OFFICE OF THE
City Auditor

Review of Payment Controls

June 12, 2009

THE CITY OF Edmonton

The Office of the City Auditor conducted this project in accordance with the *International Standards for the Professional Practice of Internal Auditing*

Review of Payment Controls
Table of Contents

This page is intentionally blank.

Review of Payment Controls

Executive Summary

In the last quarter of 2008, the Director of Treasury Management, Finance and Treasury Department informed the City Auditor of a possible internal control problem pertaining to processing payment in the City's corporate financial system (SAP). In collaboration with relevant City staff, the Office of the City Auditor (OCA) completed an assessment of two reported incidents.

The first incident pertained to a $21 million test payment erroneously processed in SAP's "live" production environment by an Information Technology Branch (ITB) employee. A Portfolio Manager in the Finance and Treasury Department discovered the error, and the Accounts Payable employees were able to cancel and pull the cheque before its release to a legitimate vendor. The second incident pertained to an erroneous payment of $19,895.40 to an incorrect vendor by an ITB Manager during a pilot automation project. This was later reversed and the correct vendor was paid.

Our preliminary assessment showed that the ITB employee used the "live" SAP production environment in error to complete a test transaction. The test environment is used for testing new functionality and requesting changes to existing functionality. Another reason for the error is that the ITB employee used an authorized higher access privilege to process the transaction. This provided unrestricted assess to all functions in SAP and allowed the employee to bypass all roles and restrictions that could have prevented the error. This level of authority is generally reserved for database administrators and the employee in question was in a support and maintenance role.

The inadequate access controls posed a high risk and left the City in a vulnerable position. We therefore expanded the scope of this review to assess the higher access privileges of all four corporate systems including SAP, as well as high-risk departmental systems. At the request of the then Acting Chief Information Officer (CIO), we also provided control-related feedback on the implementation steps planned by the ITB to correct the situation and report on the status of corrective action.

The ITB has implemented five of the six recommendations we made. They have restricted the higher access privileges of ITB and active contract staff to that required to perform their database, maintenance and support duties. They have also made it mandatory for their staff to change the colour of their production screens to minimize future human errors. In collaboration with the relevant departments, ITB has initiated the assessment of higher access privileges of staff to high-risk departmental systems with a view to limiting such access to that required to perform their duties. This will address our sixth recommendation.

The ITB has prepared formal access administration procedures and incorporated them into a Standard Operating Procedure. This will ensure that future requests for access to corporate and high-risk departmental systems are formally approved, tracked, monitored and removed as required to protect the City's assets.

It should be noted that the reported incident was a human error and not an attempt to defraud the City. However, the learning is that the City should be more diligent in using existing functionality to comply with best practices and ideal control standards to protect the City's interests.

The second transaction reported to us was also a human error. It pertained to an erroneous payment of $19,895.40 to an incorrect vendor by an ITB employee during a pilot project. This project pertained to the automation of the ITB's selection of consultants and the receipt of timesheets for electronic approval and processing. The error was later reversed and the correct vendor was paid. The ITB has made changes to the automated spreadsheet that is used to upload and initiate payment transactions in SAP to minimize similar errors. ITB staff has also been provided appropriate training and formal procedures to strengthen receiving and payment controls and ensure that they exercise due diligence. The same process will be used for all ITB staff when the automated pilot implementation is rolled out. We have confirmed the action taken by ITB and have not made any further recommendations.

We commend the CIO and his staff for implementing our recommendations and taking immediate action to strengthen controls, not just for SAP but for all pillar and high-risk departmental systems. We also commend the Director of Treasury Management for reporting the potential control issues to us. Their actions have demonstrated that City employees are diligent in addressing identified problems and willing to work together to protect the City's interests.

Review of Payment Controls

1. Introduction

In the last quarter of 2008, the Director of Treasury Management, Finance and Treasury Department informed the City Auditor of a possible internal control problem with the processing of payment transactions within the Accounts Payable module of the City's corporate financial system (SAP). He forwarded correspondence on two unrelated incidents to support his position. The Office of the City Auditor (OCA) undertook this project as an emerging request.

The first incident pertained to a $21 million test payment erroneously processed by an Information Technology Branch (ITB) employee. Instead of using the test environment which is used for testing new functionality and changes to existing functionality, the ITB employee processed the test transaction in the production environment that processes "live" transactions. A Portfolio Manager in the Finance and Treasury Department discovered the error, and the Accounts Payable employees were able to cancel and pull the cheque before its release to a legitimate vendor. The second transaction pertained to an erroneous payment of $19,895.40 to an incorrect vendor by an ITB Manager during a pilot automation project. This project pertained to the automation of the ITB's selection of consultants and the receipt of timesheets for electronic approval and processing. The error was later reversed and the correct vendor was paid.

2. Background on Existing Controls

In 2008, the City's Accounts Payable module of SAP processed payments of almost $1.8 billion. SAP has a production environment which processes these "live" transactions. It also has two test environments, development and "QA", which allow authorized ITB and departmental staff to test new functionality and requested changes to existing functionality. Formal procedures exist to move transactions that are tested in the development environment to the QA environment and subsequently to the production environment. These controls are meant to provide assurance that only authorized staff move tested and signed off changes and new functionality to the production environment.

During the development phase, project teams are required to ensure that there is adequate segregation of duties. Departmental users apply for the required system access and their supervisors approve the completed access forms before ITB staff can grant access. These controls are automated and users are limited to performing the tasks allowed through the access privileges granted. For instance, only Materials Management staff can maintain vendor information and initiate straight purchase orders. Authorized departmental receivers enter receipt of goods and services in SAP and authorized supervisors approve payment for the transactions based on receiving and invoice information.

3. Objectives

Our objectives for this review were:

1. To assess the risks related to the two incidents reported to the OCA and provide recommendations on how to mitigate the identified risks in the City's SAP system.
2. To identify similar risks related to other corporate and departmental systems and provide recommendations on minimizing potential loss to the City.
3. To issue a report on the failed controls and the status of corrective actions.

4. Scope and Methodology

Our initial scope was limited to evaluating payment controls in the City's SAP system in relation to the two reported transactions, and provide recommendations to strengthen failed controls. We completed a preliminary assessment of the two transactions and discussed the results with the Director of Treasury Management and the then Acting Chief Information Officer (CIO). In view of excessive employee and contractor access to high-risk corporate and departmental systems, the City was in a vulnerable position. We expanded our scope to strengthening access controls in all four corporate pillar[1] systems (including SAP), as well as identified high-risk departmental systems. Due to the nature of project, at the request of the then CIO, we also agreed to provide control-related feedback in the implementation steps planned by ITB to correct the situation. Our role was that of a controls advisor and we did not undertake any operational tasks or make decisions in the implementation process.

Our scope did not include an assessment of other controls pertaining to the four pillar systems or their use. We focussed on identifying learnings from the reported incidents and strengthening controls in the City's pillar systems as well as identifying departmental systems that face similar risks.

In collaboration with staff from Materials Management, Accounts Payable, ITB, and Finance and Treasury, we assessed existing controls over processing of payment. We researched best practices and professional standards and provided control-related feedback in ITB's implementation of corrective action in relation to identified control weaknesses.

We also initiated the identification of high-risk departmental systems so that similar steps can be taken by ITB in conjunction with departmental staff to minimize potential loss to the City.

[1] A Pillar is a computer system which supports or automates a number of citywide business processes. Currently, the City's Pillar systems are SAP, HRIS, POSSE and SLIM. They are also known as the Enterprise Resource Planning (ERP) systems.

5. Summary of Results

5.1. Incident 1 - $21 Million Test in Production

The Application Maintenance and Support (AMS) Section of ITB is the steward of SAP's production and test environments while the production data is owned by various business units in the City. In order to fulfill their database, maintenance and support function, AMS staff requires system administration (higher) access privileges to SAP. These privileges grant complete and unrestricted access to all functions in SAP and override all roles and restrictions. The ideal control standard is to reserve these privileges for database administrators and only provide it to support and maintenance staff on a temporary and as required basis. It is also essential to track the assignment of such privileges, when they are used and for what purpose.

5.1.1 What Happened?

Our review found that although pillar systems provide the ability to limit higher level access privileges, in addition to database administrators, higher access privileges were permanently assigned to other employees who perform maintenance and support functions. One of these employees used an authorized higher access privilege to test a transaction in the "live" SAP production environment in error. This employee created a purchase order for 12 units costing $20 million each, entered an invoice and receipt for one unit, and then processed a payment in the production environment. It resulted in a $21 million cheque including GST being prepared in the name of a legitimate vendor.

The City operates on Toronto time to manage its money market portfolio. A Portfolio Manager in Finance and Treasury, who is responsible for ensuring that there are sufficient funds available in the City's chequing account, discovered this error at 6:00 A.M. (Edmonton time) the next morning. Although the $21 million transaction to the vendor in question was highly unusual, there was no way to confirm the legitimacy of the cheque at that early hour. The Portfolio Manager had to assume it was genuine and was forced to draw down the City's Money Market Investment Portfolio and divert the funds to its chequing account. Later that morning, the Portfolio Manager contacted Accounts Payable staff who checked the transaction and conveyed that the cheque request was not legitimate and that this was meant to be a test in the test environment. The Accounts Payable employees were able to cancel and pull the cheque in order to mitigate the immediate problem. The funds were retained in the City's bank account and earned interest. Since the City's funds were liquidated to cover the $21 million cheque request and then reinvested the second day, the ITB employee's error cost the City $94.00 in lost investment income net of interest earned.

The Portfolio Manager alerted the ITB employee who then reversed the test transaction in SAP. We confirmed that a full reversal was processed including the 11 remaining units set up in the test purchase order. Our review found that the ITB employee failed to immediately let supervisory positions know about the error. The immediate supervisor was away that week but an acting supervisor and the Director of AMS were available at that time. The AMS team, therefore, found out about the error seven days after the ITB

employee was contacted by the Portfolio Manager. They have now made it mandatory for their staff to change the colour of their production screens to minimize future human errors. AMS staff has also been formally advised to inform their Team Leaders of all sensitive and high-risk situations so that timely action can be taken to mitigate such situations.

Since the SAP transaction logs are only maintained for one week, we consulted with several SAP experts in the City to establish how we could determine whether the ITB employee had processed other payments in production with the assigned higher access privilege. We worked with an ITB Manager who has technical expertise in SAP and conducted several tests on the transactions processed by the ITB employee. Based on the analyses completed, we confirmed that no other payment transactions have been processed by the ITB employee in the production environment.

It should be noted that although the final control worked in this case to ensure that the City did not incur a major loss, the transaction in question was to test a change to the Electronic Funds Transfer (EFT) dollar limit. The ITB employee had intended to use an EFT vendor and this would have resulted in a bank to bank transfer without the Portfolio Manager's ability to question the transaction. Fortunately, in this case, the Materials Management staff made an error in setting up the EFT vendor so the system used the original Head Office record and created a cheque request to process the payment transaction. We worked with the Materials Management staff to determine if similar errors were made when registering other EFT vendors. Two such errors were identified including the transaction in question and both vendor records have now been corrected.

5.1.2 Which Controls Failed and What is the Impact?

The ideal controls for minimizing errors and unauthorized receiving and payment transactions are:

- Appropriate segregation of duties so that no one person can initiate and complete a transaction without the scrutiny of others.
- A unique identifier exists for all assigned IDs so that there is accountability for who did what on the system and when.
- Formal access administration procedures exist and access is granted to employees based on specific roles that limit access to that needed to perform assigned tasks.

Segregation of Duties

Our review found that the use of an authorized higher access privilege allowed the ITB employee to circumvent the segregation of duties control and perform the complete transaction in production. This resulted in initiating a high value payment transaction and based on the purchase order, charging it to an operating area without their knowledge. All roles that are assigned to Materials Management, Departments, Accounts Payable and Finance and Treasury for operating transactions were bypassed with the assignment of such a powerful privilege. Further, excessive access privileges were granted to non-database employees rather than using existing SAP functionality to create and assign roles that limit their access on a need-to-know basis. **(Recommendation 1)**

Use of System IDs

Our review found that SAP records the individual IDs of all employees that process transactions and the date and time they are processed. ITB employees are encouraged to use IDs that identify them when performing their maintenance and support functions. We were able to track the $21 million and related transactions in SAP based on these records. However, there are other powerful system IDs that were also being used by ITB staff and on-call departmental staff to perform maintenance and support functions both in SAP and other pillar systems. The use of system IDs by ITB staff to perform support and maintenance functions in the production environment increases the risk of errors and misuse. In addition, such practice does not allow the City to determine who processed transactions on these systems in order to hold employees and contractors accountable for their actions. **(Recommendation 1)**

Access Administration Procedures

Although formal access administration procedures exist for other City staff, ITB staff members were not required to complete an access administration form and receive formal approval from their supervisor prior to receiving access privileges that allowed them to perform their database, maintenance and support functions. ITB staff requested this access from their supervisors either verbally or via e-mail. ITB had no formal system of tracking and monitoring such access privileges. This resulted in ITB staff and external contractors retaining extra access privileges even though they no longer required this or had transferred to other positions, thus increasing the City's risk of errors and potential misuse. The same risk applies to all other systems ITB supports. In addition, there are a number of departmental systems, both within and outside the control of ITB, that process payments or initiate transactions that ultimately result in payments. The higher access privileges assigned to employees of all high-risk departmental systems need to be reviewed and limited to that required to perform their duties. This will require coordination of ITB with authorized departmental staff, as well as guidance from ITB staff as required. **(Recommendations 2, 3 and 6)**

5.1.3 Role of System Owners

System Owners are responsible for ensuring that authorized, complete, accurate, and timely transactions are processed by their systems. ITB needs to exercise caution when assigning unrestricted access to staff since it allows them to bypass all the segregation of duties controls and thereby compromising the ability of the System Owners to maintain full control over their transactions. We have recommended that System Owners be provided with the tools and training to monitor access to their systems as required. **(Recommendation 4)**

5.1.4 Automated Password Change in POSSE

We noted that POSSE does not have an automated password change requirement even though it processes revenue transactions such as land sales, permits and licenses. This increases the risk of unauthorized access to POSSE. ITB has agreed to investigate the options for implementing automated password change requirements for POSSE, or alternatively, options for communicating with users and encouraging regularly scheduled password changes. **(Recommendation 5)**

5.2. Recommendations and Implementation Status

It should be noted that the reported incident was a human error and not an attempt to defraud the City. However, the learning is that the City should be more diligent in using existing functionality to comply with best practices and ideal control standards to protect the City's interests.

The following are our recommendations, ITB's response, action plans and their implementation status:

Recommendation	Management Response and Action Plan
1. The OCA recommends that the ITB give priority to reviewing the access privileges of all employees that have been granted higher access system administration profiles in the four corporate applications supported by ITB (SAP, HRIS, POSSE and SLIM), and limit such access to that required to perform their duties. This will require development of specific roles with the objective of limiting the use of higher access profiles by non-Database Administrators to minimal or none.	**Accepted** Comments: Higher access privileges of City and contract staff to the four ERP systems have been reviewed and restricted to an as required basis. Use of system IDs for trouble shooting has been discontinued. Their use will be monitored and tracked. Planned Implementation: Complete Responsible Party: Director of AMS.

Recommendation	Management Response and Action Plan
2. After the above review and adjustment, all future requests for the higher access system administration profiles should be formally approved and monitored by the Director of AMS/Designate, and steps be taken to assign an appropriate time limit should such access privileges be required.	**Accepted** Comments: Formal access administration procedures for all ERP systems have been prepared and incorporated in a Standard Operating Procedure. Temporary production access requests to complete support functions on ERP systems will be tracked on SAP and the access will be removed when the tasks are complete. An access form has been prepared and implemented for City and contract staff to formally request access to ERP and other systems to perform their database, support and maintenance tasks. Access privileges will be monitored and maintained. Planned Implementation: Complete Responsible Party: Director of AMS.
3. That the CIO ensure that update access privileges of all ITB employees that perform maintenance and support roles are reviewed and restricted to an as required basis to perform their duties. After the above review and adjustment, a process should be established and implemented to maintain appropriate access as duties change or employees leave the Branch.	**Accepted** Comments: The current update access privileges of all employees in the AMS and TSD Sections have been reviewed and revised to align with defined role based access requirements. The process for maintaining appropriate access has been defined in the Standard Operating Procedures for ITB ERP Application Access. Planned Implementation: Complete Responsible Party: Director of AMS

Recommendation	Management Response and Action Plan
4. That the CIO take steps to ensure that upon request, all System Owners are given the required training and inquiry access privileges to pillar and other systems managed by ITB to allow them to access and/or run reports on who has access to their systems.	**Accepted** Comments: System Owner inquiry and/or report requirements for monitoring access to ERP systems have been documented. System Owners will be provided inquiry access to the reporting functionality upon request. Training documentation for querying the systems or running the reports has also been developed. Planned Implementation: Complete Responsible Party: Project Manager
5. When the POSSE system is upgraded, the CIO should investigate the feasibility of implementing an automated password change requirement. In the interim, other controls such as reinforcing the regular change of passwords should be implemented.	**Accepted** Comments: ITB has investigated the options and will pursue procedures for communicating with users and encouraging regularly scheduled password changes. Planned Implementation: Complete Responsible Party: Project Manager

Recommendation	Management Response and Action Plan
6. For those departmental systems that are considered high-risk, the CIO in coordination with relevant departmental staff ensure that the higher level access privileges of all employees are reviewed and adjusted to that required to perform their duties. This will require coordination of ITB and authorized departmental staff, as well as guidance from ITB staff.	**Accepted** Comments: ITB will work with the System Owners/authorized representatives of the identified high-risk systems to: • complete a risk assessment and develop a schedule for detailed review. • Develop guidelines, policies, and procedures for implementing role-based access privileges where possible, along with training, documentation and reports to monitor and manage access privileges • Implement revised access privileges to reflect the new guidelines. Planned Implementation: Risk assessment – June 30, 2009 Revise Assess Privileges – Based on Risk Assessment Results. Responsible Party: ITB and respective departments.

5.3. Incident 2 - Erroneous Payment

The City is constantly looking for strategic sourcing initiatives to implement efficient and economical purchasing of goods and services. One such initiative is an outline agreement with a single primary vendor and up to three secondary vendors to provide consultants to assist in technology projects. This agreement was established with assistance from Materials Management and is currently in use. A pilot project was implemented by the ITB's Technical Solutions Delivery (TSD) Section with one of the selected vendors. This project involved using an integrated vendor management system to automate ITB's selection of consultants and the receipt of timesheets from the selected consultants. Authorized ITB Portfolio Managers access and electronically approve the completed timesheets. An Excel spreadsheet which provides support for the work performed by all the consultants using the automated system is then electronically forwarded to a Resource Manager in the TSD Section to initiate payment using the SAP system. The Resource Manager is responsible for ensuring that there is adequate funding for the projects and the expenditures are charged to the right projects and cost centres prior to uploading the spreadsheet into SAP.

5.3.1 What Happened?

A consultant working on a corporate project submitted an electronic timesheet which was approved by the relevant Portfolio Manager. A spreadsheet for all the work completed for that time period was electronically forwarded to the ITB Resource Manager to process payment. The Resource Manager detected an error while performing the required budgetary and accounting checks. During the correction process, the correction was erroneously applied to another consultant and this consultant's line item was uploaded from the spreadsheet into SAP to initiate a receiving entry. Another Portfolio Manager is required to process the payment in SAP. This control however, was not effective since a Manager in the TSD Section processed the payment without any further checks on its accuracy. This resulted in a cheque for $19,895.40 being issued to the wrong vendor.

The consultant who received the cheque cashed it and then realized the error. ITB employees were contacted and the consultant issued a personal cheque to the City to address the situation. The documents forwarded by the Director of Treasury Management to us outlined ITB staff's attempts to deposit the personal cheque, reverse the transaction, and pay the right vendor. Had the consultant not contacted the City, the error would have been discovered by the TSD Portfolio Manager through their monthly monitoring process. The final control for detecting this type of error is when the correct consultant claims non-payment and contacts the City.

5.3.2 Which Controls Failed and What is the Impact?

We met with relevant ITB, Purchasing and Accounts Payable staff to determine how and why this error occurred and which controls failed. The ideal controls for minimizing errors and unauthorized receiving and payment transactions are:

- Appropriate segregation of duties so that no one person can initiate and complete a transaction without the scrutiny of others.

- Approval of completed work and timesheets by City staff who are most knowledgeable of the work requirements.
- Automated checks for duplicate payments.
- Due diligence by staff who process receiving and payment transactions.

Our review found that there is appropriate segregation of duties in the transactions pertaining to the pilot automation. Timesheets electronically submitted by consultants are approved by Portfolio Managers who are most knowledgeable of the work performed. Automated checks for double payments exist in SAP. The error occurred during an error correction process in the integrated vendor management system and was uploaded to SAP. At that time, the automated spreadsheet did not facilitate a complete review of the transactions prior to uploading into SAP. The Portfolio Manager who processed the payment transaction in SAP did not check the supporting documentation to confirm the accuracy of the receiving entry.

5.3.3 Status of Corrective Action

We confirmed that the erroneous payment was reversed and the correct vendor was paid. During our review, we recommended that ITB undertake a detailed review to ensure that automated transactions uploaded to SAP are subjected to the same rigor and controls as manual transactions prior to processing payment. This has already been addressed by the TSD staff. They have also revised the automated spreadsheet to show the vendor's name in order to facilitate a more complete review and accurate uploading into SAP.

We also recommended that appropriate training and procedures be provided to all ITB staff that are and will be using the automated process. The TSD Section has prepared an Administrative Guide on Project Management that includes instructions on electronically approving work completed by selected consultants, and processing receiving and payment transactions in SAP. All TSD Portfolio Managers have been trained and the Administrative Guide has been provided to them. The same process will be used for all ITB staff when the automated pilot implementation is rolled out.

We believe that the corrective action taken by ITB will strengthen receiving and payment controls. ITB staff has learned from this incident and has resolved to do due diligence to prevent a recurrence. Therefore, we have made no further recommendations.

6. Conclusion

At the request of the Director of Treasury Management, the OCA investigated a possible internal control problem within the Accounts Payable module of SAP. We reviewed the controls pertaining to two unrelated incidents and identified overall risks to the City as well as the corrective action required to minimize the risks. In view of the high risk to the City, through our advisory role, we expanded the scope to provide control-related feedback in the implementation steps planned by ITB to correct the situation.

We provided six recommendations for the first incident. ITB has prepared formal action plans and has addressed five of the six recommendations. ITB, in collaboration with authorized departmental employees, will complete a risk assessment to facilitate the implementation of the remaining recommendation. They will provide us with a more accurate timeline for addressing this recommendation upon completion of the risk assessment.

Corrective action has been taken by ITB to prevent a recurrence of the second incident and therefore we have made no further recommendations.

We thank the management and staff of ITB and Finance and Treasury Management for their cooperation and support during this review. We also commend the CIO and ITB staff for taking immediate action to implement our recommendations and minimize the risk of loss to the City.