THE CITY OF SAN DIEGO

REPORT TO THE CITY COUNCIL

DATE ISSUED: December 29, 2011 REPORT NO: 12-01

ATTENTION: Honorable Members of the City Council and Audit Committee Members

SUBJECT: Annual Report on Internal Controls

REQUESTED ACTIONS:

Informational only.

Background

In October 2004, City Council adopted Ordinance 19320 to achieve a "high standard of quality in and efficacy of the City's financial and disclosure practices." Municipal Code **§22.0708 Annual Report on Internal Controls,** implements this ordinance and requires that an annual report on the City's internal controls be presented to the City Council. Accordingly, this report has been prepared for the calendar year 2011. While the Ordinance calls for an annual review and report, it is important to note that the City now has a dedicated unit, the Internal Controls Section (ICS), in the Office of the City Comptroller that is daily assessing, developing and improving the City's internal controls. The ICS continues to record and publish statistics which indicate the status and level of continued progress made in the internal controls environment, a structural improvement that surpasses the Municipal Code requirement for annual assessment and reporting.

Discussion

It is management's role and responsibility to establish an internal controls environment across all City operations and other areas that have a financial impact on the citywide financial reports. This includes City departments, offices, agencies, and affiliated "related entities" as defined in the San Diego Municipal Code Section 22.4102[1]. While it is the responsibility of every City employee to ensure that work is conducted in accordance with established policies and procedures which support the City's internal controls framework, the responsibility of internal controls design and monitoring resides with the Internal Controls Section (ICS), within the Office of the City Comptroller.

The ICS coordinates the development and documentation of the City's financial policies and procedures. The section reviews new Process Narratives and works with department personnel to ensure adequate controls exist within each process that may have an impact on the financial

[1] **"Municipal Code §22.0708 states that the term "related entity" is defined in §22.1702 of the Municipal code, however, "related entity" is actually defined in §22.4102."**

statements. These Process Narratives form the basis for the ongoing monitoring and remediation of processes and control deficiencies. The ICS is currently developing the monitoring and remediation platform utilizing the tools contained within the SAP Governance, Risk and Compliance (GRC) module to strengthen the City's control environment. Once this monitoring and remediation process has been implemented, test results will indicate the level of compliance with the City's stated policies and procedures.

Currently, the ICS utilizes the GRC module to perform several key functions, including the management of segregation of duty conflicts that arise through role assignments in SAP and specific financial transaction testing. Where necessary, the ICS either develops mitigating controls that are applied to the user violation or recommends an alternative approach which will eliminate the segregation of duty violation entirely. The transaction testing process which is currently being performed supports the objective of ensuring that only transactions that have been reviewed and authorized are posted. These key functions are performed on a continuous, daily basis.

Management's internal control efforts include the citywide coordination of completing audit recommendations. The City is audited regularly both by external auditors and our internal auditors (Office of the City Auditor). Based on the findings of each audit, there is usually a list of recommendations proposed which are designed to improve operational effectiveness or correct an on-going error or non-compliance. The ICS manages a master audit recommendation database which keeps track of all open and completed audit recommendations. This database is shared with the Office of the City Auditor.

Major Accomplishments in Internal Controls

Audit Recommendations

The Internal Control Section (ICS) plays an active role in the monitoring and reporting of management's remediation activities of Audit Recommendations put forward by both the Office of the City Auditor and external auditing entities. During 2011, in total the ICS tracked and reported the completion of 202 Audit Recommendations by management, 191 of which were deemed as implemented by the respective auditors. This resulted in the closing of 21 audit reports in the database. During the course of the year, 22 new audits were added to our database and are currently being tracked and reported.

The ICS has continued to maintain a strong relationship with the Office of the City Auditor through continuous periodic reporting of completed audit recommendations by management. As of the end of December 2011, there were 177 open audit recommendations in the database from both internal and external audits. There are 40 individual audit reports that are marked as open. An audit will remain as open until all audit recommendations have been completed by City management and have been verified by the auditing agency (i.e. the Office of the City Auditor or an external auditing firm).

During 2011, the City made considerable progress in remediating prior audit findings. Most notably, two long standing audit findings; 2003-1 Material Weakness in Internal Controls over

Financial Reporting and 2003-4 Violations of Securities Laws were deemed completed by our independent auditors Macias, Gini and O'Connell. In addition, six audit findings related to the 2009 Financial Statements were also indicated as completed by Macias, Gini and O'Connell. While it must be noted that the FY 2010 financial statement audit resulted in a material weakness and a significant deficiency being identified in Internal Controls over Financial Reporting, it is important to note these findings had been remediated and recommendations implemented prior to the publication of the Auditor's Opinion.

Process Documentation

During the course of 2011, the ICS and City departments finished work on 100 process narratives and 100 workflow diagrams for a total of 229 posted Process Narratives and Workflow Diagrams. To date, process narratives have been completed and provide instruction and support in many key functions which can have an impact on the City's Internal Controls over Financial Reporting. Process narratives have been completed which address Accounts Payable, Treasury, Payroll and numerous other functions.

During calendar year 2011, there were an additional 26 process narratives submitted to the Internal Control Section for review and approval prior to posting on Citynet. Each of these 26 submitted process narratives has been assigned to members of the Internal Control team and are currently in various stages of the completion process. ICS continues to publish its Master Schedule and distributes it via email to the desktop of each assigned process owner. The Master Schedule Summary indicates that there are now a total of 415 identified Process Narratives. At the end of December 2011, there were 103 process narratives being developed in current status and 57 past due process narratives. The ICS is in regular contact with all department stakeholders to facilitate the documentation of processes in a timely manner.

Partnership with Departments

Calendar year 2011 presented several opportunities for the ICS to enhance the internal controls culture of the City. Through partnerships with various departments, the ICS has been in a position to either participate directly or provide technical advice and guidance in several key business activities including the Annual SAP User Access Review, ERP System Enhancement Review, Development of Internal Control Policy for Managed Competition. By participating in these activities, internal controls are being integrated into the operations of the City at both the process level and the policy level.

Reporting

On a monthly basis, the ICS maintains productivity statistics for all of the continuous activities that the section is performing. When requested, the ICS is always available to prepare a report for the Audit Committee detailing current progress.

SAP Governance, Risk and Compliance (GRC) Module

ICS continues to work on resolving segregation of duties user violations. During 2011, more than 10,000 users were analyzed each month for segregation of duties user violations. The total amount of violations reported during the year was 25. As can be seen in the following table, we have been very successful in keeping the number of violations reported as close to zero as possible.

Month	Users Analyzed	Violations
Dec	10,227	0
Jan	10,224	0
Feb	10,205	0
Mar	10,192	0
Apr	10,182	0
May	10,123	0
Jun	10,123	3
Jul	10,156	10
Aug	10,190	6
Sep	10,180	1
Oct	10,186	4
Nov	10,199	1

The ICS has also continued using the GRC module to perform automated testing. Currently, testing is performed in key approval processes in the Accounts Payable, Payroll and Accounting functions. During 2011, we developed and implemented several new tests which have helped mitigate potential internal control deficiencies.

Month	Tests Performed
Dec	132
Jan	132
Feb	115
Mar	154
Apr	123
May	170
Jun	140
Jul	130
Aug	158
Sep	143
Oct	155
Nov	150

During the summer of 2011, the ICS began testing the assessment capabilities of the SAP GRC Process Control Module. The ICS loaded 37 process narratives into the SAP Governance, Risk and Compliance Module with an objective of performing process and control design assessments. These 37 process narratives resulted in the development of a library of 319 questions, which were then used to create 84 surveys to test the effectiveness of processes and

controls. A total of 51 assessment surveys were sent out to process and control owners for their response. Upon completing the initial training, process and control owners found the assessments easy to access and complete.

Due to the decreasing support that SAP is providing for the City's current version of the GRC Process Controls module, the ICS has developed a plan to migrate all GRC applications to the new version that has just been released by SAP (GRC 10.0). This plan is contained in the Internal Control plan document (see attached) which has been developed to build upon the existing internal control framework.

There are no other required reports for external entities or regulating bodies concerning the City's internal controls environment. The Office of the City Comptroller meets annually with Macias Gini and O'Connell, the City's contracted independent financial auditors, to discuss the current sufficiency of our internal controls environment. After these discussions, the independent auditor then makes an assessment as to the level of audit risk assigned to the City engagement which determines the scope of audit field work. The Audit Committee in their due diligence review of the City's CAFR asks questions of the external auditor related to the City's internal control environment.

Future Activities

As outlined in the Internal Control plan, the ICS has created a strategy to continue moving the City forward towards a sustainable internal control practice. Over the next six to nine months, several key projects will be accomplished including the completion of a Citywide Internal Controls Risk Assessment and the implementation of the recently released SAP Governance, Risk and Compliance module (GRC 10.0) which will allow the ICS to expand its testing and monitoring capabilities beyond what currently exists.

Conclusion:

Since management's evaluation of the City's internal control environment within the past 90 days, there have not been any significant changes in internal controls policies or operations or in other factors that could significantly affect internal controls over financial reporting, including any corrective actions with regard to significant deficiencies and material weaknesses.

Management is continuing to develop and strengthen its internal control environment and is making significant progress. Many material key controls have been designed and implemented. Internal controls are being embedded into the City's financial processes and the City departments have made strong gains in implementing internal controls into daily business activities. The City has at least one more year of structural development of its internal controls environment until reaching a steady operational state. Through the work described and the structural changes in developing and implementing internal controls, management will be prepared for an external risk audit beginning November 2012.

RECOMMENDATIONS N/A

FISCAL CONSIDERATIONS: N/A

COMMUNITY PARTICIPATION AND PUBLIC OUTREACH EFFORTS: N/A

KEY STAKEHOLDERS AND PROJECTED IMPACTS: N/A

Attachments:
1. Internal Controls Plan
2. Certification by the Chief Operating Officer, Chief Financial Officer and City Comptroller

cc: Mayor Jerry Sanders
Jay M. Goldstone, Chief Operating Officer
Jan Goldsmith, City Attorney
Andrea Tevlin, Independent Budget Analyst

Mary Lewis
Chief Financial Officer

City of San Diego

Internal Control Roadmap – Progress and Future Activities

Prepared by:	Gerard Lonergan, Internal Controls Manager
Under the Supervision of:	Ken Whitfield, City Comptroller
With Contributions from:	Stella Kuzukian, Supervising Accountant
	Vince Cacaro, SAP Security Manager
	Jonathan Behnke, ERP Basis Manager
	Srinu Koveta, Senior SAP Security Analyst
	Jeff Leveroni, Director of Information Technology
	Debra Bond, ERP Support Director

Date: December 29, 2011

Background

In September 2009, Management presented the Internal Controls over Financial Reporting (ICOFR) Remediation Schedule to the Audit Committee of the City of San Diego. This ICOFR remediation schedule was developed by management to build upon the completion of the remediation efforts called for in the Kroll Report, satisfy the requirements of the SEC Monitor, and ultimately, to demonstrate Management's commitment to strengthen and maintain a robust internal control framework for its financial reporting obligations.

The ICOFR remediation schedule provided insight into the methodologies that management would employ to develop the internal control framework through leveraging the capabilities provided by the implementation of the SAP Enterprise Resource. Additionally, the SAP applications (Access Control and Process Control) contained within the Governance, Risk and Compliance (GRC) module would be utilized to control access to the financial system and provide monitoring and testing capabilities at the entity and activity level. A key component of the ICOFR remediation schedule addressed the need to accurately document the key processes in a format which not only illustrated how a process was to be performed but also detailed the risks, controls and financial statement assertions applicable to each process.

Progress to Date

The schedule of processes to be documented has grown from an initial count of 148 in September 2009 to 415 as of December 2011. Of these 415 processes, 229 have been completed and published to the City intranet. A further 26 have been submitted for internal control review by their respective process owners and are in various stages of the review process. It is expected that the remaining processes will be documented within the next 18 months.

The SAP Access Control application is being used to continuously monitor the levels of risk associated with segregation of duty violations through role assignments in SAP. Approximately 52 mitigating controls have been developed and applied to users where violations exist. In addition, various capabilities of the application are used to control the application, review and approval of superuser privilege management requests.

Automated and manual testing is being performed utilizing the SAP Process Control application. Within this application, transactional monitoring is being performed on a daily or monthly basis dependent on the criticality of the process. With the start of the 2012 fiscal year, process and control design assessments have also been scheduled using the processes discussed above as a basis for evaluation.

The Internal Controls Section (within the Office of the City Comptroller), which was created in early 2009, has enhanced the internal control culture within the City through a close relationship with the SAP Security Team and through involvement in various initiatives and activities that are core to the central operation of the City. Activities performed by the section on a daily basis are always performed with the objective of integrating internal controls within the business at all levels.

Looking to the future

It is management's intention to have the City prepared for an audit of its internal controls by an external audit firm towards the end of November 2012. To facilitate the preparation for an internal control audit, it is critical to understand the principles that will guide an external auditor in their work. There are essentially two frameworks which provide guidance on internal control systems:

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

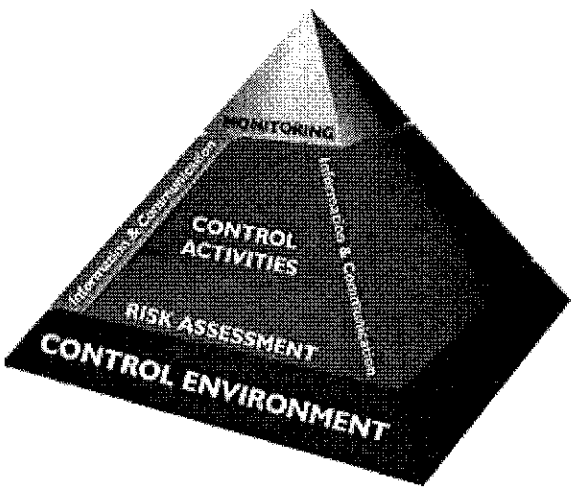
Control Objectives for Information and Related Technology (CobiT)

With the passing of the Sarbanes-Oxley (SOX) law in 2002, increased reliance on both of these frameworks has become necessary to comply with standards set forth in the legislation. While no requirement exists for the City to comply with SOX or adhere to the frameworks identified above, it is considered industry best practice to have an effective internal control program in place which is supported by both of these frameworks.

In preparation for the completion of an audit of internal control over financial reporting, it is critical to understand the intent called out in Auditing Standard No. 5 published by the Public Corporations Accounting Oversight Board (PCAOB). This standard applies "when an auditor is engaged to perform an audit of management's assessment of the effectiveness of internal control over financial reporting". In addition, the standard establishes requirements and provides guidance to facilitate the auditor's objective of expressing an opinion on the effectiveness of the internal control system.

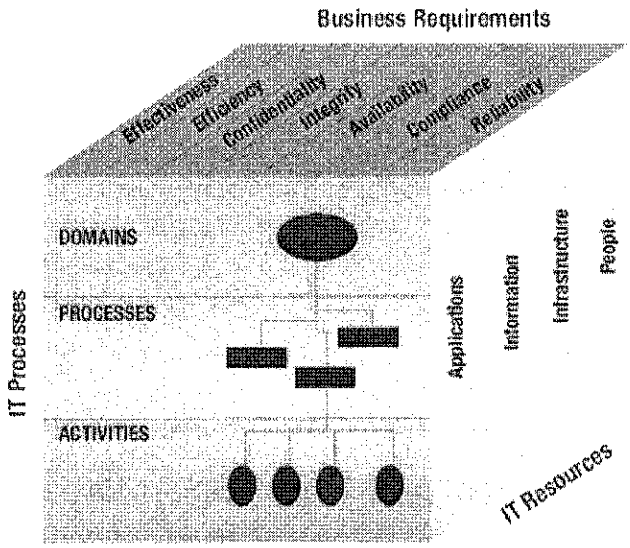
Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The guidance put forth by COSO is comprised of five fundamental components which are further broken down into twenty basic principles (Attachment A). Each of these five fundamental components (Risk Assessment, Control Environment, Control Activities, Information and Communication, and Monitoring) when working together, help to prevent or detect material misstatements of financial reports.



Control Objectives for Information and Related Technology (CobiT)

The CobiT framework is essentially focused on process oriented control to ensure that trust and quality of IT operations and management exists. It is comprised of three dimensions; IT processes, IT resources, and Business requirements. With the level of integration that exists between business and technology in today's current environment, the relevance of this framework when combined with similar components of the COSO framework cannot be understated.



Methodology

The current approach being utilized by the Internal Controls Section is comprised of five key processes:

- Planning
- Evaluating Controls at the Entity Level
- Evaluating Controls at the Process Level
- Testing Controls at the Transaction Level
- Concluding, Reporting and Correcting

Each of these five key processes is comprised of numerous steps ranging from determining the overall approach through to management's statement of assurance. With the exception of evaluating controls at the entity level, progress has been made in each of the other four processes. An audit will focus on two levels; entity level and activity level. To date, the focus has generally been placed at the activity (Process and Transaction) level. As the external auditor's evaluation of entity level controls will dictate the degree of additional testing performed, it is prudent that this focus shifts to the entity level.

Entity Level Controls

Key provisions of Entity Level Controls include:

- Controls related to the control environment

- Controls over management override
- The organizations risk assessment process
- Centralized processing and controls
- Controls to monitor results of operations
- Controls which monitor other controls (Internal Audit, Audit Committee, etc)
- Controls over period end financial reporting
- Policies covering business control and risk management

One key area that will always be a focus during an audit of internal controls is the potential for management to override internal controls. The American Institute of Certified Public Accountants (AICPA) suggests that "management may override controls to intentionally misstate the nature and timing of revenue or other transactions by (1) recording fictitious business events or transactions or changing the timing of recognition of legitimate transactions, particularly those recorded close to the end of an accounting period; (2) establishing or reversing reserves to manipulate results, including intentionally biasing assumptions and judgments used to estimate account balances; and (3) altering records and terms related to significant or unusual transactions.

In addition, the Statement on Auditing Standards No. 99: Consideration of Fraud,requires the auditor to (among other things) gather information which will allow them to identify and assess risks of material misstatement due to fraud. It also requires the auditor to evaluate the entity's programs and controls that address the identified risks of material misstatements. This standard relies on the COSO principles to ensure that the framework to prevent and detect material misstatements is functioning as designed.

Preparation for an Audit of Internal Controls

Step 1 - Risk Assessment (Activity, Entity, & IT)

A comprehensive risk assessment needs to be performed at the entity, IT, and activity level. This risk assessment will assist in determining the entity level controls that currently exist and highlight areas where controls should be in place. The same benefit will derive from the assessment of activity and IT practices and will further enhance the current process and control documentation activity.

The commitment and effort required to perform a risk assessment is, depending on the scope, significant and time consuming. However, once the initial assessment is performed, the annual assessment thereafter is more manageable as the heavy lifting has already been completed. Initially, it is suggested that the target audience for this risk assessment is all employees at the unclassified level. The target audience should also include the Audit Committee and City Council and their respective staffs.

Step 2 – Post Assessment Tasks

Using the results of the risk assessment, the following activities need to be undertaken:
Identification of the process containing the risk
Analysis of the process
Identification of current controls (at entity and activity level) and an effectiveness determination reached
Development of mitigating controls to address the identified risk
Documentation of the current/revised process and controls

Implementation of the documented process and training performed

Step 3 – SAP GRC upgrade to 10.0

SAP is in the process of phasing out support activities for the current Process Control application. Currently, the application is not receiving any enhancement packages and SAP is only focusing on break-fix requests. While the break-fix process is cumbersome and time consuming and with the recent launch of GRC 10.0, SAP may discontinue this level of support within the next year. The upgrade to GRC 10.0 will facilitate the strengthening and expansion of current transactional monitoring and enhance our ability to test and evaluate. To utilize this application effectively, it will require a roll out across the organization.

Step 4 – Evaluation and Testing

As mentioned above, it is management's assessment of internal controls that is being audited. To reach an assessment, it is necessary to evaluate and test processes and controls to ensure that risks have been mitigated. It is vital that any risks which may give rise to material misstatements are known, remediated, and monitored. This is a process that needs to take place on a continuous basis and is conducted at the three levels of the organization (entity, process & transaction). This activity is commonly referred to as Continuous Control Monitoring (CCM).

Step 5 – Reporting

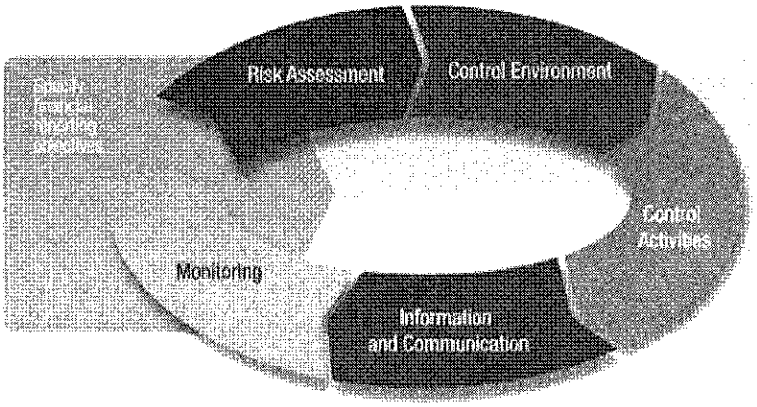
The importance of reporting cannot be overstated. As can be seen from the COSO framework, information and communication is the one component that touches all aspects of the framework. An effective information and communication practice will provide relevant information to key decision makers to support the City's objective of accurate and timely financial reporting. In addition, it also facilitates the understanding of internal control objectives both internally and externally, and supports the development of an internal control culture across the organization.

Step 6 – Corrections

The final step in the cycle deals with the activity of correcting issues that have been reported. Once issues have been identified and reported, management must actively engage in the effective correction or remediation of deficiencies in a timely manner. These correction efforts must be supported across all facets of the organization. Anything less will result in the future reporting of the deficiency in subsequent testing.

Continuity

Once the steps identified above have been completed, it is essential to understand that these activities should continue to be performed as time moves on. To maintain an effective internal control system which supports reliable financial reporting, an annual risk assessment should be performed with greater reliance on the monitoring of control effectiveness. COSO advises that monitoring should also incorporate a systematic process to identify merging risks of misstatement so that the design of the internal control system is continuously improved to mitigate new risks.



Current Resource Activities

Current staffing within the Internal Controls Section is budgeted at 4 full time positions. The range of functions performed by this group includes:

Process Documentation (process review, gap and control analysis, control identification and development, risk identification, workflow creation, web publishing, weekly progress reporting, process owner communications)

Audit Recommendations (database report input, owner and completion date determination, liaison activities, ongoing status updates, weekly reporting, recommendation tracking, bi-annual update)

Process Control (development of subprocesses and controls, creation of technical components for testing, question and survey development, test scheduling, product support, reporting)

Access Controls (development of mitigating controls, control application to users, analysis of user role requests, organization wide segregation of duty violation analysis, cross dept authorization request processing, reporting)

The section also promotes an internal control environment through involvement in various projects and activities (e.g. E&CP bid-to-award reengineering, P&C procure to pay module analysis, SAP enhancement projects, managed competition, inappropriate activity investigations, etc)

Strategy, Plan and Expected Costs

During the development phase of this plan, there were several key considerations and objectives identified that ultimately defined the strategy that would be used. One of the key factors was that a small core group of employees would complete the configuration and implementation of the SAP Governance, Risk and Compliance module (GRC 10.0) module. Furthermore, it was identified that possessing the skills and expertise to provide in-house support for the GRC 10.0 application was critical from both an efficiency and effectiveness perspective.

While the risk assessment and delivery of training components outlined in the plan would be handled entirely in house, the need to use consulting services to support the GRC 10.0 implementation was acknowledged. Rather than bring in consultants to support the implementation at the start of the project, it was felt that with an initial investment in training for key City employees, the core group would be able to achieve a significant portion of the configuration and implementation. During the configuration and testing phases, technical and functional challenges would be identified and these challenges would form the task list to be addressed by the consultants.

A key principle of the plan presented is to minimize costs while maximizing the return on investment. It was this principle which drove the core team to rethink how this plan could be achieved. Access to survey software (which is currently used by the Business Office) was obtained and this will be used to facilitate the delivery of the risk assessment and the reporting of results. It is also intended to use remote consulting, consulting hours and specific task driven assignments as opposed to broad project requirements to achieve the stated objectives.

The core team's mission is to attempt to achieve these objectives within the current budget. With advances in technology and best practices, it is evident that continuous training is essential to continue and support the City's accomplishments in internal controls. It is also anticipated that there will be some costs related to consulting and backfill (to ensure current service levels while key employees are reassigned to support the GRC 10.0 implementation,) for which funding sources will need to be identified.

Implementation

Step 1 – Development and Performance of a Risk Assessment

Tasks to be performed:

Task 1
Research and identify source material
Determine the target audience
Identify and test delivery method to target audience
Develop risk assessment questionnaires
Develop response dates and completion targets for each type of questionnaire
Develop minimum acceptable participation rates
Development and distribution of a supporting memo from Mayor, COO and CFO

Task 2
Delivery of questionnaires to recipients

Task 3
Interim monitoring and reporting of questionnaire response activity to the Comptroller

Task 4
Reporting of recipients who failed to complete questionnaires to the Comptroller

Step 1 Expected Completion Date: End of Q1, CY 2012 and annually thereafter

Step 2 – Post Risk Assessment Activities

Tasks to be performed:

Task 1
Compile all completed questionnaires received into analytical model
Analyze and categorize results and develop findings
Evaluate critical responses and if appropriate, elevate to management for further action

Task 2
Identify process gaps and control weaknesses
Review existing documentation to remediate areas of concern
Departmental outreach to identify Process Owners and request completion of process narratives
Develop mitigating controls where necessary

Task 3
Receive, review and publish process narratives

Step 2 Expected Completion Date: Ongoing Annual Activity

Step 3 – SAP GRC Upgrade to GRC 10.0

Tasks to be performed:

Task 1
Acquire GRC 10.0 module from SAP (Includes Process Control, Access Control, Risk Management etc)
Installation of GRC 10.0 module to a sandbox environment
Development of a portal to access GRC 10.0 module

Task 2
Utilize consultant resources to assist in configuration and documentation while facilitating the knowledge transfer process
Configuration and integration of GRC 10.0 module (back end) with SAP by Internal Controls and SAP Security Sections
Development of a proof of concept document to guide an effective implementation
Functional and technical training

Task 3
Configuration and development of GRC 10.0 module including the creation of roles, users, hierarchies, processes, controls, risks, tests, assessments, reports etc.

Task 4
Functional testing of GRC 10.0 module in the sandbox environment using connections to real historical data
Identification and documentation of errors and module deficiencies

Task 5
Movement of GRC 10.0 module from a sandbox to development environment

Task 6
Remediation of errors and deficiencies using external consultant resources
Ongoing continuous testing
Development of custom queries and programs to enhance monitoring capabilities

Task 7
Movement of GRC 10.0 module from development to production environment

Step 3 Expected Completion Date: End of Q3, CY 2012

Step 4 – Evaluation and Testing

Tasks to be performed:

Task 1
Development of process and control design assessments and control monitoring tests

Task 2
Development of a testing calendar for entity, process, and transactional testing

Task 3
Assignment of test owners and monitors

Task 4
Development of a training program
Training of test owners and monitors

Task 5
Initial execution of process and control design assessments and control monitoring tests

Task 6
Continuous control, process and transaction monitoring

Step 4 Expected Completion Date: **Ongoing activity**

Step 5 – Reporting

Tasks to be performed:

Task 1
Determination of testing results reporting cycles and recipients

Task 2
Identification of uncompleted tests
Review and analysis of results returned for executed tests
Inadequate or critical response issues addressed and if appropriate, elevated to management for further action

Task 3
Results reported to key stakeholders for review and further action
Report sign-off received, non-compliance issues highlighted

Step 5 Expected Completion Date: **Ongoing activity**

Step 6 – Corrections

Task 1
Identification of an issue owner and determination of a correction timeframe
Expected Completion Date: Issue driven

Task 2
Oversight of remediation efforts to ensure an effective and efficient implementation
Expected Completion Date: Issue driven

Task 3
Re-perform test to ensure issue remediated
Expected Completion Date: Issue driven

Step 6 Expected Completion Date: Ongoing activity

Risks to Implementation of the Plan

The risks associated with each step are identified below:

Step 1 - Risk Assessment (Risk Level: High)

Timeframe to develop assessments may be extended due to the need to tailor assessments to specific activities or business areas

Poor response rate may skew the results either favorably or unfavorably

Inadequate resources dedicated to the development of the assessments may result in time delays

Lack of advance communication about the importance of the activity may impact timeliness and quality of response

Step 2 - Post Assessment Risk Activities (Risk Level: Medium)

Time requirement to compile results may be significant given the size of the population

Critical issues raised may require greater resources than anticipated to address

Step 3 - SAP GRC Upgrade to GRC 10.0 (Risk Level: Extreme)

This plan is being developed prior to the SAP GRC application upgrade and therefore, the level of effort required for a successful installation is to be determined

SAP GRC application upgrade may require significant configuration and customization

Sufficient resources (Security, Internal Controls, Developers, ERP Support, Hardware etc.) must be secured in a timely manner and will have a critical impact on the implementation of GRC 10.0

Competing priorities (Supplier Relationship Management (SRM), Enterprise Asset Management (EAM) integration, etc) may place considerable strain on existing resources

Lack of funding will have an impact on the ability to secure a dedicated consultant to address issues beyond the level of expertise currently possessed within the City

Technical issues may surface during the sandbox, development and implementation phases

Inadequate time and resources dedicated to testing will result in increased efforts and costs post implementation to address issues

Steps 4,5,6 – Evaluation and Testing, Reporting, Corrections (Risk Level of each step: Medium)

Additional workload created through implementation of this plan may impact participation and completion rates across all of the impacted business areas

Lack of a quality training program and instructions will directly impact the ability of the users to perform the desired functions

Failure of users to participate in all training opportunities will create costly inefficiencies in the administration of the internal control system within the City

Inadequate testing, reporting and corrective activities may result in future adverse audit findings

Lack of sufficient resources to ensure the annual risk assessment is performed in a timely manner and the continued use of the GRC module and all related components

Benefits of Implementation of the Plan

General:

Increased effectiveness and efficiency of operations

Increased reliability of financial reporting through timely error detection

Compliance with applicable laws and regulations

Improvements in the documentation of processes, controls, and related evaluations

Greater awareness of risks to the organization and its objectives resulting in enhanced targeting and mitigation of identified risks

Enhanced design of business processes to integrate organization-wide processes with systems

Potential continued reduction of audit findings

Potential reduction in audit expenses and associated costs

Specific:

Master data within the GRC tools can now be shared between the Access Controls, Process Controls, and Risk Management applications and now supports collaborative risk assessment. Risks can also be assigned to corporate policies.

Business Objects integration gives user the ability to have real-time reporting and dashboards with similar interfaces to what the user's already know.

Multiple rule sets across different production environments can run in parallel within one instance of Risk and Remediation (RAR), each running according to established workflow.

RAR data can now be personalized for viewer layout, sorted, filtered, and split into separate files for downloading.

Role analysis (role mining) is a new feature within Enterprise Risk Management (ERM) which allows administrators or business owners to see when and how often transactions are being used. Security personnel can use this functionality to optimize role design and assignments which will greatly save on licensing costs and significantly reduce the risk of users having access to functions that are not necessary in the performance of their position.

Client User Provisioning (CUP) has customizable request forms and approver screens with integration to HCM position based provisioning for system activated role assignments.

Increased testing capabilities for transactions, processes, and controls.

Content Lifecycle Management (CLM) helps content providers deliver application content and its subsequent changes via content packages. Over the lifetime of any content, CLM highlights changes and helps users manage the evolution of content as regulations change, companies undergo mergers, acquisitions, reorganizations, expand into new regions, etc.

Notes:

Many of the benefits described in the "Specific" section above have been derived from material published by SAP. The actual functionality and potentially derived benefits from a GRC 10.0 implementation, will be determined with greater accuracy during the phase where the application is installed and rigourously tested in the sandbox and development environments.

The timeline presented above is aggressive. Unforeseen delays, technical issues, and competing priorities may have negative consequences on adhering to the timeline and the degree of success experienced. While every effort has been made to incorporate these risks into the timeline, the implementation team may experience severe difficulty in managing issues beyond their control.

Attachment A

Principles of Effective Control over Financial Reporting

Control Environment

1. Integrity and ethical values. Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.

2. Board of directors. The board of directors (Mayor, City Council, Audit Committee) understands and exercises oversight responsibility for financial reporting and related internal control.

3. Management's philosophy and operating style. Management's philosophy and operating style support achieving effective internal control over financial reporting.

4. Organizational structure. The company's organizational structure supports effective internal control over financial reporting.

5. Financial reporting competencies. The company retains individuals competent in financial reporting and related oversight roles.

6. Authority and responsibility. Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.

7. Human resources. Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

Risk Assessment

8. Financial reporting objectives. Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.

9. Financial reporting risks. The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.

10. Fraud risk. The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Control Activities

11. Integration with risk assessment. Actions are taken to address risks to the achievement of financial reporting objectives.

12. Selection and development of control activities. Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.

13. Policies and procedures. Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in the implementation of management directives.

14. Information technology. Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Information and Communication

15. Financial reporting information. Pertinent information is identified, captured and used at all levels of the company and distributed in a form and time frame that supports the achievement of financial reporting objectives.

16. Internal control information. Information used to execute other control components is identified, captured and distributed in a form and time frame that enables personnel to carry out internal control responsibilities.

17. Internal communication. Communications enable and support understanding and execution of internal control objectives, processes and individual responsibilities at all levels of the organization.

18. External communication. Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Monitoring

19. Ongoing and separate evaluations. Ongoing or separate evaluations enable management to determine whether internal control over financial reporting is functioning.

20. Reporting deficiencies. Internal control deficiencies are identified and communicated in a timely manner to parties responsible for taking corrective action, and to management and the board as appropriate.