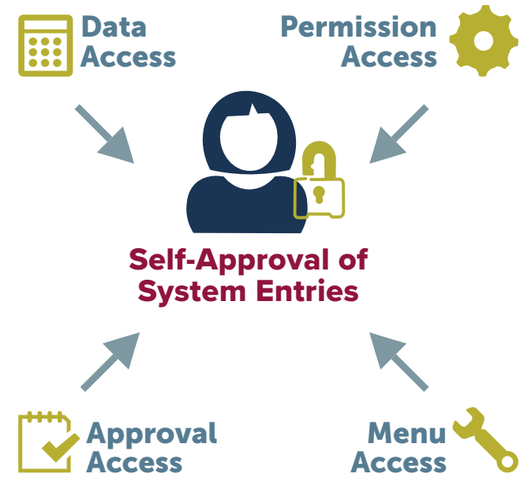
In total, there are 12 roles with superuser permissions, which grant widespread functional access. Management has indicated that certain roles currently possessing superuser permissions should not have such extensive privileges. Ensuring that role configurations align with the actual job requirements of users helps to adhere to the principle of least privilege. However, this alignment has not always been consistently maintained within the City.

While job responsibilities change over time, roles do not always reflect these changes. During our review of permission access, we found that the Financial Support Specialist (FSS) position, which handles Accounts Receivable (AR) and Vendor Management responsibilities, still had access to Accounts Payable (AP) functions. Historically, the FSS position was responsible for some AP functions. However, over time, changes in accounting processes and increased staffing have allowed these functions to be segregated. Despite these process changes, the privileges allotted to the FSS position were not in sync, but they still granted them access to AP functions. This means that from a system perspective, the permissions for AP, AR, and Vendor Management functions were not segregated among three users.

Management concurred that changes should be made to the current role assignments, or new roles should be created. The lack of SoD was further compounded by the absence of a dedicated role for the FSS position, leading to them having a conglomeration of several roles assigned to other users in financial reporting. While the FSS position did not have approval access for any of these functions, which could allow for self-approvals if it was on, there are still instances of overlap with the four levels of system controls.

There are SoD conflicts that can occur when there is an overlap of the four levels of system controls. The levels of system controls within Tyler Munis are designed to ensure SoD and prevent unauthorized activities. However, these controls can be ineffective due to the configurations of roles, approval access for users, and system limitations within Munis. Specifically, Munis will not prevent an approver from approving their own entries. One way a user has the necessary privileges and is an approver in a single-step approval process, they can process and approve their own entries. The system controls, such as role-based permissions, menu security, and data access, are meant to work together with process controls, such as approval workflows. Vulnerabilities arise when these controls are not properly aligned, or the system's capabilities are insufficient to enforce strict separation. This breakdown can occur when roles are configured to allow users to bypass controls or when the system does not have the necessary mechanisms to prevent self-approval of entries (See **Figure 3**).

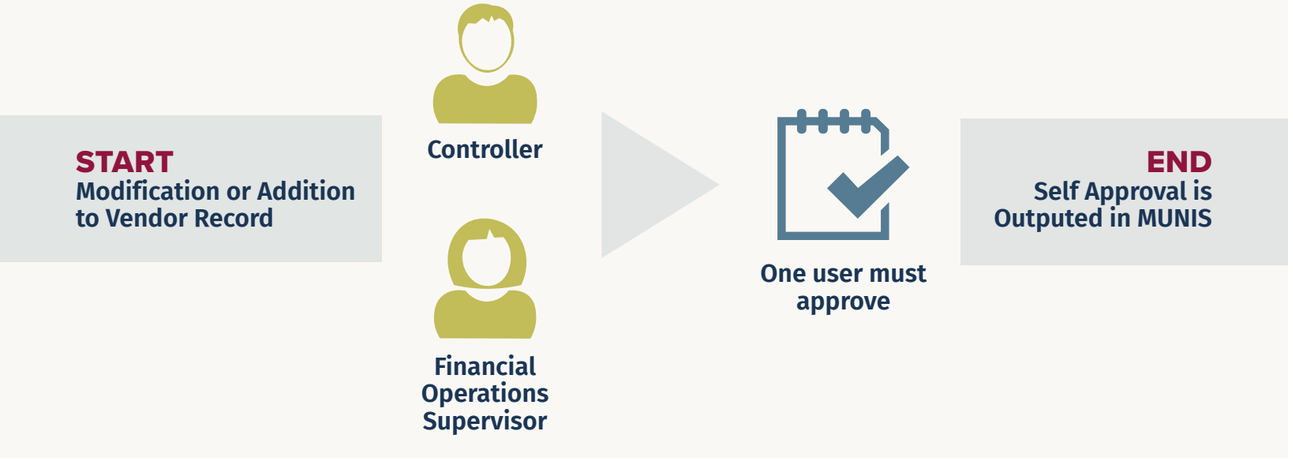
Figure 3: Self-Approval in Munis



Vendor Banking Modifications and General Ledger entries can be self-approved. One notable example of this breakdown is in the context of vendor banking modifications and General Ledger (GL) journal changes. For instance, the Finance Operation Manager role, assigned to the Controller and Financial Operations Supervisor positions, grants significant privileges, including the ability to view and maintain vendor banking information. Additionally, there is only one approval step in the workflow for changing a vendor record, and these two positions are the approvers (see **Figure 4** on the next page). The audit team, along with IT, were able to verify that these two users can self-approve vendor changes. In project 24.03, we found over 5,132 self-approvals related to additions and modifications to vendor records between 2015 and 2022. Despite manual processes, such as an additional review by another manager, these safeguards are external to the system and rely on human oversight. However, since 2022, there have been no self-approvals, but the opportunity remains in the vendor management process and other approval processes.

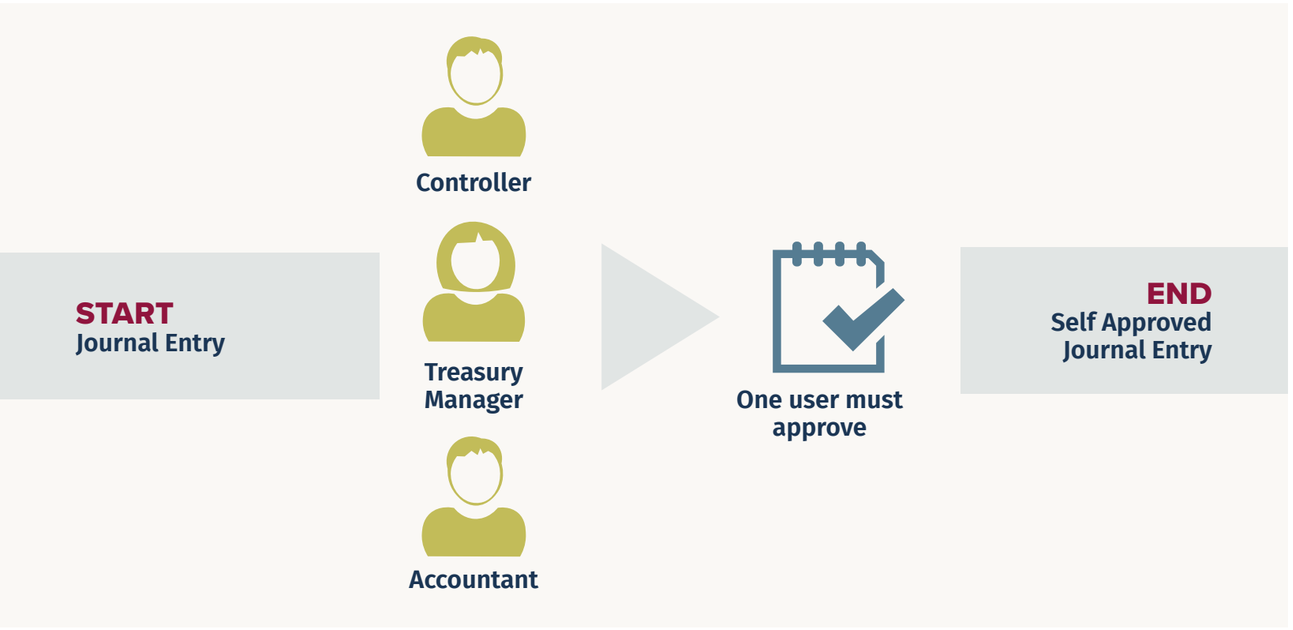
Assigning multiple roles to a user makes it difficult to assess the full impact of their access, increasing security and SoD risks.

Figure 4: Vendor Change Workflow and Self-Approval Risk



Similar to vendor records, the workflow for GL journal changes allows three users to approve their own entries. Notably, the approval process for GL differs from vendor changes because the preparer can select an approver group. However, three users that have permission access are in the ALL-approver group (see **Figure 5**). There is nothing preventing a user from choosing the ALL group, to which they belong. This allows for the self-approval of GL journal changes. It is important to note that our analysis is not comprehensive on all workflow configurations that allow for self-approval. However, it highlights that system configurations can result in self-approvals in the business workflow.

Figure 5: General Ledger Workflow and Self-Approval Risk



Risk of Misuse of Terminated Users' Privileges

Ensuring the timely removal of user access for terminated employees helps to maintain authorized action in the ERP system. Failure to do so could result in security risks, including potential data breaches and system misuse. The current process can lead to potential delays, inconsistencies, and ambiguity in the audit logs. Despite detective controls, some terminated employees retain access to the ERP system.

There is a reliance on departments as the key control for notifying IT of a user's termination. The current process for deactivating users relies on departments submitting IT service tickets (see **Figure 6**). If a department does not promptly submit a termination ticket, IT remains unaware of the need to deactivate the user's access until other detective controls are performed. This dependency introduces delays and inconsistencies in the deactivation process, potentially allowing terminated employees to retain access for an extended period. Reliance on manual notification from departments can lead to IT being unaware of necessary deactivations.

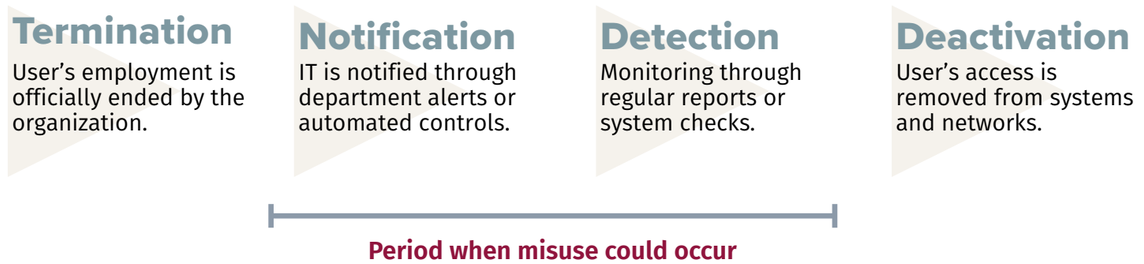
In addition to this key control, IT has implemented detective controls to identify terminated users who may still have active access. For instance, Payroll sends a monthly report of all employees being removed from the payroll to IT who will then reconcile this list with the Active Directory to identify users needing deactivation. While this detective control helps catch instances where the departments did not promptly submit termination notifications, it has limitations. Specifically, it does not account for system users not on the payroll, such as volunteers or unpaid interns. As a result, these users may still retain access despite no longer being active, highlighting a gap in the control mechanism.

IT can promptly deactivate user access, if they are made aware of the termination. For calendar year 2023, we reviewed all 57 user deactivations to assess the time taken from an employee's termination date to account deactivation. On average, IT deactivated accounts 32 days after an employee's termination. According to IT, delays often occurred because notifications of terminations are more consistently received through the monthly payroll report, since departments may not submit service tickets in a timely manner or, in some cases, may fail to submit them altogether.

To evaluate how departmental notifications impact IT's ability to deactivate accounts promptly, we analyzed 21 IT service tickets for full- and part-time employees' ERP accounts since the implementation of IT's new ticketing system, Jira. We found that departments submitted termination tickets an average of 23 days after the employee's termination. Once notified, IT can typically deactivate accounts within one business day. However, system limitations may prevent this from happening.

The approval workflow is one obstacle that prevents IT from timely deactivating terminated users. If a user has outstanding approvals at the time of termination, IT and Finance must resolve them by transferring the approvals to another user. This is a system limitation within Munis, which prevents deactivation until all pending actions are addressed. Overall, these delays caused by notification failures and system limitations highlight a gap in the user deactivation process that could be exploited by terminated employees.

Figure 6: The User Deactivation Process



There were still terminated employees that had ERP access. We found that six terminated employees[7] still had active ERP access (see **Table 5**). One of which had superuser access to the approval workflow. This issue arises from either the failure of departments to submit termination tickets or administrative oversights in the deactivation process. Such lapses pose security risks, as these individuals could potentially misuse their retained access. Fortunately, the employees had been disabled in Active Directory, which prevented them from logging into Munis, as both Munis and Active Directory accounts must be active for a user to access the system. However, there are still potential risks, as other users could exploit terminated users' accounts for unauthorized actions. Given the past issue of employees sharing login information, there is a risk that someone could misuse a terminated user's privileges, particularly during the period when neither Active Directory nor Munis access has been disabled—such as when a department has not yet submitted a service ticket, and IT is still awaiting the monthly payroll report.

Table 5: Terminated Employees with ERP Access on 2.21.24

Position	Termination Date	Days Since Termination	Permissions	Superuser	Conflicts
Electric Supervisor	07/31/2023	205	463	-	-
Laboratory Technician	07/31/2023	205	287	-	-
Compensation Analyst	09/11/2023	163	402	1	6
Streets Division Manager	10/13/2023	131	391	-	1
Marketing Coordinator	11/30/2023	83	320	-	-
City Marshall	1/16/2024	36	374	-	-

The current naming conventions in the Active Directory make it difficult to maintain a transparent audit log. Specifically, the practice of recycling user IDs after a 12-week period[8] introduces challenges in evaluating user activity. Once a user ID is removed from the Active Directory after this period, it can be reassigned to a new employee. This can create confusion and complicate audit trails because it becomes challenging to accurately trace activities back to the correct individual, especially if records from the previous user are not thoroughly transitioned to a new user ID. During our analysis, we identified instances where user IDs were incorrectly flagged as terminated users because the City no longer employed the previous employees associated with those IDs. Without due diligence in tracing user records, it is difficult to determine if user IDs are recycled.

According to standards such as NIST SP 800-53[9], particularly in section 3.3, "Audit and Accountability," organizations must ensure the unique identification of users and maintain accurate audit records to support accountability. Specifically, section 3.3.1 requires organizations to create and retain system audit logs and records to monitor, analyze, investigate, and report unlawful or unauthorized system activity. Additionally, section 3.3.2 mandates that the actions of individual system users can be uniquely traced to those users, enabling accountability. Adhering to these standards helps in maintaining a clear and precise audit log, ensuring that every action within the system can be attributed to a specific user without ambiguity. The current process that allows for recycled user IDs does not support these best practices.

[7] IT staff were informed of these terminated users and promptly deactivated their accounts.
[8] Due to Microsoft configurations, deactivated user IDs will remain on the active directory for 12 weeks before they are completely removed.
[9] National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Risk of Misuse of Superuser Access

According to ISACA standards, superusers are classified as users with elevated access rights and permissions that exceed those of standard users, enabling them to perform critical administrative tasks across systems and applications. The advantages of utilizing superusers include streamlined system management, efficient problem resolution, and enhanced ability to perform high-level troubleshooting and maintenance. However, the drawbacks include increased security risks due to the potential for abuse of power, greater vulnerability to insider threats, and the possibility of impact from errors or unwarranted system use. Proper management, including strict access controls, monitoring, and periodic reviews, helps to mitigate these risks.

In the Munis system, there are five superuser permissions that grant extensive access and control over various applications. The Payroll, Personnel, Utility, and Fixed Asset Superuser permissions grant unrestricted access to all functionality within their respective programs. For example, the Personnel Superuser permission allows a user to modify the employee master file, regardless of a user's approval access. The Workflow superuser permission allows the ability to maintain workflow pending actions in the maintenance program, which is the responsibility of IT and workflow administrators. While this level of access is helpful in efficiently performing operations, it allows the possibility for misuse. Therefore, best practices recommend monitoring controls for superusers.

The number of superusers within the City could be reduced without negatively impacting operations. There are 71 active superuser permissions across the City's 33 superusers (see **Table 6**). We identified instances where superuser privileges did not adhere to the least privilege principle. For example, all the Budget and Purchasing divisions had access to the workflow superuser, even though they did not interact with workflow maintenance. Management agreed that removing these superuser privileges would not negatively impact the current business process. Additionally, management proposed that the number of Payroll superusers in Finance be reduced from 5 to 4 and Fixed Asset superusers from 5 to 4; management will also investigate methods of setting projection-only access for Fixed Asset superusers.

Table 6: Distribution of Superuser Permissions

Location	Superusers	Workflow	Payroll	Personnel	Fixed Asset	Utility	Total
FIN – Accounting	7	5	5	-	5	-	15
FIN – Administration	2	2	-	-	2	-	4
FIN – Budget	5	5	-	-	-	-	5
FIN – Purchasing	5	5	-	-	-	-	5
Human Resources	7	1	-	6	-	-	7
IT – Administration	2	2	2	2	2	2	10
IT – Business Systems	5	5	5	5	5	5	25
Total:	**33**	**25**	**12**	**13**	**14**	**7**	**71**

IT superusers will remain active to assist with technical issues related to Munis. However, superusers will still exist in Finance and HR departments, although HR plans on reducing the Personnel superusers from 6 to 2, if testing with IT shows a minimal impact on operations. Overall, management had indicated that the number of superusers could be reduced from 33 to 17, and the number of active superuser permissions could be decreased from 71 to 48 (see **Appendix B**). As a best practice, it is recommended to implement appropriate detective controls to monitor for unauthorized use when granting superuser privileges.

Payroll fraud presents various forms of financial risk to organizations, especially when excessive permissions are granted to certain users. Common types of payroll fraud, such as ghost employees, improperly adjusting pay ranges, and accrual theft, further compound the risks associated with Payroll Superuser permissions. Ghost employees involve the creation of fictitious employee records in the payroll system, allowing fraudulent individuals to collect salaries for non-existent workers. Improperly adjusting pay ranges can enable unauthorized changes to salary structures, resulting in inflated wages for certain employees or unauthorized bonuses. Accrual theft occurs when unauthorized adjustments are made to employee accruals, such as sick leave or vacation time, which can be cashed out or used illicitly. These fraudulent activities can be facilitated by excessive access granted through Payroll Superuser permissions, as individuals with such access can manipulate payroll data without detection.

The Payroll Superuser permissions grant extensive access to personnel applications, presenting significant risks. These permissions allow users the privileges to create ghost employees by granting them the ability to manually add records onto the employee master file, assign pay to fictitious employees, maintain direct deposit accounts, enter time, and process payroll. This level of access creates an opportunity for payroll fraud, a situation that demands immediate attention. During the audit, the audit team was able to successfully complete these steps in the Munis testing environment. Additionally, we were able to freely adjust employee's pay.

While the payroll administrator is responsible for and can freely adjust employee accruals, this is done through another permission to be discussed in the next section. IT was able to successfully recreate the audit team's work, thereby verifying the fraud risk associated with the superuser permission. This confirmed that such permissions could indeed facilitate fraudulent activities within the payroll system.

However, removing the Payroll Superuser permission is not straightforward due to the role these permissions play in payroll operations and how certain functionality has been locked behind the Payroll Superuser permission by Tyler Munis. For instance, the update/delete functionality allows users to edit the processing steps for bi-weekly and miscellaneous payrolls, is only accessible through the superuser permission. Representatives from Tyler Munis have confirmed this system limitation.

During a walkthrough in the test environment, payroll administrators were asked to complete the payroll process without using the Payroll Superuser permission. The results revealed limitations, as administrators reported that certain functions, such as global add/delete operations in the Employee Job/Salary application were impeded without the superuser permission. With these challenges in mind, payroll administrators indicated that the current payroll process necessitates the superuser permission. However, potential process redesigns could enable payroll to be completed without requiring superuser permissions. While these changes may impact staff efficiency, this cannot be confirmed until the process is tested.

Risk of Unauthorized Access to High-Risk Permissions

ThirdLine has identified permissions within an ERP system as being deemed high risk due to the significant impact on the integrity and security of organizational data. For instance, permissions such as "delete audit," which allow the deletion of audit records, pose a high risk as they can potentially enable users to erase traces of their actions, thereby hindering transparency and accountability. Fortunately, based on our review, this permission has not been enabled for any users within the system, but there is no policy governing whether this permission could be turned on. There should be a clear awareness of which high-risk permissions should be exclusively assigned to a limited number of designated positions, ensuring certain system functions are secure.

There are 85 high-risk permissions that have been identified within the Munis system that warrant close attention (see **Appendix F**). These are distributed across various functional areas, such as Accounts Payable and HR management. We identified multiple employees, particularly within the Finance and IT department, who hold numerous high-risk permissions, potentially leading to an authorized level of access.

High-risk permissions should be limited to designated positions. Finance employees with disbursement permissions range from 8 to 12 users (see **Table 7**). For example, the permission to "Generate EFT File," which was found to be accessible by FSS staff, poses a risk as it could potentially lead to unauthorized disbursements. While the FSS staff did not have approval access for disbursements, there remains a likelihood that human error by an approver could lead to a payment made by a FSS being sent out. Management explained that permissions related to AP disbursements should only be accessible to management. Similarly, category access permissions to update or delete records, such as those within the employee master, employee job/salary, employee accruals, or personnel actions, can allow users to modify records, potentially leading to inaccurate compensation and compromising the integrity of Munis data.

Table 7: Active Users with AP Disbursements Permissions

Permission	IT Users	Finance Users	Roles
Maintain check runs	6	12	8
Print Checks	6	9	7
Generate EFT File	6	12	8
Create AP positive pay file	6	11	7
Maintain own posted invoices	6	9	8
Modify 1099 codes	6	9	7
Stale checks processing	-	8	5

Category access permissions enable users to edit records even when additional processes are in place to ensure proper approval. This is evident in the case of personnel actions (PA). The PA process begins with the initiation of a PA by either a designated department initiator or HR staff who then forward the PA to an HR administrator to receive the necessary approvals before posting the action. Typically, payroll staff will then process the PA by uploading the requested changes to the appropriate table. However, payroll staff and other payroll backups in Finance have update/delete access to the "Employee Pay - Personnel actions" permission, which allows them to access records related to employee pay within the PA system. We observed that the system allows for edits in-progress and approved PAs related to employee pay. According to management, only four employees in Finance should have access to the functions, but we identified that there was a fifth employee that had access. Management plans to remove that access (see **Appendix B**).

Appendix A: Management Response Summary

The following summarizes the recommendations issued throughout this report. The auditors found that staff and the Departments were receptive and willing to make improvements to controls where needed. Management has provided their response to each recommendation.

Risk: High	**1. Enforce Least Privilege:** To enhance the effectiveness of the City's system controls, enforce the least privilege principle by conducting a review of current user roles and permissions, disabling unnecessary access at the permission, menu, data, and/or approval level, granting inquiry only privileges, and/or reassigning privileges to other roles. Additionally, temporary roles can be created to award a user privileges for nonroutine and emergency situations.	**Expected Completion:** 2024
	Plan of Action: Management concurs, and Fiscal Services staff has already gone in and made changes to roles and permissions identified to address this recommendation.	**Responsibility:** CMO/Fiscal
Risk: Medium	**2. Automate Terminated User Notifications:** The key control in notifying IT of a user's termination is a department submitting an IT support ticket requesting the deactivation of the ERP account. However, departments are not always timely in notifying IT, allowing terminated users to maintain access. IT should coordinate with Human Resources a trigger point that signifies an employee's termination. Once this trigger point has been identified, IT should develop reporting controls to automatically notify the business systems team of an employee's termination.	**Expected Completion:** 2024
	Plan of Action: Management concurs and the appropriate staff in IT and Human Resources will review and improve the process to terminate users from the ERP system.	**Responsibility:** CMO/IT
Risk: High	**3. Reassess Approval Processes for Users with Permission Access:** Management should reassess permission access within Tyler Munis to address business processes where self-approvals can occur. Currently, employees can enter and self-approve vendor modifications, including banking changes, and General Ledger entries due to the current system configurations. To mitigate this risk, management could ensure that anyone who is an approver for vendors does not have access to edit or enter any changes. Additionally, they could change workflow steps that are high risk of self-approval to require approvals from multiple users in that step. Another option is to add a step with more refined criteria, directing specific vendor changes to an additional approval step. It is important to note that while these changes might help enhance segregation of duties, it may come at the cost of staff efficiency.	**Expected Completion:** 2024

	Plan of Action: Management concurs and due to the limitations of our ERP system, this audit will help identify and monitor that risk. When the ERP was initially implemented this risk was identified and mitigated through the development of policies and procedures related to approvals. This audit provides an opportunity to reassess and determine if additional revisions are merited to mitigate the risk.	**Responsibility:** CMO
Risk: Medium	**4. Investigate Changes to Naming Conventions:** Currently, the naming conventions utilized by the City allow for user IDs to be recycled creating ambiguity in the audit log. Best practices indicate that organizations must ensure the unique identification of users and maintain accurate audit records to support accountability. Therefore, IT should investigate system or process changes that would grant each user a unique identifier in the ERP system, even after their employment with the City has ended.	**Expected Completion:** 2024
	Plan of Action: Management concurs that user IDs should not be recycled. IT staff will review and if necessary change the user ID naming provisions.	**Responsibility:** CMO/IT
Risk: High	**5. Develop and Document Policies and Procedures for Superuser Privileges:** The City should establish policies and procedures for role-based access tailored to organizational needs and job functionality. These policies should define superuser responsibilities and set conditions for granting and revoking superuser privileges, including specifying which positions are eligible for such access. Regular reviews of access rights and continuous monitoring of superuser activities should be conducted to ensure compliance and mitigate security risks. Moreover, options should be investigated to prevent instances of end users being setup as superusers.	**Expected Completion:** 2024
	Plan of Action: Management concurs. Staff is in agreement that system controls are critical, and that additional assessment will be needed to understand impacts including additional resources or cost to implement.	**Responsibility:** CMO/HR/Fiscal
Risk: Medium	**6. Respond to Privilege Access Reviews:** The Audit Office plans to conduct periodic privilege audits. In response to the results of these audits, management should take the appropriate corrective actions to ensure that the risks of fraud, misuse, or abuse are mitigated. This includes verifying that superusers need their elevated permissions, ensuring all users have appropriate access for their job responsibilities, and confirming that terminated employees do not retain active access to the system.	**Expected Completion:** 2024
	Plan of Action: Management concurs, and Fiscal Services staff has already gone in and made changes to roles and permissions identified to address this recommendation.	**Responsibility:** CMO

Appendix B: Roles and Permissions Corrective Action Plan

2024 ERP SEGREGATION OF DUTIES INTERNAL AUDIT – BUDGET RESPONSE

1. Regarding Workflow superuser access, updates should be made to mirror the City's current operations rather than the planned intent from 2014. Should operations change down the line, access can be restored at that time. The necessary changes associated with this correction are detailed in the Accounting Operations response document.

2. Budget currently only uses 1 role & has deemed that all Budget staff (including managers) should have the same access. Therefore, it is recommended that the role J_FIN_BUDGET_ANAYLST be disabled. Two users currently have access to this role, but the access should be maintained via other roles already assigned to the users.

3. Regarding the assignment of an HR staff member (compensation analyst) to the J_FIN_BUDGET_MGMT role, it is believed that they were granted this role to assist with any questions or issues that arose with the Personnel Projections as they mirror how the LIVE Personnel module functions. However, they should not have the full access associated with this role.

    i. Therefore, it is recommended that this role be removed from the compensation analyst immediately & a new inquiry only function role (for budget projections) be defined. After the role is vetted by Budget management, it can be added to the compensation analyst position. Any issues identified & future can be amended to this Functional role.

4. Regarding the J_FIN_BUDGET_MGMT role:

    i. The "Maintain Payroll Configuration" permission is believed necessary due to how the Budget Projection module works with respect to budgeting personnel. This is because the budget module mirrors nearly all the functions of a real payroll but is constrained within a defined projection. We can test removing the "Maintain Payroll Configuration" permission; however, the following tasks will need to be reviewed closely:

        - Creating a new Budget Projection
        - Developing and reconciling Salary & Benefit Budgets
        - Posting personnel budgets to the projection

    ii. The "Settle Projects" permission is required for Budget since they perform all maintenance of the project ledger.

    iii. The "Manage Accounts" permission is likely required for budget to maintain their Budget Rollup codes & the Calculate Available Budget settings at the org level. Historically they have also made accounts, however Financial Reporting currently performs this task. If the create/manage accounts should be restricted to Financial Reporting but with Budget to still have access for the budget settings, testing will need to be performed to determine whether it is possible.

    iv. The "Process Customer Invoices" was once required due to budget staff providing backup support of AP/AR. However, with the additional AP/AR staff that has been added, this permission is no longer necessary. Recommend removing but still ensuring that inquiry access is included in the role. Other related permissions can also be removed:

        - Post Own Invoices (General Billing)
        - Access to others' Batches (Accounts Receivable)

    v. The "Post Journal Entries" & "Post own Journal Entries" rules are required if only for Budget to be able to post their own Budget JEs. Any associated risk is mitigated by Approval controls, as all JEs are designed to flow through a workflow for approval prior to being able to post.

ACTION SUMMARY

- For Immediate Action
  - Remove Workflow Superuser Permissions as defined in the Accounting Operations response[1]
  - Inactivate the role J_FIN_BUDGET_ANAYLST[2]
  - Remove role J_FIN_BUDGET_MGMT from the HR Compensation Analyst[3]
  - Modify role J_FIN_BUDGET_MGMT to have Inquiry Only access to AP/AR modules[4]
    - Identify permissions that will change
    - Notify Budget of planned change & coordinate date of change for a non-critical time (i.e. not during peak Budget season)
    - Address any reported issues following change as they occur
  - Remove role F_PROJ_MAINT from the Enterprise Technology Project Management Officer
    - Inquiry Only access should be granted instead

- To Test
  - Create new functional role to provide inquiry only access to Budget Projections[3]
  - Test removing the "Maintain Payroll Configuration" permission with the following scenarios:[4]
    - Creating a new Budget Projection
    - Developing and reconciling Salary & Benefit Budgets
    - Posting personnel budgets to the projection

- To Discuss
    - Budget access for creating GL accounts[4]

2024 ERP SEGREGATION OF DUTIES INTERNAL AUDIT – ACCOUNTING OPERATIONS RESPONSE

1. The Financial Support Staff need to be trimmed down to a single job role with the correct core permissions. Any additional permissions should then be amended to their users via function roles.
    i. Two separate FSS roles will need to be created. One will be AR focused, whereas the other will be AP focused. Each role will allow inquiry access to programs/data that are classified as a conflict to segregation of duties.
        - J_FIN_AP_FSS or AP Financial Support Specialist
            1. Has all access currently within the main AP role
            2. Has read only access to AR programs
            3. Assigned to one Financial Support Specialist
        - J_FIN_AR_FSS or AR Financial Support Specialist
            1. Has AR Cashiering & AR Billing access (build out from existing AR roles)
            2. Has Vendor Maintenance access
            3. Has Check Reconciliation Access
            4. Has read only access to AP Invoices. Does not have access to Payment Manager
            5. Has PCard Statement maintenance
            6. Assigned to three Financial Support Specialists
2. Payment Manager should be restricted immediately to only the following users: Accounting Operations Supervisor, Controller, Asset Manager, one Financial Reporting staff, Treasury Manager, Finance Director, and Systems Accountant.
3. Tyler Cashiering approval controls are as follows,
    i. AR payment batch data comes into Munis from Tyler Cashiering. No AR payments are entered directly into Munis.
    ii. FSS AR staff (three users) post payment batches within Munis, however the batch must be in an Approved state prior to posting. Approvals are completed via Tyler Cashiering
    iii. FSS AR staff perform all entry into Tyler Cashiering of the daily AR payments recorded by Finance (controlled via Tyler Cashiering permissions).
    iv. FSS AP staff (one user) and Accounting Operations Supervisor perform approvals of Finance Tyler Cashiering batches (controlled via Tyler Cashiering permissions).
4. Regarding the conflicts within the J_FIN_ACCTSPAYABLE role:
    i. Deactivating “Override PO receiving variances” may remove AP’s ability to enter a direct entry.
    ii. Recurring Invoices are not used. After discussion, we recommend disabling the associated permission from this AP staff role.
    iii. Deactivating the “Override Invoice Variance” permission may remove AP’s ability to enter a direct entry. We can test turning this off to see if it impacts AP’s daily processes.
    iv. “Allow entry of credit memo without original invoice” permission is required for staff based on our current internal processes. Research is currently ongoing with respect to credit memos, so permission may be revisited again in future. All credit memos must receive workflow approval, so the risk is mitigated via Approval Access controls.
    v. “Post own invoices” permission is required for staff based on our current internal processes. All invoices must receive workflow approval, so the risk is mitigated via Approval Access controls.
    vi. Deactivating the “Adjust partial payments” permission may prevent AP from paying an invoice that is less than the total amount received on. Further research is required. We can test turning this off to see if it impacts AP’s daily processes.
    vii. The permission “Maintain Check Runs” very likely is required for AP staff to complete their normal

duties. This is because the program Invoice Entry has a field to define a check run name when creating a batch. This field is defined for all wires & as a result, when the invoice batch is posted it automatically assigns that wire to a check run by the same name. This permission does not grant any inherent program menu access, thus the risk is mitigated here via Menu Controls limiting AP's access to Payment Manager (see top immediate action item).

5. The "Print AP Checks" permission should be removed from all roles that do not print checks. Other permissions in this same category but less critical include
   i. Generate EFT File
   ii. Post AP Cash Disbursements
   iii. Create AP positive pay file
   iv. Void AP checks
6. Regarding the conflicts with the J_FIN_FR_ANALYST role:
   i. The role J_FIN_FR_ANALYST is currently the primary role for Financial Reporting staff.
   ii. In order for Financial Reporting staff to complete their normal job duties, they must have access to:
      - General Maintenance on accounts
      - Stale Check Processing
      - Post own Journal Entries – any conflicts are mitigated via Approval Controls
      - AR Access to others batches – permission does not grant access to change records, just to see them.
   iii. Currently this role is associated with the AR FSS staff who do not need access to several functions part of this role. Access for these staff members will be removed once a new cleaned up Job role is defined for their use.
7. Workflow Superuser access can be removed for all users excluding the Systems Accountant, one Financial Reporting staff & IT.
8. Regarding Capital Assets (also referred to as Fixed Assets in places):
   i. Only the Asset Manager, one Financial Reporting staff, & Management need superuser permissions to this module.
   ii. Remaining Financial Reporting staff only need inquiry access
   iii. Recommend removing certain users from the MGMT role & giving them the inquiry role instead
   iv. Additionally, there is still a temp role active that we'd recommend inactivating (J_FIN_FA_TEMP)
9. Additional review of existing job roles for Financial Operations staff is needed to re-align job role permissions with current responsibilities. Additionally, certain tasks should be broken out as functional roles that can be added to staff as needed when they have an expansion of their normal job duties. Below are listed the key positions & functions that should be considered:
   i. Positions/Job Roles
      - Assistant Director
      - Controller
      - Accounting Operations Supervisor
      - Financial Reporting Staff
      - Financial Reporting Staff Lvl 2/Lead/Manager
      - Financial Support Specialist AP & AR See #1
   ii. Functional Roles
      - AP Ops Management (Backup)
      - Stale Checks
      - Treasury Controls

ACTION SUMMARY

- For Immediate Action
  - Remove Menu access for Payment Manager from the roles: [2]
    - J_FIN_ACCTSPAYABLE
    - J_FIN_ACCTSREC
    - J_FIN_BUDGET_MGMT
    - J_FIN_OP_ANALYST
    - J_FIN_OP_AP_LEAD (Role should be inactivated)
    - J_FIN_OP_ASST
  - Remove permissions associated with recurring invoices from the J_FIN_ACCTSPAYABLE role [4]
  - Remove “Print AP Checks” & other related permissions from the roles: [5]
    - J_FIN_ACCTSPAYABLE
    - J_FIN_ACCTSREC
    - J_FIN_OP_ANALYST
    - J_FIN_OP_AP_LEAD (role should be inactivated)
    - J_FIN_OP_ASST
  - Remove Workflow Superuser permission from the roles: [7]
    - J_FIN_BUDGET_MGMT
    - J_FIN_FR_MGMT
    - J_FIN_OP_MGMT
    - J_FIN_PURCH_BUYER
    - J_FIN_TREASURY_MGMT
  - For the following users, remove the role F_FA_MGMT & replace with F_FA_INQUIRY [8]
    - Accounting Operations Supervisor
    - Systems Accountant Access will be maintained via the J_FIN_SYS_MGR role
  - Inactivate the role J_FIN_FA_TEMP [8]
- To Test
  - Design the J_FIN_AP_FSS role 1
  - Design the J_FIN_AR_FSS role 1, [7]
  - Evaluate the following permission on the J_FIN_ACCTSPAYABLE role: [4]
    - Override PO receiving variances
    - Override Invoice Variance
    - Adjust partial payments
  - Redesign middle management & financial reporting roles [9]

2024 ERP SEGREGATION OF DUTIES INTERNAL AUDIT – PAYROLL RESPONSE

1. The conflict within the F_TIME_KEEPER role between the Process Payroll & Maintain Time Data is not an issue as this is mitigate via Menu Controls. Timekeepers do not have menu access to 99% of Payroll Processing menus, they only have access to Time Entry.
    i. We can test removing the Process Payroll permission, however we believe this is required for the users to:
        - Be assigned to individual payrolls by payroll staff, and
        - Interact with the Time Entry program correctly
2. The J_FIN_OP_MGMT role is currently defined to provide the same Payroll access as the J_PR_Supervisor role, including the Payroll Superuser permission. The J_FIN_OP_MGMT role is currently assigned to the Controller and the Accounting Operations Supervisor.
    i. The Accounting Operations Supervisor should be removed from the J_FIN_OP_MGMT role, however further review of the other module permissions is needed first to ensure there is loss of critical operational permissions.
    ii. The Controller should keep the role & payroll permissions, since they supervise payroll operations.
3. The J_HR_ADMIN_SPEC & F_TIME_KEEPER conflict regarding payroll processing permissions is mitigated via Menu Controls. Neither role has access to 99% of Payroll Processing menus, F_TIME_KEEPER only has access to Time Entry.
4. The Payroll Administrator currently has both the F_ENTRY & F_APPROVALS roles.
    i. Finance has gained additional staff and does not require the Payroll Administrator to have the F_ENTRY role. Recommend removal.
        - Two users will be Finance's remaining designated Entry personnel.
    ii. The Payroll Administrator requires the F_APPROVALS role currently as it grants menu access to the various financial programs necessary for reviewing taxable AP purchases. However, review of the F_APPROVALS role's permissions is worth evaluating since this role should provide menu access only and not the ability to enter or maintain. WF approval rules are maintained separately.
5. The flagged conflict of F_TIME_KEEPER role having the ability to Merge Batches is mitigated via an external review process performed by Payroll staff after the Time Keeper submits the batch for review. However, as Time Keepers are instructed to never merge batch themselves, we'd recommend removing both the "Merge batches" and the "Move batches" permissions.

ACTION SUMMARY

- For Immediate Action
    - Remove F_ENTRY from the Payroll Administrator [4]
    - Remove "Merge batches" and the "Move batches" permissions from F_TIME_KEEPER [5]
- To Test
    - Remove Process Payroll Permission from F_TIME_KEEPER role [1]
    - Remove J_FIN_OP_MGMT role from the Accounting Operations Supervisor [2]
    - Review permissions on F_APPROVALS role [4]

2024 ERP SEGREGATION OF DUTIES INTERNAL AUDIT – PURCHASING RESPONSE

1. Regarding the proposed reassessment of role responsibilities associated with the J_FIN_PURCH_MGMT & J_FIN_PURCH_BUYER roles:
   i. Buyers should have the ability to create and manage their own contracts and purchase orders (POs). Contracts, Requisitions (REQs), & PO Change Orders go through workflows to approve them initially and any subsequent changes made to them afterwards. Thus, any risk related to buyers creating & approving their own items is mitigated by the Approval Access controls in place via the workflow.
   ii. Buyers should only modify another Buyer's contract and/or PO if they are out of the office and there is an urgent need. Buyers can't be intimately involved in each other's projects enough to toggle who enters the contract and/or PO (or related change orders) and then who completes the final approval and posting once it completes the routing process.
2. The F_CONTRACT_MGR role was intended for Purchasing to enter/manage contracts; however, previous management allowed CIP/engineers to enter their own contacts but not manage them. A handful used this feature for a while; however, Purchasing management ultimately asked them to stop because they were not entering accurate information and Buyers had to make numerous corrections. They don't need to the ability to enter/manage contracts but as stated herein, they do need the inquiry permission.
3. The city does not utilize the functionality related to designating inspectors at the REQ/PO level & instead utilizes the Receiving program for departments recording that a POs items have been accepted by the city & thus an invoice can be paid. As such, the ability to "Override Inspection Requirements on Requisitions" has no impact on current City operations. Recommend removing from all roles.
4. In regards to the Maintaining POs conclusion, the current process is that all POs should be associated with either a Requisition or a Contract. The exception to this is reserved for emergency situations prompted by CMO direction.
   i. When a PO is associated with a contract or a requisition, it directly limits the amounts & the accounts that are available in the PO.
      - When a Buyer enters a PO against a contract, it cannot exceed the amount of the contract and alternate account numbers cannot be used, only those accounts already listed on the approved contract.
      - If the account(s) or dollar amounts need to be changed, a change order is entered on the contract which will go through a workflow and then the PO can be modified to match the contract. Both the Contract Change Order & the PO Change Order will generate workflow approvals.
   ii. In the case where a PO is not automatically created via conversion (the conversion process is limited to REQs), the PO must be entered manually. Currently there is no workflow on the creation of POs due to the software not being able to exclude POs created via the conversion process (i.e. if turned on both REQs converted to POs and POs manually created from Contract would require approval. This would duplicate the approvals already performed for all REQs).
      - The risk associated with not having workflow enabled for the creation of POs is mitigated by the following:
        1. All POs have a Requisition or a Contract[10], both of which are subject to approvals.
        2. Only purchasing staff create POs
        3. POs require Receiving prior to payment.
           a. None of the purchasing staff should have access to receive on POs.
           b. In reviewing permissions, there does not appear to be a specific permission that allows a user to be able to receive. Therefore, would recommend testing access via Menu Controls & permissions that may just be unidentified at this time.
           c. Inquiry only access to receiving records should still be available to buyers.

[10] Except in emergency situations as directed by CMO.

4. All invoices go through an additional approval processes
    a. Invoices are reviewed and signed off by the relevant department
    b. Invoices are entered by AP and approved only by Accounting Operations management. Purchasing is not involved in the workflow; thus, the risk is further mitigated by this approval access control.

5. Regarding the conflicts with the Approve PO & Maintain PO permissions, Buyers need both Approve & Maintain permissions under the current process.
    i. Approval by a buyer is the final step of all existing purchasing workflows (Contracts, Requisitions, PO Change Orders, etc.). The permission "Approve PO" appears to only be associated with Purchase Orders.
        - Currently, purchase order approvals are only triggered when there is a change to an existing PO.
        - Further review of processing a PO change order is suggested as per internal discussion, buyers may not have a need to be on the PO Change Order approval workflow.
        - A broader discussion regarding the interplay of contract approvals, requisition approvals, contract change approvals, & PO change order approvals is needed to ensure approvals are not unnecessarily duplicated.
    ii. The maintain PO permission is required for Buyers to initiate PO Change Orders.

6. Regarding the Purchasing Created Requisitions conclusion,
    i. It is correct that purchasing does not engage in any purchasing for themselves & that for Finance related purchases, designated finance staff outside of purchasing initiate the requisition. However, approvals for the finance department are performed by designated finance staff and not just Mary Ellen. All department approvals for finance related purchases exist outside of purchasing.
    ii. Purchasing staff do retain the ability to create requisitions to facilitate the year end process.
        - At year end, Requisition Entry for all City Staff is restricted to expenditures in the new fiscal year.
        - Purchasing staff retain the ability to create requisitions in the prior fiscal year in order to process the invoices & pay-apps that are received late.
        - Purchasing management enters the necessary prior year requisitions, whereas the buyers perform conversions to POs once the approval workflow is completed.
        - The risk associated with purchasing having this access year-round is mitigated by requisitions requiring department approvals and all items listed in response #4.

7. Regarding the other flagged conflicts within the J_FIN_PURCH_MGMT & J_FIN_PURCH_BUYER roles:
    i. Override PO delivery method defaults
        - PO delivery methods for each City location are pre-defined in the system via the programs Purchasing Departments & Bill To/Ship To
        - This override should only allow for changing the delivery address to another pre-defined address in the system
        - Recommend reviewing who has access to the 2 programs controlling this & subsequent discussion.
        - Additionally, risk associated with this permission is mitigated by separate receiving permissions
    ii. Maintain others unposted POs
        - POs are only created by purchasing staff, thus this permission allows for Buyers to step in should there be urgent need and the responsible buyer is unavailable. See #1 for additional comments.
    iii. Modify their own PO change Orders
        - Buyers are the only ones initiating PO Change Orders, thus this permission is required.

- Risk is mitigated as all PO Change Orders must go thru a workflow that includes department approval.

iv. Delete their own POs
- Buyers manage their own POs, thus require this permission to maintain correct records.

v. Convert Requisitions to POs
- Buyers perform final approvals on all requisitions & then manually convert to POs. Thus, this is a critical permission to their current operation.
- Automatic conversion of REQs to POs is not possible as additional actions are triggered when the PO is created.

vi. Proof & Post their own open POs
- As POs are always associated with a REQ or Contract, approvals have already been performed on amounts.
- Risk is mitigated as all POs require department receiving prior to payment & invoices are subject to a separate approval process.

ACTION SUMMARY

- For Immediate Action
  - Replace the existing F_CONTRACT MGR role with an inquiry only version 2
    - Create an inquiry only functional role for contracts.
    - Replace the existing F_CONTRACT_MGR role with this inquiry only role.
    - Primarily recommended for staff that are not approvers since approvers should already have access to view contracts via the F_APPROVERS role
  - Remove the permission “Override inspection requirement on REQs” from all staff roles 3
  - Remove Workflow Superuser Permissions as defined in the Accounting Operations response
- To Test
  - Evaluate the required permissions & menu access for receiving 4
    - Verify that Purchasing staff do not have the ability to receive
- To Discuss
  - Review existing process workflows to address existing workflow duplication. 5
    - Specifically look at the interplay of contract approvals, requisition approvals, contract change approvals, & PO change order approvals.
    - Evaluate whether Buyers (purchasing) are necessary in the PO Change Order workflow.
  - Review & discuss who has access to Purchasing Departments & Bill To/Ship To 8

2024 ERP SEGREGATION OF DUTIES INTERNAL AUDIT – HUMAN RESOURCES RESPONSE

1. Regarding personnel superuser access, updates should be made to mirror the City's current operational needs with respect to but not reliance upon the planned intent from 2017. Personnel superuser access should therefore be removed from the J_HR_ADMIN_SPEC role. If operations necessitate role modifications in the future, then the applicable category access permissions will be reviewed and utilized rather than superuser permissions.
2. Regarding the assignment of a HR staff member (Compensation Analyst) to the J_FIN_BUDGET_MGMT role, HR concurs that the role should be removed from the employee. If a business need for this role arises in the future, then inquiry only access should be granted.
3. Category access can be reassessed for the following roles:
    - J_HR_ADMIN_SPEC
    - Employee Master Maintenance - personnel actions access
    - User Defined Fields - personnel actions access
    - User Defined Fields - employee master access
    - Employee Pay - personnel actions access
    - Employee Deductions - personnel actions access
    - Employee Deductions - employee master access
    - Personnel Actions - personnel actions access
    - Personnel Actions - employee master access
    - Personnel Seniority - personnel actions access
    - Personnel Seniority - employee master access
    - Employee Master Demographics - personnel actions access
    - Employee Master Demographics - employee master access
    - Employee Master Address - personnel actions access
    - Employee Master Mail Sort - personnel actions access
    - Employee Master Mail Sort - employee master access
    - Employee Years of Service - personnel actions access
    - Employee Years of Service - employee master access
    - Employee I-9 Tracking - personnel actions access
    - Employee I-9 Tracking - employee master access
    - Employee Master Dates - personnel actions access
    - J_HR_RISK_CLAIMS
    - Employee Master Maintenance - personnel actions access
    - User Defined Fields - personnel actions access
    - Personnel Seniority - personnel actions access
    - Employee Master Demographics - personnel actions access
    - Employee Master Address - personnel actions access
    - Employee Master Mail Sort - personnel actions access
    - Employee Substance Testing - personnel actions access
    - Employee Substance Testing - employee master access

- Employee Substance Testing - terminated employee access
- Employee Years of Service - personnel actions access
- Employee I-9 Tracking - personnel actions access
- Employee Training - personnel actions access
- Employee Training - employee master access
- Employee Master Dates - personnel actions access

ACTION SUMMARY

- For Immediate Action
  - Remove Personnel Superuser permissions from the J_HR_ADMIN_SPEC role
  - Remove role J_FIN_BUDGET_MGMT from the Compensation Analyst
  - Update the following category access from the associated role to Inquiry Only:
    - Employee Deductions - personnel actions access → J_HR_RISK_CLAIMS
- To Test
  - If operations necessitate J_HR_ADMIN_SPEC role modifications in the future, then the applicable category access permissions will be reviewed and utilized rather than superuser permissions
- To Discuss
  - Operational impact of removing Payroll Superuser permissions from staff outside of IT and proposed recommendations

Appendix C: ISACA's List of Conflicting Tasks that Pose a High Risk

Task 1	Task 2	Description
AP Payments	Bank Reconciliation	The user possibly has the opportunity to enter unauthorized payments and reconcile with the bank.
AP Payments	Vendor Master Maintenance	The user possibly has the opportunity to maintain a fictitious vendor and create a payment to that vendor.
Bank Reconciliation	Process Vendor Invoices	The user possibly has the opportunity to hide differences between bank payments and posted accounts payable records.
Basic Table Maintenance	System Administration	The user possibly has the opportunity to modify data in tables and run transactions and programs using the inappropriately modified data.
Cash Application	Bank Reconciliation	The user possibly has the opportunity to cover up differences between cash deposited and cash collections posted.
Create contracts	Approve own contracts	The user possibly has the opportunity to create and approve their own contracts.
HR Benefits	Process Payroll	The user possibly has the opportunity to change employee HR benefits and process payroll without authorization.
Maintain Asset Document	Process Vendor Invoices	The user possibly has the opportunity to pay an invoice and hide it in an asset that would be depreciated over time.
Maintain Asset Document	Goods Receipt to PO	The user possibly has the opportunity to create an invoice through goods receipt and hide it in an asset that would be depreciated over time.
Maintain Asset Master	Goods Receipt to PO	The user possibly has the opportunity to create the asset and manipulate the receipt of the associated asset.
Maintain Bank Master Data	Manual Check Processing	The user possibly has the opportunity to create a non bona-fide bank account and create manual checks from it.
Maintain Bank Master Data	AP Payments	The user possibly has the opportunity to create a non bona-fide bank account and create a check from it.
Maintain Bank Master Data	Cash Application	The user possibly has the opportunity to maintain a non bona-fide bank account and divert incoming payments to it.
Maintain Hierarchies	Cash Application	The user possibly has the opportunity to maintain cash application and modify hierarchy and reporting output.
Maintain Hierarchies	Post Journal Entry	The user possibly has the opportunity to post a journal entry and modify hierarchy and reporting output.
Maintain Hierarchies	Process Customer Invoices	The user possibly has the opportunity to process customer invoices and modify hierarchy and reporting output.
Maintain Hierarchies	AP Payments	The user possibly has the opportunity to process AP payments and modify hierarchy and reporting output.
Maintain Hierarchies	Manual Check Processing	The user possibly has the opportunity to process manual checks and modify hierarchy and reporting output.
Maintain Hierarchies	Vendor Master Maintenance	The user possibly has the opportunity to maintain the vendor master and modify hierarchy and reporting output.
Maintain Hierarchies	Process Vendor Invoices	The user possibly has the opportunity to process vendor invoices and modify hierarchy and reporting output.
Maintain Hierarchies	Maintain Customer Master Data	The user possibly has the opportunity to maintain customer data and modify hierarchy and reporting output.
Maintain Hierarchies	Maintain Asset Document	The user possibly has the opportunity to maintain an asset document and modify hierarchy and reporting output.
Maintain Hierarchies	Maintain Asset Master	The user possibly has the opportunity to maintain the asset master and modify hierarchy and reporting output.
Maintain Number Ranges	System Administration	The user possibly has the opportunity to reset the number ranges and possibly delete the log/audit trail.
Maintain Payroll Configuration	Process Payroll	The user possibly has the opportunity to change payroll configuration and perform maintenance on payroll settings.
Maintain Payroll Configuration	Payroll Maintenance	The user possibly has the opportunity to change payroll configuration and perform maintenance on payroll settings.
Maintain Projects and WBS Elements	Settle Projects	The user possibly has the opportunity to use a fictitious project to allocate overages of an actual project and settle the project.

Maintain Projects and WBS Elements	Process Overhead Postings	The user possibly has the opportunity to manipulate the work breakdown structure elements and post overhead expenses to the project.
Maintain Purchase Order	AP Payments	The user possibly has the opportunity to enter a fictitious purchase order and enter the covering payment.
Maintain Purchase Order	Manual Check Processing	The user possibly has the opportunity to enter a fictitious purchase order and enter the covering payment.
Maintain Purchase Order	Process Vendor Invoices	The user possibly has the opportunity to purchase unauthorized items and initiate payment by invoicing.
Maintain Purchase Order	Goods Receipt to PO	The user possibly has the opportunity to enter fictitious purchase orders for personal use and accept the goods through goods receipt.
Maintain Purchase Order	PO Approval	The user possibly has the opportunity to maintain a purchase order and release or approve it.
Maintain Time Data	Process Payroll	The user possibly has the opportunity to modify time data and process payroll resulting in inflated payments.
Maintain Time Data	Approve Time	The user possibly has the opportunity to change payroll master data and enter time data applied to incorrect settings.
Manual Check Processing	Vendor Master Maintenance	The user possibly has the opportunity to maintain a fictitious vendor and create a payment to that vendor.
Manual Check Processing	Bank Reconciliation	The user possibly has the opportunity to enter unauthorized manual payments and reconcile with the bank.
Payroll Maintenance	Process Payroll	The user possibly has the opportunity to change payroll and process payroll without proper authorization.
PO Approval	Goods Receipt to PO	The user possibly has the opportunity to approve the purchase of unauthorized goods and hide the misuse of inventory by not fully receiving the order.
PO Approval	Manual Check Processing	The user possibly has the opportunity to make unauthorized purchases and initiate manual check payments for unauthorized goods and services.
PO Approval	Process Vendor Invoices	The user possibly has the opportunity to release a non bona-fide purchase order and initiate payment for the order by entering invoices.
PO Approval	Vendor Master Maintenance	The user possibly has the opportunity to create a fictitious vendor or change existing vendor master data and approve purchases to this vendor.
PO Approval	AP Payments	The user possibly has the opportunity to approve a fictitious purchase order and enter the covering payment.
Process Overhead Postings	Settle Projects	The user possibly has the opportunity to post overhead expenses to the project and settle the project.
Process Vendor Invoices	Manual Check Processing	The user possibly has the opportunity to enter fictitious vendor invoices and then render payment to the vendor.
Process Vendor Invoices	AP Payments	The user possibly has the opportunity to enter fictitious vendor invoices and then render payment to the vendor.
Process Vendor Invoices	Goods Receipt to PO	The user possibly has the opportunity to enter fictitious vendor invoices and accept the goods via goods receipt.
Vendor Master Maintenance	Process Vendor Invoices	The user possibly has the opportunity to maintain a fictitious vendor and enter a vendor invoice for automatic payment.
Vendor Master Maintenance	Maintain Purchase Order	The user possibly has the opportunity to create a fictitious vendor and initiate purchases to that vendor.

Appendix D: Permission Access SoD Conflicts Amongst Active Users

Conflict	CIP	CMO	CSD	CSO	EDS	ELE	FDS	FIN	HRS	ITS	LGL	PCS	PDS	PKS	POL	PWS	WTR	Total
Create contracts - Approve own contracts	9	3	3	-	2	8	-	9	4	7	2	2	-	4	1	8	4	66
Maintain Payroll Configuration - Process Payroll	1	1	2	1	1	3	2	16	2	9	1	-	3	3	2	2	3	52
Maintain Time Data - Process Payroll	1	1	2	1	1	3	2	16	2	9	1	-	3	3	2	2	3	52
Maintain Payroll Configuration - Payroll Maintenance	-	-	-	-	-	-	-	12	13	6	-	-	-	-	-	1	-	32
Maintain Projects and WBS Elements - Settle Projects	-	-	-	-	-	4	-	16	1	7	-	-	-	-	-	-	-	28
Maintain Number Ranges - System Administration	-	-	-	-	-	-	-	16	1	6	-	-	-	-	-	-	-	23
Maintain Hierarchies - Cash Application	-	-	-	-	-	-	-	16	1	6	-	-	-	-	-	-	-	23
Maintain Hierarchies - Post Journal Entry	-	-	-	-	-	-	-	16	1	6	-	-	-	-	-	-	-	23
Maintain Hierarchies - Process Customer Invoices	-	-	-	-	-	-	-	14	1	6	-	-	-	-	-	-	-	21
Maintain Purchase Order - AP Payments	-	-	-	-	-	-	-	14	1	6	-	-	-	-	-	-	-	21
Maintain Purchase Order - Manual Check Processing	-	-	-	-	-	-	-	14	-	6	-	-	-	-	-	-	-	20
Process Vendor Invoices - Manual Check Processing	-	-	-	-	-	-	-	13	-	6	-	-	-	-	-	-	-	19
Maintain Purchase Order - Process Vendor Invoices	-	-	-	-	-	-	-	13	-	6	-	-	-	-	-	-	-	19
Process Vendor Invoices - AP Payments	-	-	-	-	-	-	-	13	-	6	-	-	-	-	-	-	-	19
Cash Application - Bank Reconciliation	-	-	-	-	-	-	-	11	-	6	-	-	-	-	-	-	-	17
Maintain Hierarchies - AP Payments	-	-	-	-	-	-	-	11	-	6	-	-	-	-	-	-	-	17
AP Payments - Bank Reconciliation	-	-	-	-	-	-	-	11	-	6	-	-	-	-	-	-	-	17
Maintain Purchase Order - Goods Receipt to PO	-	-	-	-	-	-	-	11	-	6	-	-	-	-	-	-	-	17
AP Payments - Vendor Master Maintenance	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Maintain Hierarchies - Manual Check Processing	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Bank Reconciliation - Process Vendor Invoices	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Manual Check Processing - Vendor Master Maintenance	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Vendor Master Maintenance - Process Vendor Invoices	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Maintain Hierarchies - Vendor Master Maintenance	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Manual Check Processing - Bank Reconciliation	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Maintain Hierarchies - Process Vendor Invoices	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Vendor Master Maintenance - Maintain Purchase Order	-	-	-	-	-	-	-	9	-	6	-	-	-	-	-	-	-	15
Maintain Hierarchies - Maintain Customer Master Data	-	-	-	-	-	-	-	8	-	6	-	-	-	-	-	-	-	14
Payroll Maintenance - Process Payroll	-	-	-	-	-	-	-	5	2	6	-	-	-	-	-	-	-	13
Maintain Purchase Order - PO Approval	-	-	-	-	-	-	-	7	-	6	-	-	-	-	-	-	-	13
PO Approval - Goods Receipt to PO	-	-	-	-	-	-	-	7	-	6	-	-	-	-	-	-	-	13
Maintain Hierarchies - Maintain Asset Master	-	-	-	-	-	-	-	7	-	6	-	-	-	-	-	-	-	13
Basic Table Maintenance - System Administration	-	-	-	-	-	-	-	6	-	6	-	-	-	-	-	-	-	12

Process Vendor Invoices - Goods Receipt to PO	-	-	-	-	-	-	-	5	-	6	-	-	-	-	-	-	-	11
Maintain Time Data - Approve Time	-	-	-	-	-	-	-	3	-	6	-	-	-	-	-	-	-	9
Maintain Asset Document - Process Vendor Invoices	-	-	-	-	-	-	-	2	-	6	-	-	-	-	-	-	-	8
HR Benefits - Process Payroll	-	-	-	-	-	-	-	2	-	6	-	-	-	-	-	-	-	8
Maintain Hierarchies - Maintain Asset Document	-	-	-	-	-	-	-	2	-	6	-	-	-	-	-	-	-	8
PO Approval - Manual Check Processing	-	-	-	-	-	-	-	1	-	6	-	-	-	-	-	-	-	7
PO Approval - Process Vendor Invoices	-	-	-	-	-	-	-	1	-	6	-	-	-	-	-	-	-	7
PO Approval - Vendor Master Maintenance	-	-	-	-	-	-	-	1	-	6	-	-	-	-	-	-	-	7
PO Approval - AP Payments	-	-	-	-	-	-	-	1	-	6	-	-	-	-	-	-	-	7
Maintain Asset Document - Goods Receipt to PO	-	-	-	-	-	-	-	1	-	6	-	-	-	-	-	-	-	7
Maintain Asset Master - Goods Receipt to PO	-	-	-	-	-	-	-	1	-	6	-	-	-	-	-	-	-	7
Maintain Bank Master Data - Manual Check Processing	-	-	-	-	-	-	-	6	-	-	-	-	-	-	-	-	-	6
Maintain Bank Master Data - AP Payments	-	-	-	-	-	-	-	6	-	-	-	-	-	-	-	-	-	6
Maintain Bank Master Data - Cash Application	-	-	-	-	-	-	-	6	-	-	-	-	-	-	-	-	-	6
Maintain Projects - Process Overhead Postings	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	1
Process Overhead Postings - Settle Projects	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	1
Unique Conflicts Present in Department:	**3**	**3**	**3**	**2**	**3**	**4**	**2**	**49**	**11**	**44**	**3**	**1**	**2**	**3**	**3**	**4**	**3**	**49**

Appendix E: Permission Access SoD Conflicts Amongst Roles

Role	Description	Internal Conflicts	External Conflicts	Total Conflicts	Users[11]	Superuser Permissions
J_IT_SYS_ADMIN	Job Role for System Administration w/o Security Administration	44	0	44	8	5
J_FIN_SYS_MGR	Job Role for Financial Systems Manager (Superuser for FIN)	44	0	44	1	2
J_FIN_OP_MGMT	Job Role for Finance Operations Management	32	2	34	2	2
J_FIN_TREASURY_MGMT	Job Role for Finance Treasury Management	27	0	27	3	1
J_FIN_DIRECTOR	Job Role for Finance Director	26	0	26	1	0
J_FIN_OP_LEAD	Job Role for Finance Operations Senior Lead	14	10	24	2	0
J_FIN_OP_ASST	Job Role for Finance Operations Assistant	9	12	21	3	0
J_FIN_OP_ANALYST	Job Role for Finance Operations Analyst	4	15	19	1	0
J_FIN_ACCTSREC	Job Role for Finance Accounts Receivable	0	17	17	4	0
J_FIN_FR_ANALYST	Job Role for Finance Reporting Analyst	8	6	14	8	0
J_FIN_BUDGET_MGMT	Job Role for Finance Budget Management	6	3	9	10	1
J_PR_CLERK	Job Role for Payroll Clerk	4	5	9	2	1
J_FIN_FR_MGMT	Job Role for Finance Reporting Management	5	3	8	1	1
J_FIN_BUDGET_ANALYST	Job Role for Finance Budget Analyst	5	3	8	2	0
J_PR_SUPERVISOR	Job Role for Payroll Supervisor	5	2	7	1	1
J_FIN_ACCTSPAYABLE	Job Role for Finance Accounts Payable	7	0	7	4	0
J_FIN_PURCH_BUYER	Job Role for Finance Purchasing Buyer	4	0	4	5	1
J_FIN_FA_TEMP	Job Role for Finance Fixed Assets Temp	0	4	4	2	1
J_FIN_PURCH_MGMT	Job Role for Finance Purchasing Manager	4	0	4	1	0
F_ENTRY	Functional Role for General Entry	0	4	4	70	0
J_FIN_SUPPORT_SPEC	Job Role for Financial Support Specialist	0	4	4	3	0
F_APPROVALS	Functional Role for Access to Approval functions	0	3	3	132	0
F_TIME_KEEPER	Functional Role for Payroll Timekeepers	2	1	3	50	0
F_BFR_CASH_MGMT	Functional Role for Finance Cash Management	0	3	3	2	0
F_FA_MGMT	Functional Role for Fixed Asset Management team	0	2	2	7	1
F_RECEIVING	Functional Role for Receiving	0	2	2	63	0
F_EE_VIEW_W_PAY	Functional Role for Employee Info View with Pay	0	2	2	90	0

F_PA_ENTRY	Functional Role for the Entry of Personnel Actions	0	2	2	57	0
F_EE_VIEW_WO_PAY	Functional Role for Employee Info View without Pay	0	2	2	100	0
J_HR_PA_ENTRY	Job Role for the Entry of Personnel Actions for HR Personnel	0	2	2	5	0
J_HR_COMPENSATION	Job Role for HR Compensation Manager and Analyst	1	1	2	5	0
J_HR_ADMIN_SPEC	Job Role for HR Administrative Specialist	1	0	1	14	1
J_HR_OPER_MGMT	Job Role for HR Operations Management	1	0	1	1	1
F_GL_MEMO_BAL	Functional Role to Perform GL Memo Balance Diagnostics Function	1	0	1	1	0
J_FIN_ENTRY	Job Role for General Entry for Finance Personnel Only	0	1	1	6	0
J_HR_RISK_SAFETY	Job Role for HR Risk Safety Coordinator	1	0	1	2	0
F_FA_TRANSFERS	Functional Role for Fixed Asset Journal Approvers	0	1	1	1	0
F_PROJ_MAINT	Functional Role for Project Maintenance	1	0	1	6	0
J_HR_RISK_CLAIMS	Job Role for HR Risk Claims Coordinator	1	0	1	2	0
J_HR_BENEFITS	Job Role for HR Benefits Coordinator	1	0	1	2	0
J_HR_GENERALIST	Job Role for HR Generalist	0	1	1	3	0
J_HR_DIRECTOR	Job Role for HR Director	1	0	1	1	0
J_HR_RISK_MGR	Job Role for HR Risk Manager	1	0	1	1	0
F_CONTRACT_MGR	Functional Role for Contract Administrators	1	0	1	67	0

[11] Active and Inactive Users; in some cases, IT maintains the roles assigned to inactive users, allowing for the possibility of seamless reactivation if they return to the City.

Appendix F: High Risk Permissions

High-Risk Permission	Application	Number of Users[12]	Number of Roles
Allow invoices to be deleted at or below status	Accounts Payable	89	13
Maintain own purchase cards and statements	Accounts Payable	77	7
Allow vendor name maintenance	Accounts Payable	35	12
Maintain check runs	Accounts Payable	22	8
Generate EFT File	Accounts Payable	22	8
Create AP positive pay file	Accounts Payable	21	7
Maintain own posted invoices	Accounts Payable	19	8
Modify 1099 codes	Accounts Payable	18	7
Allow override of the default document number in invoice entry	Accounts Payable	17	5
View purchase card account numbers	Accounts Payable	16	3
Override contract expiration/extension date restrictions on invoices	Accounts Payable	14	5
Override invoice variance	Accounts Payable	13	6
Override contract retainage	Accounts Payable	13	6
Allow entry of credit memo invoices without original invoice	Accounts Payable	13	6
Stale checks processing	Accounts Payable	11	5
Release batch status	Accounts Receivable	43	5
Batch posting permission level	Accounts Receivable	19	6
Maintain AR settings	Accounts Receivable	16	7
View confidential customer information	Accounts Receivable	11	4
Override special conditions preventing payment	Accounts Receivable	11	4
Access to Customer Banking Data	Accounts Receivable	11	4
Access to customer SSNs	Accounts Receivable	11	4
Process lockbox payment files	Accounts Receivable	10	3
Change contract method	Contract Maintenance	16	5
Delete others contracts up to/including status	Contract Maintenance	16	5
Delete contract change orders up to/including status	Contract Maintenance	16	5
Delete others contract change orders up to/including status	Contract Maintenance	16	5
Employee I-9 Tracking - personnel actions access	Employee Records	22	7
Employee I-9 Tracking - employee master access	Employee Records	16	3
Employee Master Dates - personnel actions access	Employee Records	72	9
Employee Master Dates - employee master access	Employee Records	9	2

[12] Active and Inactive Users; in some cases, IT maintains the roles assigned to inactive users, allowing for the possibility of seamless reactivation if they return to the City.

Employee Professional Development - personnel actions access	Employee Records	10	3
Employee Substance Testing - employee master access	Employee Records	13	4
Employee Substance Testing - personnel actions access	Employee Records	11	3
Employee Substance Testing - terminated employee access	Employee Records	11	3
Employee Training - employee master access	Employee Records	14	5
Employee Training - personnel actions access	Employee Records	14	5
Employee Years of Service - personnel actions access	Employee Records	22	7
Employee Years of Service - employee master access	Employee Records	16	3
Access invoice GL accounts	General Billing	12	3
Override budget amounts	General Ledger	24	8
Override accounting period	General Ledger	23	8
Allow personnel actions to be updated at or below status	Payroll	28	17
Status/Start/Change access	Payroll	21	8
View SSNs	Payroll	18	7
Stored entries access	Payroll	10	3
Employee Master Maintenance - personnel actions access	Payroll Security	75	11
Employee Master Maintenance - employee master access	Payroll Security	10	3
User Defined Fields - personnel actions access	Payroll Security	27	10
User Defined Fields - employee master access	Payroll Security	17	4
Employee Pay - personnel actions access	Payroll Security	25	9
Employee Deductions - personnel actions access	Payroll Security	29	11
Employee Deductions - employee master access	Payroll Security	19	5
Employee Accruals - employee master access	Payroll Security	14	5
Employee Accruals - personnel actions access	Payroll Security	14	5
Personnel Assignments - personnel actions access	Payroll Security	9	2
Employee Certifications - employee master access	Payroll Security	10	3
Employee Certifications - personnel actions access	Payroll Security	10	3
Employee Evaluations - personnel actions access	Payroll Security	13	5
Employee Evaluations - employee master access	Payroll Security	11	4
Personnel Actions - personnel actions access	Payroll Security	70	8
Personnel Actions - employee master access	Payroll Security	21	6
Personnel Seniority - personnel actions access	Payroll Security	22	7
Personnel Seniority - employee master access	Payroll Security	16	3
Employee Master Demographics - personnel actions access	Payroll Security	24	8

Employee Master Demographics - employee master access	Payroll Security	16	3
Employee Master Address - personnel actions access	Payroll Security	70	8
Employee Master Mail Sort - personnel actions access	Payroll Security	22	7
Employee Master Mail Sort - employee master access	Payroll Security	16	3
Override default GL account on entry	Project Accounting	51	8
Delete project strings	Project Accounting	27	7
Delete budget adjustments	Project Accounting	19	7
Delete encumbrance adjustments	Project Accounting	19	7
Delete actual adjustments	Project Accounting	19	7
Override PO delivery method defaults	Purchase Orders	77	5
Modify PO after invoice has been paid	Purchase Orders	58	4
Delete own POs up to and including status	Purchase Orders	18	7
Convert Reqs to POs	Purchase Orders	17	6
Delete others PO change orders up to and including status	Purchase Orders	17	6
Delete others unposted POs up to and including status	Purchase Orders	17	6
Maintain own posted POs	Purchase Orders	17	6
Override PO receiving variances	Purchase Orders	13	3
Restrict to creating NY Reqs and POs only	Purchase Orders	10	4
Workers Compensation - personnel actions access	Worker's Compensation	13	4
Workers Compensation - employee master access	Worker's Compensation	11	3

The Office of City Internal Auditor was established in accordance with the City of College Station Charter as an independent office reporting to City Council to help establish accountability and improve City services. The Office of City Internal Auditor is responsible for conducting performance audits of Departments, Offices, Boards, Activities, and Agencies of the City and providing recommendations for improvement.

Audit Team

Matthew Ragaglia, Program Auditor

City Auditor

Ty Elliott, CIA, CFE, CGAP, COSO

Office of the City Internal Auditor
979.764.6269
telliott@cstx.gov
cstx.gov/AuditReports