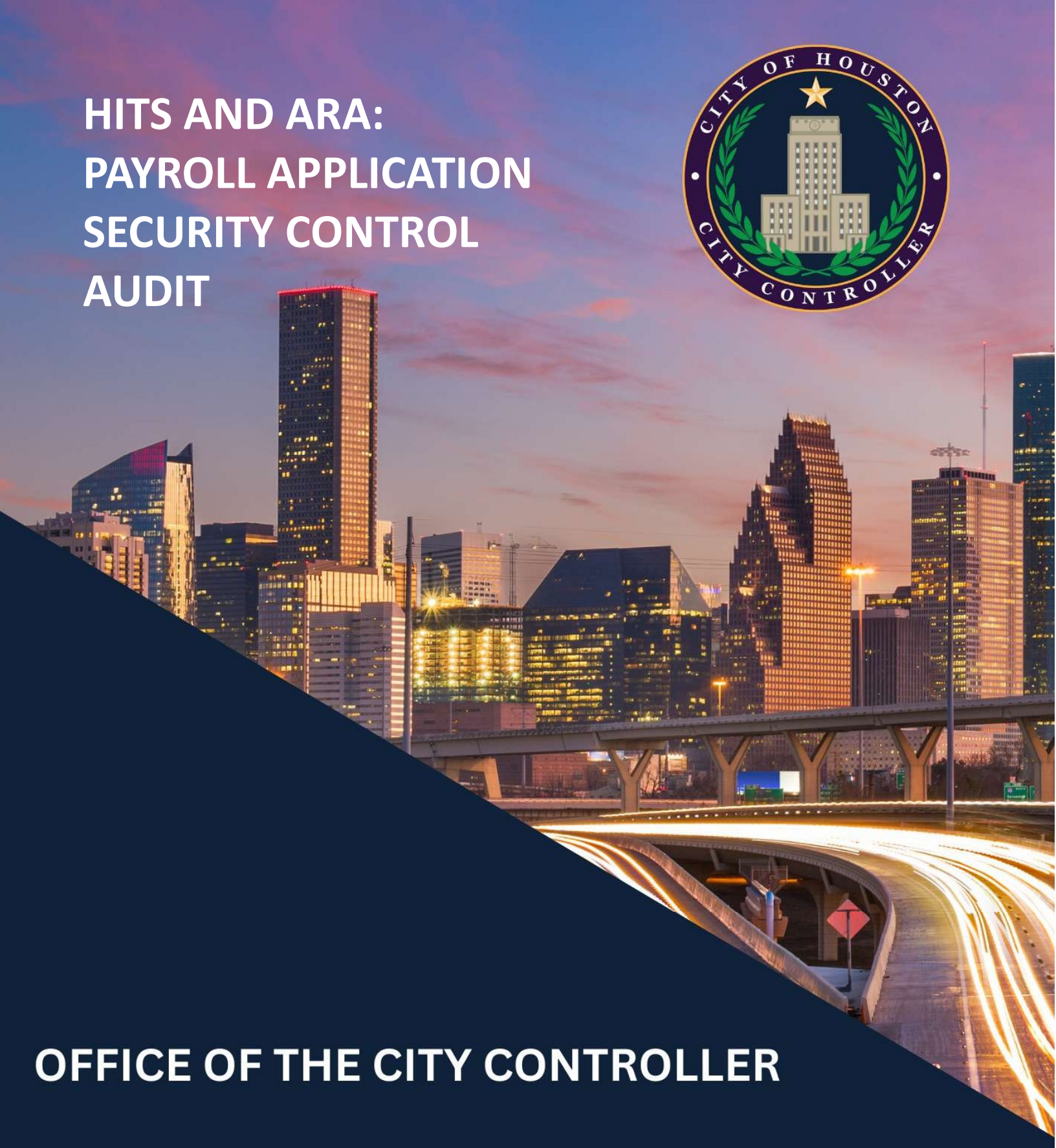
HITS AND ARA: PAYROLL APPLICATION SECURITY CONTROL AUDIT



OFFICE OF THE CITY CONTROLLER

CHRIS HOLLINS
CITY CONTROLLER

FY2026
Report #2026-07
April 14, 2026

CHRIS HOLLINS
City Controller

The Honorable John Whitmire, Mayor
City of Houston, Texas

SUBJECT: HITS AND ARA – PAYROLL APPLICATION SECURITY CONTROLS

The Audit Division has completed its review of the City of Houston's Payroll Application Security Controls, which are primarily administered by Houston Information Technology Services (HITS) and Administrative and Regulatory Affairs (ARA). To support this work, the Audit Division engaged Baker Tilly, LLP to conduct the performance audit.

The audit objectives were to assess whether user access to the payroll application is properly authorized, payroll payments are accurate and based on approved time and pay rates, and payments are issued to the correct employees. The audit covered Fiscal Year 2025.

The audit procedures resulted in seven (7) findings, which collectively represent significant internal control deficiencies warranting the attention of management and those charged with governance. These deficiencies relate primarily to payroll administration, SAP IT access, and approval processes. While some issues may be addressed through operational enhancements, others will require strengthened governance and, where appropriate, revisions to existing policies.

Key areas requiring improvement:

- Implement automated controls to ensure timesheets are approved by employees and supervisors prior to payroll processing.
- Enforce the requirement that all SAP access provisioning and modifications be supported by documented approvals before implementation.

We appreciate the time, effort, and cooperation of the HITS and ARA management and staff throughout this audit. Addressing the above areas will strengthen the overall management and control of payroll and IT related matters.

Respectfully submitted,

Chris Hollins
City Controller
City of Houston, Texas

xc: City Council Members

901 Bagby, 6th Floor • Houston, Texas 77002
Chris.Hollins@houstontx.gov

Dr. Cynthia Wilson, Chief of Staff, Mayor's Office
Tina Paez, Director, Administration and Regulatory Affairs
Lisa Kent, Director, Chief Information Officer
Kalpana Pillai, Deputy Chief Information Officer, Applications/PMO, HITS
Jane Wu, Deputy Director, Data Privacy and Business Operations Management, HITS
Karen Davidson, Deputy Director, Administration and Regulatory Affairs
Aubrey Hooper, Chief Administrative Officer, Office of the City Controller
Jennifer Pierce, Deputy Director, Audit Division, Office of the City Controller

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Baker Tilly, serving as City of Houston Internal Audit (IA) function, performed an audit of the Payroll Application Environment as part of its core IA activities for Fiscal Year (FY) 2025.

The primary objectives of this audit include determining whether current payroll application controls are adequate to:

- Ensuring user access to the payroll application is authorized based on job responsibilities
- Confirm payroll payments are accurate and reflect approved time and rate inputs
- Verify that payments are made to the appropriate employees.

The detailed report provides additional information regarding the audit scope and approach, risk ratings, identified strengths, and detailed findings, enhancement opportunities, and recommendations identified during this engagement.

The following table provides a summary of the findings, enhancement opportunities, and related recommendations identified during our engagement

Process area	Summarized finding or enhancement opportunity	Summarized recommendation	Risk or priority rating	Report reference
Kronos-SAP Payroll	Discrepancies in payroll hours reconciliation; manual errors	Automate reconciliation controls and enhance documentation standards	High	Finding #1
Timesheet Approval	No system-enforced requirement for timesheet approval prior to payroll processing	Reinforce approval requirements and implement control	High	Finding #2
Privileged SAP Profile Assignment	Unrestricted Dialog user assigned to privileged SAP profile	Regularly review privileged accounts and restrict interactive access	Medium	Finding #3
SAP Access Approval	Inconsistent documentation and enforcement of access approvals	Enforce documented approvals and implement workflow restrictions	Medium	Finding #4
SAP Access and Role Review	Insufficient documentation of access and role review process	Establish formal review and documentation processes	Medium	Finding #5
Password Policy	Outdated password policy	Update policy to include passphrases, MFA, and regular review	Low	Finding #6
Change Management Policy	Policy lacks evidence of periodic review	Implement recurring review cycle and revision history log	Low	Finding #7

Internal Audit used the following criteria to draw its overall conclusion regarding the internal control environment. Overall, we concluded that the processes and internal controls in place regarding the Payroll Application Environment are some improvements needed.

Overall Conclusion	Rating Description
Effective	Controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and business objectives should be met.
Some Improvement Needed	A few specific control weaknesses were noted; however, controls evaluated are generally adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Major Improvement Needed	Numerous control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives should be met
Unsatisfactory	Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and business objectives should be met.

CONCLUSION

Based on the results of our audit, Baker Tilly concludes that the City of Houston's Payroll Application Environment is generally adequate, but some improvement is needed. While key controls over payroll processing, user access, and change management are established and operating, the audit identified specific weaknesses such as inconsistent enforcement of access approvals, outdated password policies, and gaps in multi-level payroll approvals that should be addressed to further strengthen the control environment and provide greater assurance that payroll processes are secure, accurate, and compliant with City policy.

AUDIT REPORT

INTRODUCTION

Baker Tilly was engaged by the City of Houston Controller's Office to perform an internal audit of the City's Payroll Application Environment, with a focus on the SAP system. The objective of the audit was to assess the design and operating effectiveness of internal controls related to change management, user access provisioning and deprovisioning, payroll processing, and segregation of duties.

The engagement also included walkthroughs of key payroll processes and related system configurations to determine whether controls were in place to support data accuracy, authorization, and compliance with City policy.

We appreciate the cooperation and assistance provided by City of Houston personnel throughout the audit.

BACKGROUND

The City of Houston processes payroll for thousands of employees across numerous departments, including Public Works, Police, Fire, and Administrative Services. Payroll operations are centralized through the City's SAP system, which serves as the primary platform for managing entry time, employee data, wage calculation, garnishments, tax processing, and payroll disbursement.

The payroll process involves coordination between several functional groups, including Human Resources, department-level supervisors, and the Controller's Office. These teams are responsible for entering and reviewing employee information, approving time records, initiating payroll runs, and performing reconciliations.

Given the complexity of City operations and the large number of stakeholders involved, strong internal controls are necessary to safeguard payroll data, prevent unauthorized access, and ensure accurate, timely payments to employees. This includes controls over system access, segregation of duties, configuration changes, and audit logging within SAP.

AUDIT SCOPE AND OBJECTIVE

The scope of this performance audit was to evaluate the adequacy and effectiveness of payroll application security controls in place across the City of Houston's SAP environment. Specifically, the audit focused on controls designed to:

- Ensure user access to the payroll application is authorized based on job responsibilities
- Confirm payroll payments are accurate and reflect approved time and rate inputs
- Verify that payments are made to the appropriate employees.

Baker Tilly conducted audit fieldwork across three primary phases in collaboration with the Administration and Regulatory Affairs (ARA) Department and the Houston Information Technology Services (HITS) team. Activities included walkthroughs with City personnel, review of internal policies and procedures, testing of system configurations, and inspection of payroll processing documentation. The performance audit was conducted in accordance with the City Controller's Office requirements and the engagement objectives outlined in Contract No. 4600017134. Fieldwork was performed in 2025.

CONCLUSION

Each conclusion below aligns with the related audit objective. For detailed findings, recommendations, management responses, and assessment of those responses, see the "Detailed Findings, Recommendations, Management Responses, and Assessment of Responses" section of this report.

CONCLUSION #1 – (OBJECTIVE #1: ENSURE ACCESS IS AUTHORIZED)

Based on the procedures performed, it was concluded that user access controls within the payroll application require further strengthening. While formal access provisioning and termination processes exist, instances were noted where approval documentation or timely access removal was lacking. Opportunities also exist to enhance privileged access reviews and segregation of duties. (See Findings 1, 2, 3, 7)

CONCLUSION #2 – (OBJECTIVE #2: PAYMENTS ARE ACCURATE)

Audit procedures indicated that payroll payments were generally processed accurately and supported by timekeeping and pay rate documentation. However, certain manual processes—such as one-time payments and adjustments—would benefit from additional oversight and verification to improve accuracy. (See Findings 4, 5, 6)

CONCLUSION #3 – (OBJECTIVE #3: PAYMENTS ARE MADE TO THE APPROPRIATE PERSON)

The payroll system was found to appropriately align employee master data with payment processing. Nevertheless, enhanced automation and reconciliation controls would provide increased assurance that payments are issued solely to authorized and eligible individuals. (See Findings 4, 5, 6)

ACKNOWLEDGMENT

We would like to express our appreciation to the management of ARA and HITS for their cooperation and assistance throughout the engagement.

AUDIT TEAM

Baker Tilly, LLC
Deputy Director: Jennifer Pierce
Audit Manager: Olaniyi Oyedele, CPA
Quality Assurance: Mohammad Haroon, CPA

DETAILED FINDINGS

FINDING #1: INACCURATE KRONOS-SAP PAYROLL HOURS RECONCILIATION

Criteria	Administrative Policy (AP) 2-4 *Electronic Timekeeping Policy*. Section 6, Subsection 6.1.1
Finding(s)	The payroll system automatically pulls work hours from Kronos Workforce Management (WFM), and a reconciliation is performed to ensure hours are integrated correctly. However, testing identified eight (8) exceptions where payroll records did not accurately reflect work hours from Kronos and support could not be obtained for resolution of reconciliation issues. Discrepancies included mismatches in hours, missing reconciliation notes, and unresolved variances between SAP and Kronos records.
Background and Root Cause	SAP integrates with Kronos to retrieve employee work hours for payroll processing, with employees required to review and approve timesheets. Supervisors submit corrections for missed punches or unapproved leave, which are updated in both Kronos and SAP. Although an Audit Summary report is generated and reconciled to the Kronos Payroll Export Summary, the process is manual and tedious, especially when historical corrections are involved. The root cause of the exceptions is the lack of automation and comprehensive reconciliation controls, leading to unresolved discrepancies and manual errors in integrating and validating work hours.
Risk	**HIGH**
Recommendation(s)	Strengthen the reconciliation process between Kronos and SAP by implementing automated controls to flag and resolve discrepancies, including historical corrections. Enhance documentation standards for reconciliation activities and provide additional training to payroll representatives to ensure all variances are investigated and resolved with resolution documented before payroll processing.
Management Response(s)	We would like to note that in addition to Human Resources, department-level supervisors, and the Controller's Office mentioned in the Audit Report Background, HITS also plays a vital role in the automated controls built into the payroll system. ARA has been working with HITS since 2020 to identify the system changes needed to implement an improved, automated process for reconciling time batches from Kronos to SAP. In 2025, ARA and HITS hired consultants to accelerate this process. The current interface captures the current period time entries but does not include historical corrections, leading to extensive manual reconciliation that can take several hours to days to complete. Because the reconciliation process is manual, errors may occur. We are actively working with ERP and the consultant to create a report that will identify the time entries by department, employee, and time codes. We have plans to continue working with HITS to develop more automated controls specifically designed to strengthen the reconciliation process.
Owner(s)	Karen Davidson, CPP
Due Date	March 31, 2026

Assessment of Response	Management response is considered sufficient to address the finding noted.

FINDING #2: ABSENCE OF SYSTEM-ENFORCED TIMESHEET APPROVAL CONTROLS PRIOR TO PAYROLL PROCESSING

Criteria	Administrative Policy (AP) 2-4 Electronic Timekeeping Policy. Sections 5.15, 5.21, Section 6, Subsection 6.21.
Finding(s)	There is no system-enforced requirement mandating either employee or supervisor approval of timesheets prior to payroll submission. While review and approval are encouraged and may be practiced in some departments, the process is not consistently enforced across the organization, allowing payroll to be processed without formal employee or supervisor sign-off.
Background and Root Cause	The payroll system lacks automated controls or policies requiring timesheet approval by employees and supervisors before payroll processing. This results in inconsistent review practices across departments and increases the risk of payroll errors due to unreviewed or unapproved timecards.
Risk	**HIGH**
Recommendation(s)	Implement system-enforced controls that require both employee and supervisor approval of timesheets prior to payroll submission. Standardize procedures across all departments and establish periodic compliance monitoring to ensure consistent review and approval practices.
Management Response(s)	ARA currently distributes bimonthly reports to all department directors, highlighting supervisors and managers who repeatedly fail to approve their direct reports' timecards, with the intent that the Department Directors take action to mitigate missed approvals. We have also changed our biweekly notices to employees and supervisors to explain the importance of timecard review and approval, as well as the fact that this review and approval is mandatory. As a result of this audit, we plan to engage HR and Legal to discuss accountability practices that can be incorporated into the City's time and attendance policies, including what disciplinary actions that can be enforced against supervisors, managers, and even Department Directors when repeated failure occurs. However, we have a group of employees (field workers) who do not have access to a computer or device to review and approve their timecards. We will work with HR and HITS to find a way for all timecard approvers to have an appropriate method for review and approval of timecards before an escalation and disciplinary feature is built into the City policies.
Owner(s)	Karen Davidson, CPP
Due Date	March 31, 2026
Assessment of Response	Management response is considered sufficient to address the finding noted.

FINDING #3: UNRESTRICTED DIALOG USER ASSIGNED TO PRIVILEGED SAP PROFILE

Criteria	Administrative Policy (AP) 8-1 *Acceptable Use of City Data.* Section 6.3.
Finding(s)	During testing, it was identified that while most accounts assigned to high-risk SAP profiles (SAP_ALL and SAP_NEW) were appropriately restricted to non-interactive System or Service users, one account (DDIC) assigned to SAP_NEW was configured as a Dialog user, was not locked, and was valid through 03/24/2025. Dialog users permit interactive login, and such access to privileged profiles may pose a risk if not properly justified or restricted.
Background and Root Cause	Administrative access to SAP is intended to be restricted to authorized personnel, with privileged profiles such as SAP_ALL and SAP_NEW tightly controlled. The ERP team maintains these restrictions primarily for non-interactive accounts used for automated processing. However, the presence of an unlocked Dialog user (DDIC) with access to SAP_NEW indicates a lapse in the enforcement of access controls for privileged profiles. The root cause is the lack of a formal process to routinely review and validate the necessity and status of interactive accounts assigned to high-risk profiles, resulting in potential exposure to unauthorized or unnecessary access.
Risk	**MEDIUM**
Recommendation(s)	Implement a formal review process to regularly assess all accounts assigned to privileged SAP profiles, ensuring that interactive (Dialog) users are locked if unused or have documented business justification for access. Periodically validate account status and restrict privileged profile assignments to only those accounts where access is necessary and properly authorized.
Management Response(s)	ERP Management acknowledges the audit findings and agrees with the recommendation to strengthen controls over privileged SAP access, particularly for interactive (Dialog) users assigned to high-risk profiles such as SAP_ALL and SAP_NEW. Actions Already Taken • **Event-Based Enablement of Privileged Accounts:** The DDIC account and other privileged technical users are only enabled during approved upgrade or maintenance activities (e.g., HRSP upgrades). These accounts are not enabled for day-to-day operations and are disabled upon completion of the activity, limiting exposure to defined, time-bound events. • **Post-Upgrade Deactivation:** The DDIC account was enabled as part of the HRSP upgrade process and was not available after the upgrade activities concluded. A process changes to

	lock the DDIC is made in the upgrade documentation and was followed during 12/12/2025 Annual HRSP upgrade. • **Continuous Security Monitoring:** All privileged technical accounts, including DDIC, are logged and monitored via the SAP Security Audit Log (SM19) whenever enabled, ensuring full traceability of access and activity. • **Increased Review Frequency:** ERP Management has enhanced oversight by moving privileged user reviews from a monthly cadence to a weekly review, allowing for more timely validation of account status and configuration.
Owner(s)	Siva Tanuku, Assistant Director, IT Applications Jane Wu, Deputy Director, Data Privacy & Business Operations Management, HITS
Due Date	November 1, 2025
Assessment of Response	Management response is considered sufficient to address the finding noted.

FINDING #4: INCONSISTENT DOCUMENTATION AND ENFORCEMENT OF SAP ACCESS APPROVAL PROCESSES

Criteria	Department Policy (DP) HITS Access Control Policy.
Finding(s)	SAP access provisioning and modification processes are not consistently supported by documented approvals. An instance was identified where access was granted based solely on verbal authorization, and where access modifications were executed without attached approval documentation. • In 1 of 5 cases, access was granted based on verbal approval, with no ServiceNow request ticket retained to support the decision.
Background and Root Cause	The established procedures for SAP access provisioning and modification require documented business justification and approval, but these controls are not consistently enforced. This is due to insufficient oversight of the approval workflow and a lack of validation controls within the ticketing system.
Risk	**MEDIUM**
Recommendation(s)	Enforce the policy that all SAP access provisioning and modifications must be supported by documented approvals prior to implementation. Implement workflow restrictions or automated validation checks in the ticketing system to prevent actions from proceeding without attached approval documentation and ensure all access requests are recorded for audit purposes.
Management Response(s)	ERP Management acknowledges the audit findings and agrees that all SAP access provisioning and modification activities must be supported by documented business justification and formal approval prior to implementation. Clarification of Exception Identified The instance cited in this finding involved the onboarding of an ERP team's consultant requiring time-sensitive system access. While verbal approval was provided by the ERP Technical Manager and a ServiceNow ticket was created, the approval documentation was not attached to the ticket prior to access being provisioned. ERP Management acknowledges that verbal approval alone does not meet policy requirements. Actions Already Taken • **Reinforcement of Documentation Requirements:** ERP leadership has reinforced with all access administrators that verbal approvals are not sufficient and that access must not be provisioned or modified without documented approval attached to the ServiceNow request. • **Centralized Ticket Requirement:**

	All SAP access requests and modifications are required to be initiated and retained within ServiceNow to ensure auditability and traceability. These actions will strengthen governance over SAP access provisioning, eliminate reliance on verbal approvals, and ensure consistent enforcement of documented authorization requirements in alignment with City policy.
Owner(s)	Siva Tanuku, Assistant Director, IT Applications Jane Wu, Deputy Director, Data Privacy & Business Operations Management, HITS
Due Date	November 1, 2025
Assessment of Response	Management response is considered sufficient to address the finding noted.

FINDING #5: INSUFFICIENT DOCUMENTATION OF SAP ACCESS AND ROLE REVIEW PROCESSES

Criteria	Administrative Policy (AP) 8-1, Acceptable Use of City Data. Section 6.1.
Finding(s)	Documentation and tracking of SAP user access reviews and role profile assessments are insufficient. The IT user access review process lacks user-specific details and formal tracking, and role profile reviews are not separately documented or scheduled
Background and Root Cause	The absence of a formal tracking mechanism and comprehensive documentation standards within the ERP team results in insufficient evidence to validate the effectiveness of user access and role review processes. Reviews are often performed ad hoc and are not independently evidenced apart from general user access reviews.
Risk	**MEDIUM**
Recommendation(s)	Establish formal processes for conducting and documenting SAP user access reviews and role profile assessments. Maintain comprehensive documentation of review decisions, removal actions, and supporting evidence, and provide training on documentation standards to ensure all review activities are fully documented and retained for audit purposes.
Management Response(s)	ERP Management acknowledges the audit findings and agrees that user access reviews and role profile assessments must be supported by formal tracking and comprehensive documentation to demonstrate effectiveness and auditability. **Current Controls in Place** The ERP team performs weekly, monthly, and quarterly SAP security reviews using established checklists that have been developed and refined over time to support changing business processes and prior audit recommendations. These reviews include coordination with City departments and formal signoff for user access where applicable. **Identified Gap** While these reviews are performed regularly, ERP Management acknowledges that documentation and tracking were not consistently centralized or structured in a manner that clearly distinguishes: • User-specific access review evidence • Role profile review activities • Review decisions and resulting actions Actions Already Taken • **Centralized Documentation Awareness:**

	ERP Management has begun centralizing security review artifacts in a dedicated SharePoint location to improve retention, accessibility, and audit support, in addition to existing email-based approvals and communications. • **Defined Repository for Security Reviews:** A centralized SharePoint repository has been designated for storing SAP security review documentation, including access review evidence, signoffs, and related artifacts. • **Scheduled Review Cadence:** Reviews are formally scheduled in the team calendar and documented independent of user access reviews to ensure complete coverage and traceability. **Planned Process Improvements** To address the documentation and tracking gaps identified in this finding, ERP Management is implementing the following improvements: • **Automation:** ERP team members involved in SAP security reviews will be automating the reports needed for the reviews, The reviews will be triggered within the SAP system automatically removing the need to trigger the process. • **Formalized Review Tracking:** User access reviews and role profile assessments will be documented as separate, clearly identifiable review activities, each with defined review frequency, scope, and evidence requirements. This removes the need for security teams to depend on a single resource to run these reviews. These actions will ensure SAP security reviews are repeatable, fully evidenced, centrally tracked, and retained, aligning with City policy and strengthening governance over user and role access management.
Owner(s)	Siva Tanuku, Assistant Director, IT Applications Jane Wu, Deputy Director, Data Privacy & Business Operations Management, HITS
Due Date	April 30, 2026
Assessment of Response	Management response is considered sufficient to address the finding noted.

.

FINDING #6: OUTDATED PASSWORD POLICY

Criteria	Administrative Policy (AP) 8-4 *Password Policy*.
Finding(s)	The SAP system at the City of Houston enforces password security controls that align with the City's documented policy; however, the current password policy has not been reviewed or updated since 2012 and does not reflect modern cybersecurity guidance, as industry practices now emphasize stronger authentication methods such as passphrases and multi-factor authentication rather than traditional complexity rules.
Background and Root Cause	The City of Houston's SAP system enforces password security controls in accordance with the documented password policy, which was last reviewed and updated in 2012. Although system configurations align with this policy, the policy itself has not kept pace with evolving cybersecurity standards and industry's best practices. The root cause of this issue is the lack of a formal process for periodic review and update of the password policy to ensure it reflects current guidance, such as the adoption of passphrases and integration with multi-factor authentication.
Risk	**LOW**
Recommendation(s)	Update the City's password policy to reflect current cybersecurity best practices by incorporating guidance on passphrase usage, integrating multi-factor authentication (MFA) where applicable, and establishing a regular review cadence (such as annually). This will ensure the policy remains aligned with both system configurations and evolving security standards.
Management Response(s)	Management acknowledges the audit findings and recognizes the importance of maintaining up to date polices to ensure compliance and safeguard organizational assets. We agree with the recommendation to update the City's password policy to reflect current cybersecurity best practices and perform policy reviews regularly. **Planned Process Improvements** To address this, we plan to implement a process to regularly review and update this policy to ensure that it remains current and effective. This review will be conducted on a scheduled basis and will incorporate industry standards and regulatory requirements as applicable.
Owner(s)	Chris Mitchell, Chief Information Security Officer, HITS Jane Wu, Deputy Director, Data Privacy & Business Operations Management, HITS
Due Date	June 30, 2027

Assessment of Response	Management response is considered sufficient to address the finding noted.

.

FINDING #7: LACK OF PERIODIC REVIEW OF CHANGE MANAGEMENT POLICY

Criteria	HITS Change Management Process
Finding(s)	The City of Houston has a documented Change Management Policy that defines objectives and outlines procedures for planning, testing, approving, and implementing changes. It includes requirements for documentation, CAB involvement, and maintenance windows. However, the policy lacks evidence of a formal review cadence or an approval and revision history. Metadata and content review did not indicate regular oversight or re-approval by responsible personnel.
Background and Root Cause	The City of Houston's Change Management Policy provides a structured framework for managing IT changes, covering planning, testing, approvals, documentation, and CAB involvement. However, the policy does not include a formal review schedule or documented approval and revision history. This lack of oversight indicates that the policy may not be regularly evaluated or updated by accountable personnel. The root cause is a governance gap in policy lifecycle management, specifically in maintaining responsibility for periodic reviews and formal approvals.
Risk	**LOW**
Recommendation(s)	The City should implement and enforce a recurring review cycle, such as annually or biannually for the Change Management Policy to ensure it remains current and effective. Additionally, the policy should incorporate a revision history log that records review dates, approving authorities, and descriptions of changes made. This will enhance transparency, support governance oversight, and demonstrate accountability in policy maintenance.
Management Response(s)	Management acknowledges the audit findings that our current management process lacks a formal documented departmental policy. However, at present, we do have change management processes that follow industry standards and that follow ITIL practices, including but are not limited to activities that are regularly scheduled and conducted where changes are reviewed and approved. Furthermore, changes are documented in our industry's standard change management system. To address this, we plan to develop and implement a formal Change Management departmental policy that includes: • A defined review cycle to ensure the policy remains current and effective; and • A documented approval process and revision history for the policy. This initiative will align our practices with industry standards and provide clear governance for changing management activities moving forward.

Owner(s)	Bert Quarfordt, Deputy Chief Information Officer, IT Infrastructure, HITS Jane Wu, Deputy Director, Data Privacy & Business Operations Management, HITS
Due Date	June 30, 2027
Assessment of Response	Management response is considered sufficient to address the finding noted.

MANAGEMENT ACKNOWLEDGMENT STATEMENT (HITS)

April 8, 2026

Chris Hollins
City Controller
Office of the City Controller

SUBJECT: PAYROLL APPLICATION SECURITY CONTROLS AUDIT – ACKNOWLEDGMENT OF MANAGEMENT RESPONSES

Management acknowledges responsibility for the operations, processes, and internal controls within the Houston Information Technology Services (HITS). Management confirms that it has reviewed the audit report and the associated findings and recommendations.

Management's responses included in this report reflect its position regarding each finding, including agreement or disagreement, and outline planned corrective actions where applicable. Management is responsible for the timely and effective implementation of agreed-upon corrective actions as noted in their management response(s) and for addressing identified issues within the stated timeframes.

Management understands that this report, including its responses, will be finalized and published on the Controller's website.

Sincerely,

DocuSigned by:
44FF0FE8CC97401...

HITS offers clarification that Finding #1 requires a pre-requisite task by business owner (ARA/Payroll) to define and prioritize needed control(s), followed by HITS implementation of technical system modifications. Therefore, Finding #1 bears shared responsibility.

Lisa Kent, CIO
HITS

MANAGEMENT ACKNOWLEDGMENT STATEMENT (ARA)

April 13, 2026

Chris Hollins
City Controller
Office of the City Controller

SUBJECT: PAYROLL APPLICATION SECURITY CONTROLS AUDIT – ACKNOWLEDGMENT OF MANAGEMENT RESPONSES

Management acknowledges responsibility for the operations, processes, and internal controls within the Administration and Regulatory Affairs (ARA). Management confirms that it has reviewed the audit report and the associated findings and recommendations.

Management's responses included in this report reflect its position regarding each finding, including agreement or disagreement, and outline planned corrective actions where applicable. Management is responsible for the timely and effective implementation of agreed-upon corrective actions as noted in their management response(s) and for addressing identified issues within the stated timeframes.

Management understands that this report, including its responses, will be finalized and published on the Controller's website.

Sincerely,

Tina Paez, Director
Administration & Regulatory Affairs

APPENDIX 1: OBSERVATIONS

Observations are matters of concern that do not rise to the level of findings but are nonetheless appropriate to bring to the attention of management and those charged with governance.

No such observations were identified during the audit.

APPENDIX 2: INTERNAL CONTROLS

Internal controls are processes established by management to provide reasonable (not absolute) assurance that the organization's objectives will be achieved. Our work included procedures to identify the internal controls that were significant to the objectives of this audit and to determine the effectiveness of those controls. A deficiency in design exists when (a) the control is missing entirely or (b) the control is in place but is not properly designed. A deficiency in operation exists when (a) the control is properly designed but does not *operate* as designed or (b) the person performing the control does not possess the necessary competence to perform the control effectively.

We identified three (3) design deficiencies and four (4) operational deficiencies. In total, 21 of the 24 controls (88%) were appropriately designed, while 20 (83%) were operating as intended. These results indicate control gaps that heighten the risk of unauthorized access and approval of payroll transactions.

The City's payroll application key controls were categorized as follows:

- **Policies and Procedures**
  - Controls around the establishment of policies and procedures to guide operations
  - Controls around the renewal and update of policies and procedures Controls to separate the functions of requesting, approving, usage, and monitoring of fuel cards.
- **Authorization and Approval**
  - Controls over payroll entries, review and approval
  - Controls over payroll runs and batches authorization and approval
- **Access**
  - Controls over IT/SAP access
  - Control over user group role, profile and configuration
  - Controls over password and password renewal
  - Controls over admin access privileges and restrictions on authorized personnel
- **Segregation of Duties**
  - Controls to separate the functions of payroll data entry, review, authorization and approval
- **Reconciliation**
  - Controls that restrict card use to authorized personnel and ensure transactions are appropriate and compliant with policy.
- **Training**
  - Controls over payroll reconciliation

The scope of our work did not constitute an evaluation of the overall internal control structure of the city or that of ARA and HITS. Management is responsible for establishing and maintaining a system of internal controls to ensure City assets are safeguarded, financial activity is accurately reported and reliable, and management and employees are following laws, regulations, policies, and procedures. The objectives are to provide management with reasonable, but not absolute assurance that the controls are in place and effective.

APPENDIX 3: PROCEDURES AND STANDARDS

AUDIT PROCEDURES PERFORMED

In order to obtain sufficient evidence to achieve engagement objectives and support our conclusions, Baker Tilly took the following steps:

PLANNING

- Conducted kickoff meeting with the City Controller's Office, ARA, and HITS personnel
- Developed and submitted an initial data request to obtain payroll policies, system access procedures, and change management documentation related to SAP
- Reviewed payroll processing policies, system architecture diagrams, and access control documentation to gain an understanding of current processes and key controls
- Conducted interviews and walkthroughs with key personnel in ARA (payroll operations) and HITS (SAP security and change management)
- Identified key risks related to payroll accuracy, user access provisioning, change management, and segregation of duties
- Evaluated the design of controls intended to prevent unauthorized access and support accurate payroll processing
- Refined audit work plan and developed testing procedures based on walkthrough results

FIELDWORK

- Performed testing of key controls and system configurations to verify:
    - User access is properly requested, reviewed, and approved prior to provisioning
    - Access is revoked upon termination or role change
    - Payroll transactions are supported by approved time entries and applicable pay rates
    - Changes to SAP configurations follow documented change management processes, including testing and approval
- Conducted sample-based testing over payroll batches and system access reports
- Assessed segregation of duties between payroll processing and approval functions
- Documented audit findings and reviewed them with process owners

REPORTING

- Prepared a draft report summarizing testing results, conclusions, and recommendations for process improvements

Held a closing meeting with key stakeholders to validate findings and obtain management responses.

AUDIT STANDARDS

Baker Tilly conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.