The Corporation of the City of Windsor
Manage Information Security

Final Internal Audit Report

29 October 2014

Distribution List

For action
Harry Turnbull, Executive Director of IT
Steve Francia, Technical Support Analyst

For information
Helga Reidel, Chief Administrative Officer
Onorio Colucci,Chief Financial Officer
Stephen Cipkar, Executive Initiatives Coordinator

Limitations & Responsibilities

pwc

Contents

Summary of Internal Audit Results

The engagement has been performed in accordance with the scope of work per Appendix A.

Report Classification

City of Windsor (CoW or City) has established and defined controls around logical access security at the infrastructure and key applications. The City is aware of the need to implement comprehensive security controls and embed a culture of security consciousness. Roles and responsibilities in managing information security are clearly defined through security policies and job descriptions.

Control Environment

The City has policies and procedures around managing Information Security. The policies and procedures establish responsibility and authority for protecting information assets. It also manages the risk of security exposure within the technology systems and creates policy framework for protecting information assets. These policies and procedures applies to all employees of the City, elected officials, contractors, consultants, and all other individuals affiliated with third parties who access, either from internal or external locations, any of the City-owned information assets, network facilities, and technology systems, or any outsourced data or applications run by third parties on behalf of the City. While the City has well established and defined policies and procedures, there are some areas of importance in Information Security that still need to be incorporated.

Also, the City has an established IT organization structure with defined roles and responsibilities. The IT organizational structure is segregated into departments according to business functions and job responsibilities. This approach allows the organization to define responsibilities, lines of reporting and communication in managing the Information Security. The City's IT department is headed by the Chief Information Officer (CIO) who has responsibility for its organizational structure to ensure that it is appropriate to meet changing needs, maintain efficiency, provide for effective internal controls and maximize individual expertise.

Risk Assessment

The City has a developed "Information Security Risk Assessment Methodology" which serves as a systematic approach for the risk assessment process of the Information Assets within the City. The risk assessments performed by the City are designed to identify threats associated with the system functions, Information Assets and the evaluation of current security controls to safeguard against the identified threat.

The City performs Information Security risk assessments on an ongoing basis including the following instances: introduction of a new system and/or IA, major system, infrastructure and IA modification, increase of overall security level, serious security violation(s) and as a result of adverse security evaluation and/or audit.

Control Activities

Control activities around managing Information Security are based on IT policies and procedures and procedures. Below are control activities around Information Security:

User Authentication

User requesting access to information assets shall be uniquely identified to the system before access is granted. Each City's employee and contract worker shall have a uniquely assigned User ID to permit individual authentication and accountability. Exceptions to this are Shared IDs used by a limited number of authorized

individuals for privileged access at the database, network and application for the Amanda and CLASS systems. Shared IDs are used to increase efficiency in the support and administration of the systems

In addition to the unique user IDs, password controls are also in-place at the network, database and application to reasonably prevent unauthorized access to the systems. However, we noted that password settings of the Amanda and CLASS applications are not maximized for security purposes.

Remote access to the City's network is limited to few users and should be authorized by the users' manager. Remote access is done through an encrypted VPN tunnel that requires user name and password.

Powerful User Privileges

Powerful user privileges in the network, database and application layers are limited to authorized individuals. Privileged accesses are mostly used for administration of the systems. Shared privileged IDs are used for some systems to increase efficiency in managing them.

For PeopleSoft Financial, we noted that Six IT Support personnel have "superuser" privileges to all menus. This access allows them to update information in the associated menus. We noted in our review that the City is relying on business process controls to detect any unauthorized changes made by IT Support in the application.

User Administration

All access requests for new users to information security resources require documentation of approval from the employee's manager or supervisor before access is granted. Approvals are documented in the computer access form through physical signature or in the form of an e-mail. Terminations are initiated by HR who informs Service Desk through email of the list of users terminated or resigned during the period. Service Desk then manages the revocation of the access in the different systems. While processes are in place for managing new and terminated users, we noted in our review that on occasion the evidence of authorization of access or termination request were not available for examination.

Access reviews are performed for critical applications including PeopleSoft Financials, PeopleSoft HR and Amanda. The reviews are performed semi-annually by the business process managers/owners to determine user's accesses are still appropriate. Periodic access reviews are not performed for the following: network, database, data centre and CLASS application.

Anti-Virus and Firewall Protection

The City maintains anti-virus software on workstations and servers. Anti-virus signatures and engines are updated with the latest vendor releases using automated software. Regular updates are applied centrally and then pushed to servers and personal computers.

The City has also firewall system installed protecting the city's internal network and IT resources from external threats.

Physical and Environment Security

Computer systems hosting the different applications reside in the City's main data centre. An electronic card access system using two factor authentication (card and PIN code) manages access to the data centre. Access requests to the data centre are authorized by the data centre manager. Procedures are in place to review users with data centre access. However, we noted that data centre access review is currently done informally by the data centre manager. Visitors to the data centre are escorted by authorized individuals at all times. CCTV cameras are placed throughout the building, at access point to the data centre and are recorded to assist with investigations.

The data centre is equipped with fire detection suppression systems, air conditioning systems, water and temperature control systems, uninterruptible power supply ("UPS") systems, and back-up generators.

Information & Communication

The City has training materials available online on the proper use of the computer security system and the importance of personal information security. Employees are required to read and accept the "Acceptable Use Policy" online every time they access the City's network. In addition, security awareness is promoted by the City on a continuous basis through the city's newsletter and email updates of emerging security threats.

Information Security policies and procedures are available to all employees through the City's SharePoint and intranet.

Monitoring

The City's Information Security Policy clearly documents responsibility and authority for protecting information assets. The Chief Administrative Officer (CAO) ensures rules governing information security are developed, enforced and reviewed at least once every term of Council. In addition, Corporate Technology Advisory Group (TAG) is an executive level committee overseeing the Corporation's information security policies and plans, and recommends changes to the Information Security Policy to City Council.

The city has process in place document and response to incident involving security, and post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information. However, policies and procedures around monitoring and responding to security incidents are not yet formally documented.

Significant Findings:

Internal audit identified no findings at a significant level.

Based on the controls identified and tested as part of the Internal Audit of the City's Information Security process and controls we have determined that there is reasonable evidence to indicate that:

	No or limited scope improvement	No Major Concerns Noted	Cause for Concern	Cause for Considerable Concern
Controls over the process are designed in such a manner that there is:				
Sample tests indicated that process controls were operating such that there is:				

Management has provided comprehensive action plans, which we believe will address the deficiencies noted.

Summary of Positive Themes

Overall, City of Windsor has developed process and controls around Information Security.

Procedure and Process Documentation & Availability: Many of the process and controls are formally documented through policies and procedures. These policies and procedures are available to employees through the city's SharePoint or intranet.

Security Risk Management: The City has "Information Security Risk Assessment Methodology" in place that serves as a systematic approach for the risk assessment process of the Information Assets within the city.

User Authentication: Password settings at the network layer and PeopleSoft applications.

User administration procedures (new and terminated request) are defined and followed for all systems. All applications for new users to have access to IS resources must consistently require documentation of approval from the employee's manager or supervisor before access is granted. This approval should be in the form of an e-mail or physical signature and should be retained for audit purposes. For terminations, HR sends a daily notification of terminated users to Service Desks who manages revocation of accesses to the corresponding systems.

Periodic access review of user access rights are performed for critical applications namely PeopleSoft Financials, PeopleSoft HR and Amanda.

Anti-virus and malware protection tools are configured to automatically receive up-to-date patches and virus definitions on a regular basis. The updates are automatically forwarded to all servers and workstations.

Physical access controls are implemented to restrict access to the data centre and workstations.

Though not formally documented, City has processes in-place for the *security training and awareness* proper use of the computer security system and the importance of personal information security.

Summary of Findings

Finding #	Topic	Rating[1]			Management Action
		Significant	Moderate	Low	
Security Policies and Procedures					
1	Component of the Security Policy and Procedures			**X**	Update existing security documentation – Executive Director of Information Technology – 2015 Q2
Password Settings					
2	Password parameter for Amanda and CLASS			**X**	Implementation of complex passwords for Amanda and CLASS systems – Executive Director of Information Technology – 2016 Q4 (Amanda) & 2014 Q4 (CLASS)
Privileged IDs					
3	Control of Privileged Shared IDs			**X**	Conduct a cost/benefit analysis of advanced system monitoring tools – Executive Director of Information Technology – 2014 Q4

Finding	Topic	Rating[1]			Management Action
4	Monitoring of PeopleSoft Financial Superuser's activities			**X**	Enhance controls over Peoplesoft Financials superuser monitoring – Executive Director of Information Technology – 2014 Q4
User Administration					
5	User access account administration – add, change and delete			**X**	Conduct review of IT record keeping procedures – Executive Director of Information Technology – 2014 Q4
Periodic Access Monitoring					
6	Periodic access review of key systems			**X**	Formalization of existing access reviews of key systems – Executive Director of Information Technology – 2014 Q4
Audit Log Monitoring					
7	System audit logs are not formally reviewed and followed up			**X**	See Management Action Plan for Finding #1 and #3
Total Findings		**0**	**0**	**7**	

Summary of Significant Findings

There were no significant findings noted.

Management Comments

It is important to note that all of the findings in the report are of low risk and no significant findings were noted. This is a good indication that we are doing the right things to protect the corporation's critical information. Overall we are in agreement with the findings and for the most part were already aware of the noted issues. Current funding and limited resources available have resulted in a focus on the higher risk areas and ensuring they are adequately addressed. This report clearly indicates that we have done a good job in those areas.

For the items noted below some items are out of our control due to system limitations and others require significant financial and human resources to address. We will have to determine if the low risk level warrants the effort required to mitigate the risk in some cases. Item 3 below provides an estimate as to the expense and resources required to mitigate several of these items. Our approach to security is sound, we can do more and need to balance that decision with other corporate priorities.

Name: Harry Turnbull
Title: CIO and Executive Director of IT
Date: 31/10/2014

Detailed Observations

Findings & Action Plans

<table>
<tr><th>Finding</th><th>Rating[1]</th><th>Recommendation & Action Plan</th></tr>
<tr><td colspan="3">1. Components of the Security Policy and Procedures</td></tr>
<tr><td rowspan="3">Observation
The City has existing policies and procedures on the use of computers, networks, electronic communication, and responsibility and authority for protecting information assets. However, we were not able to acquire documentation (policy/standards)associated with the following elements of importance:

• Password settings acceptable standards and exception process
• Required activities and independence of personnel responsible for monitoring of security-related activities.
• Information security awareness program for all employees.
• System logging, monitoring and auditing requirements.</td><td rowspan="3">Overall
Low

Impact
Low

Likelihood
Unlikely</td><td>Recommendation
Update the existing security documentation to include:

1. Acceptable password standards and either and exception process or preapproved deviations for known system limitations. These include minimum acceptable password length, character combination, reuse history, change frequency, transmission and storage, etc...
2. Minimum expected security monitoring activities, responsible parties, frequency and independence/capability of the monitoring party and escalation/resolution process.
3. Documentation of the requirements, process and content to be provided to new personnel within a timeframe of commencing employment.
4. Minimum expected activities for systems logging, monitoring and management auditing with frequency, systems applicability, responsibilities and resolution processes defined.</td></tr>
<tr><td>Management Action Plan
Management agrees with the finding and will have a revised Security Policy and supporting documents addressing the above items ready for approval in the first half of 2015. Important to note that this is about refining the policy to match the practices that are already in place

Responsibility
Harry Turnbull, Executive Director of Information Technology

Due Date
2015 Q2</td></tr>
<tr><td>Implication
Without policies and procedures around some security processes and controls, users have no formal guidance on security requirements and expectations of the city. Inconsistent user practices could put the integrity or confidentiality of company's financial information at risk.

Root Cause
City does not have these policies, procedures or standards documented.</td></tr>
</table>

[1] See Appendix B for Basis of Finding Rating and Report Classification

Finding	Rating	Recommendation & Action Plan
2. Password parameter for Amanda and CLASS		
Observation Password settings for the Amanda and CLASS applications are below recommended control practices. The following password settings are not maximized: For Amanda: • Minimum password length, and • Account lockout. For CLASS: • Minimum password length, • Password complexity, and • Account lockout. In addition, Amanda and CLASS currently have the functionality to enable modified settings. While these password control weaknesses exist there are partially contained by the fact that password controls at the network level are designed and implemented close to recommended practices.	**Overall** Low **Impact** Low **Likelihood** Likely	**Recommendation** Update the password configuration parameters for the Amanda and CLASS applications to align with good practices and City standards (to be defined – see finding #1). **Management Action Plan** Management agrees with the finding. These are both purchased packages. For the Amanda system we have attempted to resolve this issue and have found that there is a system issue that prevents us from increasing the complexity. The company is actively working to resolve this and we will implement as soon as that bug in the system is addressed. For the Class system recent changes have introduced functionality that allows us to force the application to use the complexity we use at the network level. This functionality is currently being tested and expected to be in place soon. **Responsibility** Harry Turnbull, Executive Director of Information Technology **Due Date** 2014 Q4 for CLASS, in the case of Amanda we are Pressuring Vendor to resolve in our current version but we may have to upgrade to a newer version to resolve this and that is a major initiative that is already underway but will be at least 2 years before completed.
Implication Increased risk of unauthorized access to data and systems resulting in breaches of privacy, confidentiality or data integrity by persons with access to a computer logged into the network may occur.		
Root Cause Minimum password settings are not defined in a policy or standard and existing configuration is system specific with some elements not in alignment with recommended good practices.		

Finding	Rating	Recommendation & Action Plan
3. Control of Privileged Shared IDs		
Observation Shared IDs are used by a limited number of authorized individuals for privileged access at the database, network and application for the Amanda and CLASS systems however there is no monitoring of the use of these shared privileges. Examples of the shared privileged IDs are as follows: • DBAs have administrator rights to the data through the use of a shared privileged user ID. • Administrators in CLASS and Amanda application uses shared user IDs for administrating access. • Default "Administrator" account is used as a domain administrator.	**Overall** Low	**Recommendation** The City should consider creating unique user IDs for each privileged users in the systems. Unique user IDs allows user accountability. While it may not be effective to delete or remove shared IDs their use should be controlled and monitored to reduce error and enable accountability given the power of these privileges. Share IDs should be disabled where possible. When use is required they can then be enabled for a period of time. Use of shared IDs with privileged access should be monitored by an independent person (not access to the shared IDs) with the competency to review the activities on a periodic basis.
Implication Accountability for actions undertaken cannot be established with any certainty for the use of the shared id. Errors and misuse may go undetected. Increased system and data integrity risks may results as well as a higher potential for breaches of data privacy and confidentiality.	**Impact** Low	**Management Action Plan** Management agrees with the finding. Important to note that other controls mitigate the risk and aid in ensuring this remains a low risk item. System limitations prevent the complete elimination of shared accounts. An informal periodic review of these accounts is already performed and this review will be more formalized. Monitoring is a much more complicated item to resolve and will require additional tools that can escalate and de-escalate privileges for unique accounts as needed and additional tools for logging activity and establishing red flags that are automated. The volumes of information generated make it impossible for this to simply be reviewed by an individual without the aid of these tools. These are substantial projects and additional research will be required to determine if the expense and effort is warranted for the low level of risk. Estimated costs for the above noted tools is $200,000 up front and $20,000 annual maintenance. There is also significant ongoing support required that would require an additional staff member to manage these and other security related initiatives that we currently are not staffed to accommodate.

Finding	Rating	Recommendation & Action Plan
Root Cause Privileged IDs are shared among limited authorized individuals in the City in order to increase efficiency in the support and administration of the systems. For e.g., privileged IDs can be accessed immediately by a substitute when the owner of the ID is not available.	**Likelihood** Likely	**Responsibility** Harry Turnbull, Executive Director of Information Technology **Due Date** Formal review to be established 2014 Q4. Tools required to monitor subject to budget and resource availability as well as a determination if warranted given the low risk.

Finding	Rating	Recommendation & Action Plan
4. Monitoring of PeopleSoft Financial Superuser's activities		
Observation Six IT Support personnel have "superuser" privileges to all PeopleSoft Financials menus. This level of access allows them to update information in the associated menus. These privileges are used as part of IT's responsibility to support the application. However, we determined the IT Support's access allows them to have incompatible function (access segregation issue) within the application. There is no monitoring of the IT Support's "superuser" activities in the application to determine if incompatible function was performed. City is relying on the business process controls to identify unauthorized updates to information by the IT Support in the application. Currently IT management relies on downstream business operational controls to detect any errors or misuse of the PeopleSoft super user privileges.	**Overall** Low **Impact** Low **Likelihood** Likely	**Recommendation** Superuser account activity should be monitored by a competent and independent member of IT to detect errors and/or misuse. **Management Action Plan** Management agrees with the finding. These accounts are reviewed as part of our regular review for appropriateness. In addition, the operational controls in Finance are significant and do mitigate this risk substantially. Steps are underway to strengthen those existing controls so that they more directly protect against this particular risk. In addition the tools for logging and monitoring activity mentioned in item 3 could also be used to mitigate this risk but are currently unbudgeted. **Responsibility** Harry Turnbull, Executive Director of Information Technology **Due Date** Enhanced controls complete 2014 Q4
Implication Unauthorized access to or modification of information and data could occur.		
Root Cause Use of the indicated powerful access privileges has the ability to violate segregation of duties issues and is not monitored as part of IT Management's responsibilities. Significant data integrity issues may be detected but privacy and confidentiality issues would not be detected by the downstream controls.		

Finding	Rating	Recommendation & Action Plan
5. User access account administration – add, change and delete		
Observation In testing the user account administration process we noted: 1. Exceptions in 3 of 15 samples for new user account administration a. Evidence of authorization was not documented on the required access request for two of fifteen sampled new users. b. The computer access form was completed out for one new user; however, there no approval (manual sign-off) was evident. Based on the job title/responsibility of the above titles the access privileges appear reasonable however the evidence of authorization for IT to administer this access is not evident. 2. Exceptions in 6 of the 15 samples for terminated users testing a. For 6 of the 15 samples termination access requests were not detected. As such, we were not able to assess if users were removed in a timely manner. For these users we did note access was revoked or disabled.	**Overall** Low **Impact** Low **Likelihood** Likely	**Recommendation** All user access forms should be retained centrally. IT should not act on any access forms until they are appropriately authorized. A process to enable timely and effective communication from HR and operations as to personnel changes should be reviewed for effectiveness and evidence of prompt action and account removal or disablement should be retained. Consideration to automating the access request administration process (add, change and deleted) should be evaluated – i.e. through a ticketing system, workflow or filing solution. **Management Action Plan** Management agrees with the finding. It is important to note that the issue is around record keeping and in all examples noted the appropriate actions had been taken but the record keeping was lacking. A review of the record keeping is underway to resolve this issue. Our current process is manual and labour intensive. A project is underway to significantly improve the automation of many IT Service processes that will significantly reduce the manual nature of many of our processes and by default also improve the record keeping. **Responsibility** Harry Turnbull, Executive Director of Information Technology **Due Date** Record keeping review to be complete 2014 Q4.
Implication Unauthorized access to systems and data may occur impacting data integrity, privacy and confidentiality.		
Root Cause City uses manual form and email request for their user administration process (new and terminated user requests). Due to the manual nature process, there is a probability that the access requests are not properly documented and retained.		

Finding	Rating	Recommendation & Action Plan
6. Periodic access review of key systems		
Observation While a semi-annual access review is performed for critical applications including PeopleSoft Financials, PeopleSoft HR and Amanda we noted other key systems which are not included in this review. Periodic access reviewed is not performed for the following areas/systems: 1. Network (Key Users) 2. Database 3. Data Centre 4. CLASS application As a control, periodic access review is a monitoring control designed to ensure that the right t people have the right access to the right information and to identify and act on unauthorized users with access. In addition, it is a detective control over timely removal of terminated personnel and changes in personnel roles. We understand that an application access review procedure for Class has already been developed and due to the implemented in second half of the year.	**Overall** Low **Impact** Low **Likelihood** Likely	**Recommendation** The four system areas should be included in the scope of the semi-annual periodic access review and inappropriate access resolved in a timely manner. A full review of network access in such a manner may not be feasible and consideration to an automated comparison of active network IDs to active employee listings may be beneficial for all non-administrator accounts. **Management Action Plan** Management agrees with the finding. Informal reviews are already done for all of these areas as the volume of users is small and easy to manage. These processes will all be formalized and in place before the end of this year. **Responsibility** Harry Turnbull, Executive Director of Information Technology **Due Date** 2014 Q4
Implication Unauthorized access to systems and data with the potential for privacy and confidentiality breaches. Terminated users may not be removed from the system in a timely manner. Segregation of duties issues may not be detected.		
Root Cause Periodic reviews of the systems identified are not currently required as part of the existing broader control.		

Finding	Rating	Recommendation & Action Plan
7. System audit log monitoring		
Observation The City has no policies and procedures for monitoring security-related events in its network environment. In particular, system logging facilities (Active Directory, Servers, Database Intrusion Detection System) for environments we reviewed are enabled, but we were not able to detect evidence that the logs are reviewed. Existing policies and procedures provide not direction as to how to respond to security incidents.	**Overall** Low **Impact** Moderate **Likelihood** Unlikely	**Recommendation** Management should develop a formal process for recording and monitoring critical system activities and security-related incidents in the network. Evidence of review and relevant follow up should be retained. **Management Action Plan** Management agrees with this finding. Policies will be updated as part of the review stated in item 1 above. The tools required to do the logging and detection are discussed in item 3 above and are currently unfunded. **Responsibility** Harry Turnbull, Executive Director of Information Technology **Due Date** 2015 Q2 for the policy update
Implication Unauthorized system activities may occur and remain undetected for an unacceptable period of time. Suspicious activity may not be detected and addressed in a timely fashion. The City many not be able to effectively address any security incidents such as attempted, suspected, or actual compromise of sensitive information.		
Root Cause System logging review requirements are not defined and documented.		

Considerations for Improvement

No additional considerations for improvement noted.

Appendix A: Background & Scope

Background

Linkage to the internal audit plan

As part of the Council approved 2013 Internal Audit Plan, Internal Audit will review the process surrounding managing information security at The Corporation of the City of Windsor (the "City") and the associated processes and controls to ensure that City policies are implemented.

As part of the internal audit plan development this business process area has processes and controls associated with mitigating and managing the following risks: Legislative & Regulatory, Public Reaction/Expectation, Terrorism, Public Safety, Governance, Reputation, Third Party Performance, Service Delivery, Information for Decision Making, Security and Privacy, Technology Enablement, Technology Experience, Asset Protection, Accountability, Fraud & Corruption, Compliance, and Transition/Implementation.

Scope

Overview of the business/process to be reviewed

The objective of this internal audit is to assess the internal controls in place surrounding managing information security at the City enterprise level. A large quantity of information maintained within the City's IT systems, as well as physically on site, is sensitive and confidential in nature. It is therefore imperative that sufficient and appropriate system access controls exist and function as intended. Key security processes and protocols must also exist in tandem with said controls in order to ensure there is logical security at the infrastructure and key application levels.

Evaluation of these controls, processes and protocols will determine if they are designed and implemented appropriately, to ensure that the risks surrounding the City's IT systems are aptly mitigated. Mitigation of said risks contributes to the accuracy, reliability and timeliness of information that management uses for decision making.

The scope of the engagement will be limited to the following systems and environments:

- PeopleSoft
- Amanda
- SharePoint
- CLASS

Specific scope exclusions

While our engagement may involve the analysis of financial information and accounting records with IT Systems, it does not constitute an audit or an audit related service in accordance with Canadian generally accepted accounting standards, and accordingly no such assurance will be provided in our report.

Although there may be processes present at the departmental level, our internal audit will focus on the review of these processes at the City enterprise level.

Appendix B: Basis of Finding Rating and Report Classification

Findings Rating Matrix

Audit Findings Rating		Impact		
		Low	**Medium**	**High**
Likelihood	**Highly Likely**	Moderate	Significant	Significant
	Likely	Low	Moderate	Significant
	Unlikely	Low	Low	Moderate

Likelihood Consideration

Rating	Description
Highly Likely	• History of regular occurrence of the event. • The event is expected to occur in most circumstances.
Likely	• History of occasional occurrence of the event. • The event could occur at some time.
Unlikely	• History of no or seldom occurrence of the event. • The event may occur only in exceptional circumstances.

Impact Consideration

Rating	Basis	Description
HIGH	Dollar Value[2]	Financial impact likely to exceed $250,000 in terms of direct loss or opportunity cost.
	Judgemental Assessment	**Internal Control** Significant control weaknesses, which would lead to financial or fraud loss. **An issue that requires a significant amount of senior management/Board effort to manage such as:** • Failure to meet key strategic objectives/major impact on strategy and objectives. • Loss of ability to sustain ongoing operations: - Loss of key competitive advantage / opportunity - Loss of supply of key process inputs • A major reputational sensitivity e.g., Market share, earnings per share, credibility with stakeholders and brand name/reputation building. **Legal / Regulatory** Large scale action, major breach of legislation with very significant financial or reputational consequences.
MEDIUM	Dollar Value	Financial impact likely to be between $75,000 to $250,000 in terms of direct loss or opportunity cost.
	Judgemental Assessment	**Internal Control** Control weaknesses, which could result in potential loss resulting from inefficiencies, wastage, and cumbersome workflow procedures. **An issue that requires some amount of senior management/Board effort to manage such as**: • No material or moderate impact on strategy and objectives. • Disruption to normal operation with a limited effect on achievement of corporate strategy and objectives • Moderate reputational sensitivity. **Legal / Regulatory** Regulatory breach with material financial consequences including fines.
LOW	Dollar Value	Financial impact likely to be less than $75,000 in terms of direct loss or opportunity cost.
	Judgemental Assessment	**Internal Control** Control weaknesses, which could result in potential insignificant loss resulting from workflow and operational inefficiencies. **An issue that requires no or minimal amount of senior management/Board effort to manage such as:** • Minimal impact on strategy • Disruption to normal operations with no effect on achievement of corporate strategy and objectives • Minimal reputational sensitivity. **Legal / Regulatory** Regulatory breach with minimal consequences.

[2] Dollar value amounts are agreed with the client prior to execution of fieldwork.

Audit Report Classification

Report Classification	The internal audit identified one or more of the following:
Cause for considerable concern	• Significant control design improvements identified to ensure that risk of material loss is minimized and functional objectives are met. • An unacceptable number of controls (including a selection of both significant and minor) identified as not operating for which sufficient mitigating back-up controls could not be identified. • Material losses have occurred as a result of control environment deficiencies. • Instances of fraud or significant contravention of corporate policy detected. • No action taken on previous significant audit findings to resolve the item on a timely basis.
Cause for concern	• Control design improvements identified to ensure that risk of material loss is minimized and functional objectives are met. • A number of significant controls identified as not operating for which sufficient mitigating back-up controls could not be identified. • Losses have occurred as a result of control environment deficiencies. • Little action taken on previous significant audit findings to resolve the item on a timely basis.
No major concerns noted	• Control design improvements identified, however, the risk of loss is immaterial. • Isolated or "one-off" significant controls identified as not operating for which sufficient mitigating back-up controls could not be identified. • Numerous instances of minor controls not operating for which sufficient mitigating back-up controls could not be identified. • Some previous significant audit action items have not been resolved on a timely basis.
No or limited scope for improvement	• No control design improvements identified. • Only minor instances of controls identified as not operating which have mitigating back-up controls, or the risk of loss is immaterial. • All previous significant audit action items have been closed.