

Audit Report



January 2011

Audit of the Enterprise Resource Planning System Implementation

Management identified and addressed most system implementation risks but improvements are needed related to security, payment controls and training

This Page Intentionally Left Blank



THE CITY OF SAN DIEGO

DATE: January 31, 2011
TO: Honorable Mayor, City Council, and Audit Committee Members
FROM: Eduardo Luna, City Auditor
SUBJECT: Audit of the Enterprise Resource Planning System Implementation

Transmitted herewith is an audit report on the Implementation of the Enterprise Resource Planning System. The Executive Summary is presented on page 1. The Administration's response to our audit recommendations can be found after page 31 of the report.

If you need any further information please let me know. We would like to thank the OneSD team, as well as representatives from other City departments for their assistance and cooperation during this audit. All of their valuable time and efforts spent on providing us information is greatly appreciated. The audit staff responsible for this audit report is Stephen Gomez, Kyle Elser and Chris Constantin.

Respectfully submitted,

Eduardo Luna
City Auditor

cc: Jay M. Goldstone, Chief Operating Officer
Wally Hill, Assistant Chief Operating Officer
Mary Lewis, Chief Financial Officer
Ken Whitfield, City Comptroller
Debra Bond, OneSD ERP Support Director
Jan Goldsmith, City Attorney
Andrea Tevlin, Independent Budget Analyst

OFFICE OF THE CITY AUDITOR
1010 SECOND AVENUE, SUITE 1400 • SAN DIEGO, CA 92101
PHONE 619 533-3165, FAX 619 533-3036

To Report Fraud, Waste, or Abuse, Call Our Fraud Hotline: (866) 809-3500



This Page Intentionally Left Blank

Table of Contents

Executive Summary	1
Introduction.....	2
Background.....	2
Objectives, Scope and Methodology	3
Audit Results.....	7
Conclusion	21
Appendix A – Definition of Audit Recommendation Priorities	22
Appendix B – Reviewed Areas with No Current High Risk Issues	23
Appendix C – Previously Reported Remediated High Risk Issues	27

Executive Summary

The City recently completed the Enterprise Resource Planning (ERP) implementation project that began in February 2007. We have been auditing this implementation since October 2008 due to the risk inherent to a project of this size and scope.

We found management was generally quick and proactive in identifying and addressing risks in project management, integration testing, and data conversion, cut-over, and retiring legacy systems. However, while the City made improvements in security, the City remains at risk. Furthermore, we found additional improvements are needed in payment controls and the City requires more focus on employee training in order to fully utilize the City's significant investment in the system.

We released an update report in June 2009 which presented our identified issues, which included project governance, potential project delays, system functionality, and security issues. The majority of these issues were remediated prior to the system went live for the Financials and Logistics module in July 2009 and the Human Resources module in December 2009. Overall, our view on the project was favorable with some high risk concerns in the areas of:

- Missed deliverable dates which could potentially delay project components or the project as a whole;
- Having not received the Accounts Receivable (AR) component contract update, potentially resulting in an inadequate implementation or a delayed implementation of the AR module;
- Having not received the overall strategy for implementing Security, and unable to identify if certain key areas of implementing security were being addressed such as monitoring;
- Missing key governing/contractual documents over the entity managing the implementation contract and project expenses.

Medium and low risk issues as well as general suggestions were conveyed to the project team as they were identified. The project team resolved most issues prior to the respective date the system went live. Currently, the project team is in the process of resolving any remaining concerns.

Status of Identified Issues

In our previously issued update report in June 2009, we made seven recommendations addressing high risk issues. Five of the issues were resolved, and the two remaining issues,

which address the Security Strategy and Security Policy, are scheduled for completion by the end of this year.

Since our June 2009 update report, we identified three additional issues in the areas of post-implementation security, training and payment controls. In general, management has been proactive in identifying and addressing issues within the new Enterprise Resource Planning system. They are currently in the process of addressing these three additional issues.

Introduction

In accordance with our audit work plan, we conducted an audit of the Enterprise Resource Planning (ERP) Implementation. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We would like to thank the implementation management and staff, as well as representatives from other departments for their assistance and cooperation during this audit. All of their valuable time and efforts spent on providing us information is greatly appreciated.

Background

In February 2007, the City began an Enterprise Resource Planning (ERP) system implementation. The City selected SAP as the system to implement with Axon, currently a division of the HCL Company, as the implementer. The push to upgrade, secure, and bring the City's legacy systems up to date came in a large part from the 2006 Kroll Report, which identified significant control weaknesses that the City accepted and agreed to remediate. In December 2008, the City dismissed Axon as the implementer of the project and made significant adjustments to the City management team as they had run into several difficulties, including falling behind schedule on several occasions and concerns over the quality of work being delivered. SAP was brought on to complete the implementation as both the ERP vendor and ERP implementer.

The City selected and purchased the Finance and Logistics Module and the Human Capital Management Module to replace its core legacy financial and human resource systems. The project took a two phase approach for implementing these SAP modules. Phase one implemented the finance and logistics module; phase two implemented the human resources module. Due to complications with the Accounts Receivable component of the Finance module,

implementation of the Accounts Receivable component was delayed. The go-live schedule for the various phases is described in the table below.

Table 1: Initial Completion Schedule vs. Actual Completion

Phase Name	Scheduled “Go-Live” date	Actual “Go-live” date
Finance and Logistics	July 2009	July 2009
Human Capital Management (Human Resources)	October 2009	December 2009
Accounts Receivable (A component of the Finance module)	December 2009	March 2010

Source: Project Management Office Schedules

As of August 2010, the City projects the final cost of the ERP Implementation to be \$51.8 million, not including the cost of debt service.

An ERP implementation with the scope of replacing core financial, logistical and human resource systems involves inherent risk. There is significant risk of unanticipated cost and the potential for creating systems which are inadequate to perform the day to day business. Therefore, proper planning and an ongoing audit function become necessary to reduce this risk.

Objectives, Scope and Methodology

We conducted a review of ERP implementation activities to:

- Determine if the City’s key financial activities are being adequately reviewed and documented prior to the new system implementation to ensure key financial processes are properly addressed by the new system, and;
- Determine if the system was adequately tested prior to implementation.

The scope of this report covers the implementation from where SAP took over as the implementer in December 2008 to the completion of the Accounts Receivable Module in March 2010. Additionally, the scope includes post implementation testing for Security and Support current to June 2010. Post implementation review is an essential component of an implementation review to confirm key stabilized components where executed as planned. As the

project had previously encountered significant schedule and implementation management issues, our audit aimed to detect risks that may derail, delay, or significantly impact the required functionality of the implementation and report these issues to the Audit Committee.

Implementation Review Standards

An ERP implementation consists of taking a commercial enterprise product and customizing the selected modules to replace and improve business functionality over the systems being replaced. An implementation of this magnitude is a very complex process, and presents unique challenges to each implementation. However, there are standard aspects to each implementation as well. A system implementation is a part of a standard process known as the System Development Life Cycle (SDLC). The Information Systems Audit and Control Association (ISACA) defines the SDLC as:

The system development life cycle is the process, involving multiple stages (from establishing the feasibility to carrying out post implementation reviews), used to convert a management need into an application system, which is custom-developed or purchased or is a combination of both.

ISACA further provides standards and guidelines for performing audits of these implementations. Our Scope was developed incorporating ISACA's Control Objectives for Information and related Technology (COBIT) standards, SDLC Review Guidelines (ISACA Document G23) and ERP Systems Review Guidelines (ISACA Document G21). This approach allows us to review the standard implementation components, as well as providing a standardized methodology for reviewing the unique challenges within this implementation.

The following audit scope was developed using the ISACA standards and guidelines discussed above, following a risk based methodology. We separated our audit into the following categories or key risk areas:

Table 2: Implementation Audit Review Categories

Category for Review	Includes the following Areas
Project & Contract Management	Deliverable & Issue Management, Project Team Training, Governing Documents, Project Requirements, and Blueprint Management
Integration Testing	Integration Testing Cycles
Data Conversion	Conversion Strategies, Cross Walk, Mock Conversion Testing Cycles
Reporting	Roll-out Strategy, Requirements prior to go-live, post go-live support and roll-out
Cut-Over and Stabilization	Strategy, Support Level Requirements & Delivery Methodology
Training and Communication	Training Roll-out, Methodology, Key Areas Addressed
Retiring Systems	Historical Data Storage, Access, System Phase Out
Security	Security Implementation Strategy, Governing Documents, Role Mapping, Access Controls, Process Controls

We should note that entity level SAP controls for individual business units were not included in this audit due to the resulting increase in scope. We did however perform a high level centralized internal controls review of the Governance Risk and Compliance (GRC) module and City access. These controls will be comprehensively reviewed in future audits of those entities. Further, the comptroller’s internal controls group is in the process of reviewing and documenting these controls through their Internal Controls over Financial Reporting (ICOFR) project.

In the review of each section, we employed the following methodology customized for each primary area reviewed.

- We first determined components within each category to review based on risk to the implementation completion, intended functionality, and schedule;
- Reviewed component implementation methodology and plans for sufficiency (such as the strategy for Integration Testing, and sampled the planned tests to perform);
- Observed components implementation and tracked to planned methodology to ensure that there was no disconnects between what was planned and documented and the work that was actually performed;

- Reviewed implemented components using judgmental sampling to confirm that the end result came out as planned, or was appropriately adjusted;
- Reported issues discovered throughout the process based on risk, and conveyed recommendations directly to the implementation component lead.

Due to the nature of the ERP implementation, reporting issues in a timely manner presented unique challenges as compared to a standard audit. As is the case with system implementation audits, issues present a moving target. Our reporting process takes into account the fact that issues are expected to occur during an implementation and do not necessarily present a risk to the project. Further, management had several methods available at any given time during the project to identify and remediate issues. As a result of the fast pace of the implementation and the immediate management need for information, we developed the following reporting process.

- Initially, we approach each potential issue with the appropriate section team lead. Medium and low risk issues are not formally reported though may be presented to a higher level of management if required. This results in quick response times to most issues and quick resolution of the larger amount of smaller issues as they arise;
- High risk issues, based on potential impact to project, are brought to management's attention. Issues that could have a potential impact to the project's implementation are formally reported at a high level if they are not remediated in a short time frame or carry a significant risk to the project's adequate and on-time completion;
- High risk issues are communicated defining the condition, criteria, cause, and effect.

Our focus on reporting exists for the purpose of first, ensuring that project management is independently aware of any issues that arise. We further developed a process to ensure that any high risk issues which could potentially affect the adequate and on-time project's completion are reported to the audit committee regardless if the management states that they will remediate it.

No issues requiring immediate action by the Audit Committee occurred during our review, though as previously described, we provided an interim report in June 2009 summarizing high risk findings identified to that point. Most of the issues reported in June 2009 were in the process of being addressed or had already been addressed at the time of reporting due to management's strong issue resolution processes in place.

The issues reported to the committee are high level, such as requiring a policy verses the technical details of what needs to be implemented, while those presented to the team leads will contain the required details for appropriately addressing the issue.

Audit Results

Management identified and addressed most system implementation risks but improvements are needed related to security, payment controls and training

We found that Management was generally quick and proactive in identifying and addressing risks in project management, integration testing, data conversion, reporting, cut-over, and retiring legacy systems. However, the City needs to address concerns related to system security, controls associated with vendor payments, and training for City staff. By so doing, the City can fully utilize its significant investment in the OneSD ERP system. Specifically, we found the following issues still requiring attention –

- **Security Issue** – Monitoring over ERP support department staff system access controls have not been fully implemented,
- **Payment Controls Issue** – Controls against the creation of vendors and payment of invoices should be strengthened,
- **Training Issue** – Inconsistent on-going City training for utilizing the ERP system, and
- **Previously Reported Issues** – Two of seven previously reported issues, primarily in security, remain outstanding.

During December 2008 through June 2010, we conducted an on-going review of the OneSD implementation as the system was implemented. We identified a number of issues in which we communicated to OneSD staff our observations of implementation risks in eight areas. These areas included:

1. contract & project management;
2. integration testing;
3. data conversion;
4. reporting;
5. cut-over & stabilization;
6. retiring of legacy systems;
7. security; and
8. training.

Other than the issues discussed above, management addressed most of the implementation risks. A summary of our detailed testing performed is presented in Appendix B, and Appendix C provides information on the five issues and recommendations previously provided in the City Auditor's June 2009 report that have been implemented.

Standardized monitoring over high risk system access of the ERP Support Staff has not been implemented within the production SAP environment to ensure circumvention or misuse of access will be identified

Security addresses the controls within the SAP system to ensure that users are not able to make inappropriate changes to the City's new financial system.

Our review of security included the following areas:

- General User Creation (Provisioning) - *The process of adding users to the system;*
- General User Segregation of Duties Management - *Managing users access to make sure they can't perform conflicting functions such as the ability to add a vendor and pay that vendor;*
- Implementation and use of the Governance Risk and Compliance (GRC) Module - *The GRC module is a tool built into the SAP system to make managing user access for the thousands of users in the system and managing controls over countless daily transactions preventing unauthorized activity easier, more comprehensive, and automated;*
- Technical User Creation (Provisioning) - *The process of granting ERP Support Technical Staff access, and management of that access;*
- Technical User Security & Monitoring – *The processes in place to prevent highly powered ERP Support Department Technical Staff from misusing their access;*
- Post Implementation Security Review – *A review of the stabilized and implemented security in place primarily focused on the SAP IT type roles and SAP IT type risks, but includes a review of the security in place for the normal user as well.*

During our post implementation security review, we found the current security level appropriately focuses on the role aspect of implementing security and the team is consistently working on tightening the security within the system. This aspect of security primarily addresses the creation of users to ensure that they are not granted too much access when their roles are initially created or additional access is requested through the approved City process. The security and internal control teams have successfully managed to bring the amount of "Segregation of Duty" conflicts for standard users down to zero as of August 2010.

However, the monitoring aspect of security has not been adequately addressed as applied to the ERP support Department Technical Staff. While the tools with monitoring capability are built

within the system or have been implemented as separate components, security monitoring is not taking place with any consistency.

If an ERP technical staff member misused their access, their actions would most likely go undetected. We identified additional risks that were provided to security and were immediately addressed. The detailed remaining high risk issues are described below.

Results of Testing

We found that the City does not have a defined and consistent monitoring program for technical users within the ERP system. Specifically, individuals retain unfettered access to critical areas exposing the City to the risk that unauthorized SAP IT Support staff can steal data or modify the ERP system without proper authority, or worse, without the City's knowledge.

Currently, the City does not have a defined and consistent monitoring program over technical users within the SAP system to ensure that misuse of technical access will be identified. For example, we found that an IT user had created a "generic user" with "SAP_ALL" access. The problem with this type of access existing on the City's new financial system lies in the fact that this access allows the user to do anything in the system without being able to see who did it.

Further, overlap exists between technical user types. For example, security team members have access to system administrative type functions normally restricted to "BASIS" users, or SAP system administrators¹. In the extreme case, as occurred in June of 2010, where an IT user had "SAP_ALL" access using a generic account (an account not directly tied to anyone) – that user essentially had the access of every type of user in the system. This type of access includes access to all payroll, personnel, and IT system administration staff, essentially creating a Segregation of Duties (SOD) problem. The ERP support department is implementing additional controls to prevent this from happening again.

Finally, the production environment does not require the use of complex passwords for authentication as required by the City IT policy (section 2.5.1). The lack of strong password requirements increase the risk of an account being compromised, such as the generic account with the access described above.

The Information Systems Audit and Control Association (ISACA) specifies in its Control Objectives for Information and related Technology (COBIT) that a logging and monitoring function over the security implementation should be implemented to enable the early prevention

¹During our SAP security review, security users had access to programs normally restricted to SAP system administrators (BASIS) such as the ability to modify the SAP clients, and the ability to maintain the technical settings table.

and/or addressing abnormal activities². In the case of the City's new financial system, special attention should be paid to the ERP support department's access to the system, as they will always have more access than a standard user. Accordingly, this requires that the highest risk areas be identified and monitored using appropriate methods to mitigate the correlating risk.

Standardized and consistent monitoring of the ERP support access has not been implemented for several reasons.

- 1) The system has only been live since July 2009 with various components going live as recently as May 2010. According to an IT official, the priority has been designing roles to grant user's appropriate access and fine tune that access.
- 2) Monitoring can carry a high added expense in three key areas.
 - a. Time and expense for performing the risk assessment to identify the key risk areas, and design appropriate monitoring to mitigate those risks.
 - b. The storage and computing resources needed to maintain effective monitoring.
 - c. Time and resources required to regularly review the monitored controls.
- 3) A comprehensive security strategy has not been completed to ensure the risks of insufficient monitoring would be identified.

If the IT user was malicious, he or she would be able to steal, delete or modify financial data in the system without being detected. According to the Identity Theft Resource Center, there were at least 662 data breaches in 2010, exposing more than 16 million records. Internal data theft was among the leading causes. The data stolen primarily consisted of personal and financial data with the estimated average annual cost of 3.4 million per compromised organization per year. The actual number of breaches is most likely much larger as many organizations do not disclose data breaches.

In order to correct the identified deficiencies, we recommend management:

Recommendation # 1:

Implement targeted security monitoring over ERP support staff access in the production environment. Specifically, management should: **(Priority 2)**³

- a. Perform a risk assessment/cost benefit analysis over the access and system functions that pose the greatest risks to determine which controls merit the associated expense of generating logs or using personnel's time to regularly review. Automated review, such as the use of scripts to identify certain unauthorized or high risk activity should be used wherever possible to cut back on personnel time and log retention requirements.

² COBIT DS5.5 Security Testing, Surveillance and Monitoring

³ See Appendix A for information on recommendation priority setting.

- b. Critical controls should have an automated trigger or alert such as an email generated from the use of a critical transaction, and sent to the appropriate party for review.
- c. Risks, controls implemented/mitigated risk, method of implementation, and frequency of review should be documented in the monitoring portion of the SAP Security Policy.
- d. Documented reviews of monitoring controls should be performed at least semi-annually over the implemented monitoring to ensure that the monitoring defined through this exercise are adequate, effective and consistently in place.

Recommendation # 2:

We recommend the security group clearly document technical roles within the SAP environments and enforce Segregation of Duties between technical roles wherever possible. Specifically, we recommend: **(Priority 2)**

- a. Access for each ERP support department staff should be restricted to only the access that user requires to perform their day to day functions.
- b. ERP support department staff access should be reviewed at defined regular intervals on a semi-annual basis at a minimum.
- c. Additional access beyond standardized support staff roles must be approved by management external to the ERP support department staff, and should be provided through a monitored account such as a Firefighter account.⁴
- d. Unmonitored generic accounts should not exist in the production (live financial) environment.
- e. Logs generated from monitored accounts (such as firefighter accounts) should be reviewed at defined points and signed off by the supervising manager when they are in use. Simplified automation can be employed such as automating the generation and sending of the log to the manager via email, whose reply can serve as his auditable electronic sign-off.
- f. Security logs should be stored in a location where the SAP IT teams do not have access to modify the logs.

⁴ In emergencies, SAP GRC Access Control (AC) enables users to perform activities outside their role under superuser-like privileges in a controlled, auditable environment. This account is known as a firefighter account.

Recommendation # 3:

Ensure that production client authentication settings meet and continue to meet the City Standard authentication requirements defined in the City Security Policy (Section 2.5.1). **(Priority 2)**

Recommendation # 4:

Management should take precautions to ensure that no user can increase or modify their own access⁵. If it is not feasible to limit this capability to users required to provision access, controls such as monitoring their account permissions for modifications using a standardized methodology should be implemented to mitigate this security risk. **(Priority 2)**

Additional controls should be added to reduce the risk of duplicate payments to vendors

We found that additional controls should be added to reduce the risk of duplicate payments to vendors as a result of the existence of duplicate vendor names in the SAP. The SAP's vendor database includes duplicate vendor names that were imported from the old system. Management advised that they "cleansed" a significant number of duplicates from the vendor master record prior to importing them to SAP and continue to remove them as they are identified, but duplicates still exist. Adding to this problem, controls were not as strong around the creation of vendors initially after SAP go-live, which increased the risk that additional duplicate vendor names may have been created. Further, there is no longer a report checking across vendors for duplicate payments as existed in the previous system.

Management has implemented tighter controls around the creation of vendors and payment through Purchase Orders (PO's) since SAP has gone live. PO's reduce the likelihood of duplicate payments through additional controls including assigning a defined fund amount available for a defined purpose. Currently, most payments go through PO's, which greatly reduces the risk of a duplicate payment. However, significant payments are paid through the use of one time vendor payments or direct invoice payments to vendors, which have a higher risk that a duplicate payment would not be detected.

According to the Office of the Comptroller's documented process, once a department approves a payment, the Comptroller staff reviews the payment by comparing the data entered into SAP to the invoice. For SAP to detect a duplicate payment, the invoice number, invoice date and vendor number must match. However, if that same payment had been made to a different vendor name (including duplicates) there is no standard control that will catch the duplicate payment. For Example, if two vendors had been created and one was entered as "Interactive Data" and the other as "Interactive Data Corporation," they appear as two completely different vendors in SAP.

⁵ The security team has begun implementing controls to address this access, starting with removing access to modify users in the Production Environment (not confirmed).

If one invoice is then accidentally processed twice to each of these vendors, SAP will not stop the transaction. Also, in the case of a one time vendor payments, the SAP control cannot catch a duplicate payment using this methodology, as there is no vendor number to match.

If the comptroller's manual review does not catch a difference in the vendor name or invoice number, a duplicate payment can be processed. If the Comptroller were to require a "unique identifier" for all vendor/businesses, it would significantly aid in identifying duplicate vendors.

Moreover, in the previous system, duplicate vendors were allowed, but reports were set-up to run daily that would identify duplicate payments. However, SAP does not have a duplicate payments report that runs across multiple vendors, but a similar report could be created for SAP and used to help identify duplicate payments among high risk payment types (non PO invoices).

By adding these additional controls to reduce the risk of duplicate payments, it may save the City from significant overpayments. According to a study by the Institute of Finance and Management, duplicate payments – most of which arise from duplicate vendor entries - are estimated to account for 1.3 billion in losses per year. Invoice fraud, which may be prevented or detected by sound master vendor file controls such as ensuring duplicate vendors do not exist.

Recommendation #5:

To mitigate the control weaknesses related to the vendor database, we have made the following recommendations: **(Priority 2)**

- a. Create and run a periodic report across non PO invoices looking for duplicate payments similar to the previous mitigating controls report that was in place prior to the implementation of SAP.
- b. Analyze the City's vendor database and remove all duplicate vendor data.
- c. Implement a required "unique identifier" for a vendor/business, such as the tax ID, for new vendors and create a process for adding the unique identifier to existing vendors.

Inconsistent Post-Implementation City training for utilizing the ERP system impacts the City's ability to fully utilize its ERP system

The Training and Communications areas were selected for review as the primary components for the general employee's acceptance and use of the system once it has been implemented. We participated both as an office incorporated into the changes as well as objectively reviewing the strategy, execution, and completion of the training and communications processes.

Training is the process of introducing City employees to the new methods of performing their function within SAP. There are always complications with training in that it depends not only on how well the information is presented, but also in how attentive the employees being trained are and how much exposure they have to the fundamental concepts within SAP prior to the training. Communication assisted training as well as general preparation for the implementation of the ERP system and what type of things to expect for the various departments. The communication strategy employed in this rollout included two primary general department communication levels, in that the "Change Champions" addressed the general employee and allowed general information to be brought to the departments as well as general department employees providing feedback to the project team. The Project Action Committee or "PAC" provided a management layer of two way communication to keep each department updated on current progress as well as management feedback regarding their respective departments.

Taking the training and communication approach into account, our review included the following components:

- Training and communications strategy review;
- Participation in both general levels of communications;
- Observation of training rollout;
- Training and communications rollout assessments;
- Issue resolution evaluation;
- Post-implementation training review.

During our review of Communication and Training, we found that the communications and training staff provided a strong level of communication and training. The team consistently adjusted the training to the challenges that arose and City needs as the project progressed. The further integrated a strong issue resolution process to quickly adapt their methodology to challenges as they occurred. We did not identify any high risk issues during the ERP implementation in the area of training and communication, and all low and medium issues as well as any suggestions were communicated to the project lead and management where appropriate during the implementation.

Continuing education should be provided in a centralized and consistent manner available to core departments at a minimum. Complications included the level of minimal exposure most employees had to SAP prior to the training and the amount of personnel trained in a relatively short amount of time have presented challenges for departments after the implementation. This is a normal challenge for departments to adjust for a significant amount of time after the initial system stabilization period.

Initially, after the stabilization period had ended, departments were responsible for additional training. The training would be conducted through the super users and super trainers that had participated in the implementation. Departments able to include more staff as super trainers or super users during the implementation would have more trainers in their department after the implementation was complete. New training would be provided through a citywide training team. However, as SAP is a centralized system with centralized functions, this results in various departments addressing similar on-going training in various ways with varying resources, which do not necessarily meet a sufficient standard. In other cases, employees may not receive any additional training other than the original SAP introduction sessions originally provided by the ERP Implementation Team.

Results of Testing

We found training is being inconsistently implemented in various departments resulting in some departments not receiving enough training for their personnel to fully utilize the ERP system, and provide a strong return on the City's multi-million dollar investment.

Effective education of all users of IT systems requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training program increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls⁶.

Users' ability to use the SAP system effectively results partially from the user's previous exposure to SAP and the amount of training received. In the case of the implementation, most users had no previous or minimal exposure to SAP before receiving initial training. This results in additional and on-going training requirements.

Management planned for this requirement in training "super-users" who were involved in the implementation of their respective components for their departments. They further planned to make each respective department appropriately responsible for training their employees. However, not all departments are able to provide adequate on-going training for their personnel.

⁶ COBIT Control DS7 – Educate and Train Users

According to City personnel, various departments do not have enough resources to provide on-going training for their personnel, or the more highly trained personnel are those most in demand to perform their functions and not available for training users.

Management has already identified this issue prior to our notifying them of our tandem efforts, and pro-actively issued a survey to determine the current impact to City departments. We recommend City Administration should:

Recommendation #6:

Complete an evaluation for providing centralized continuing education, and ensure that at a minimum, classes addressing the core functions of SAP should be provided on a periodic basis, and made available to the appropriate departments. Specifically, management should:

(Priority 2)

- a. Develop a training schedule for specific requirements based on the results of the survey they conducted.
- b. Make the training schedule available to City Employees, using means such as email or the OneSD intranet site. Further a method for feedback after each training should be provided, such as a survey, to ensure the trainings remain effective.
- c. Ensure enough resources are dedicated to provide on-going training.
- d. Ensure that skilled employees have scheduled dedicated time to train users in their respective proficiency.

Interim Audit Report Results

In June 2009, we presented an interim Implementation Audit Report identifying seven high risk issues that were in various stages of remediation. We found management remediated five of the seven issues and the remaining two issues affecting security remain in progress.. The first issue is the lack of a documented comprehensive security strategy to ensure that all areas of security were planned for and addressed. The second issue addresses the lack of a documented security policy to define the manner in which the security would be maintained. This section provides a status update on the two issues still outstanding and management's timeline for implementation.

PREVIOUS ISSUE 1: A Comprehensive Security Strategy, defining security risk areas to the ERP implementation and mitigation of those risk areas to ensure that all key components have been addressed and compliment the City's security strategy has not been documented.

During the Implementation, a comprehensive security strategy should have been prepared and provided to audit for review. Without a comprehensive security strategy, it is not possible to comprehensively determine the aspects of security that were planned for implementation, or the approach that was planned.

We found that the general security would be role focused, access would be controlled and monitored through the Governance Risk and Compliance (GRC) module and Support would use firefighter (emergency privileged accounts with monitoring) roles when operating outside their standard role. However, specific areas to be addressed and the manner in which they would be addressed were not documented. For example, any references to monitoring during interviews tended to be vague, such as stating that the GRC module would be used for monitoring, while not defining even the types of monitoring and the frequency of the monitoring to be performed within the GRC module.

The Information Systems Audit and Control Association (ISACA) provides guidance for implementing a security architecture for environments such as an ERP implementation. The reference model ISACA provides is known as Control Objectives for Information and related Technology (COBIT), which specifies that business risks and compliance requirements should be translated into an overall security plan⁷. In the case of the ERP system, a comprehensive security strategy should addresses the security threats posed to the individual system environments with the primary focus on the live financial system, known as the production

⁷ COBIT Control DS5 – Ensure System Security

client. This strategy would define controls over access, technical user provisioning, areas to be monitored, and restrictions over technical roles in all environments.

The strategy should further tie into the network infrastructure security to ensure that external security policies address vulnerabilities such as those over the infrastructure and operating system on which the SAP application and database reside.

We presented the following information during the implementation update to the audit committee in June 2009.

During our review of the security implementation as late as April 2009, we found that the project was lacking a comprehensive, unified, and concise Security Strategy for the implementation of Security within the SAP implementation.

If not corrected, the risks include:

- *Additional time and resources required to rework Security aspects during the implementation;*
- *An inadequate and incomplete security solution;*
- *Insufficient and ineffective use of the security features provided within SAP;*
- *A reactive and segmented approach to security implementation and management.*

Audit recommended creating a comprehensive and unified security strategy which will tie into the security goals of the City's IT organization

Management is in the process of addressing the recommended areas in the Strategy document

Management is in the process of completing these missing components for a comprehensive, unified and concise SAP security strategy that will map to the City's strategy. The current blueprint document will be expanded to include the recommended areas and complete security strategy.

We continued to monitor the implementation of Security, and when the security team informed us the security within the SAP Environments had stabilized, we performed a security audit. One high risk item comprised of several components remains, while the others issues were quickly corrected. Medium and low risks as well as recommendations and suggestions were communicated to the security team both formally and informally depending on the associated risk.

Previous Recommendation #3 (Report 09-018):

In our report issued in June 2009, we recommended that the SAP IT security group:

Create a comprehensive and unified security strategy which will tie into the security goals of the City's IT organization.

To fully implement this recommendation, the IT security group should ensure that:

- a. The expected primary risks within each environment and the mitigation methodology of those primary risks.

- b. The appropriate standards of security for each environment.
- c. The strategy should further differentiate the type of risks to the environment, such as those presented by the standard user and the technical user, as well as the data risks such as raw production data in the development and quality assurance environments.

Status

The Security Strategy was provided to audit as of December 30, 2010 and will be reviewed as part of our current audit follow-up process.

PREVIOUS ISSUE 2: A policy defining and standardizing security parameters within the SAP environments has not been documented

A security policy describing the expected security standards and criteria to ensure consistent and complete security on a daily basis has not been created.

SAP Security comprises of both automated and manual security processes. Automated security processes must be defined and documented to ensure that they are adequate and the manual processes do not overlap. Manual security processes pose the greater risk however, as they require consistent upkeep by personnel. These requirements must be documented to ensure that security personnel know all their daily, weekly, monthly, and annual requirements as well as to allow review of sufficiency and compliance by outside sources such as an audit.

Areas addressed within the SAP Security Policy should include Standard User Provisioning, General Controls approach, and General User and Transaction Monitoring. General User provisioning overall is being managed well through the security teams provisioning methodology and Internal Controls progress in mapping and managing current City controls through their Internal Controls over Financial Reporting (ICOFR) project.

The higher risk area addresses the management of technical roles, including Support, Development, Basis (Administration), and Security as well as the mitigation of the segregation of duty conflicts inherent within those roles.

The technical roles, which carry a higher risk than the standard user as a result of their functions within the system, should have the following areas clearly defined within the security policy.

- Standard use for each group within the following environments, as well as any high risk exceptions to that use:
 - Development
 - Quality Assurance
 - Production

- All critical controls over technical access, including standard access restrictions, and firefighter account use;
- Monitoring appropriate to each group must be defined in monitoring type, method of monitoring, as well as frequency of monitoring.

General Monitoring should be documented as well, such as those surrounding the detection of circumvented general user access. Lack of a documented process encourages lax and vague manual security practices, and more potential for circumvention of automated controls where they present an “inconvenience”.

Based on our review it appears this policy has most likely not been created due to the various prioritizations of the project. However, lack of this policy can result in:

- Unbalanced focus in security, such as overdue reliance on improperly targeted automated security and inadequate manual security;
- Missed controls such as standardized critical access monitoring.

Previous Recommendation #4 (Report 09-018):

In our report issued in June 2009, we recommended that the SAP IT security group “Create an SAP Security Policy that maps to the City’s IT Security Policy.”

To fully implement this recommendation, the IT security group should ensure that:

- a. The Policy defines the expected security standards and criteria to ensure consistent and complete security is implemented on a daily basis have not been created.
- b. Expected Technical Roles activity within the SAP Development, Quality Assurance, and Production Environments.
- c. Standards for providing additional access beyond standard technical role activity within the SAP Environments.
- d. Standard controls around each technical user type.
- e. Monitoring appropriate to each group within the production environment defining monitoring type, method, and frequency. Where logs are employed, the retention policy over the logs must be defined as well.
- f. Standardized monitoring should be employed to detect circumvention of controls.

Status

The Security Policy was provided to audit as of December 30, 2010 and will be reviewed as part of our current audit follow-up process.

See Appendix C for remediated previously reported high risk issues.

Conclusion

The ERP system has been successfully implemented, and is in use within the City's Financial, Logistical, and Human Resources capacities. Additional training and time will be required to fully use the system as it is implemented today and additional modifications such as adding reports will make the system even more functional. However, several security issues and a payment control issue still remain within the system that must be addressed to ensure that the data within the system remains reliable as the core financial system for the City.

Appendix A – Definition of Audit Recommendation Priorities

Definition of Audit Recommendation Priorities

DEFINITIONS OF PRIORITY 1, 2, AND 3 AUDIT RECOMMENDATIONS

The Office of the City Auditor maintains a classification scheme applicable to audit recommendations and the appropriate corrective actions as follows:

Priority Class⁸	Description⁹	Implementation Action¹⁰
1	Fraud or serious violations are being committed, significant fiscal or equivalent non-fiscal losses are occurring.	Immediate
2	A potential for incurring significant or equivalent fiscal and/or non-fiscal losses exist.	Six months
3	Operation or administrative process will be improve	Six months to one year

⁸ The City Auditor is responsible for assigning audit recommendation priority class numbers. A recommendation which clearly fits the description for more than one priority class shall be assigned the higher number.

⁹ For an audit recommendation to be considered related to a significant fiscal loss, it will usually be necessary for an actual loss of \$50,000 or more to be involved or for a potential loss (including unrealized revenue increases) of \$100,000 to be involved. Equivalent non-fiscal losses would include, but not be limited to, omission or commission of acts by or on behalf of the City which would be likely to expose the City to adverse criticism in the eyes of its residents.

¹⁰ The implementation time frame indicated for each priority class is intended as a guideline for establishing implementation target dates. While prioritizing recommendations is the responsibility of the City Auditor, determining implementation dates is the responsibility of the City Administration.

Appendix B – Reviewed Areas with No Current High Risk Issues

Contract & Project Management

Contract management is the process of defining what tasks need to be performed to complete the project, and who is responsible for completing them. It addresses timetables as well as methods for resolving issues and disputes. Project management governs the execution of those tasks, and is arguably the most important group in the implementation of the project.

Our review of Contract and Project Management included:

- Review of Contractual and Project Governance documents such as the SAP Statement of Work, the Project Charter, and SDDPC related contractual documents. Our goal was to ensure that the project was adequately defined to meet the City's requirements;
- Tracking of Project progress and deliverables according to the contractual documents;
- Management of key project and contractual documents. This included ensuring that items such as blueprints had an enforced change control process restricting excessive modifications or adding potential project delays;
- Tracking of project organization based on contractual documents;
- Review of project issue resolution processes, both documented and in practice;
- Participation in relevant project meetings for different aspects of the project;
- We further performed reviews of project and contract management for each tested area of the implementation.

During our review, we identified 5 high risk issues in the areas of deliverables, governing contractual documents, and insufficient delivery, which we reported in our June 2009 update. These issues have since been corrected. We identified any low and medium risks as well as made recommendations to address these risks to the appropriate management during the project.

Integration Testing

Integration Testing is the stage in the project where the various components that have been designed and built are tested together. The team does this by developing testing scripts designed to run business processes on the newly integrated components to ensure they work as intended.

Our review of Integration Testing included:

- Review of Integration Testing management strategy and methodologies;

- Live observation of testing process to ensure that testing followed defined practices and results as well as to confirm testing results;
- Randomized attendance of daily meetings reviewing progress and issues encountered;
- Review of testing scripts;
- Review of issue identification, escalation, and resolution;
- Management review and oversight.

During our review of Integration testing, we found that the Integration Testing team had a very strong issue resolution processes, were very well prepared for the testing, and adjusted quickly where necessary. No high risk issues were identified during our review of integration testing. We conveyed identified low and medium risks as well as improvement recommendations to the appropriate team leads during the implementation as defined within our standard reporting process.

Data Conversion

Data conversion is the process of modifying data from the format it is stored in the legacy system to the format accepted by the new system.

Due to the risk related to a poor conversion process, we performed extensive testing in the following areas of the conversion process.

- Reviewed data conversion strategy to confirm that adequate data cleansing and testing were planned prior to moving the data from the legacy system to SAP;
- Observed & tested data load process in test and production loads;
- Reviewed issue tracking and resolutions to ensure that issues were effectively identified and addressed;
- Confirmed that adequate reviews occurred at each of the testing and load stages;
- Performed final testing of production data loaded into the live SAP environment.

We provided our suggestions as well as any findings to the project lead, and where appropriate, to project management. Items identified and presented to the team included very specific data type occurrences, such as a small range of job orders mistranslating to Internal Orders in less than 1% of a specific data type sampled, but no significant risks in the conversion methods or testing employed. We found that the conversion team was very thorough in their testing, and quick to address any challenges that occurred during conversion.

Reporting

Reports are used to view data in a usable method from the system. The reporting process is actually a portion of the design phase or blueprinting. However, as it impacts how users access the data in the system, we considered it for separate review.

In our review of this section, we focused on the teams overall reporting strategy for the initial go-live, as well as their continuing support and development of reports. Our review included:

- The strategy for providing the initial reports;
- The report selection process for go-live and future reports;
- Planning for data accessibility for current and future reports;
- Testing of report delivery;
- Final reports delivered;
- Request process and future report development process.

We found that management focused on implementing the most essential reports required for go-live and provided for ongoing support to prioritize and create additional reports after go-live. A large amount of new reports and added functionality to existing reports are still required as was expected and planned for based on management's strategy.

Cut-Over & Stabilization

The cut-over and stabilization phase is essentially where the old system is "turned off" and the new system is "turned on", and the support that is provided to the City after the new system is live. The official stabilization phase was scheduled for five weeks, however, this is only the initial high level support required immediately after go-live. We included the on-going support and stabilization plan in our review.

Our review of the Cut-Over and Stabilization process included:

- We reviewed the system cut-over plans to ensure that planning was adequate and fallback plans existed if something happened;
- Reviewed the cut-over schedule to ensure that logistical concerns were addressed. These included items such as the Human Capital Management phase going live during the Holiday season, which the City planned for and adjusted where required;
- Reviewed on the support that was planned for stabilization and on-going support planning as well as the methods used to roll out the support;
- Tested support/ticket tracking system to confirm that issues were being identified and addressed.

During our review, we found that staff adequately planned for the Cut-over and stabilization processes. Further, during the stabilization process, the team adjusted where necessary to optimize the support they were providing. Some challenges encountered in the longer term support included large volume ticket management, such as ensuring that longer term issues were completed and closed. The team continues to work on improving efficiencies in their new system. We did not find any high risk project implementation issues during our review. All low and medium risks were conveyed to the appropriate level of project management as well as any suggestions for improvement.

Retiring of Legacy Systems

When a system's functionality has been replaced and no longer required, as is the case of the systems replaced by SAP, these systems should be retired when appropriate. This saves cost in expensive data center resources as well as personnel resources.

Our goal was to confirm that the systems were in fact planned for retirement, and completely shut down were possible to save the maximum resource costs. We included the following areas in our review:

- Reviewed scope of systems to be retired to ensure adequate planning is in place to remove systems once their functionality has been replaced by SAP;
- Confirmed that the effort would remove applications and systems where appropriate;
- Reviewed shutdown procedures and processes;
- Reviewed available plans for legacy data availability.

We found that as of the time of our review in December 2009, that a group comprised of ERP project members, City IT staff, and SDDPC staff, had been formed to comprehensively retire all legacy systems resulting both from the ERP implementation and prior system upgrades and implementations. The project had identified systems for removal, and levels of shutdown, but had not yet determined all the methods for making legacy data available and still had to further develop and detail shutdown procedures and processes. The project was adequately underway for the stage in the ERP project, and was tasked with a larger scope than the ERP project. At a later date, this entire project would merit a separate audit, but we detected no high risk issues for the ERP implementation and found the project on track for the review time.

Appendix C – Previously Reported Remediated High Risk Issues

Remediated Issue 1: A formalized approach for mitigating Segregation of Duties (SOD) conflicts does not exist to ensure the SOD conflicts will be mitigated or remediated in a timely manner.

Resolution:

At the time of the June update, we had received a plan and were reviewing it for adequacy. The plan was sufficient and accepted as an appropriate remediation.

Risk Details

At the time of our review, there was no formalized approach to the management of SOD conflicts, where as the GRC module was already in the process of being installed and configured. As the planned methodology would have an impact on how the GRC components were configured for use, it was a high risk that the purpose was not defined. We presented the following information during the implementation update to the audit committee in June of last year.

During our review of the security implementation as late as April 2009, we found that the project was lacking a documented global strategic plan and methodology for addressing the mitigation of Segregation of Duties (SOD) conflicts.

If not corrected, the risks include:

- *A wide spectrum of mitigation methodologies without uniform resolutions;*
- *Additional overhead required to manage and track SOD conflicts, resulting in additional costs;*
- *Overly complex methods of managing conflicts;*
- *Inability to effectively manage conflicts;*
- *Inadequately controlled conflict mitigation.*

***The OneSD Team has provided a draft SOD Mitigation Strategy for Audit's review
Audit is in the process of reviewing the SOD Mitigation Strategy***

Remediated Issue 2: The planned Accounts Receivable (AR) module does not meet business requirements of the City and the adjustments to the Statement of Work to correct the AR implementation shortcomings have not been provided.

Resolution

The Accounts Receivable module was successfully implemented, and went live on March 1st, 2010.

Risk Details

As with all issues identified, we had had an open discussion with management over our concerns regarding the AR implementation. When we hadn't received an amendment to the SOW by April, the decision was made to include this issue in the report, as it was unlikely that if it was implemented it would meet the December deadline, or worst case as we reported, the modifications would not be made to the SOW to make the AR implementation meet the City's requirements. In the end, the implementation of the AR module was modified to be a core implementation meeting the City's initial needs and providing a platform that can be expanded in the future. While the module was delayed three months, it was successfully implemented and went live in March 2010 without any high risk issues. During our June update, we presented the following information:

During our January review of Contract Management, we noted that the AR implementation as defined within the Statement of Work (SOW) does not meet the business requirements of the City

The current Statement of Work (SOW) states that "AR will be implemented on a pilot basis for one City department yet to be determined six months after the initial Go- Live"

This presents an incomplete Accounts Receivable solution to be addressed at a later date

If not corrected, the risks include:

- *Potential failure to meet initial ERP objectives as defined in the project charter;*
- *Future costs to remediate;*
- *Additional complications due to running the legacy system in parallel.*

Audit notified management of their concern and recommended the creation of an implementation plan for a complete solution. Management advised they were aware of this issue, and are creating an Amendment to the SOW for the implementation of a core AR module to replace the current system

Remediated Issue 3: The contract defining work to be performed for the Implementation of the SAP ERP does not adequately define the items to be delivered to ensure they meet the City's requirements

Resolution

A document defining and tracking the deliverables was created in March 2009 to supplement the Statement of Work, ensuring that the completed deliverables met the City's Requirements.

Risk Details

We found that the contractual document, known as the Statement of Work (SOW), is vague both in timeline and deliverable document content. In the case of the blueprinting phase requirements, the document states that certain activities will be performed, but does not state what evidence will be submitted to ensure that these activities have been performed to the City's satisfaction.

A defined deliverable document created sufficiently in advance of a deliverable deadline will ensure that the phase activities have been performed to the City's requirements and provide a measurable timeline to ensure these tasks have been adequately completed. Upon delivery by SAP of a completed deliverable, the SOW provides the City with five Business days to accept or reject the deliverable, after which time the deliverable will be deemed to be accepted¹¹. Lack of a timely defined deliverable document can result in:

- Missed or inadequate deliverable items;
- Delays while mapping items to the SOW after the fact;
- The mandatory acceptance of a deliverable not reviewed and approved within the five business day allowance.

In order to help ensure that the City does not miss any items to be delivered, and to aid in timely deliverable sign-offs as a project progress indicator (especially important given the project's history, and the public's view of past failures) I recommend that deliverables be defined both in expected document items/contents and a more precise timeline well in advance of the deliverable due date, and preferably prior to the beginning of that deliverable phase.

¹¹ SAP Statement of Work, Exhibit 1 p. 2

Remediated Issue 4: Several Key Milestone Deliverables have not been approved on schedule, posing a risk to the project's on-time completion for components or entire implementation

Resolution

The late milestone deliverables were signed and approved prior to the June reporting update.

Risk Details

During Audit's February and March review of Milestone Deliverables, we identified several deliverables that had not been completed on time. For the first three months of the project, a large portion of Milestone deliverables for the Finance, Logistics, and Human Capital Management modules were not approved and could potentially delay portions of the implementation or the project as a whole.

Late milestone deliverables indicate the portions of the project or the project as a whole are falling behind schedule, and may pose a significant problem to an on-time project delivery. Given the projects history of delays during the initial management of the implementation, prior to the significant change in management of the project in January 2009, we treated this as a red flag for the project going live on the June timetable.

Remediated Issue 5: The agency responsible for hiring and managing the City's 47 million dollar ERP implementation contract does not currently have an Service Level Agreement (SLA) with the City, further, the Master Service Agreement does not provide guidance or requirements in the case of a missing SLA

Resolution

The FY09 SLA was approved on March 4th, 2009 and is posted on the City Website. Further, the SLA for FY10 was approved on July 30th, 2009. The City's Fiscal Year goes from July 1st through June 30th. The new Master Service Agreement was approved by the City Council in April 2010, and includes the SLA requirements.

Risk Details

During our review of Contract Management, we found that there had been no active Service Level Agreement since FY07, which would define how San Diego Data Processing Corporation would manage the SAP Implementation Contract. Essentially, since the inception of the ERP project, no benchmarks or requirements were defined in an executed contract for the management of the City's multi-million dollar project. It is also worth noting that FY10's SLA defines the service levels for the SAP Helpdesk as well. Furthermore, the Master Service Agreement (MSA) did not define the Service Level Agreement (SLA) criteria & requirements to ensure the City's required service levels were met. The SLA's for approved years going back

most of this decade have been consistently signed late in the Fiscal Year, sometimes only active for the last two months of a year.

SLA's are important as they define the criteria in the form of expected service levels, required benchmarks, costs for services, the management of contracts as well as support levels including those of SAP. The lack of an SLA gives the agency far more room to report only statistics that are favorable to them that do not represent the true picture of service, and manage services including contracts in a manner that is not cost effective or does not provide the services required to complete the job.

If not corrected, the risks include:

- Untimely Service Level Agreements (defining expected Service Levels such as SAP Help Desk response time);
- Inability to mitigate risk of knowledge loss and retraining, specifically regarding SAP knowledge transfer from the implementation;
- Inadequate governance over IT services provided to the City.



THE CITY OF SAN DIEGO

M E M O R A N D U M

DATE: January 27, 2010

TO: Eduardo Luna, City Auditor

FROM: Mary Lewis, Chief Financial Officer
Debra Bond, OneSD ERP Director
Ken Whitfield, City Comptroller

SUBJECT: Audit of the Enterprise Resource Planning System Implementation Responses

In 2008, the OneSD Project Team accepted the City Auditor's request to participate in the project from an audit perspective, with the objective of proactively identifying potential issues before they occur. It was explained that these activities did not constitute a formal audit, but rather an opportunity for the City Auditor and the OneSD team to work together in a collaborative manner to review the ongoing status of internal controls as related to SAP. From 2008 forward, the OneSD Project team provided unrestricted access to documents and data, shared network folders, SAP systems for development and test, as well as participation in weekly team lead and integration meetings where issues were identified and discussed in a candid and open environment. City Auditor had the unique opportunity to observe this high-intensity, large-scale project first hand, and in real-time. After project completion, and into the summer of 2010, the ERP Department staff continued open dialog with City Auditor staff regarding the progress in stabilization and maturation of the City's new ERP system, and of the processes within the ERP Department itself, including security and internal controls. Since that time, City Auditor staff has continued to attend the ERP Department's monthly communication and change management sessions with all City departments, where topics common to the group are discussed, such as new features in SAP, operational training needs, and process improvements. The ERP Department has appreciated the long-standing dialog and communication with the City Auditor's staff.

Recommendation # 1:

Implement targeted security monitoring over ERP support staff access in the production environment.

Response: We agree with this recommendation. Management places the highest importance on system and data security. This importance was at the forefront of the security controls implemented during the OneSD project, and continues in the ongoing support of the SAP ERP system. The highest and first priority to be accomplished was to ensure the defined security and internal control standards were met within the SAP system and applied to all general business users of the system. This has been accomplished.

By the nature of the ERP Department technical support team's role, they must possess significantly greater access to the system than a general business user. It is the very access that allows them to perform their daily tasks, that also causes the increased security risk. The next step in the maturation of any ERP system, including ours, is to apply monitoring to the activities performed by the technical support team members who maintain the complex SAP software.

The sub-recommendations “a” through “d” describe common practices and standards for implementing and monitoring the recommended controls over the technical staff. Since fall, 2010, we have planned use of SAP’s Governance Risk and Compliance (GRC) module to accomplish the recommendations documented by Internal Audit. The GRC module is used to conduct monitoring over the general business users of the SAP system, and now will be configured to conduct the monitoring over the technical team.

Specifically, Management Should:

Recommendation #1a:

Perform a risk assessment/cost benefit analysis over the access and system functions that pose the greatest risks to determine which controls merit the associated expense of generating logs or using personnel’s time to regularly review. Automated review, such as the use of scripts to identify certain unauthorized or high risk activity should be used wherever possible to cut back on personnel time and log retention requirements.

Response: We agree with this recommendation and it is currently in process. We expect it to be completed by July 1, 2011. The task will be conducted jointly by Internal Controls and the ERP Department’s security team.

Recommendation #1b:

Critical controls should have an automated trigger or alert such as an email generated from the use of a critical transaction, and sent to the appropriate party for review.

Response: We agree with this recommendation and we expect it to be completed by July 1, 2011 – the details regarding how the notification will be implemented will be modeled after best practices and standard processes that exist with the SAP GRC module.

Recommendation #1c:

Risks, controls implemented/mitigated risk, method of implementation, and frequency of review should be documented in the monitoring portion of the SAP Security Policy.

Response: We agree with this recommendation and it has been completed. It is documented within sections 4 and 7 of the SAP Security Policy, dated December 30, 2010.

Recommendation #1d:

Documented reviews of monitoring controls should be performed at least semi-annually over the implemented monitoring to ensure that the monitoring defined through this exercise are adequate, effective and consistently in place.

Response: We agree with this recommendation. We expect this recommendation to be implemented by July 1, 2011.

Recommendation # 2:

We recommend the security group clearly document technical roles within the SAP environments and enforce Segregation of Duties between technical roles wherever possible.

Response: We agree with this recommendation. Segregation of Duties identification, resolution and continued monitoring was a significant component of the OneSD project's security implementation. In fact, any typical SAP system may contain 400,000 combinations of activities and roles that could cause Segregation of Duties permission risks. As indicated in the Auditor's Report, all combinations of Segregation of Duties risks in our system have been identified and eliminated or mitigated for 10,500 City users through SAP's GRC module. The next step in the maturation of our ERP system is to now apply these same risk reduction measures to the handful of ERP Department team members and technical consultants who maintain the complex SAP software.

Specifically, We Recommend:

Recommendation # 2a:

Access for each ERP support department staff should be restricted to only the access that user requires to perform their day to day functions.

Response: We agree with this recommendation and it has been completed. A review of each ERP support department staff member has been conducted and excessive or conflicting access has been removed.

Recommendation # 2b:

ERP support department staff access should be reviewed at defined regular intervals on a semi-annual basis at a minimum.

Response: We agree with this recommendation and it has been completed. A review of each ERP support department staff member has been reviewed and excessive or conflicting access has been removed. The requirement to review access is documented in section 6.3 of the ERP Security Strategy Document.

Recommendation # 2c:

Additional access beyond standardized support staff roles must be approved by management external to the ERP support department staff, and should be provided through a monitored account such as a Firefighter account.

Response: We agree with this recommendation. We expect this recommendation to be implemented by July 1, 2011 as part of the GRC module's Compliant User Provisioning (CUP) deployment.

Recommendation # 2d:

Unmonitored generic accounts should not exist in the production (live financial) environment.

Response: We agree with this recommendation and it has been completed. The mechanism used in place of staff members using generic accounts is documented in section 4.9 of the ERP Security Policy. Specifically, ERP Department access for extraordinary events is now managed using GRC SuperUser Privilege Manager (SPM).

Recommendation # 2e:

Logs generated from monitored accounts (such as firefighter accounts) should be reviewed at defined points and signed off by the supervising manager when they are in use. Simplified automation can be employed such as automating the generation and sending of the log to the manager via email, whose reply can serve as his auditable electronic sign-off.

Response: We agree with this recommendation. We expect this recommendation to be implemented by July 1, 2011.

Recommendation # 2f:

Security logs should be stored in a location where the SAP IT teams do not have access to modify the logs.

Response: We agree with this recommendation. We expect this recommendation to be implemented by July 1, 2011.

Recommendation # 3:

Ensure that production client authentication settings meet and continue to meet the City Standard authentication requirements defined in the City Security Policy (Section 2.5.1).

Response: We agree with this recommendation and it has been completed.

Recommendation # 4:

Management should take precautions to ensure that no user can increase or modify their own access. If it is not feasible to limit this capability to users required to provision access, controls such as monitoring their account permissions for modifications using a standardized methodology should be implemented to mitigate this security risk.

Response: We agree with this recommendation. We expect this recommendation to be implemented by July 1, 2011 as part of the GRC module's CUP deployment.

Recommendation #5:

To mitigate the control weaknesses related to the vendor database, we have made the following recommendations:

Recommendation #5a:

Create and run a periodic report across non PO invoices looking for duplicate payments similar to the previous mitigating controls report that was in place prior to the implementation of SAP.

Response: We partially agree with this recommendation. SAP has internal programming which automatically checks vendor code, invoice number and other invoice criteria to prevent the instance of a duplicate invoice payment. In addition, our accounts payable staff manually verifies the invoice document to the coded information for payment in SAP before the invoice is authorized for payment. For invoices processed for a purchase with a purchase order, SAP has a three way match system which verifies the purchase order, the receiving document and the associated invoice, before payment is authorized. Because there are duplicate vendors in our vendor master database, there is a possibility that an invoice could have been double applied for transactions that were directly coded, without the purchase order three way match verification.

Creating a customized periodic report to look for duplicate payments in SAP would be redundant to the automated processes already existing in SAP. We propose that a more effective approach is to hire a Payments Auditing Company to review for duplicate payments against a dataset of all of the invoice documents processed in SAP since its implementation date. This would occur after our efforts to cleanse the vendor master dataset of all duplicate vendors (see response to recommendation #5b and #5c). The external audit would be completed by June 2012.

Recommendation #5b:

Analyze the City's vendor database and remove all duplicate vendor data.

Response: We agree with this recommendation. Management implemented a process narrative (PN-0157) for the creation of new vendor records in January 2010. All newly added vendors are examined against existing vendor records to ensure that the new vendor record does not already exist in our master vendor database. However, during the conversion process from our legacy system to SAP, it is likely that not all duplicate vendor records were identified. Researching the vendor master database for duplicates has been an identified project as part of our post go-live activity. Management is scheduled to complete the project of reviewing the vendor master database for duplicates by December 2011. Duplicate vendor records will be identified and deleted or inactivated, depending upon SAP system constraints.

Recommendation #5c:

Implement a required "unique identifier" for a vendor/business, such as the tax ID, for new vendors and create a process for adding the unique identifier to existing vendors.

Response: We agree with this recommendation. Adding a unique identifier to each vendor master record will support our efforts to prevent duplicate vendor records from appearing in our vendor master database. We will implement this recommendation by December 2011.

Recommendation #6:

Complete an evaluation for providing centralized continuing education, and ensure that at a minimum, classes addressing the core functions of SAP are provided on a periodic basis, and made available to the appropriate departments.

Response: We agree with this recommendation and had already implemented it prior to the issuance of the City Auditor's Report. The recommendation has been implemented in three ways.

- Continuing SAP training is coordinated by the citywide training team in the Human Resources Department. This has been the case since July 2010.
- On-line self-serve training tools have been made available via the intranet. Time Entry and Recording is an example of on-line self-serve training.
- In August 2010, the ERP Department conducted a survey of all Departments to identify and address challenges encountered in using SAP. Based on that survey, several additional training sessions were provided to targeted Departments who requested assistance.

In the last quarter of calendar year 2010, trainings in four core functions were provided to almost 900 staff. Trainings in five additional core functions are scheduled for 2011.

When trainings are offered, those that are role-mapped for that course(s) will be invited to attend and register via the intranet postings in the eReg system.

Specifically, Management Should:

Recommendation #6a:

Develop a training schedule for specific requirements based on the results of the survey they conducted.

Response: We agree with this recommendation and it has been completed. We expect to conduct a survey each year and will develop a training schedule based on the feedback of the annual survey. Training schedules are posted on the intranet and those employees that are role-mapped will be invited to attend and register.

Recommendation #6b:

Make the training schedule available to City Employees, using means such as email or the OneSD intranet site. Further, a method for feedback after each training should be provided, such as a survey, to ensure the trainings remain effective.

Response: We agree with this recommendation and it has been completed. Training schedules are posted on the intranet and those employees that are role-mapped will be invited to attend and register. Surveys are conducted at the end of each course

Recommendation #6c:

Ensure enough resources are dedicated to provide on-going training.

Response: We agree with this recommendation and will evaluate needs on a yearly basis in conjunction with the annual operating budget process. We will continue to work with the Super Users and Business Process Coordinators as resources for on-going training efforts.

Recommendation #6d:

Ensure that skilled employees have scheduled dedicated time to train users in their respective proficiency.

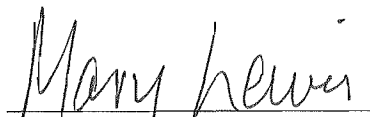
Response: We agree with this recommendation and will evaluate needs on a yearly basis in conjunction with the annual operating budget process. We will continue to work with the Super Users and Business Process Coordinators as resources for on-going training efforts.


Internal Audit Comment #1: Two of seven previously reported issues, primarily in security, remain outstanding.


PREVIOUS ISSUE 1: A Comprehensive Security Strategy, defining security risk areas to the ERP implementation and mitigation of those risk areas to ensure that all key components have been addressed and compliment the City's security strategy has not been documented.

PREVIOUS ISSUE 2: A policy defining and standardizing security parameters within the SAP environments has not been documented.

Response: The recommendations associated with each of these issues were implemented in December 2010.


Mary Lewis
Chief Financial Officer


Debra Bond
OneSD ERP Director


Kenton Whitfield
City Comptroller