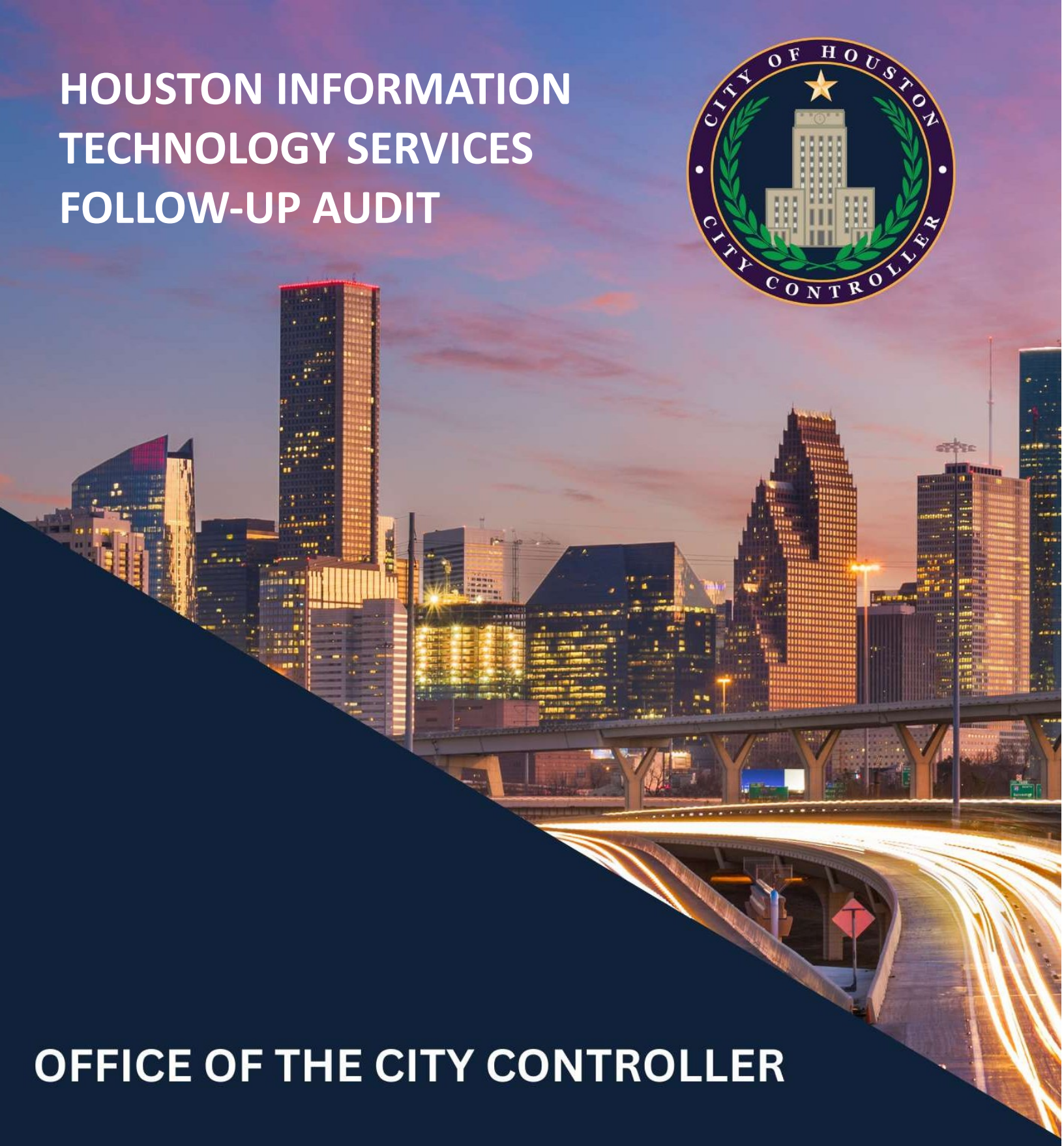
HOUSTON INFORMATION TECHNOLOGY SERVICES FOLLOW-UP AUDIT



OFFICE OF THE CITY CONTROLLER

CHRIS HOLLINS
CITY CONTROLLER

FY2027
Report #2027-05
October 30, 2026

CHRIS HOLLINS
City Controller

The Honorable John Whitmire, Mayor
City of Houston, Texas

SUBJECT: HOUSTON INFORMATION TECHNOLOGY SERVICES FOLLOW-UP AUDIT REPORT

We have completed follow-up procedures on remediation efforts carried out by the Houston Information Technology Services Department management relating to the following audit reports:

REPORT NUMBER	REPORT TITLE	TOTAL FINDINGS
2012-12	Information Technology Department Enterprise Resources Planning (SAP) Security	8
2018-09	Houston Information Technology Services Cloud Governance Performance Audit	8
2018-11	Houston Information Technology Services Information Technology Processes Performance Audit	6

Based on the follow-up procedures outlined in this report, and in accordance with professional auditing standards, we obtained sufficient and appropriate evidence to support the conclusions presented in Appendix 1.

FINDINGS[#]	FINDING REMEDIATION STATUS	DESCRIPTION
9	**Fully Implemented**	Successful implementation of processes to address the audit finding.
5	**Partially Implemented**	Significant efforts and implementation of processes to address the audit finding.
6	**Incomplete/ Ongoing**	Ongoing development of a process and/or efforts toward a policy to address the audit finding.

[#] Two (2) of the 22 findings were considered fully remediated in a prior audit report and not included in these follow-up audit procedures.

This assessment reinforces our commitment to conducting thorough and objective audits, ensuring that identified issues have been properly addressed, and corrective actions have been effectively implemented.

We would like to thank the management and staff of the Houston Information Technology Services Department for their cooperation during the follow-up audit process.

Respectfully submitted,



Chris Hollins
City Controller
City of Houston, Texas

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

xc: City Council Members
Dr. Cynthia Wilson, Chief of Staff, Mayor's Office
Kevin Berry, Director, Houston Information Technology Services
Aubrey Hooper, Chief Administrative Officer, Office of the City Controller
Jennifer Pierce, Deputy Director, Audit Division Office of the City Controller

TABLE OF CONTENTS

Follow-Up Audit 5
Summary 5
Audit Objectives 5
Scope 5
Conclusions 5
Objective 1: Status of Open Findings 5
Objective 2: Remediation Assessment 5
Acknowledgment 6
Audit Team 6
Appendix 1: Detailed Remediation Assessment 7
Appendix 2: Follow-Up Audit Plan 25
Audit Objectives 25
Procedures Performed 25
Audit Approach 25
Management Status Updates 25
Audit Testing / Verification 25
Auditing Standards 26
Government Auditing Standards (Yellow Book) 26
Global Internal Audit Standards (Red Book) 26

FOLLOW-UP AUDIT

SUMMARY

The Audit Division is tasked with providing independent and objective assurance services to enhance organizational performance, ensure compliance, and safeguard assets. As part of this mandate, follow-up audits are conducted to verify that corrective actions have been implemented for issues identified in prior audits.

This follow-up audit evaluates the remediation efforts carried out by Houston Information Technology Services (HITS) Department's management in response to the findings from the Audit Report:

- Information Technology Department Enterprise Resources Planning (SAP) Security (2012-12)
- Houston Information Technology Services Cloud Governance Performance Audit (2018-09)
- Houston Information Technology Services Information Technology Processes Performance Audit (2018-11)

The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Government Accountability Office (GAO) and the Global Internal Audit Standards as established by the Institute of Internal Auditors (IIA).

AUDIT OBJECTIVES

The follow-up audit was conducted to:

- Determine the status of the 22 open findings from Audit Report #2012-12, 2018-09, and #2018-11.
- Evaluate the adequacy of management's remediation processes to address the findings.

SCOPE

The scope of the audit included:

- Audit Report #2012-12 had eight (8) findings, two (2) of which were considered fully remediated in a prior audit report and not included in these audit procedures.
- Audit Report #2018-09 had eight (8) findings.
- Audit Report #2018-11 had six (6) findings.

CONCLUSIONS

OBJECTIVE 1: STATUS OF OPEN FINDINGS

Management provided status updates related to all 20 open findings.

OBJECTIVE 2: REMEDIATION ASSESSMENT

Management's remediation efforts were adequate for Nine (9) audit findings and 11 findings remain open. See Appendix 1: Detailed Remediation Assessment for details.

Findings[a]	Finding Remediation Status	Description
9	Fully Implemented	Successful implementation of processes to address the audit finding.
5	Partially Implemented	Significant efforts and implementation of processes to address the audit finding.
6	Incomplete/ Ongoing	Ongoing development of a process and/or efforts toward a policy to address the audit finding.

ACKNOWLEDGMENT

We extend our appreciation to the management of the Houston Information Technology Services Department for its cooperation and commitment to addressing the audit findings. Their efforts facilitated a thorough and effective follow-up audit process.

AUDIT TEAM

Deputy Director: Jennifer Pierce
Audit Manager: Ola Oyedele, CPA
Lead Auditor: Samuel Ojo
Quality Assurance: Mohammad Haroon, CPA, CIA

APPENDIX 1: DETAILED REMEDIATION ASSESSMENT

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
1	**Lack of Internal Controls for Superuser SAP System Logon**	**Recommendation** We recommend the powerful profiles SAP_ALL and SAP_New be removed from the SAP* User and that ERP management establish periodic monitoring of audit logs for its use. ERP management should also require management's approval and written logs of its assignment to users just as they do with FIREIDs. **Management Response** **June 2012** The ERP security team keeps control and monitors any usage of the SAP* id. This id is kept locked at all times as shown by the system logs. It has been approved for use by ERP management only twice since the initial SAP implementation for upgrade migrations. Only the ERP security team and the Basis firefighter id have access to delete this user within SAP. The system parameter "logon/no_automatic_user_sapstar" is used in our systems to further protect the usage of the SAP* id. The verification of this parameter is included in the Security monthly review process where thirty-three security parameters are verified to be following our approved baseline parameter values. This monthly review process documentation was provided to the internal audit team. The use and protection of the SAP* id was also shown and reviewed by the external auditors during their yearly security audit and was not cited as an issue during all the audits completed since implementation. We do agree with your finding on the importance of data in the Sandbox systems. Although this is a sandbox system and is continually modified, open for configuration and testing, and refreshed, we have asked and re-emphasized to the basis team to ensure all parameters and security are reinstated after any refresh or change due to testing. We have also included the Sandbox system in our production monthly security review for verification of security parameters and a formal step for reviewing the SAP* user Id. Since we do not use the SAP* user id and it remains locked we do not have an issue with removing any system profiles. **May 2013** Actions Taken: We have included the sandbox system in our monthly review process for sensitive ids such as SAP* and logon parameters. We removed 'SAP_ALL' and 'SAP_NEW' profiles from the SAP* ID. **August 2015** We continue to monitor the systems which include Sandbox.	Audit Division obtained evidence to support that management implemented the corrective action governing the SAP* privileged account. The SU01 user maintenance screens and RSUSR003 reports demonstrate that the SAP* account remains configured in a locked status across the reviewed SAP environments since 2021, is assigned to the SUPER authorization group, and contains no authorization roles or authorization profiles. The RSPFPAR_LOGIN configuration report further demonstrates that the logon/no_automatic_user_sapstar profile parameter is configured to prevent automatic activation of the SAP* account. In addition, recurring SAP security parameter review documentation demonstrates that this preventive configuration forms part of management's routine SAP security administration. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		August 2022 The SAP* id continues to be disabled in all systems and is controlled by SAP best practices. The SAP* id has the following controls in all systems. 1) The system parameter, logon/no_automatic_user_sapstar, is used to prevent the id from being used. When this parameter is set it prevents the usage of the SAP* id. 2) The SAP* user id is also locked in the system, and the password is changed from the default. This is verified during our monthly security review process and after any system refresh via transactions RSPFPAR_LOGIN and RSUSR003. No record of the password is maintained and is randomly generated and saved when the SAP* id is locked. Only the ERP Security and Basis Team have the ability to change the system parameter or unlock the id.		
2	**Lack of Internal Controls for Firefighter and Super User IDs**	**Recommendation** We recommend that the assignment of all super user IDs, e.g. SAP* and SOLMAN_ADMIN, be approved and logged as the FIREIDs are. ERP Management should produce and review audit logs of Super User-ID usage in SAP while assigned to staff. Although Firefighter logs are run and stored each month ERP Management should establish a review process for these logs. **Management Response** **June 2012** The ERP Security team adheres to the Firefighter procedures approved by ERP Management. This procedure includes that all firefighter ids must be approved by ERP management, upon approval be assigned to only the individual making the request and be logged. We believe that this process is being adhered to and proper justification is being provided to ERP management before approval. All requests must state the reason for the request. This is documented in the emails provided to the internal audit team showing the request and approval. In addition, the approval of a firefighter id almost always is discussed with the ERP Director and/or ERP Technical Manager on the reason and approach for the production fix. In regard to the findings; Firefighter and Superuser IDs were used to reset personal user-ID and superuser passwords without detection. This indicates that ERP Management had no formal documented process for reviewing firefighter audit logs to oversee their appropriate usage while assigned to ERP staff.	Audit Division obtained evidence demonstrating that management implemented portions of the original recommendation. Firefighter access requests are processed through a standardized workflow requiring documented business justification, management approval, access provisioning, and request closure. Management also established an Emergency Access Policy and procedures governing Firefighter access. In addition, SAP security logs demonstrated that privileged-user activity is recorded and available for review. However, evidence was not provided demonstrating that all Super User IDs are subject to the same documented approval and governance requirements as Firefighter IDs. Evidence was also not provided, demonstrating that management regularly reviewed and documented its review of Firefighter and Super User activity logs. The finding will remain open with status of "Partially Implemented" until management provides evidence that all Super User IDs are subject to documented approval and governance requirements and that Firefighter and Super User activity logs are regularly reviewed and documented.	**Partially Implemented**

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		We do concur that one ERP team member used a Firefighter id and super user id to reset their own password and/or unlock their own account after locking themselves from too many incorrect login attempts to their own account. This was done during the time period when they were approved for using the firefighter id or super userid. Although the access was only used to reset their own password or unlock their own account we have spoken with the individual to reiterate our firefighter policy as well as procedures for resetting passwords. Also, we will re-disseminate the policy to all ERP team members. ERP does review firefighter logs and will continue to review the logs accordingly. We will also log all super user ids as firefighter ids going forward. The review of the logs will be included in our policies to be drafted. (see ERP response for Finding #6). **May 2013** Actions Taken: ERP management discussed the usage of Firefighter ids with all ERP members. All firefighter requests follow a standard email template when request is initiated. The firefighter id that is assigned is the requester is logged and management is notified of which it was assigned via email. Firefighter logs are exported from the system as backup and are reviewed. **August 2015** ERP continues to adhere with the procedure described in the original response. **August 2022** Firefighter ID access is tightly controlled and approved only by ERP management. ERP utilizes workflow in the HITS Service portal, Service Now. All requests for a Firefighter id must be entered in the Service Now system which will require information to support the request and then route for manager approval, The ERP Manager can approve/reject the request. If approved an automated TASK is created in Service Now with a unique number and assigned to the ERP Security Team for processing. All date/times of the request are recorded. The screen shot attached shows the audit log for all firefighter and superuser ids. Firefighter ID access is tightly controlled and approved only by ERP management. ERP utilizes workflow in the HITS Service portal, Service Now. All requests for a Firefighter id must be entered in the Service Now system which will require information to support the request and then route for manager approval, The ERP Manager can approve/reject the request. If approved an automated TASK is created in Service Now with a unique number and assigned to the ERP Security Team for processing. All		

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		date/times of the request are recorded. The screen shot attached shows the audit log for all firefighter and superuser ids.		
3	**Locking Powerful Transaction Codes**	**Recommendation** Unless there is a business reason to the contrary, we recommend that ERP management lock the ISACA suggested transactions in the production system. Even if staff do not have direct access to these transactions, having them locked ensures that there is one more layer of security protection to keep these transactions codes from being used inappropriately. **Management Response** **June 2012**: We have reviewed a list of transactions provided and have entered into the ones that are suitable for the City's configuration and environment to be blocked. These transactions were already restricted by not being available in roles, limited to display access, or to only the ERP Basis team. We will continue to restrict them if for any reason the transaction block is removed for an approved reason. **May 2013** We reviewed the list of ISACAS suggested transactions and have blocked the transactions applicable for our implementation. **August 2015** Complete as per original response **August 2022** We continue to monitor the transactions available for end users and the ERP team. In addition to locking tcode we limit access by not including the transactions in roles assigned to users if they are not needed. Transactions are restricted by not being available in roles, limited to display access, or to only the ERP teams that need access. We will continue to monitor and update as our business needs change.	Audit Division reviewed role-assignment documentation for the identified high-risk SAP transaction codes. The documentation demonstrated that SCC1 and SCC5 are excluded from production business roles and that access to SM30, SM49, and SM69 is limited to SAP Basis administrative roles. However, restricting access through user roles does not demonstrate that the applicable transaction codes were locked in the production system as recommended. System-generated configuration evidence demonstrating the current lock status of the identified transaction codes was not provided. Management's action plans are in progress but have not fully resolved even parts of the original findings. Accordingly, the finding will remain open with a status of "Incomplete / Ongoing".	**Incomplete / Ongoing**
4	**Table Logging in Production System**	**Recommendation** We recommend that ERP management perform and document the decision process based on valid business justifications for table logging in the SAP production system. **Management Response** **June 2012** ERP has instituted multiple layers of security to protect unauthorized table updates. Roles are restricted for any table maintenance, browsing of table data, execution of programs unless under firefighter ids, and control of the production system being opened. Tables that are accessed via roles and need to be restricted are assigned to a unique table authorization group.	Audit Division obtained evidence demonstrating that table auditing is enabled across the applicable SAP environments. However, documentation was not provided demonstrating that management formally evaluated and approved which SAP tables require logging based on documented business justifications. Evidence of table-level logging configurations and change logs for the identified tables was also not provided. Management's action plans are in progress but have not fully resolved even parts of the original findings. Accordingly, the finding will remain open with a status of "Incomplete / Ongoing".	**Incomplete / Ongoing**

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		In addition, SM30 for table maintenance is not used in our production environment and per SAP best practice we do not update directly standard SAP tables. Programmers are not given access to create programs in production. Table updates that require logging by Business owners are recorded for changes. Also, sensitive HR infotype updates such as base pay, HR actions, personal data, payroll status, etc. are configured for logging to provide detailed snapshots of any change to a record. ERP management will undertake a review of table logging with our Business Owners and ERP sections to determine which tables maybe needed to have logging. We expect this review to be completed within 90 days and appropriate logging implemented. **May 2013** Actions Taken: Table logging was tested and implemented. **August 2015** Complete as per original response **August 2022** ERP has limited the ability to change tables by utilizing multiple security practices. Table logging is on in Production clients by specifying the clients for parameter, rec/client (see screenshot). By utilizing a three-tier landscape all table changes must be done in Development by an approved developer. These changes are limited to the development client DRA 420. Any changes to a table whether an SAP table or a customer defined table must be transported. Tables that are accessed via a role are restricted by placing them in a table authorization group. No changes to tables are allowed directly in the production systems. SM30 for table maintenance is not used in our production environment and the system setup does not allow table changes without transport. Transport is only created in development and moved to the QA and production systems when being tested by the ERP Team and Business users. Transports moved to production are reviewed by ERP management and presented to a change review board before being moved into production. In addition, developers are not given access to make any table or program changes directly in production. We also have logging of sensitive data in HR activated for info types such as base pay, actions, personal data, payroll status and others. AP production system.		
5	**Lack of Internal Controls for System Parameter Changes**	**Recommendation** We recommend that EPR evaluate the staff with parameter change ability for the necessity of their having this ability. Also, they should perform periodic	Audit Division obtained documentation assigning responsibility for SAP security parameter administration to the SAP Basis Team and describing the approval and review process for parameter changes. Audit also reviewed system-	**Incomplete / Ongoing**

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		monitoring of all system parameter changes via TU02 transaction code. **Management Response** **June 2012** ERP management restricts the maintenance of system parameters to only the Basis Team per SAP best practices. The Basis Team can only make changes to SAP parameters upon approval by ERP Management. The verification of thirty-three security related parameters is done monthly to ensure compliance as part of the monthly security review process. In order to show that a formal review is being done, ERP management has implemented an additional step in the monthly review procedures to include a report being sent to ERP management if any parameter has been changed. **May 2013** Actions Taken: System parameters review was increased to review TU02 in systems as part of the monthly review process. Supporting Documentation: System Logs and monthly reviews. **August 2015** The security report is a part of monthly security review/ **August 2022** The maintenance of system parameters is restricted to only the Basis Team per SAP best practices. The Basis Team is the SAP system administrator and can only make changes to SAP parameters upon approval by ERP Management and approval from the change management board (CAB). The verification of security related parameters is done monthly to ensure compliance as part of the monthly security review process. In addition, when a system refresh occurs the security parameters are checked via transaction, RSPFPAR_LOGIN (see screenshot attached).	generated reports showing the security parameters configured in the reviewed SAP environments. However, documentation was not provided demonstrating that management evaluated whether employees with the ability to change system parameters continued to require that access. Evidence was also not provided demonstrating that parameter changes were approved and regularly reviewed as required. Management's action plans are in progress but have not fully resolved even parts of the original findings. Accordingly, the finding will remain open with a status of "Incomplete / Ongoing".	
6	**Policies and Procedures**	**Recommendation** Security should develop policies for the areas noted above and any other areas deemed important to managing SAP security. **Management Response** **June 2012** It is our understanding based on our meeting with the Audit Division team that we need specific policies that support our function and outline management control, reflect strategy, vision, consideration of risk, uniform application, and succession planning. These will contain an "effective date" and "formal signoff" by ERP Management. The ERP Security Team will draft	Audit Division obtained policies and procedures addressing SAP system configuration changes, user account management, employee terminations and transfers, and Firefighter access. These documents demonstrate that management established governance addressing portions of the original recommendation. However, the documentation did not fully establish SAP-specific requirements for privileged roles and sensitive transaction codes, segregation of ERP responsibilities, new-user approvals and role assignments, or the management of contractor and temporary-user accounts.	**Partially Implemented**

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURCES PLANNING (SAP) SECURITY (REPORT #2012-12)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		this type of document(s) based on our operational procedures and guidelines and present to ERP management for approval by 12/31/2012. In regard to the item "Managing segregation of duties for the ERP team ", it is ERP policy to only assign access to the team member that is required for them to perform their duties and responsibilities. All ERP access is reviewed during the monthly security review process which includes two reports that outline the team's access and lists any access outside of ERP support update access. A copy of the ERP org chart and section responsibilities have been provided to the internal audit team. The ERP team is segregated into five sub-sections: Functional Team – HR, Functional Team - Financial/MM, Development, Security, and Basis. **May 2013** Actions Taken: ERP has started to align SAP policies with the HITS department security policies. The SAP password and logon parameters were changed to be in compliance with the Mayor's approved policy on passwords. As new policies are approved the SAP policy will be aligned with the new standards. ERP team continues to improve and outline weekly and monthly review policies and checklists. Supporting Documentation: Change process implemented through change control and system logs show new parameter values. **August 2015** ERP team will work with CISO on developing standard policies as requested. **August 2022** Please see attached copies of IT security policies.	The finding will remain open with status of "Partially Implemented" until management establishes and approves SAP-specific policies and procedures addressing the remaining areas identified in the original recommendation.	

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
1	**Governance of Cloud Computing Services - Inventory of Services from Cloud Providers**	**Recommendation** Creation of Cloud Inventory management procedures for HITS and communication to other departments in COH. **Management Response:** **June 2018** HITS will develop and implement a Cloud Computing Services Policy and distribute it to department directors and CTOs. The policy will also officially establish a HITS managed cloud computing services governance committee to ensure cloud services requests are properly vetted prior to approval and implementation. Vetting responsibilities include but are not limited to business requirements, bandwidth consumption, information security/risk, maintenance and ownership. This approach will allow HITS to properly develop and maintain an accurate inventory of all cloud-based services across the City of Houston's information technology enterprise. **February 2026** HITS implemented a Cloud Governance Policy around 2019/2020. The policy includes establishing a Cloud Governance Committee to evaluate risks of all proposed COH cloud-based solutions. The Committee: (1) Ensures that all cloud-based solutions receive proper evaluation from a business perspective, vetting from a security and privacy perspective and proper CIO and CISO approvals prior to going live, (2) Evaluates the necessity to encrypt data and information residing within cloud-based solutions on the basis of risks (e.g., security, privacy, protection and recovery of COH data and information), cost and benefit analysis, (3) Develops and maintains a list of commercial cloud service providers that have been approved for the purposes of hosting moderate or high impact COH information resources. This list specifies individual cloud service offerings or products, and the model under which they have been approved (IaaS, PaaS, or SaaS). This Committee was formally established in 2021. The committee meetings began on 9/15/2021 and are held bi-weekly to review proposals for cloud-based solutions to evaluate the risk to the COH. The committee has reviewed more than 225 applications to date and continues to focus on this on an ongoing basis.	Audit Division obtained evidence to support that management implemented corrective action governing cloud-based services. The Cloud Governance Policy and Cloud Governance Committee Charter establish responsibility and oversight for reviewing cloud-service requests. The Cloud Intake/Request Form establishes a standardized submission process, while committee meeting records from 2021 through 2026 demonstrate that the review process was implemented. In addition, the Application Review Status Spreadsheet and Approved Cloud Provider List demonstrate that management centrally tracks cloud-service requests and approved providers. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
2	**Governance of Cloud Computing Services - Review of Provider Security Capabilities**	**Recommendation** As a best practice based on COBIT 5 framework, create a checklist/template for consistently evaluating application security and availability capabilities that include data control, ownership, and survivability and is in line with HITS data classification, information architecture, information security architecture and risk tolerance. **Management Response:** **June 2018** HITS will develop and implement a Cloud Computing Services Policy and distribute it to department directors and CTOs. The policy will also officially establish a HITS managed cloud computing services governance committee to ensure cloud services requests are properly vetted prior to approval and implementation. Vetting responsibilities include but are not limited to business requirements, bandwidth consumption, information security/risk, maintenance and ownership. This approach will allow HITS to properly develop and maintain an accurate inventory of all cloud-based services across the City of Houston's information technology enterprise. **February 2026** HITS implemented a Cloud Governance Policy around 2019/2020. The policy includes establishing a Cloud Governance Committee to evaluate risks of all proposed COH cloud-based solutions. The Committee: (1) Ensures that all cloud-based solutions receive proper evaluation from a business perspective, vetting from a security and privacy perspective and proper CIO and CISO approvals prior to going live, (2) Evaluates the necessity to encrypt data and information residing within cloud-based solutions on the basis of risks (e.g., security, privacy, protection and recovery of COH data and information), cost and benefit analysis, (3) Develops and maintains a list of commercial cloud service providers that have been approved for the purposes of hosting moderate or high impact COH information resources. This list specifies individual cloud service offerings or products, and the model under which they have been approved (IaaS, PaaS, or SaaS). This Committee was formally established in 2021. The committee meetings began on 9/15/2021 and are held bi-weekly to review proposals for cloud-based solutions to evaluate the risk	Audit Division obtained evidence to support that management implemented corrective action governing cloud-based services. The Cloud Governance Policy and related governance documentation establish responsibility and oversight for reviewing cloud-service requests. The Application Review Status Spreadsheet, containing more than 225 cloud application entries, demonstrates that management established a centralized process for tracking cloud solutions. In addition, Cloud Governance Committee agendas demonstrate recurring meetings, applications scheduled for review, and an ongoing queue of cloud-service requests awaiting committee consideration. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		to the COH. The committee has reviewed more than 225 applications to date and continues to focus on this on an ongoing basis		
3	**Enterprise Risk Management – Risk Framework**	**Recommendation** Creation of an ERM model and risk management process including risk framework and assessment guidelines (collectively an ERM Process). These processes should include the practices and activities that are required to govern and manage risk effectively, including their identification, analysis and management. In most programs, risk is primarily owned by line management with oversight from independent risk, compliance and/or management oversight functions. Both the COSO ERM framework and the COBIT 5 framework are considered best practices in this area and can be used to help establish an ERM program. **Management Response:** **June 2018** HITS will evaluate the development and implementation of a tailored risk framework specific to the governance and management of cloud-based risks. Overall, HITS is currently aligning to the National Institute of Standards and Technology (NIST) Risk Management Framework. **February 2026** Enterprise Risk Management (ERM) is an organizational governance function rather than a technical one, as it encompasses a multitude of strategic, operational, financial, and legal risks across the entire COH. HITS is appropriately positioned to identify, assess, and manage technology and cybersecurity risks as a key contributor to the enterprise risk management framework. However, the ERM function should reside within a centralized governance organization such as Administrative and Regulatory Affairs (ARA) or Finance (FIN) to ensure enterprise-wide visibility, consistency, accountability, etc. Since then, HITS has implemented a Cloud Governance Policy that established a Cloud Governance Committee to evaluate risks of all proposed COH cloud-based solutions. This committee ensures that all cloud-based solutions receive proper evaluation from a business perspective, vetting from a security and privacy perspective and proper CIO and CISO approvals prior to going live. It also evaluates	Audit Division obtained evidence to support that management implemented the corrective action governing technology and cybersecurity risk management within HITS' organizational responsibilities. The HITS Risk Management Policy establishes responsibilities and processes for identifying, assessing, addressing, accepting, and monitoring technology and cybersecurity risks. The Cloud Governance Policy and Cloud Governance Committee provide additional oversight of cloud-related risks, while Administrative Procedure 8-2 incorporates technology risk-management activities into the City's cybersecurity governance structure. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		the necessity to encrypt data and information within cloud-based solutions on the basis of risks (e.g. security, privacy, protection and recovery of COH data and information), cost/benefit analysis, and develops and maintains a list of commercial cloud service providers that have been approved for the purposes of hosting moderate or high impact COH information resources.		
4	**Service Transition Planning**	**Recommendation** Although plans to transfer to a different application are not in the near future, the transfer process still needs to be developed, evaluated, and documented. Depending on the risk and impact of the individual application, alternate contracts may need to be in place. **Management Response:** **June 2018** HITS will develop a departmental service transition process that addresses the transfer of cloud computing operations to an alternate service provider in the event that the selected service provider is unable to meet contractual requirements or ceases operations. **February 2026** HITS recognizes the importance of service continuity and has taken steps to mitigate risks associated with vendor disruptions. In alignment with the recommendations, we have incorporated 4 measures. First, where feasible and appropriate, we evaluate and identify potential alternate service providers or establish pre-positioned contractual vehicles that can be leveraged in the event of disruption. This approach is applied on a case-by-case basis, considering criticality, cost-effectiveness, and operational impact. Second, during procurement and contract negotiations, we work with vendors to assess portability of services and ensure fallback options are available, including reviewing technical and contractual provisions that support transition or continuity should a vendor become unavailable. Third, we collaborate with the legal department to ensure contracts include survival clauses for key provisions like confidentiality, security, indemnity as well as assignment clauses that address continuity in the event of acquisitions or ownership changes. These provisions also preserve COH's rights and remedies. Finally, while redundancies for all services may be not fiscally responsible, we apply a risk-based approach to determine where alternate providers or contingency	Audit Division obtained evidence demonstrating that management implemented portions of the corrective action. The sampled selected contract amendment and the agreements contain provisions addressing service transitions, vendor exits, data return and migration, confidentiality, and service continuity. However, documentation was not provided demonstrating that HITS established a department-wide process for initiating, approving, coordinating, monitoring, and completing service transitions. The finding will remain open with status of "Partially Implemented" until management establishes and documents a department-wide process governing the initiation and execution of service transitions.	**Partially Implemented**

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
		plans are most appropriate. This ensures resources are allocated effectively to mitigate high-impact risks		
5	**Information Risk Management – Contractual Requirements**	**Recommendation** As a best practice based on COBIT 5 framework, document and formalize the list of controls/evaluation points to be used by HITS executives to make risk decisions regarding each service and incorporate those into the product selection & evaluation and contract negotiation phases of cloud governance. Additionally, evaluate the risk of the lack of an SLA with the vendor and establish an SLA, or other compensating control, with the vendor. **Management Response:** **June 2018** In conjunction with Finding #8, HITS will develop and implement a formalized process to evaluate contractual terms with vendors providing cloud services. **February 2026** COH's Cloud Governance Committee evaluates new cloud-based contracts/purchases in which through this committee will identify applicable support/SLA requirements. Furthermore, the Security Addendum has been added to the City's Procurement Purchase Order terms and conditions to be applied to all purchase orders. In addition, HITS has worked with City Legal - Contracts section to ensure that any IT contract City Legal works on has HITS participation/knowledge to ensure alignment and proper contractual controls. The HITS DBM division also works on contracts on a case-by-case basis, in coordination with the business and technical owners, to ensure proper SLA and security/privacy requirements are addressed	Audit Division obtained evidence to support that management implemented the corrective action governing security and privacy requirements for technology vendors. The 2026 Security Addendum establishes standard security and privacy requirements for technology contracts, while the IT Contract Review Checklist establishes criteria for reviewing IT and cloud-related contract provisions. The Tyler contract demonstrates that the Security Addendum was incorporated into a vendor agreement, and the PayByPhone documentation demonstrates that exceptions to established requirements are documented and retained. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**
6	**Governance of Cloud Computing Services – Survivability of Service**	**Recommendation** Include clauses for the survivability of service in the standard terms and conditions that are negotiated with each contract. The survival clause should specify which contract provisions will remain in effect after the termination or expiration of the agreement. Common obligations covered by survivability of service clauses include Confidentiality, Access to Data, and/or Support.	Audit Division obtained evidence to support that management implemented the corrective action governing contract survivability requirements. The executed sample selected agreement contains provisions addressing vendor obligations that continue after contract termination or expiration, including requirements involving successors and contract assignments. The updated IT contract template incorporates these requirements into standard contract language, while the Tyler contract provides additional evidence that the requirements were applied in current contracting activities.	**Fully Implemented**

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	**Finding Name**	**Recommendation and Management Response(s)**	**Conclusion**	**Remediation Status**
		Management Response: **June 2018** HITS will continue to work with the COH Legal Department to ensure contractual language is included in all cloud service provider contracts highlighting specifics regarding provisions that will remain in effect after the termination or expiration of the agreement. **February 2026** HITS has been working with City Legal Department to ensure survival language is present in IT contracts, including survival of applicable provisions including confidentiality, security, indemnity, access, support etc. and reserving the City's remedy rights. Furthermore, the provision that covers assignments (acquisitions included) will address the continuation of the services if the contract/company is acquired.	The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	
7	**Governance of Cloud Computing Services - Responsibilities for Governance**	**Recommendation** Formalize roles and responsibilities for the governance process in a way that can be published and used as an ownership and accountability mechanism. The best practice is to use a RACI chart. chart. A RACI (responsible, accountable, consulted, and informed) chart is a matrix of all the activities and/or decision-making authorities undertaken in a process set against all the people or roles in the process. At each intersection of activity and role it is possible to assign somebody responsible, accountable, consulted, or informed for that activity or decision. **Management Response:** **June 2018** HITS will research and develop a cloud governance computing services RACI chart to outline cloud governance responsibilities. **February 2026** HITS will continue to research and develop a cloud governance computing services RACI chart to outline cloud governance responsibilities. HITS endeavors to complete this by 12/31/2026 subject to applicable approvals.	Audit Division obtained evidence demonstrating that HITS established a Cloud Governance Committee, documented its membership, approved a Cloud Governance Policy, and developed a draft RACI matrix assigning responsibilities for cloud-governance activities. However, management's response and the documentation reviewed demonstrate that the RACI matrix remains under development and has not been finalized and formally approved. Management's action plans are in progress but have not fully resolved even parts of the original findings. Accordingly, the finding will remain open with a status of "Incomplete / Ongoing".	**Incomplete / Ongoing**

HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD GOVERNANCE PERFORMANCE AUDIT (REPORT #2018-09)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
8	**Third-Party Management – Risk Assessment**	**Recommendation** Require that a service provider's annual SSAE16 SOC Report be delivered to COH and reviewed by HITS for any changes in control effectiveness reported since the prior year. When the vendor does not have a SOC report, evaluate the use of a right to audit clause to conduct a risk assessment of the vendor. Also, FAMCare COH should conduct a supplemental review of the other risk areas through an SOC report or expanded compliance report. **Management Response** **June 2018** HITS will continue to work with the COH Legal Department to ensure contractual language is included in all cloud service provider contracts requiring the formal submission of SSAE16 SOC reports annually. HITS resource constraints will not allow the performance of formal risk assessments on all service providers that do not provide an annual SSAE16 SOC report. **February 2026** HITS has created and implemented a Security Addendum that requires contractually for vendors to provide the SSAE18 SOC reports (updated from the SSAE16). This Security Addendum is added to IT contracts as well as to COH's purchase order terms and conditions.	Audit Division obtained evidence demonstrating that management implemented a portion of the corrective action. The Security Addendum requires applicable service providers to furnish annual Service Organization Control reports. However, documentation was not provided demonstrating that the Security Addendum was incorporated into applicable vendor agreements or that HITS obtained and reviewed annual reports, evaluated changes from prior-year reports, performed alternative assessments for providers without reports, or completed the supplemental FAMCare review. The finding will remain open with status of "Partially Implemented" until management provides evidence that the Security Addendum has been applied to applicable vendor agreements and that the annual report review, alternative vendor assessment, and FAMCare supplemental-review processes have been implemented.	**Partially Implemented**

Houston Information Technology Services Information Technology Processes Performance Audit (Report #2018-11)				
#	**Finding Name**	**Recommendation and Management Response(s)**	**Conclusion**	**Remediation Status**
1	**Mobile Device Plan Charges Are Not Reviewed**	**Recommendation** HITS should implement a review system to ensure department coordinators have information regarding users going over assigned data plans which result in additional costs to the City of Houston. Furthermore, we recommend amendments to the City of Houston's Administrative Procedure No. 8-8 Mobile Device Eligibility to allow HITS oversight of department wireless coordinators. A designated HITS person should prepare and review monthly reports to ensure data usage charges are in line with data plans assigned to staff. **Management Response** **June 2018** Effective January 2018, HITS moved most COH device users to an unlimited plan to eliminate service overage charges. HITS will continue to review usage reports to identify any discrepancies requiring adjustment. In terms of device eligibility, HITS will defer selection and approval to the individual departments responsible for funding devices to approve. Regarding recommended modifications to AP 8-8 and assigning HITS additional responsibility to oversee wireless coordinators and provide monthly reports on data usage, HITS will engage the IT Governance Board and IT Operating Committee to identify effective financial and eligibility controls. **February 2026** HITS has implemented a Telecom Expense Management Services (TEMS) solution. Each department has assigned a focal point to review the invoices to ensure accuracy. Furthermore, HITS has implemented a process to review zero usage wireless numbers on a quarterly basis, leveraging the TEMS solution, and taking action to suspend billing for the service to minimize costs to COH and then disconnect the service entirely 30 to 60 days later if HITS is not requested to restore the service. HITS will research and propose revisions to AP 8-8 relating to HITS having additional responsibility to overseeing wireless coordinators in ensuring that the City coordinators are periodically auditing the usage, charges, on/off boarding, and other services. HITS may collaborate with ITGB and ITOC if and as applicable and appropriate.	Audit Division obtained dashboards and reports providing information on wireless usage, inactive devices, overage charges, provisioning activity, cost trends, and vendor performance. However, the availability of this information does not demonstrate that management implemented the recurring monthly review and follow-up process required by the corrective action. Documentation was not provided demonstrating completed monthly reviews, oversight of departmental wireless coordinators, follow-up actions on identified issues, or the required amendment to Administrative Procedure 8-8. Management's action plans are in progress but have not fully resolved even parts of the original findings. Accordingly, the finding will remain open with a status of "Incomplete / Ongoing".	**Incomplete / Ongoing**
2	**System Backups are Periodically Not Tested**	**Recommendation** We recommend that HITS formalize data backup testing procedures for all critical data backups and incorporate those procedures into the COOP to ensure: • the integrity of transactions and data held in storage	Audit Division obtained evidence demonstrating that management implemented portions of the corrective action. The Backup Restore procedures document the restoration process, while a point-in-time restore and additional service documentation demonstrate that restoration capability has been used in the	**Partially Implemented**

Houston Information Technology Services Information Technology Processes Performance Audit (Report #2018-11)				
#	**Finding Name**	**Recommendation and Management Response(s)**	**Conclusion**	**Remediation Status**
		• information from the most recent backup process is available • disruptions in operations can be restored with minimal loss. **Management Response** **June 2018** HITS will develop a procedure to routinely test data backup to restore processes designed to test the integrity of data backups. **February 2026** Backups are tested every 2-3 months; related documentation can be provided.	production environment. Management also implemented automated verification of selected backup-recovery attributes. However, documentation was not provided demonstrating that complete restoration testing was consistently performed every two to three months, as stated by management. Automated backup verification and successful backup jobs do not, by themselves, demonstrate completion of recurring restoration tests. The finding will remain open with status of "Partially Implemented" until management provides a series of dated restoration-test records demonstrating that complete restoration testing is performed every two to three months.	
3	**No Formal Written Policies and Procedures**	**Recommendation** HITS should create, develop and finalize formally written departmental policies and procedures for all IT processes. Written policies and procedures are considered best practice because they provide uniformity and consistency in operations and can serve as reference tools for existing staff and provide training materials for new employees. **Management Response** **June 2018** HITS acknowledges that formal policies governing vendor contract management, system and data backup restores and mobile device assignment and usage as nonexistent. These deficient areas were already identified and plans to develop appropriate polices are documented on the HITS Cyber Division's 4-Year Master Plan. The following are details on the alignment of planned policies and specific content that will be addressed: Policy Title (Addressed Audit Finding) 1. System and Services Acquisition (Vendor contract management) 2. Business Continuity and Disaster Recovery (System data backup and restores) 3. Mobile Device Management (Mobile device assignment and usage) **February 2026** HITS continues to work to document and implement departmental policies and procedures, including the mobile device management policy. We will continue to work documenting and implementing departmental policies and procedures.	Audit Division obtained evidence to support that management implemented the corrective action governing the operational areas identified in the original recommendation. Administrative Policy 5-8 establishes requirements for informal procurement and vendor-related activities. The HITS Data Backup Policy establishes requirements for backup, recovery, restoration testing, retention, and monitoring. The HITS Mobile Device Management Policy establishes requirements for mobile-device issuance, security, access, monitoring, usage, and sanitization. These approved policies assign responsibilities and establish written governance for each of the three operational areas identified in the original recommendation. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**

Houston Information Technology Services Information Technology Processes Performance Audit (Report #2018-11)				
#	Finding Name	Recommendation and Management Response(s)	Conclusion	Remediation Status
4	**System Backups are Not Stored Offsite**	**Recommendation** We recommend that HITS establish an offsite data backup storage site for all critical data backups in accordance with the NIST requirements. **Management Response** **June 2018** HITS is not in agreement with the findings. HITS currently backs up data and information to hardened data centers. NIST acknowledges that replication of data from one data center to another meets the requirement. Although replication was not in place at the time of the audit, the deficiency was already identified, and an FY18 project had been planned; funding became available July 1, 2018. The backup enhancements were implemented in FY18 and are well documented. Replication of data is scheduled to be completed by the end of 1Q FY19. **February 2026** Backups are stored Offsite, related documentation can be provided.	Audit Division obtained evidence to support that management implemented the corrective action governing continuity and disaster recovery. The HITS Continuity of Operations Plan Annex identifies essential functions, recovery priorities, critical systems, alternate facilities, responsible personnel, and recovery procedures. Supporting documentation demonstrates that management established multiple backup and recovery locations, offsite data replication, protected backup storage, and recovery capabilities for critical systems and applications. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**
5	**Mobile Device Orders and Device Pickup Do Not Require Signatures and are Not Recorded in TEMS**	**Recommendation** HITS should ensure that orders for mobile devices have been appropriately approved by management and that the requested devices are for eligible users. In addition, HITS should ensure that the department's procedures are in line with the requirements of AP 8-8 by fully implementing Telecom Expense Management Software (TEMS) or by making the appropriate revisions to AP 8-8. **Management Response** **June 2018** HITS is in the process of fully implementing a Telecom Expense Management System (TEMS) to support and manage the inventory, ordering, and billing of COH wireless devices and voice services. As a stop gap solution, HITS currently utilizes our wireless providers portal to purchase, upgrade and activate new devices, and to provide usage reports and billing inquiries. The stop gap solution proved to be adequate as HITS was able to produce and provide usage data to the SavingsStat wireless dashboard (http://citypointe/govt/mayor/HouStat/sstat/) for review by Department Directors. Lastly, TEMS is not intended to perform as a device approval tool. Departments will be required to develop internal policies to manage device eligibility, justification and submit evidence of approval. **February 2026**	Audit Division obtained evidence to support that management implemented the corrective action governing mobile-device requests and assignments. ServiceNow workflow records demonstrate that mobile-device requests are processed through a standardized workflow and retained with requestor, departmental, and approval information. The Wireless Communication Order Form documents user eligibility, departmental approval, funding, and requested services, while device-assignment records provide traceability from the original request through equipment assignment. In addition, the HITS Mobile Device Management Policy establishes requirements for device authorization, administration, monitoring, and accountability. The management action plan is adequate to address the audit findings and is considered "Fully Implemented". This finding is Closed.	**Fully Implemented**

Houston Information Technology Services Information Technology Processes Performance Audit (Report #2018-11)				
#	**Finding Name**	**Recommendation and Management Response(s)**	**Conclusion**	**Remediation Status**
		HITS has implemented a TEMS solution. Furthermore, HITS has implemented a formal process to ensure that orders or mobile devices have been appropriately approved by departmental management and that the requested devices are for eligible users. The request for a mobile device is submitted via a ServiceNow request, and it must first be approved by the specific Department. Then, HITS uses the TEMS solution to order the device.		
6	**No Contract Vendor Performance Assessment Reviews**	**Recommendation** HITS should begin providing vendor contract performance evaluations for all vendor contracts and submit them to the Chief Procurement Officer (CPO) in accordance with the requirements of Section 5.2 of AP 5-13. **Management Response** **June 2018** HITS will utilize the Contractor Performance Evaluation form created by Strategic Purchasing to evaluate vendor contract performance. **February 2026** HITS has been providing vendor evaluation feedback as we receive the evaluation requests from SPD. HITS also logs poor vendor performance/incidents on an internal departmental site for future reference and documentation.	Audit Division obtained evidence demonstrating that HITS established mechanisms for retaining and submitting vendor performance information. The Vendor Performance Documentation SharePoint repository supports retention of vendor issues and performance information, while Procurement provides a Citywide mechanism for submitting supplier performance reviews. However, documentation was not provided demonstrating that HITS completed and submitted the required vendor performance evaluations in accordance with Administrative Procedure 5-13. Evidence was also not provided, demonstrating that HITS established a departmental process assigning responsibility for completing and submitting the evaluations. Management's action plans are in progress but have not fully resolved even parts of the original findings. Accordingly, the finding will remain open with a status of "Incomplete / Ongoing".	**Incomplete / Ongoing**

APPENDIX 2: FOLLOW-UP AUDIT PLAN

AUDIT OBJECTIVES

The objectives of the follow-up audit were to:

1. Determine the status of each open item.
2. Evaluate the adequacy of the department's remediation process to resolve open findings.

PROCEDURES PERFORMED

Audit procedures performed to meet the audit objectives and provide a basis for our conclusions were as follows:

- Obtained, reviewed and assessed management's status updates to open findings.
- Determined the findings for which management's status updates indicated remediation.
- Determined and requested the documentation necessary to support the status of each finding reported by management.
- Reviewed supporting documentation and other evidence provided for sufficiency and appropriateness.

AUDIT APPROACH

Our follow-up audit process utilizes a risk-based approach, which contains the two primary components:

- Management Status Updates
- Audit Testing/Verification

MANAGEMENT STATUS UPDATES

Our follow-up audit process includes sending requests for status updates related to management's progress toward the remediation of open findings. Management provides status updates through an online portal. This information is then assessed by the follow-up auditor, who considers responsiveness to the original issue and remediation of the issue.

AUDIT TESTING / VERIFICATION

A management status update indicating that a finding has been remediated is then tested/verified by the follow-up auditor prior to being closed.

The information received through management status updates form the basis for follow-up testing. If needed, additional supporting information is gathered by the follow-up auditor to provide sufficient and appropriate evidence to achieve our objectives. Once the testing and verification of a department's remediation processes have been completed, Audit then assess each finding based on one of the following four categories:

- **Fully Implemented**: Successful implementation of processes to address the audit finding.
- **Partially Implemented**: Significant efforts and implementation of processes to address the audit findings.

- **Incomplete/Ongoing**: Ongoing development of a process or efforts towards a policy to address the audit finding.
- **Not Implemented**: No effort to implement processes to address the audit finding.

AUDITING STANDARDS

The Audit Division conducted follow-up audit procedures in accordance with the Generally Accepted Government Auditing Standards (GAGAS) issued by the Government Accountability Office (GAO) and the Global Internal Audit Standards as established by the Institute of Internal Auditors (IIA).

These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the findings and conclusions drawn in alignment with audit objectives.

GOVERNMENT AUDITING STANDARDS (YELLOW BOOK)

GAGAS 8.30

> "Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant within the context of the audit objectives. When planning the audit, auditors should ask management of the audited entity to identify previous engagements or other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives."

GLOBAL INTERNAL AUDIT STANDARDS (RED BOOK)

IIA Standard 15.2

> "Internal auditors must confirm that management has implemented internal auditors' recommendations or management's action plans following an established methodology, which includes:
>
> - Inquiring about progress on the implementation.
> - Performing follow-up assessments using a risk-based approach.
> - Updating the status of management's actions in a tracking system.
>
> The extent of these procedures must consider the significance of the finding."