The Corporation of the City of Windsor
Manage Changes to Information Systems

Final Internal Audit Report

8 July 2015

Distribution List

For action
Harry Turnbull, Executive Director of Information Technology
Matt Caplin, Deputy CIO / Manager of Project Management
and Applications

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

In general, City of Windsor (CoW or City) has established and defined controls around Manage Changes to Information Systems ("IS"). The City is aware of the need to implement a good IS change management process to minimize the risk of unauthorized changes to IT Systems and also minimize the impact of changes on IT and business operations/service levels. The City has standardized IS change management process and controls in place to administer changes to the IT production environment. In addition, roles and responsibilities are assigned to individuals or groups within the IS change management process.

During review of the IS change management process, we noted that the City is in process of implementing a new IT service management (ITSM) process using a new ticketing system ("ServiceNow"). The new ITSM will address some of the observations that were identified in the IS change management process during this review.

Policies and Procedures

The City has formal IS change management procedures for critical applications such as PeopleSoft (Financials and HRMS) and Amanda. These change procedures provide consistent and reliable approach to manage changes within these critical applications. This procedure applies to all members of the Analyst Programmers, Technical Support Analysts, Business Analysts and Enterprise System Support Analysts Teams in the Information Technology Department.

In addition, the City has "Project Management Methodology Policy" that governs at execution of all projects within the city including that of project changes to the IT Systems. The policy defines the activities identified to be projects and provides standard methods and guidelines for project implementation.

While IS change management procedures for significant applications and "Project Management Methodology Policy" are formally documented, we noted that there is no centralized IS change management policy that is used in managing all type of changes (e.g., non-projects, emergency, and configuration) to all applications and supporting infrastructure. The City's existing policies and procedures covers specific applications and/or types of changes.

Initiation/Authorization

Application changes (including configuration and direct data changes) requests are initiated through the Issues Tracking System. Change requests can be a result of a variety of management processes, including Incident Management and Problem Management. Depending on the application, changes request are created by business users/super users or IT (Functional Support Analyst). Details of the change requests (application affected, description, issue type, priority, etc.) are documented in the change ticket.

For applications (e.g., CLASS and Hansen) managed by third party, change requests are usually initiated by the service provider. The requests are still logged by the City in the Issue Tracking System. For the applications covered by the review (CLASS and Hansen), there were no changes or modification that were made to these applications during the audit period.

Infrastructure changes are usually initiated by business partners or third party (i.e. patches) and logged through the City's SharePoint site. Currently, there is a process and procedure in place requiring that all changes need to be logged into a centralized ticketing system.

Testing

Changes are tested prior to promotion to production. Unit and Integration Testing are performed by Developers. User Acceptance Testing (UAT) is then performed by business users or IT (Functional Support Analyst) in the QA/Test environment. For significant changes (e.g., project and upgrades), detailed test plans and scripts are created and reviewed. Any defects or issues identified during the testing are logged into the Issues Tracking System. Testing results and sign-offs are documented through email and/or Issue Tracking Ticket. While a process is in place to test changes prior to promotion, we noted in our review that on occasion (9 out of 55 samples) the evidence of testing results and sign-off for selected changes were not available for examination.

Approval

Every change requires a formal approval from the appropriate change authority before a change can be implemented. Approvers are determined depending on the type of change, change category and/or system affected. For example, project changes should be approved as per "Project Management Methodology Policy" before they can be implemented. Enterprise System Support or Technical Support Analysts review that all approvals were obtained for the changes before it can be implemented. The City currently has no formal documented "approval matrix/table" that list the required approvers for the different type of changes.

Approvals to promote changes are documented through email or Issue Ticketing System. Similar to that testing process above, we noted during our review that on a few occasions (11 out of 55 samples), evidence of approval was not available for our examination.

Once approvals are completed, Technical Support Analysts promote or implement changes to production environment. For applications managed by a third party, changes are usually promoted by the service providers. Back-out plans are identified for changes if implementation fails. However, back-out plans are not formally documented in the change tickets.

Monitoring

Management User Group meetings are held at least monthly for critical applications such as PeopleSoft and Amanda. The meeting is attended by representatives from both IT and business. During the meeting the status of changes for the applications as well as updates/upcoming changes that will be implemented are discussed. Minutes of the meeting are documented and retained.

System generated log of changes is not available or generated for some applications and infrastructure due to system limitations, functionality not enabled or no monitoring tool in place. As such, the City does not have a process in place to monitor or review that only authorized changes have been implemented in production environment.

Post Implementation or validation is performed and documented for significant changes (projects). However, post implementations performed for other type of changes are not formally documented.

Privileged Users

Ability to promote changes to production is a limited number of Technical Support Analysts of each application or infrastructure (database and operating system).

Segregation of Duties

The City has a separate development, QA/testing, pre-production (in some applications) and production environments. For infrastructure changes, there is no dedicated development or testing environments due to

limited resources. However, virtual servers are created as required to test infrastructure changes which are then deleted after.

The City has appropriately segregated developers from that of the implementers. Developers do not have the ability to promote changes to the production environment.

Emergency Changes

Emergency changes may occur within to resolve incidents or to restore service as soon as possible. Emergency changes follow the same process as that of standard changes, wherein testing and approval need to be completed prior to promotion production. However, in this case, the testing and approval process is accelerated in order changes can be implemented as soon as possible. The City has no formal documented policies or procedures in place for emergency changes.

Projects

As documented above, projects or major upgrades are managed following the City's "Project Management Methodology Policy". Projects follow detailed processes and standards which may include the following:

- Project Assessment
- Project Charter Creation
- Business Requirement Documentation
- Detailed Test Plan and Scripts
- Issue Tracking
- Comprehensive Approval Process
- Post Implementation Review
- Training and Manuals Creation
- Satisfaction Survey

Based on the controls identified and tested as part of the Internal Audit of the City's Information System Change Management 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:		✔		

Internal audit identified no findings at a significant level. 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 System Change Management.

Change Management Procedures for critical application: An IS change management procedure is formally documented for critical applications. The procedure provides detailed guidance and process instruction for managing changes for these applications. These procedures are posted on the City intranet.

Logging of Changes: Changes requests are logged either through a ticketing system or SharePoint. The tickets contain details of the changes.

Testing: Changes are tested by business users or IT as required before changes are promoted to production.

Change Status Monitoring: For critical applications (Amanda and People), Management User Group meetings are held at least monthly to discuss the status of changes and also upcoming updates to the application.

Privileged Users: The City has setup that only a limited number of Technical Support Analysts have the ability to promote changes to production for each technology they managed.

Segregation of Duties: Developers are appropriately segregated from implementers. In addition, there are separate development, testing and production environments for applications.

Projects: A formal documented "Project Management Methodology Policy" exists and is followed for projects and major upgrades.

Summary of Findings

Finding #	Topic	Rating[1]			Management Action
		Significant	**Moderate**	**Low**	
Policies and Procedures					
1	Centralized and Comprehensive IS change Management Policies and Procedures		X		Implementation of ITSM system – Manager of Project Management & Applications – 2015 Q4
Change Documentation					
2	Change Testing and Approval Documentation		X		See #1 above.
Approval					
3	Change Approval Matrix Documentation			X	Development of an approval matrix – Manager of Project Management & Applications – 2015 Q4
Monitoring					
4	Change Log and Monitoring			X	Development of a central system change log – Manager of Technology Infrastructure – 2016 Q1
Infrastructure Changes					
5	No formal process for infrastructure changes		X		See #1 above.
Total		**0**	**3**	**2**	

Summary of Significant Findings

There is no significant finding noted.

Management Comments

It is important to note that this report has "No Major Concerns Noted".   Similar to the findings in the October 2014 Manage Information Security Audit Report, this is a good indication that we are doing the right things to protect the corporation's critical systems, data and infrastructure.

We are in agreement with the findings in this report and we were already aware of the noted issues.   The City of Windsor Information Technology Department (IT) has understood the minor gaps in our IS change management practices for several years. These gaps were the result of the rapid growth in technology used by the corporation, the expansion of departments and services supported by IT, and funding and resource constraints. The IS change management gaps have constantly been monitored by IT, and incrementally addressed based on risk assessment and resource availability.   Examples of actions taken to date include the in-house development of small issue tracking systems to better manage various changes, and the development of application specific change management procedures.

In 2014, as the expansion of corporate technology and corporate structure continued, IT recognized that it was the appropriate time to replace its segmented systems and procedures for tracking and managing incidents, requests and changes, with a comprehensive Information Technology Service Management (ITSM) System. ITSM Systems are common in mid-size organizations because the technical complexity in such organizations requires a system to ensure good processes in the management of the enterprise IT environment. IT is currently implementing a third-party ITSM System. The initial implementation will be complete this summer. The implementation of this system will facilitate four of the five action plans noted below.

This report clearly indicates that we have done a good job in managing changes for the corporation's critical systems, data and infrastructure.

Name: Matt Caplin
Title: Deputy CIO / Manager of Project Management and Applications
Date: 3/07/2015

Detailed Observations

Findings & Action Plans

Finding	Rating[1]	Recommendation & Action Plan
1. Centralized and Comprehensive IS change Management Policies and Procedures		
Observation The City has existing IS change management procedures and project policy in place to manage changes and projects implemented with the City's systems. However, we noted that these policies or procedures are applicable to specific types of changes (projects) or changes to specific applications (Amanda and PeopleSoft). The City does not have centralized change management policies and procedures to manage all types of changes (e.g., emergency, standard, data change) in information systems. In addition, due to lack of centralized change management policies and procedures, we noted in the change samples selected that IS change management standards are not consistently performed or documented including: • Testing and approval • Back out Plan • Post Implementation Review	**Overall** Moderate **Impact** Low **Likelihood** Likely	**Recommendation** Management should develop and implement comprehensive change management policies and procedures to manage all type changes within the City's systems. These policies and procedures should include key areas of the change process, including: • Change Request/Initiation • Change Prioritization, Impact Assessment and Categorization • Formal IT Testing Procedures • User testing and acceptance sign-offs • Back out Plan • Approval by users, project management, quality assurance, and/or IT Steering Committee • Logging and monitoring • Post Implementation Review • Documentation (i.e., use of the Change Tickets) • Training • Data and System Migration The policies and procedures should be reviewed, updated as required and approved on a periodic basis.

---

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

Finding	Rating[1]	Recommendation & Action Plan
Implication Without IS change management policies and procedures, users have no formal guidance on managing changes implemented to the City's systems. In addition, lack of centralized and comprehensive IS change manages policies and procedures make it difficult to enforce performance and documentation of IS change management process and standards. **Root Cause** Comprehensive policies, procedures or standards are not documented.		**Management Action Plan** The ITSM system noted above will allow IT to supplement its application specific procedures with a comprehensive IS change management procedure(s) that governs all IS changes. While new IS change management processes have been developed during the ITSM project, a formal procedure should wait until later in the year to ensure that process requirements and the practical use of system capabilities have been fully reconciled. A comprehensive IS change management procedure(s) will be developed by IT before the end of 2015. **Responsibility** Matt Caplin, Deputy Chief Information Officer / Manager of Project Management and Applications **Due Date:** 2015 Q4

Finding	Rating	Recommendation & Action Plan
2. Change Testing and Approval Documentation		

Observation
In testing the operating effectiveness of the IS change management process, we noted that evidence of testing and approval to promote was not available or documented for some samples selected. Results of the testing are as follows:
 	
• Amanda: (30 samples)
   1. Seven (7) samples does not have testing evidence available
   2. Nine (9) samples does not have approval evidence available
 	
• PeopleSoft: (25 samples)
   1. Two (2) samples does not have testing evidence available
   2. Two (2) samples does not have approval evidence available
 	
Based on additional investigation performed together with the City, we determined that the exceptions identified above were appropriate changes.
	Overall
	Medium
	
	Impact
	Medium
	
	Likelihood
	Likely
		Recommendation
		Testing and approval of changes should be documented and retained as per IS change management policies and procedures (see finding # 1)
		
		The City should consider making testing and approval a requirement in the new ticketing system/process.

Implication Without proper documentation, there is no reasonable assurance that appropriate control procedures were observed during the IS change management process. Also, changes may not be properly tested and approved before they are promoted to production.		**Management Action Plan** IT does conduct testing and obtains approvals on changes but the documentation retention of these actions is not consistent. The implementation of the ITSM system and comprehensive procedure(s), as noted in #1, will provide a method to consistently capture and retain this information. **Responsibility** Matt Caplin, Deputy Chief Information Officer / Manager of Project Management and Applications
Root Cause The creation and retention of required evidence is not enforced.		**Due Date:** 2015 Q4

Finding	Rating	Recommendation & Action Plan
3. Change Approval Matrix Documentation		
Observation The City's does not have a formal documented "Approval Matrix" that summarizes the required change approvers for each system and also the different type of changes. **Implication** Without a documented "Approval Matrix", changes may be promoted to production without all the required approvals. **Root Cause** Required approvers by system are not centrally defined, maintained and referred to	**Overall** Low **Impact** Low **Likelihood** Likely	**Recommendation** Management should develop an "Approval Matrix" summarizing the people or group that are required to approve the changes for each system or type of change prior to promotion to production. The cost benefit of automating the change approval process (including identification) should be evaluated – i.e. through a ticketing system or workflow. **Management Action Plan** The various corporate IT systems do have identified staff members who can authorize changes, including a formal governance structure for the corporation's enterprise systems. IT does agree that a formalized approval matrix would be an enhancement to the current processes. An Approval Matrix will be developed in conjunction with the development of the policy and procedure(s) action plan in #1. **Responsibility** Matt Caplin, Deputy Chief Information Officer / Manager of Project Management and Applications **Due Date:** 2015 Q4

Finding	Rating	Recommendation & Action Plan
4. Change Log and Monitoring		
Observation System change logs were not available or generated for applications and infrastructure systems we reviewed. The logs were not available due to system limitations, functionality not enabled (limited resources) and/or no monitoring tools in place. The City has no process in place to monitor or review changes implemented into the production environment. **Implication** Unauthorized access to and modifications of programs may remain undetected or programs may be corrupted. In addition, completeness of changes for audit or review purposes. **Root Cause** Change logs are not available due to system limitations, functionality not enabled (limited resources) and/or no monitoring tools in place. No policies and procedures around change monitoring.	**Overall** Low **Impact** Medium **Likelihood** Unlikely	**Recommendation** Management should consider implementing tools or enabling functionality that will allow logging of changes implemented to the City's significant applications and systems. Management should also implement a process to monitor or review changes implemented to production to detect unauthorized changes. For example, the City, on a monthly or weekly basis, can select a sample of changes from the change log and then trace the change to the corresponding documentation to determine if it was authorized and implemented following the City's change process. **Management Action Plan** System logging is a risk / resources decision. The level of current logging at the corporation varies depending on the system and infrastructure. Consistent with this recommendation, IT recently began the process to procure and implement a system dedicated to centrally logging system changes – a syslog server. The new system should be implemented in early 2016 and the level of logging and monitoring will incrementally grow based on risk and resources. **Responsibility** Norm Synnott, Manager of Technology Infrastructure **Due Date:** 2016 Q1

Finding	Rating	Recommendation & Action Plan
5. Infrastructure Changes		
Observation During review of infrastructure changes, we noted that changes were logged starting in the second half of the 2014. Infrastructure changes were manually logged in SharePoint which is not consistent with that of application changes which are logged in Issue Tracking System. Also, we noted that evidence of testing and approval of infrastructure changes are not formally documented or retained. While there is no formal change process for infrastructure changes, we noted that a Technical Support Analyst(s) is assigned to review and manage changes implemented to each server. **Implication** Without formalized program change procedures there is a risk that unauthorized programs or enhancements may be implemented in the infrastructure. Infrastructure change management is not robustly formalized.	**Overall** Moderate **Impact Medium** **Likelihood** Likely	**Recommendation** Management should develop and implement IS change management procedures for Infrastructure changes which are integrated with the City's centralized change management policies and procedures (see finding # 1). Infrastructure changes should follow a similar process as that of the application changes. Specifically, infrastructure changes should have key activities documented such as: • Changes Request • Testing Results and Sign-off (if required) • Change Approval **Management Action Plan** Agreed. This will be incorporated into Action Plan #1. **Responsibility** Matt Caplin, Deputy Chief Information Officer / Manager of Project Management and Applications **Due Date** 2015 Q4

Appendix A: Background & Scope

As part of the Council approved 2014/15 Internal Audit Plan, Internal Audit reviewed the process surrounding managing changes to information systems 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

As part of the internal audit plan development, this business process area has processes and controls associated with the development or significant modification of software and/or hardware systems. The Changes to IS process refers to the following projects which the City may be involved in:

- Standard Changes/Normal Changes
- Emergency Changes
- Configuration Changes
- Direct Data Changes
- Infrastructure Changes (Database and Network)

Overview of the business/process to be reviewed

As part of the internal audit of the business processes and controls in effect, the internal audit considered:

1. Initiation/Authorization
2. Testing
3. Approval
4. Monitoring
5. Privileged Users
6. Segregation of Duties

The City is using applications or systems in processing and controlling a number of critical business processes and accounting activities. It is therefore imperative that sufficient and appropriate IS change management process and controls are in place for these systems. Change management responds to the City's changing business requirements while maximizing value and reducing disruption.

The evaluation of IS change management controls and process was to determine if they designed and implemented appropriately, to mitigate risk of unauthorized changes made to City's applications or systems. The objective of the change management process is to ensure that changes are recorded and then authorized, tested, approved and monitored.

The scope of this internal audit included an assessment of systems change management activities related to the most recent 12 month period (i.e. January 1, 2014 to December 31, 2014).

The initial in-scope systems or applications, subject to refinement as part of planning discussions, were as follows:
- PeopleSoft (HR and Financials)
- Amanda
- CLASS
- Hansen
- Supporting Infrastructure (Network and Database)

Control Objectives

The objective of this internal audit is to assess the selected internal control objectives in place within the City. The in-scope process areas were assessed against the following control objective:

- "IT Change Management controls are implemented to ensure appropriate controls are evaluated and implemented during the development or significant modification of software and/or hardware systems."

Specific Scope Limitation

While our engagement may have involved the analysis of financial information and accounting records with IT Systems, it did 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.

Consistent with commonly accepted practices, our work was dependent on the following management activities which are excluded from the scope of this review:

1. The review and assessment of changes made to configurable application controls administered by non-IT personnel.
2. The effective design, implementation and operation of business system and application controls related to the capture, processing, storage, reporting/presentation and exporting of information and data.
3. Controls over the completeness, accuracy, reliability and validity of the evidence, information and data provided by management during the course of this review.

Appendix B: Basis of Findings 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.