Delegation of Financial Signing Authority Audit

October 22, 2021

Mayor

Mattie Parker

Council Members

Carlos Flores, District 2††
Michael D. Crain, District 3
Cary Moon, District 4†
Gyna Bivens, District 5
Jared Williams, District 6††
Leonard Firestone, District 7††
Chris Nettles, District 8
Elizabeth Beck, District 9

† Audit Committee Chair
†† Audit Committee Member

City of Fort Worth
Department of Internal Audit
200 Texas Street
Fort Worth, Texas 76102

Audit Staff

Patrice Randle, City Auditor
Brian Burkland, Assistant City Auditor
Vanessa C. Martinez, Audit Manager
Leona High-Lasker, Auditor

The Delegation of Financial Signing Authority Audit was conducted as part of the Department of Internal Audit's Fiscal Year 2021 Annual Audit Plan.

Audit Objectives

The objectives of this audit were to:

- determine whether delegated authority (for specific transactions) is made explicit regarding who has been granted specific authority, and by dollar threshold;
- determine whether delegated authority is appropriate;
- evaluate configuration of automated forms used to grant approval authority;
- ensure retention of authorizing records; and,
- determine whether transactions were approved as authorized.

Audit Scope

Our audit included a review of delegated financial signing authority for procurement and journal entry transactions from October 1, 2019 through September 30, 2020. Activity beyond this period was reviewed as deemed necessary.

Opportunities for Improvement

User access corresponding with job requirements

Consistent policies and procedures

Executive Summary

As part of the Fiscal Year 2021 Annual Audit Plan, the Department of Internal Audit conducted a Delegation of Financial Signing Authority Audit. Based on our test results, authorizing documents, such as the Fort Worth City Code and the City of Fort Worth's Finance Directives, explicitly and appropriately delegated authority for specific transactions, by job title. Also, dollar thresholds were explicitly noted for transactions related to the City's procurement of goods and services.

We concluded that authorization to process financial transactions was properly delegated, and employee job duties/responsibilities and necessary internal controls were taken into consideration when delegating such authority. Based on our review of randomly-sampled transactions, we concluded that transactions were executed within the delegated authority.

City departments used an automated Security Request Form to request finance-related security user access roles. Security Request Forms had two levels of supervisory approval, and were properly retained to adequately support user access changes and corresponding approvals.

We did, however, identify internal control weaknesses when employees transferred to other departments. Based on our audit results, PeopleSoft Financials access (granted to nine of 48 employees who transferred to other departments) was not adequately managed. For example, in some instances, security access user roles associated with employees' former departments were not removed in a timely manner. In other instances, transferring employees had unnecessary access to multiple business units. It should be noted, that Internal Audit saw no evidence that any of the employees completed transactions that were unrelated to their job function.

Based on our audit results, guidance related to journal entry approvals was contradictory. For example, the City's Finance Directive (FD02) indicated that a designated Senior Accountant or above could approve journal entries. However, the Financial Management Services Department's FY2020 procedures for manual journal entries indicated that Accountants and above could approve journal entries.

These audit findings are discussed in further detail within the Detailed Audit Findings section of this report.

Internal Audit provided management with additional information that is excluded from page 7 of this report, due to potential security concerns. Internal Audit follow-up will be conducted at a later date to ensure that the potential security risk has been adequately addressed.

Table of Contents

FORT WORTH

Background

The ability to delegate financial authority helps ensure that business transactions and processes are completed in a timely manner, by those who have the necessary knowledge and skillset, and by those whose placement within the organization is most appropriate for the task. When properly delegating financial authority, businesses must take into consideration necessary internal controls (e.g., separation of duties), as well as avoid delegations that place subordinates in positions to approve their supervisors' transactions. Delegated financial authority can include, but is not limited to, requesting and procuring goods and services, signing contracts, approving journal entries, adding and/or editing transactions, etc.

The Texas Local Government Code and the City's Administrative Regulations authorize the City Manager to delegate authority. The Fort Worth City Manager has, therefore, delegated signing authority for City of Fort Worth (CFW) financial transactions (e.g., purchasing requisitions, purchase orders, journal entries, etc.). Some examples are noted below.

- Section 252.048 (c-1) of the Texas Local Government Code states that if a change order for a public works contract (in a municipality with a population of 300,000 or more) involves a decrease or an increase of $100,000.00 or less, or a lesser amount as provided by ordinance, the governing body of the municipality may grant general authority to an administrative official of the municipality to approve the change order.

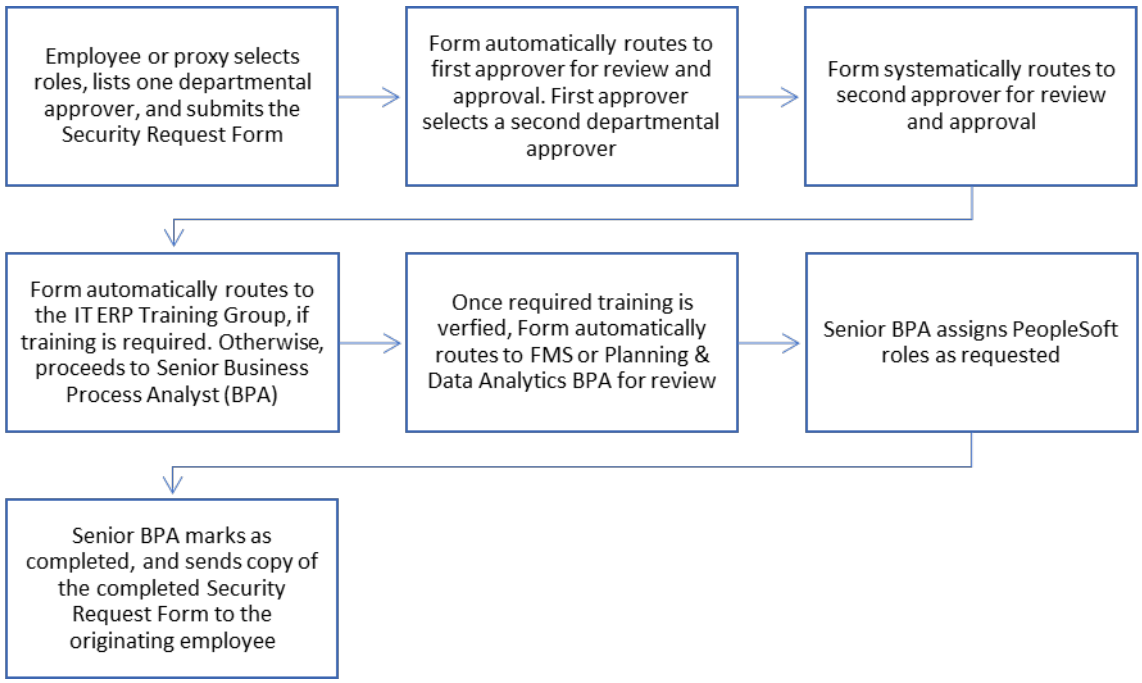
- Section 2-9 of the Fort Worth City Code requires that all contracts be approved by the City Council prior to execution by the City Manager. However, in some instances, authority is delegated to the City Manager. For example, Section 2-9(d)(1) of the Fort Worth City Code states that the City Manager may execute any contract or purchase order involving an expenditure of $100,000.00 or less without City Council approval, if funds have been previously appropriated by the City Council and if the award complies with state law.
- Section III.C.b.2. of the City's Procurement of Goods and Services Administrative Regulation states that the Fort Worth City Council has delegated authority to the City Manager to establish policies and procedures for the purchase of all goods and services. Section IV.A.b. of that same policy states that by adopting the Administrative Regulation, the City Manager has designated the City's Chief Procurement Officer (or Purchasing Manager in the Chief Procurement Officer's absence) as an Acting Assistant City Manager solely for the purpose of executing agreements or otherwise authorizing or engaging in procurements that meet established criteria.

In October 2018, the City implemented the eProcurement, Purchasing and Supplier modules within the PeopleSoft Financials software. PeopleSoft Financials user roles are assigned to employees based on employee positions and job responsibilities within the organization. PeopleSoft Financials security uses business units (departments), roles, permissions, and user preferences. In November 2019, the Financial Management Services (FMS) Department made an automated Security Request Form available for City departments to complete when requesting user access and/or access changes to finance-related systems such as PeopleSoft Financials, iNovah (point-of-sale system) and SymPro (Treasury debt management software).

The FMS Department provided a job aid for the Security Request Form. The job aid indicated that either the transferring employee or a proxy could submit the Security Request Form to add or remove user access roles. The form requires two levels of departmental management approval, and is systematically routed to the FMS Department after the form is properly approved and the employee has successfully completed

required training. The FMS Department is responsible for reviewing and processing Security Request Forms. Based on conversations with FMS staff, the FMS Department relies on user departments to submit Security Request Forms when user access role changes are needed (e.g., departmental transfers, promotions, etc.). Documentation provided by FMS staff indicated that they perform an annual security review of PeopleSoft Financial roles. The following flowchart depicts the automated process.

Security User Access Roles Change Process



As noted in the following table, some procurements made by City departments must be approved by a department other than the procuring department. For example, the Information Technology Solutions Department is responsible for approving computer hardware, software, and any consulting services for which computer hardware and/or software are involved. The Property Management Department is responsible for approving City fleet purchases, maintenance, fueling, and auction services.

FORT WORTH®

Examples of Delegated Financial Authority

Authorization	Chief Procurement Officer (CPO)	Central Accounts Payable Supervisor and/or Coordinator	Dept. Head	Dept. Designee (Supervisor)	Senior Accountant or above	City Attorney	Fleet Services (Property Mgmt. Dept.)	ITS Dept.
Approve posting transactions and journal entries					X			
Approve departments pick-up of vendor paper checks, up to $25,000.00		X						
Approve requisitions, purchase orders, and invoices				X		X	X	X
Approve procurements of external legal services, city-wide						X		
Approve vehicles and equipment purchases, city-wide							X	
Approve software, hardware, and system management purchases, city-wide								X
Initial and second review of positive pay exception checks		X						
Proceed with emergency purchases under $50,000.00, with the concurrence of the CPO and the City's Attorney's Office	X		X			X		

Source: CFW Finance Directives, Administrative Regulations and Finance Policies and Procedures

FORT WORTH

Objectives

The objectives of this audit were to:

- determine whether delegated authority (for specific transactions) is made explicit regarding who has been granted specific authority, and by dollar threshold;
- determine whether delegated authority is appropriate;
- evaluate configuration of automated forms used to grant approval authority;
- ensure retention of authorizing records; and,
- determine whether transactions were approved as authorized.

Scope

Our audit included a review of delegated financial signing authority for procurement and journal entry transactions from October 1, 2019 through September 30, 2020. Activity beyond this period was reviewed as deemed necessary.

Since the Department of Internal Audit routinely conducts wire transfer and procurement card reviews, this audit did not include delegated financial signing authority related to wire transfers or procurement card transactions. Financial signing authority related to grants management, contract change orders, and travel expenses were also not reviewed, as the Department of Internal Audit has audited these processes within the past five years. Additionally, the Department of Internal Audit routinely follows up to determine corrective action taken by management.

Methodology

To achieve the audit objectives, the Department of Internal Audit performed the following:

- surveyed City departments regarding delegation of financial signing authority;
- interviewed FMS Department staff;
- reviewed applicable policies and procedures related to the delegation of financial signing authority (e.g., state purchasing regulations, the Fort Worth City Code, and Fort Worth city ordinances);
- reviewed and analyzed procurement requisitions, purchase orders, contracts, and vendor invoices;
- reviewed departmental organizational charts;
- determined authorized signers on City bank accounts;
- reviewed journal entry approvals; and,
- evaluated internal controls related to the delegation of financial signing authority.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we 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.

Chapter XXVIII of the Fort Worth City Charter established the City of Fort Worth's Department of Internal Audit independent of management, reporting directly to the Fort Worth City Council. We utilized the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework when evaluating internal controls. The following internal control components and corresponding principles were considered significant to the audit objectives. COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

Internal Control Component	Principles
Control Environment	Managerial oversight, integrity, ethics and responsibility; established organizational structure to achieve objectives; staff recruitment, development, retention, performance and accountability
Risk Assessment	Clearly-defined objectives to identify risks, define risk tolerances and respond to significant changes
Control Activities	Designed control activities, information systems and policies to achieve objectives and mitigate risks
Information and Communication	Communication of necessary quality information
Monitoring	Monitoring and evaluating the effectiveness of internal controls

Audit Results

Based on our test results, workflows (within PeopleSoft Financials) were configured to require appropriate approval of purchase requisitions, purchase orders, journal entries, etc. We concluded that user access role configurations were set up to help ensure that financial tasks were appropriate, taking into consideration applicable City policy and necessary internal controls. We saw no evidence that roles were configured to allow subordinate approval of a supervisor's transactions. Additionally, records evidencing proper delegated authority (e.g., Security Request Forms, interoffice memorandums, etc.) were properly retained.

We randomly selected contracts (42), purchase requisitions (42), purchases orders (42), non-purchase order procurements (30) and journal entries (25), and concluded that financial transactions were executed within the delegated authority. As required by City policy, purchases for legal services, information technology and fleet-related purchases, regardless of the procuring department, were routed to (and approved by) the City Attorney's Office, the Information Technology Solutions Department, and the Property Management Department, respectively.

City directives were explicit in reference to which positions were authorized to process and approve specific transactions. For example, City Finance Directives specify job titles that are responsible for processing or approving journal entries. Other than authorized procurement dollar limits mandated by the State of Texas (and incorporated into the City Code, and the City's Administrative Regulations and Finance Directives), CFW delegations of financial authority did not include dollar limits. Although this audit did not include a review of wire transfers or procurement card transactions, dollar limits were established within CFW wire transfer and procurement card policies.

Based on our audit results, user access granted to two employees (who transferred to other departments) was not updated in a timely manner. As a result, the employees had access to security roles that were unnecessary for their positions. We also identified nine employees who had access to multiple business units, or a business unit different from their current department. Another employee had access to approve purchase requisitions although approving requisitions was not a part of the employee's job duties.

While CFW Administrative Regulations, Finance Directives and departmental procedures document who should approve journal entries, some journal entry approval authority was contradictory. For example, delegated authority within the Journal Entry and Account Reconciliation Finance Directive (FD02) differed from what was within the FMS Department's procedures for manual journal entries. Furthermore, based on our testing results, a total of eight employees had security user access roles within PeopleSoft that allowed them to approve journal entries, although they were not Senior Accountants or above (one of the employees was a contractor) as required by the City's Financial Directive.

We also concluded that PeopleSoft Financials access rights, granted to employees, remained active after some individuals terminated their employment with the CFW. For example, purchasing, accounts payable and/or accounts receivable access (assigned to five former CFW employees) remained active from 39 to 101 days after the employees' termination dates. FMS staff indicated that their standard practice is to lock user access, when users are identified during monthly security reviews. However, FMS staff stated that a miscommunication within FMS (during the time that FMS began automating the process) resulted in taking longer than 30 days. Since the process is now automated, access to PeopleSoft Financials is reportedly locked the night employees are classified as "inactive" within the PeopleSoft Human Capital Management (HCM) module. We, therefore, did not include this issue as a reportable finding. However, it should be noted that the effectiveness of this automated process is dependent upon the timeliness in which PeopleSoft HCM is updated.

[redacted]

FORT WORTH®

Overall Risk Evaluation

High	Medium	Low
User access not changed after employees transferred to other City departments		
	Contradictory guidelines	

FORT WORTH

Detailed Audit Findings

1. PeopleSoft Financials user access roles were sometimes not effectively managed.

PeopleSoft security user access roles (assigned to 48 employees who transferred to another City department) were not effectively managed. We identified two instances where security user access roles were not updated or changed; and eight instances where employees were granted security user access roles beyond the authority needed to adequately perform their job duties.

- The two instances where PeopleSoft security user access roles were not updated or changed, applied to two employees who transferred to other departments. One employee transferred from the Planning and Data Analytics Department to the Transportation and Public Works (TPW) Department. Another employee transferred from the FMS Department to the Park and Recreation Department. Neither employee's PeopleSoft security user access roles (related to their former department assignments) were removed upon their job transfer.

  - Access provided to the former Planning and Data Analytics Department employee was removed approximately 14 months after the employee transferred to the TPW Department. The TPW Department submitted an automated Security Request Form to activate security user access roles that would be assigned to their new employee. Although the form is intended to auto-populate with all security user access roles assigned to the employee, the form did not auto-populate with the employee's finance-related security user access roles. The TPW Department had no knowledge of the employee's prior security user access roles, and was therefore unaware that some of the employee's security user access roles did not populate. FMS indicated that the finance-related security user access roles that did not populate were associated with access that was only applicable to the FMS and Planning and Data Analytics Departments. After Internal Audit's inquiry, FMS staff removed the employee's finance-related security user access roles applicable to the Data Analytics Department.

  - The other employee's finance-related security user access roles were removed approximately three months after the employee's job transfer. The Park and Recreation Department submitted a comment, within the automated Security Request Form, requesting that the employee's finance-related security user access roles be removed. However, since the Park and Recreation Department, reportedly, did not select the applicable boxes within the form, the employee's finance-related security user access was not removed. Upon Internal Audit inquiry, FMS removed the finance-related security user access roles granted to this employee.

Written policies did not specify who was responsible for ensuring that PeopleSoft security user access role changes (for employees who changed departments) were processed timely. For instance, written policy did not indicate whether the department *to which* the employee was transferring was responsible, or whether the department *from which* the employee was transferring was responsible. The written policy also did not specify a timeframe in which user access changes should be made. Additionally, departmental job transfers were not taken into consideration when automating the Security Request Form.

- In reference to the eight instances where employees were granted PeopleSoft security user access roles beyond the necessary authority:

  - two (2) of those employees had PeopleSoft access to multiple business units. FMS staff indicated that access to multiple business units is sometimes necessary for employees within the Purchasing

and Accounting Divisions. However, based on our test results, the two employees were not assigned to the Purchasing or Accounting Divisions.

- the remaining six employees had access to their previous (versus newly-assigned) department/business unit. FMS staff indicated that they plan on automating the PeopleSoft Financials business unit assignment process.

We also identified the following exceptions.

- One former employee was hired as a CFW contracted staffer, as an Accountant. However, the former employee/contracted staffer retained accountant and journal approval security user access roles, both of which allowed adding, editing, updating, and journal entry approval capabilities. Although this former employee/contracted staffer's access was approved by the two required levels of FMS management, FMS staff indicated that contracted staffers should not be authorized to approve journal entries. Internal Audit saw no evidence that the former employee/contracted staffer used their role to add, edit, update or approve journal entries.
- Seven employees (five Accountants, one Senior Account Technician and one Account Technician) had access to approve journal entries. However, City Finance Directive (FD02) limits journal entry approval to a designated Senior Accountant or above. Two of the seven employees (the Senior Account Technician and the Account Technician) also had access to the accountant security user access role, which allowed them to add, edit and update journal entries. Internal Audit saw no evidence that any of the seven employees added, edited, updated or approved journal entries during the audit period.

  FMS staff indicated that when the City first implemented PeopleSoft, the system was set up to automatically grant the journal approver role to FMS staff who were granted the Accountant role. Based on Internal Audit's inquiry, FMS staff indicated they are planning to eliminate the process of automatically granting the approver role to FMS accountants.
- Based on our review of People Financials access, one Information Technology Solutions (ITS) Department employee had buyer requisition approval access during our audit period. With buyer requisition approval access, the ITS employee, therefore, had the authority to approve purchase requisitions. It should be noted that the ITS employee's buyer requisition approval access was canceled upon notification by Internal Audit, and we saw no evidence that the employee used their user access role to approve purchase requisitions.

When PeopleSoft security user access roles are not managed properly, there is an increased risk of inappropriate transactions that could be processed, without detection. Section 9.1 of the City's Information Technology Security Administrative Regulation (AR-D5) states that IT Asset Owners are responsible for the initial establishment of the right of access, evaluation of authorized access when workforce responsibilities change, and timely termination of access for users ending their tenure at the City. Section 2.18 of AR-D5 defines IT Asset Owner as the person responsible for the protection and use of a specific IT asset.

Recommendation 1A: *The Chief Financial Officer should ensure that user access (granted to City employees) complies with City policy, and is based on least* privilege *(i.e., minimum level of access needed to perform job duties).*

Auditee's Response: Concur. In conjunction with IT (ERP), an automated system to remove unnecessary Business Units has already been developed and is being tested by Finance. This will ensure that employees will only have access to the Business Unit they work in, with the exception of some employees that require Citywide access to properly perform their job duties.

In addition, an automated process to remove the access to PeopleSoft for employees who leave the City has already been put in place. This automation and the account lockout will occur once the ePar is processed by HR to terminate the employee.

Target Implementation Date: December 31, 2021

Responsibility: Brad Cromer, Financial Systems Manager
Donlen Ruffin, Assistant IT Solutions Director

Applicable Department Heads: Reginald Zeno, Chief Financial Officer
Kevin Gunn, Chief Information Officer

Applicable Deputy City Managers: Jay Chapa and Valerie Washington

Recommendation 1B: *The Chief Financial Officer should ensure that user roles, that auto-populate within the automated Security Request Form, include all user access roles assigned to the employee.*

Auditee's Response: Concur. A new project has already been established with IT to make several enhancements to the automated Security Request Form, including this recommended change. In addition, all user roles will be removed in PeopleSoft when an employee changes positions or departments, and a new request form will be required to regain access.

Target Implementation Date: December 31, 2021

Responsibility: Brad Cromer, Financial Systems Manager
Mark DeBoer, Assistant IT Solutions Director
Donlen Ruffin, Assistant IT Solutions Director

Applicable Department Heads: Reginald Zeno, Chief Financial Officer
Kevin Gunn, Chief Information Officer

Applicable Deputy City Managers: Jay Chapa and Valerie Washington

Recommendation 1C: *The City Manager should either require that: 1) Department Heads of departments from which employees transferred, request termination of roles that were applicable to their departments, and that Department Heads of departments to which employees transferred, submit access requests for roles that are applicable to the employee's new job assignment/department; or 2) PeopleSoft Financials access be terminated after an employee transfers to a different City department, and reinstated based on the employee's new role.*

Auditee's Response: Concur. See response for recommendation 1B.

Target Implementation Date: December 31, 2021

Responsibility: Brad Cromer, Financial Systems Manager
Mark DeBoer, Assistant IT Solutions Director
Donlen Ruffin, Assistant IT Solutions Director

Applicable Department Heads: Reginald Zeno, Chief Financial Officer
Kevin Gunn, Chief Information Officer

Applicable Deputy City Managers: Jay Chapa and Valerie Washington

2. Policies regarding the delegation of authority, related to journal entry approvals, were contradictory.

Journal entry approval authority, noted within City of Fort Worth Finance Directives, differed from that noted within FMS Department policy. The specific Finance Directive that addressed journal entry approval had a FY2015 revision date, was approved by the City's Chief Financial Officer, and was made available to all City employees. FMS' departmental policy was limited to distribution within the FMS Department.

- Section V.C. of the City's Journal Entry and Account Reconciliation Finance Directive (FD02) states that all posting transactions and journal entries must be approved by a designated Senior Accountant or above.
- The City's procedures for manual journal entries, within the FMS Department, state that staff at the *accountant level and higher* are given access to enter, submit and approve journal entries; and only Senior Accountants and higher have access to post journal entries to the general ledger.

Although the policies were contradictory, we saw no evidence that anyone other than a Senior Accountant or an Accounting Services Supervisor approved journal entries during our audit period. However, contradictory policies and procedures increase the likelihood of inconsistency throughout the City, could lead to inefficient processes, and possibly non-compliance with established legal requirements, if applicable.

The Government Finance Officers Association's (GFOA) Best Practices indicate that financial policies are central to a strategic, long-term approach to financial management. GFOA also recommends systemic financial policy monitoring, review, and updates, as needed. FMS staff indicated they would update relevant policies/procedures.

Recommendation 2: *The Chief Financial Officer should ensure that Finance Directives and other written policies and procedures are consistent, and/or reviewed and updated to reflect current requirements and/or practices.*

Auditee's Response: Concur. Finance will work with IT to remove the automatic role assignments in PeopleSoft that caused these Finance Directives and policies to get out of alignment. Due to the internal processes within Finance, it is noted in the write-up of this audit that no users performed duties outside of their required job functions.

Target Implementation Date: December 31, 2021

Responsibility: Brad Cromer, Financial Systems Manager
Donlen Ruffin, Assistant IT Solutions Director

Applicable Department Heads: Reginald Zeno, Chief Financial Officer
Kevin Gunn, Chief Information Officer

Applicable Deputy City Managers: Jay Chapa and Valerie Washington

Acknowledgements

The Department of Internal Audit would like to thank all City departments for their cooperation and assistance during this audit.

Exhibit I – Security Request Form

Employee Information

Employee Name	Employee ID
User ID	Position (Job Code)
Email	Phone
Business Unit	Department
Current Position	Supervisor Name

Security Roles

Security Roles Requested

Application	Role Name	Description	Detailed Description	Required Training/Course	Required Training/Course 2

Assignment of Security Access for Roles Requiring Training

1. If training is needed, the Sr. IT Business Planner-ERP IT will provide training class information when the next class is scheduled.
2. Upon successful completion of training (if applicable), the Sr. IT Business Planners in FMS/Budget will assign the requested Roles.

Submission By Proxy

Submitting Employee's Name: Subitting Employee's ID: Submission Date:

Acknowledgement

☑ I attest that only roles needed to perform required job responsibilities have been selected.

Supervisor Approval

Supervisor Employee ID: Supervisor Approval Date:

Final Approver:

(Final Approver needs to be a manager level or higher)

Final Approval

Approver: Employee ID: Approval Date:

Security Role Assignments

Source: City of Fort Worth intranet