OFFICE OF THE CITY CONTROLLER

INFORMATION TECHNOLOGY DEPARTMENT ENTERPRISE RESOURE PLANNING (SAP) SECURITY

LIMITED REVIEW PERFORMANCE AUDIT

Ronald C. Green, City Controller

David A. Schroeder, City Auditor

Report No. 2012-12

OFFICE OF THE CITY CONTROLLER
CITY OF HOUSTON
TEXAS

RONALD C. GREEN

June 8, 2012

The Honorable Annise D. Parker, Mayor

SUBJECT: REPORT #2012-12
INFORMATION TECHNOLOGY DEPARTMENT – ERP/SAP SECURITY
PERFORMANCE AUDIT

Dear Mayor Parker:

The Office of the City Controller's Audit Division has completed an audit of limited aspects of security as it pertains to the Enterprise Resource Planning (ERP) financial software, Systems Applications and Products (SAP). This audit was included in the FY2012 Audit Plan and was a direct result of our Enterprise Risk Assessment process. The four primary audit objectives were to determine whether:

1. SAP system parameters are in line with security policies and support approved authentication;
2. SAP User IDs are monitored and associated with properly authorized personnel;
3. Adequate controls are in place regarding user access to roles, profiles, transactions, data, and programs; and
4. Segregation of duties is defined, documented and maintained.

We concluded that the overall control structure in place was adequate to assure:

- SAP system parameters were supported by reasonable business purposes;
- SAP User IDs were being monitored and were associated with properly authorized personnel;
- User access, roles, profiles, transactions, data, and programs were authorized; and
- Segregation of duties for the ERP group was defined.

The following recommendations were provided to the ERP Management Group based on findings contained in the detailed report:

- ERP Security should begin reviewing details of all parameter changes (both security and non-security related)(Finding #5)
- ERP should establish and develop formal Policies and Procedures specific to ERP System Security, including parameters to support consistent practice and business process improvement (Findings #6);
- ERP management should better control the most powerful User ID (SAP*) and review activity associated with the User ID's. (Findings #1, 2);
- ERP management should better monitor activity of user roles, profiles, transactions, programs, and data (Findings #3 & #4); and
- ERP management should document Segregation of duties for the ERP group and put mitigating controls in place for designed conflicts in the SOD. (Finding #6, 2).

We appreciate the cooperation and professionalism extended to the Audit Division during the course of the project by the ERP team and ITD management.

Respectfully submitted,

Ronald C. Green

Ronald C. Green
City Controller

cc: City Council Members
Charles Thompson, Director, Information Technology Department
Chris Brown, Chief Deputy City Controller, Office of the City Controller
Waynette Chan, Chief of Staff, Mayor's Office
David Schroeder, City Auditor, Office of the City Controller

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

The Office of the City Controller's Audit Division has completed an audit of limited aspects of security as it pertains to the Enterprise Resource Planning (ERP) financial software, Systems Applications and Products (SAP). This audit was included in the FY2012 Audit Plan and was a direct result of our Enterprise Risk Assessment process.

BACKGROUND

SAP is the official accounting software of record that the City of Houston uses for recording transactions, maintaining personnel information, and preparing the Comprehensive Annual Financial Report (CAFR). The City implemented SAP July 1, 2006 and is administered by the ERP team in the Information Technology Department (IT) under the guidance of ERP Support Manager. SAP security is managed by the Security Team (Security), consisting of two ERP Support employees who report to the Technical and Interfaces Administrator.

System security is the aspect of SAP that controls both outside systems' and individual user's access to the system, and rights/privileges therein. Security parameters establish limits on the way Users obtain access into the system, while other aspects of System security includes establishing Unique Logon User IDs that allow access to the system and assigning authorized processes to the User. The User authorizations are contained in groups called "Roles" which give the User the ability to access and process certain transactions. Each transaction executes a unit of program coding that accomplishes specific tasks. Examples of transactions can include creating a purchase order; recording goods received; transferring an employee between Departments; or approving a journal entry.

Security sets up User IDs for employees, temporary workers and contract workers to enable them to enter and/or approve transactions. The SAP system also comes with some default User IDs already established. These default User IDs can be very powerful, having access to tables and transactions that can be very sensitive, so their use must be controlled and monitored. We used the book "Security, Audit and Control Features SAP ERP 3rd Edition" issued by Information Systems Audit and Control Association (ISACA) as a resource for our Audit.[1] It contains information about SAP's structure and audit procedures for testing different aspects of the system, including powerful/sensitive User IDs and powerful/sensitive Roles, Authorizations, and Transactions.

[1] ISACA developed and continually updates the CoBIT and Risk IT Frameworks, which was considered throughout the book referenced above.

AUDIT SCOPE AND OBJECTIVES

In developing the scope and objectives we consider various aspects of SAP system security, including users, profiles, roles, transactions and tables. The objectives as communicated in the Notification Letter to management were broadly defined as determining whether:

1) SAP system parameters are in line with security policies and support approved authentication;
2) SAP User IDs are monitored and associated with properly authorized personnel;
3) Adequate controls are in place regarding user access to roles, profiles, transactions, data, and programs; and
4) Segregation of duties is defined, documented and maintained.

After conducting our initial research on system security as well as interviews with key personnel to gain an understanding of the functions of the Security Team, we focused on the areas defined as Security's responsibility.

PROCEDURES PERFORMED

In order to obtain sufficient evidence to achieve engagement objectives and support our conclusions, we performed the following:

- Reviewed ERP security Policies and Procedures;
- Reviewed SAP system parameters (including table logging) in contrast to policy and relevant guidance;
- Identified and reviewed the existence, classification, status, and parameters of the default SAP User IDs for appropriate security settings;
- Identified, and reviewed users that have assignment to powerful or sensitive roles/profiles
- Verified a sample of users and their authorizations for proper management approval;
- Reviewed access and authorizations to powerful transactions for appropriate restrictions
- Identified user profiles of all members of the ERP group and reviewed the various roles assigned for proper segregation of duties;
- Obtained listing of terminated/transferred employees and reviewed for timely updating to system access;
- Verified whether Contractor User IDs had the existence and reasonableness of a login access expiration date; and
- Verified a sample of active employee User IDs for proper existence and status in the HR records.

AUDIT METHODOLOGY

Our work was conducted in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Practice of Internal Auditing as promulgated by the Institute of Internal Auditors. Those 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 our audit objectives.

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

SUMMARY CONCLUSIONS AND SIGNIFICANT ISSUES

We are required to obtain sufficient and appropriate evidence to adequately support our conclusions. We believe we have fulfilled the requirements promulgated by professional auditing standards and show the results below. For detailed findings, recommendations, management responses, comments and assessment of responses see the Detailed Section of this report.

SUMMARY CONCLUSION 1

Based on the results of the procedures performed, the system parameters were set supported by reasonable business purposes. (**Audit Objective #1**) However, we noted that ERP Security should begin reviewing details of all parameter changes (both security and non-security related (**see Finding #5**) and develop and maintain formal Policies and Procedures specific to ERP System Security, including parameters to support consistent practice and business process improvement. (**see Finding #6**)

SUMMARY CONCLUSION 2

Based on the results of the procedures performed, SAP User IDs were being monitored and were associated with properly authorized personnel, however the most powerful User ID (SAP*) was not adequately controlled . **(see Finding #1)** Also, activity associated with the User ID's[2], were not being reviewed by management. ***(see* Finding #2)** (**Audit Objective #2**)[3]

SUMMARY CONCLUSION 3

Based on the results of the procedures performed, controls as implemented by ERP regarding user access, roles, profiles, transactions, data, and programs were adequate. (**Audit Objective #3**)

SUMMARY CONCLUSION 4

Based on the results of the procedures performed, Segregation of duties for the ERP group was defined, however are not documented (see Finding #6). Mitigating controls did not exist for designed conflicts in the SOD (see Finding #2). (**Audit Objective #4**)

[2] The set-up of User IDs is under the responsibility of ERP Security.

[3] See Findings #3 & #4 for control deficiencies related to monitoring activity of user roles, profiles, transactions, programs, and data

ACKNOWLEDGEMENT AND SIGNATURES

The Audit Team would like to thank ERP management and the Security Team, especially Deepak Gidvani, for their cooperation, time, and efforts throughout the course of the engagement.

Marda Waters

Marda Waters, CPA
Assistant City Auditor IV

David Baszile
Assistant City Auditor III

David Schroeder, CPA, CISA
City Auditor

DETAILED FINDINGS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

1. LACK OF INTERNAL CONTROLS FOR SUPERUSER SAP* SYSTEM LOGON

BACKGROUND:
SAP* is the default Superuser ID supplied with the SAP ERP software. If not properly protected, it could be used to access the system and perform unauthorized processing of transactions that may circumvent established controls in the system. Furthermore, this account can be used without individual accountability.

ISACA's Security, Audit and Control Features guideline suggests that the SAP* user account should be secured by:

- Being setup in all new clients created;
- Assigning SAP* to the security administration's authorization group (e.g., SUPER);
- Changing the default password;
- Segregating SAP* capabilities across newly created superusers with less functionality;
- Deleting all profiles/roles and authorizations from the SAP* user;
- Locking the user; anf
- Monitoring audit logs for the user

While our audit focused primarily on the production system, the importance of protecting this super user id (SAP*) in all clients required we verify its set-up status in the sandbox system.

FINDING:
The production and sandbox system Super User ID settings showed the following[4]:

Production System

- SAP* User was not assigned as a SUPER user in the administrative authorization group. Any user assigned to Firefighter ID and users with transaction and/or authorization could delete the user account.
- Powerful authorizations SAP_ALL and SAP_NEW were assigned to it. While there are several levels of security protection provided if this User was breached by an unauthorized user, those Roles would provide access to ALL transaction codes in the system.

Sandbox System

- The SAP* user ID was not created in the Sandbox client which allows the well know default user ID password to be used to access this client system. Even though Sandbox is a test system it is an exact copy of our production system which contains employee personal data.

[4] NOTE: During our audit, the SAP* User was added to the security administration's authorization group SUPER. ERP security also changed the SAP system parameter logon/no_automatic_user_sapstar to further protect this SUPER USER ID.

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.

ERP SECURITY
MANAGEMENT RESPONSE:

"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 in compliance with 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 the 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 review of the SAP userid.*

Since we do not use the SAP userid and it remains locked we do not have an issue with removing any system profiles."*

ASSESSMENT
OF MANAGEMENT RESPONSE:

ERP management has placed SAP* in the Super group in the production system and has agreed to remove the powerful profile from the user-id although no estimated completion date was given.

2. Lack of Internal Controls for Firefighter and Super User IDs

Background:

Firefighter (FIREID) user accounts allow personnel to take responsibility for tasks outside their normal job function. Firefighter describes the ability to perform tasks in emergency situations. Firefighter enables users to perform duties not included in the roles or profiles assigned to their user IDs. Firefighter provides an audit log of activities performed using these Firefighter IDs that should then be independently reviewed for appropriateness.

Each FIREID provides security and controls for the access granted. Each one has specific authorization rights, is built and structured for certain functions or modules, and has a validity date. They are assigned to one user at a time to ensure accountability.

To ensure separation of duties is enforced, administrators should not be able to assign a firefighter ID to themselves. Establish ownership by assigning an owner to each Firefighter ID and determine procedures and documentation requirements for using each Firefighter ID.

We reviewed assignment and the documentation of use for both Firefighter and other Super User IDs assigned to ERP staff.

Finding:

Our testing showed the following:

- 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.

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.

ERP Security
Management Response:

“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 regards to the finding;

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.

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)."

ASSESSMENT OF MANAGEMENT RESPONSE:

While the justification provided in the initial response attempts to minimize the magnitude and impact by citing one incident, the volume of circumvention occurrences are one aspect of assessment. Depth and breadth should also be considered, especially with powerful transactions and authorizations, as is the case here.

However, ERP management has agreed to strengthen the control process by logging super user-ids assignments as they currently log firefighter user-ids and create formal policies relating to reviewing audit log after each assignment of these powerful user-ids, which, if comprehensive will quickly detect inappropriate access to data.

3. Locking Powerful Transaction Codes

Background:
Some critical and sensitive transaction codes are used only in a development environment or sparingly in production. Other production-sensitive transaction codes should be closely monitored and locked when not in use. Most organizations choose to secure transaction codes through the use of S_TCODE authorization object. However, power users still have access to sensitive transaction codes.

Locking transaction codes provides another mechanism to prevent the inadvertent execution of these transactions in production. ISACA's Security, Audit and Control Features guideline lists 54 sensitive transaction codes and suggests they be locked in the production environment. For example, transaction codes SCC1, SCC5, SM49, SM69 and SM30 are appropriate in a development/QA environment, but it would be highly uncommon to ever use them in production. The organization should have procedures for locking and unlocking these transactions codes, and access to perform such functionality should be appropriately restricted.

We tested the following five (5) sensitive transactions to determine if they were locked by using the transaction code which reports all locked transaction codes:

- SCC5 - allows deletion of a client;
- SCC1 - allows clients to be copied;
- SM49 AND SM69 - allow users to run operating system commands; and
- SM30 - allows table data maintenance.

Finding:
We found none of the ISACA suggested sensitive transactions locked. ERP Security Management has no procedures in place for locking and unlocking sensitive transactions codes based on a defined needs assessment and approval system.

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 does 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.

**ERP Security
Management Response:**
"We have reviewed a list of transactions provided and have entered 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."

**Assessment
of Management Response:**
The commitment contained in the response adequately addresses the issue and proposes to remediate.

4. TABLE LOGGING IN PRODUCTION SYSTEM

BACKGROUND:

The SAP system consists of various changeable components, each independent of the others. Because of the system's complexity, modifications can easily lead to security lapses and instability. The complexity of an SAP system and the accompanying error risk if modifications are not monitored can lead to instabilities that might be abused. If no appropriate monitoring mechanisms are established, the fundamental possibility of system manipulation also exists.

SAP provides parameters and table settings which allow an organization to independently establish logging for "critical" tables, such as tables that control the flow of quantities and values. ISACA's Security, Audit and Control Features guideline has a list of over 135 tables that should be reviewed for possible logging based on the organization's needs. It also states that all changes to critical SAP ERP tables should be logged by the system and the periodic review of these logs should form part of the security procedures. Although SAP standard security reports provide some logging, table logs for key tables will show the changes and the User ID of who made the changes.

Examples of critical tables are the data dictionary tables DD02* and DD09*. If these are changed, it could dramatically affect how SAP operates. As another example, changes to TOBJ_OFF can be used to disable authorization checking.

FINDING:

ERP Security had all table logging turned off and had communicated that SAP provides adequate standard security reporting of table changes. However, the standard SAP security reports will not record if someone makes a change directly to a table using a table maintenance transaction like SM30, or if a programmer wrote a program to update that table outside of the standard SAP functionality, but table logging will.

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.

ERP SECURITY
MANAGEMENT RESPONSE:

"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 a unique table authorization group.

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 requires 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 detail 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."

ASSESSMENT OF MANAGEMENT RESPONSE:

The commitment and corrective measures to improve detective controls as contained in the response adequately addresses the issue and proposes to remediate accordingly.

5. Lack of Internal Controls for System Parameter Changes

Background:
System parameters are used to define how security is enforced in the SAP system. If any of these values are changed, the integrity of the system can be compromised. The system parameters are stored in text files on the operating system level in the global profile directory. Changes to profile parameters may not be done in the text file directly, but only through a corresponding transaction within SAP [e.g. RZ10], otherwise the change history will not be complete. Because of the risk of potential file violations, the access to these files needs to be restricted accordingly and all changes reviewed on a timely basis.

SAP provides a transaction code which allows reporting of all system parameter changes of each client system. We ran the SAP transaction report showing all recent parameter changes in the production system. We then selected five (5) parameter changes and asked that ERP management to present prior approval and log documentation for these parameter changes.

Finding:
ERP Security management provided some system parameter change approval documentation, and we found that a selected group of system parameters are checked for changes on a regularly basis, however we saw no evidence of reporting to assure that no SAP system parameter could be changed without management knowledge and approval.

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 monitoring of all system parameter changes via TU02 transaction code.

ERP Security
Management Response:
"ERP management restricts the maintenance of system parameters to only the Basis Team per SAP best practices. The Basis Team can only makes 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 a formal review is being done, ERP management has implemented an additional step in the monthly review procedures to include a report be sent to ERP management if any parameter has been changed."

Assessment
of Management Response:
The commitment to enhance and strengthen the controls as contained in the response adequately addresses the issue and proposes to remediate.

6. Policies and Procedures

Background:

Formally documented and disseminated policies and procedures (P&Ps) provide employees with concrete guidance on how to conduct their day to day operations. Additionally, they outline consistent activities that are aligned with the goals and objectives of the organization and help ensure seamless transition and succession.

System security includes parameters, which provide some controls over the system. An example of a system parameter is how many times the system allows a User to try their password before they are locked out. Some other SAP specific system security items include powerful or sensitive roles/profiles/transactions, to which access should be more restricted than usual, and powerful user IDs. An example of a powerful user IDs is a Firefighter ID, a user account which allows personnel to perform tasks outside their normal job function in emergency situations to correct system issues.

The ERP Security team has operating procedures, security review procedures, checklists and standards developed during and after implementation. Examples of these are listed below.

1. Firefighter ID procedure.
2. System Parameters procedure.
3. User setup procedures for all access (employees, temps, contractors) for all modules.
4. Terminations and transfers – included in monthly and weekly security procedure.
5. Transport and role change form and transport procedure.
6. Role risk methodology.
7. Role naming conventions.

We asked Security for the following specific policies related to system security:

- Changes to system parameters; (See also finding # 5)
- Changes to powerful or sensitive roles/profiles/transactions; (See also findings # 1, 2, &3)
- Managing segregation of duties for the ERP team; (See also finding # 2)
- New user setup;
- Updating security related to employee terminations and transfers; (See also finding # 8)
- Firefighter IDs Controls; and (See also finding # 2)
- Contract and temporary Users. (See also finding # 7)

FINDING:

The following table shows the results of our request:

Policy requested	Policy provided
System Parameters Changes	No (There is a weekly review of some parameter changes, but not for all of them)
Powerful or sensitive roles/profiles/transactions changes	No
ERP team segregation of duties	No
New user setup	No (New user setup procedures and forms do include policy elements, such as the approval process and the User's Acknowledgement of Responsibility.
Terminated and transferred employees security updates	No (There is a weekly review for these employees and follow-up procedures
Firefighter IDs Controls	No (There are Firefighter IDs use approval and logging procedures)
Contract and temporary Users	No (Each one has Access Request Forms)

RECOMMENDATION:

Security should develop policies for the areas noted above and any other areas deemed important to managing SAP security.

ERP SECURITY
MANAGEMENT RESPONSE:

"It is our understanding based on our meeting with the Internal Audit team that we need specific policies that support our function and outline management control as reflecting 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 this type of document(s) based on our operational procedures and guidelines and present to ERP management for approval by 12/31/2012.

"It is our understanding based on our meeting with the Internal Audit team that we need specific policies that support our function and outline management control as reflecting 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 this type of document(s) based on our operational procedures and guidelines and present to ERP management for approval by 12/31/2012.

In regards 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 has been provided to the internal audit team.*

The ERP team is segregated into five sub-sections.

1. *Functional Team – HR*
2. *Functional Team – Financial/MM*
3. *Development*
4. *Security*
5. *Basis"*

**ASSESSMENT
OF MANAGEMENT RESPONSE:**

ERP management has referred to formal policies and procedures as "requested by Internal Audit". It is important for the Information Technology Department to establish their formal policies and procedures related to all aspects of security. This reflects the existence of governance, strategy, vision, awareness of risk, priorities of management controls, and succession planning. This also provides a baseline to ensure proper procedures are adhered to by all personnel in a uniform manner.

We understand ERP Security will compose formal policies based on their current procedures and present them to management for approval by December 31, 2012.

7. Contract and Temporary Workers Access Period

Background:

ERP Security creates a User Master record (UMR) when they give an employee or another authorized worker, such as a contractor or temporary worker, access to SAP. The UMR includes the end date of their access, called the “Valid Through” field. Thus, if this field contains a value of “12/31/9999” or is blank, the UMR (user access) will remain valid indefinitely.

The ERP team provides all departments every quarter with a listing of SAP access for all employees, temporary, contractors, and consultants. The departments are asked to review and signoff on all access. These procedures were approved and recommended by the external auditors to demonstrate a review process with signoff by the departments is being conducted and repeated every 90 days.

The ERP team does not know unless notified by the department how long a temporary or contactor will be engaged and therefore need access. If a department decides to delimit access at a certain date, the security team enters the expiration date. The security team does check for users that have not logged on for more than 120 days and if they see a contractor or temporary ID on the list. There currently are no contract or temporary users that meet this criterion.

We reviewed a sample of contract and temporary workers’ UMR for a reasonable validity period.

Finding:

We noted the UMRs for all contract/temp employees were set up with no Valid Through date or one of “12/31/9999”. Because contract/temporary workers are not the same as permanent employees, there is a risk of having an open user account subject to unauthorized access.

Recommendation:

Security should grant a definite period for access to contract and temporary workers. This might be 90 days for contractors and temporary workers engaged on a short term basis, or a year for contractors and temporary workers engaged for an indefinite period.

ERP Security
Management Response:

“We will raise this issue with IT management and align our policy with other network and system access that is granted to temporary and contractor personnel. In the interim, we have notified the departments that any Temporary or Contract employee that has not logged in within the past 90 days will be terminated.”

Assessment
of Management Response:

The proactive security protocol of terminating temporary or contract employees who have not logged in within 90 days proposed by ERP will remediate the issue.

8. Transferred Employee’s Access

Background:

Access for much of the daily business transactions has been tied to a Department level. When an employee transfers from one Department to another, their SAP transactional access will have to be granted for the new Department and should be deleted for the transferring Department. Each week, Security pulls a list of the transferred employees from the Human Resources records and sends an e-mail to both the transferring and receiving Departments, requesting management’s instructions on changes to the employee’s access. We reviewed a sample of transferred employees for consistency of this procedure.

Finding:

No specific SAP system security action is taken (preventative control) when an employee is transferred. Without specific preventative controls, unauthorized transaction abilities or system access may exist.

Recommendation:

We recommend that Security remove all but the general display roles assigned to all FI/MM Users when they find a transferred employee, but have not already received instructions from the transferring and new Departments. Also, we recommend that Security require a completely new User Access Request form from the new Department so the User only has the access required for their new job and cannot inadvertently enter a transaction for another area.

ERP Security Management Response:

“As part of the weekly security procedures the Security Team checks for any intradepartmental transfers. The outgoing and incoming departments for the employee are always notified and provided with a list of access the employee has in SAP. In addition, access for all employees is sent to each department for signoff on a quarterly basis. These procedures were approved and recommended by the external auditors to demonstrate a review process with signoff by the departments is being conducted.

Departments are inconsistent in providing a timely and accurate response back to the ERP team. Often the department is notified multiple times via email or phone calls. These items result in burdening the ERP team (in both time and responsibility) with trying to get an appropriate response from the incoming department. We have concluded the best course of action is to discontinue all access until the incoming department has communicated what access the employee will require. This has been communicated as a policy to all departments.”

Assessment of Management Response:

The commitment to discontinue a transferred employee’s access until they have received direction from the new department is a sufficient proactive measure that satisfactorily improves the current process and will remediate the issue.

CITY OF HOUSTON

Information Technology
Department

Interoffice

Correspondence

To: Ronald Green
City Controller

From: Mary Ann Grant
Deputy Director
ERP Business Support Team

Date: May 21, 2012

Subject: **ERP Security Audit**

Controller Green,

In regards to the ERP security audit conducted by the Controller's Office, we have reviewed the audit findings and have verified the Information Technology Department responses contained in the report are those of ITD management.

We recognize that security is an evolutionary process that must always be monitored and continuously refined in today's Information Technology environment. Please review our detailed responses to the audit findings and the action items we deem necessary. We thank your internal audit team for working with our ERP Business Support Team.

Sincerely,

Mary Ann Grant

Mary Ann Grant
Deputy Director
ERP Business Support Team

Cc: David Schroeder ✓
City Auditor

Read:

CTT 5-22-2012

Charles T. Thompson, CIO, CGEIT
City of Houston – Chief Information Officer