Audit of
iNovah Application Controls

MARTIN MATSON
City Comptroller

STACEY MAZMANIAN
Audit Manager

City of Milwaukee, Wisconsin

February 2016

TABLE OF CONTENTS

Martin Matson
Comptroller

Glenn Steinbrecher, CPA
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Aycha Sirvanci, CPA
Special Deputy Comptroller

Office of the Comptroller

February 15, 2016

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee
Milwaukee, WI 53202

Dear Mayor and Council Members:

The attached report summarizes the results of our audit of the iNovah Application Controls. The objectives of the audit were to: 1) assess the adequacy and effectiveness of controls surrounding the iNovah application and whether they are in compliance with City policies, procedures and best practice; 2) evaluate the adequacy and effectiveness of the security administration and access controls surrounding the iNovah application and data; 3) assess whether the application controls over iNovah are adequate to ensure accurate and complete system and data integrity, transaction processing, inputs, outputs, and control reporting; 4) determine if application change management is adequately controlled; and 5) determine whether third party vendor oversight and management is adequate and effective. The scope of the audit included the iNovah information systems application and general controls from September 2012 through October 2014.

The audit concluded that the application controls in place over the iNovah application are adequately designed and are operating effectively. However, gaps exist in the control design and operational effectiveness of the general controls over the iNovah application that have been identified within this report. This audit report identifies six recommendations to address these issues.

Audit findings are discussed in the Audit Conclusions and Recommendations section of this report, which is followed by management's response.

Appreciation is expressed for the cooperation extended to the auditors by the staff of the Office of the City Treasurer.

Sincerely,

STACEY MAZMANIAN BY: GREG LOTZE,

Stacey Mazmanian, CIA, CGAP
Audit Manager

INTERIM AUDIT MANAGER

SM:acf

City Hall, Room 404, 200 E. Wells Street, Milwaukee, WI 53202 • Phone (414) 286-3321 • Fax (414) 286-3281
www.milwaukee.gov/comptroller

I. Audit Scope and Objectives

The audit examined the Office of the City Treasurer's administration of the iNovah cashiering system application. The application was implemented in October 2005 and is utilized to process all payments tendered to the City Treasurer's Office. The scope of the audit included the access and application controls for the iNovah application. The audit focused on policy and procedure, user access, change control management, security and administration, application controls, and vendor and application oversight. The audit period was September 2012 through October 2014.

The objectives of the audit were to:

1. Assess the adequacy and effectiveness of controls surrounding the iNovah application and whether they are in compliance with City policies and procedures, and best practice.
2. Evaluate the adequacy and effectiveness of the security administration and access controls surrounding the iNovah application and data.
3. Assess whether the application controls over iNovah are adequate to ensure accurate and complete system and data integrity, transaction processing, inputs, outputs, and control reporting.
4. Determine if application change management is adequately controlled.
5. Determine whether third party vendor oversight and management is adequate and effective.

The audit excluded activities performed by the Information Technology and Management Division (ITMD). The audit also excluded the application system backup controls because this process was tested during the 2014 Audit of System Backup and Recovery Controls.

This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that the audit obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Internal Audit believes that the evidence obtained provides a reasonable basis for the audit's findings and conclusions based on the audit objectives.

Audit methodology included developing an understanding of the processes and controls over the iNovah application. To establish appropriate evaluation criteria for this audit, controls and procedures specific to the iNovah application and the Office of the City Treasurer were compared to a best practice based controls testing program. This program was developed by using the Federal Information Systems Controls Audit Manual (FISCAM). FISCAM presents a methodology for performing information system control audits of federal and other governmental entities in accordance with professional standards (as presented in the *Generally Accepted Government Auditing Standards*, known as the "Yellow Book"). This information was used as a reference for the planning and program development of this audit. The audit program and procedures also included elements from best practice criteria COBIT/ISACA, COSO, and NIST 800-14 and 800-53 (Revision 4).[1] These standards were relevant during audit testing, finding identification, and recommendation development.

The audit procedures developed to evaluate the processes and controls to meet the audit objectives included process walk-throughs, inspection of relevant control documentation, and the testing of controls as follows:

- Reviewed internal policies, procedures, guidelines and system information.
- Assessed compliance with the City Password Policy.
- Reviewed system user access based upon the principle of least privilege.
- Assessed the adequacy of user access change control management and monitoring.
- Verified that application change control management demonstrated appropriate authorization, approval, testing and implementation.
- Determined whether the application security violation reporting and monitoring is adequate and is compliant with best practice criteria.
- Assessed the application's internal controls.
- Assessed performance of the ongoing monitoring of the application risks and its third party vendor.

[1] - Control Objectives for Information and Related Technology (COBIT), created and managed by the Information Systems Audit and Control Association (ISACA);
- Committee of Sponsoring Organizations of the Treadway Commission -2013 (COSO);
- National Institute of Standards and Technology (NIST).

II. Organization and Fiscal Impact

The Treasurer's Office, consisting of the Administration and Tax Enforcement, Customer Services, Financial Services, and Revenue Collection Divisions, fulfills the duties and responsibilities of the City Treasurer. Its purpose is to receive, record and account for all monies paid to the City, make authorized disbursements, invest City funds that are not needed to meet current expenditures, collect property taxes and delinquencies for all six tax levies within the City of Milwaukee taxing authority, and remit to each taxing jurisdiction their share of the monies collected. The Financial Services Division performs the noted cash management activities, fund accounting, investment portfolio management, payment distribution, and tax levy collection settlements and the Revenue Collection Division is responsible for cashiering control and revenue collection. The iNovah Cashiering System application, developed and supported by System Innovators, Inc., is a third party vendor software package that manages the revenue collection and processing activities from the City's collection sources to its accounting and information systems.

The iNovah application is administered by the Office of the City Treasurer. The servers hosting the application and application data tables are maintained by the ITMD; however, ITMD does not have update or change capabilities for this application and is out of scope for this audit. The Office of the City Treasurer iNovah administrators possess application change authorities which include system user access maintenance and remittance configuration changes. Remittance configuration changes include additions, edits, or the disablement of payment types, allocation codes, tender codes, etc., that facilitate the proper Financial Management Information System (FMIS) General Ledger (GL) coding of City revenues. System changes including upgrades, version changes, or programming/coding changes are developed and tested by the application's vendor prior to implementation and use with oversight provided by the Office of the City Treasurer iNovah administrators, and ITMD when necessary.

The application produces data files used to update the City's Tax Collection System, the FMIS GL and other City department accounts receivable systems. Collected revenues are processed and are uploaded to the FMIS GL daily.

The iNovah Cashiering System is a high transaction volume financial application. From August 1, 2013 through August 1, 2014, over 219,000 transactions at a net general ledger allocation total of $2.8 billion were processed (excluding voids and adjustments).

III. Audit Conclusions and Recommendations

For information systems, there are two main types of control activities: application and general control. Application controls include the software's internally programmed controls over data input, processing, and output that provide assurance to management that all transactions are valid, complete, authorized and recorded. General controls include logical and physical access, security, change control management, separation of duties, and contingency planning. The audit assessed the adequacy and effectiveness of the procedures and application and general controls in place that promote efficient and secure cashiering, revenue collection, and processing for the iNovah financial application.

The audit concluded that the application controls in place over the iNovah application are adequately designed and are operating effectively. However, gaps exist in the control design and operational effectiveness of the general controls over the iNovah application that have been identified within this report. This audit report identifies six recommendations to address these issues.

1. Document and retain periodic user access reviews.
2. Document and retain user access change control management activity.
3. Document and retain the application change control management activity.
4. Implement procedures for the use and monitoring of access violation control reporting.
5. Configure all passwords to be compliant with the City's Password Policy.
6. Develop and document policies and procedures over the iNovah application's key processes and controls.

Additional details regarding the recommendations for improvement are provided in the remaining sections of this report.

A. Application Access and Change Control Management

In accordance with best practice requirements, including the *2013 COSO Framework – Principle 11*: Management should select and develop general control activities over technology to support the achievement of objectives and respond to risks.

Points of focus:

- Management should establish relevant security management processes which are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities.
- By preventing unauthorized use of, and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into the technology).

User Access Monitoring and Maintenance

In accordance with best practice, applications should undergo periodic user access and user account reviews, user access should be granted using least privilege criteria based on job responsibilities and approved by an authorized resource owner, access should be disabled on a timely basis for terminated or transferring personnel, and user access changes should be tracked, monitored, and documented.

In the Office of the City Treasurer, periodic reviews are performed by management in April and October to ensure appropriate user access levels and user accounts. Audit testing results confirmed that the iNovah user access levels and user accounts were appropriate; however, the audit identified that supporting documentation demonstrating the performance of the periodic system access reviews, and any notable results or follow-up, is not being retained. Documentation was not available during the audit scope period for October 2013, April 2014, and October 2014.

Recommendation 1: Document and retain periodic user access reviews.

To strengthen access monitoring controls over the iNovah cashiering management should:

1. Continue to perform and document the system user access and user account periodic reviews for all iNovah users for appropriate access levels and permissions, terminations or transfers.
2. Retain the documentation evidencing the completion of these periodic reviews, any changes made as a result of the reviews, and management approvals for the two most recent reviews.

User Access Change Maintenance

In accordance with best practice requirements, maintenance of information systems should ensure that user access to these systems is appropriately restricted and that this user access change control management is tracked, monitored, and documented. User access changes must also be performed utilizing the standard concept of adequate separation of duties. This is intended to prevent errors and mitigate fraud risks by ensuring that no one individual monitors or reviews their own work or tasks. User access change controls help protect the integrity of the application data.

A standard operating procedure is utilized when a request to change (grant, revoke, disable) an iNovah user's access is generated by Office of the City Treasurer supervisory or management personnel. This procedure requires the use of the department's standard user access change form. The form indicates the stages of the process (request, approval, completion, and verification) and includes signatory/date confirmation of each stage. The annual user access changes to the tax seasonal temporary teller personnel are documented via management email. The retention of the user access change forms and the noted management emails is recommended, per best practice, for all access changes.

Audit testing results indicated that the user system access change forms and management emails used to document the granting, revoking, or disabling of iNovah user accesses were not consistently retained during the audit period by the Office of the City Treasurer. Documents supporting the following user access changes were not available:

- The authorization, granting, and addition of advanced user access for a new iNovah system administrator;

- Management email authorization of the annual tax-seasonal temporary teller user access;
- For a total of seven iNovah access changes performed since May 2013, only one of ten intra-departmental requests to change user system access change forms provided, by the Office of the City Treasurer, documented a user access change performed within the audit scope period from September 2012 through October 2014.

Review of the user system access change forms for the granting and revoking of user access determined that approval and verification of access changes are not always performed independently. Specifically, the audit identified:

- Three access changes where the approver was the same individual as the requestor (i.e., approving one's own request);
- Five access changes where the change was implemented and verified by the same individual (i.e., verifying one's own work).

Recommendation 2: Document and retain user access change control management activity.
To strengthen user access change control management over the iNovah cashiering application, Management should utilize a standard and formal process that requires:

1. The retention of documentation for the granting, revoking and disablement of all iNovah user access which includes the user system access change forms and management approval emails, as applicable.
2. The separation of duties for access requests, approvals, performance of an access change, and final verifications of the changes.
3. The development and ongoing use of a system generated log to track user access changes.

Application Change Maintenance

In accordance with information system control standards, the maintenance controls over information systems and applications, or application change control management, should ensure that changes to an application are tracked, monitored, and documented; and were performed utilizing the standard concept of adequate separation of duties. Application change control management practices help protect the integrity of the application data by reducing errors.

Standard operating procedures have been developed and documented regarding iNovah application change controls. A standard application change request form has been developed and is required to request new allocation, tender, and payment codes. This application change request form indicates the stages of the process (request, request/approval, completion, testing, testing/approved, and verification) and includes signature/date confirmation of each stage. The retention of the application change request form is required by Office of the City Treasurer's management procedure, and recommended per best practice, for all application changes.

Audit testing results indicated that the application change request form was not consistently retained by the Office of the City Treasurer to document standard application maintenance:

- The Office of the City Treasurer does not maintain a system generated log of application changes.
- The two application change request forms provided did not include signatures and dates for the testing, testing/approved, and verification stages of the change process.

Recommendation 3: Document and retain the application change control management activity.

To strengthen the iNovah application change control management practices, Management should utilize a formal process that requires:

1. The retention of the documentation supporting the performance of iNovah application changes which includes, at a minimum, the appropriately completed application change request form.
2. The development and ongoing use of a system generated log to track iNovah application changes.

B. Security Administration and Monitoring

In accordance with best practice requirements, including the *2013 COSO Framework-Principle 8*: Management should consider the potential for fraud when identifying, analyzing and responding to risks.

Points of focus:

- The assessment of fraud considers fraudulent reporting, misappropriation of assets, and the override of implemented controls.
- The assessment of fraud risk, and subsequent mitigating control development, considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records or GL, or committing other inappropriate acts.

Per referenced best practice requirements, including the *2013 COSO Framework-Principle 10*: Management should select and develop control activities that contribute to the mitigation of risks to the achievement of objectives.

Points of focus:

- Control activities can include a range and variety of controls, including both manual and system automated controls, and preventive and detective controls.
- Attributes contributing to the effective design and implementation of controls:
  - Purpose - a control activity that prevents or detects issues is more precise than one that identifies and explains differences.
  - Aggregation - control activities performed at a more granular level are more precise than one performed at a higher level.
  - Consistency - control activities performed routinely and consistently are generally more precise than those performed inconsistently.

The Securance Risk Assessment for the City of Milwaukee, dated March 2012, rated the iNovah application with a high risk score indicating that the application is critical to the City (and thus, the Office of the City Treasurer). However, excessive access attempts, non-standard, and unapproved access attempts (those outside of standard business operating hours or operating parameters) to the iNovah application are not being tracked, monitored, and followed-up on. The audit noted the following:

- User access profile testing, and discussions with Office of the City Treasurer personnel, confirmed that there are four individuals with advanced administrator user access (and there is one default administrator profile) in the iNovah application. The advanced access and application change capabilities of an iNovah user maintaining an administrator's

access levels requires the implementation of monitored, detective access controls, per best practice.

- A systematic, security violation control report has not been enabled regarding all iNovah users.
- Security violation reporting over user access for all iNovah users is not being monitored.
- A formal process has not been implemented regarding subsequent, documented, independent follow-up for all identified and reported access violations.

Recommendation 4: Implement procedures for the use and monitoring of access violation control reporting.

Management should implement systematically generated iNovah user access security violation control reporting over all iNovah user access (i.e., temporary tellers, tellers, administrators, vendors, etc.) to monitor excessive access attempts, unapproved access attempts, and access during non-standard business hours (including evenings, weekends, holidays, etc.) and include:

1. A formal, independent, and regular follow-up process for identified access violations that demonstrates appropriate separation of duties;
2. Follow-up processes that include procedures regarding appropriate management escalation and final approval and authorization of reviews, when necessary;
3. The retention of the documentation evidencing the performance of these key controls.

C. Access Control Configuration

All City departments that maintain information systems must ensure that access to these applications is adequately restricted. Passwords are an important aspect of system security. Passwords help protect the integrity of the City's data and safeguard the City's assets and data against fraud, misuse, and theft. Employees with administrative access to City applications are responsible for taking the appropriate steps to implement and secure strong end-user passwords configured to enforce the City's Password Policy[2] minimum security standards.

[2] *City of Milwaukee Password Policy dated June 11, 2011*

The iNovah application's password configuration does not comply with the City's Password Policy. The iNovah password configuration maintains a seven character password whereas the City Password Policy requires an eight character password. iNovah password configurations, were established according to the vendor's specifications when the application was originally implemented at the City in October 2005, which was prior to the June 1, 2011 implementation of the current City Password Policy. The Office of the City Treasurer application administrators do not possess the capability to alter these vendor pre-programmed password configurations.

Recommendation 5: Configure all passwords to be compliant with the City's Password Policy.

To strengthen the controls over the iNovah cashiering application and operations, management should contact the application vendor and request that the iNovah password configurations be altered to be compliant with the City's Password Policy (minimum length requirements). Policy compliant password configurations could be scheduled for implementation via the next scheduled application upgrade.

D. Policies and Procedures

In accordance with best practice requirements, including the *2013 COSO Framework–Principle 12*: Management should implement control activities through policies that establish what is expected and in procedures that put policies into action.

Points of focus:

- Personnel perform controls timely.
- Personnel investigate and act on matters identified as a result of executing the controls.
- Documented procedures may include the timing of when a control activity occurs in a process or operation and any follow-up corrective actions to be performed if deficiencies are identified.

Policies and procedures promote consistency, define expectations, serve as a training tool, and provide continuity to operations. Though iNovah technical procedures and manuals are available to the administrators, and management has developed policies and procedures over the

cashiering and financial services operations, the audit noted that the Office of the City Treasurer has not developed procedures for all of the iNovah application's key controls.

Recommendation 6: Develop and document policies and procedures over the iNovah application's key processes and controls.

Management should develop, document, and implement comprehensive policies and procedures to govern and enhance the consistent performance of the following key controls over the iNovah application:

1. Periodic system access reviews for all iNovah application users.
2. User access change processes and controls including initial approvals, authorizations, verifications, and the use of the access change form or supporting documentation, as it is applicable for all iNovah users regarding user access adds, edits or disablement.
3. Security violation reporting use, monitoring, and follow-up and escalation processes.

Management should ensure that the procedures include the processes to document and retain evidentiary support of control performance, results, and follow-up efforts.

E. Application Controls

The determination of the adequacy and effectiveness of the vendor developed, and programmed, standard iNovah application controls, configured to enforce appropriate business rules and controls over data inputs, processing, outputs, and reporting was based upon the examination of relevant and correlated:

- Prior internal audits and testing,
- Documentation reviews,
- Observations,
- Inspections, and
- Via discussions with management and personnel.

These procedures demonstrated that the vendor programmed application level controls surrounding iNovah appear to be adequately designed to mitigate their related risks.

Spencer Coggs
City Treasurer

James F. Klajbor
Deputy City Treasurer

OFFICE OF THE CITY TREASURER
Milwaukee, Wisconsin

February 12, 2016

Greg Lotze
Acting Audit Manager
Office of the Comptroller
City Hall, Room 404

RE: Audit of iNovah Application Controls

Dear Mr. Lotze:

This is the Treasurer's Office written response to the six recommendations made in the *Audit of iNovah Application Controls* dated January 2016.

Recommendation 1 – Document and retain periodic user access reviews.

The Treasurer's Office will continue to perform two user access reviews per year, the first in April, the second in October. In addition, the Administration and Tax Enforcement Division will retain electronic images of the results of the reviews, management approvals, and associated documents. The documentation scanning began with the October 2015 review.

The documentation of the April 2016 user access review will be completed and available for confirmation no later than April 30, 2016. The October 2015 periodic access review supporting documentation will also be available at that time facilitating the verification of two consecutive reviews, so as to include the ingress and egress of the temporary tellers this past current tax collection period. Completion date: April 30, 2016.

Recommendation 2 – Document and retain user access change control management activity.

The Treasurer's Office will continue to document and retain user access change control management activity. Do note that the Treasurer's Office is a small department. At times, it has been necessary for someone with approval authorization to make both a request and approve it, as there were no other authorized approvers available. Note, however, that in no circumstance was the requestor and approver requesting any access changes related to their own user access. The Treasurer's Office has and will continue to make every effort to have different requestors and approvers, but this is not always possible.

Do note that all iNovah activity is tracked in the system's audit log. The Audit Division is welcome to review the audit log at any time.

The final determination of whether or not the iNovah vendor, System Innovators, will be able to produce a system generated iNovah log to track user access changes is planned for completion on June 30, 2016. The Treasurer's Office will continue to retain all supporting inquiry documentation. Estimated completion date: June 30, 2016.

If such a log report can be produced by the iNovah vendor, the implementation date for the Treasurer's Office staff to review the log to track user access changes report is estimated to be September 30, 2016. Estimated completion date: September 30, 2016.

Recommendation 3 – Document and retain the application change control management activity.

The Treasurer's Office will continue to document and retain application change control management activity. The Audit Division is welcome to review application change control management activity at any time.

Do note that all iNovah activity is tracked in the system's audit log. The Audit Division is welcome to review the audit log at any time.

The final determination of whether or not the iNovah vendor, System Innovators, will be able to produce a system generated iNovah application change log report is estimated for June 30, 2016. The Treasurer's Office will continue to retain all supporting inquiry documentation. Estimated completion date: June 30, 2016.

If such a log report can be produced by the iNovah vendor, the implementation date for the Treasurer's Office staff to review the log to track user access changes report is estimated to be September 30, 2016. Estimated completion date: September 30, 2016.

Recommendation 4 – Implement procedures for the use and monitoring of access violation control reporting.

The Treasurer's Office adheres to tight security controls that mitigate the risk of excessive and unapproved access attempts to the iNovah System. If a user has more than three unsuccessful login attempts to the iNovah System, the system will lock the user out and require an administrator to reset their user access.

In regard to unapproved access outside of normal business hours, the Treasurer's Office uses Microsoft Active Directory to limit individual user access. Supervisory personnel are limited to the hours of 7 A.M. to 6 P.M. Monday through Friday. Support personnel are limited to the hours of 8:00 A.M. to 5:00 P.M. Monday through Friday. These settings were just verified on 01/14/2016.

Note, too, that the iNovah network cannot be accessed from outside the Treasurer's Office. Only supervisory personnel have keys to the office. In addition, the office is alarmed and under video surveillance 24 hours a day, 7 seven days a week, and 365 days a year.

With these controls already in place, the Treasurer's Office believes that the risk associated with excessive and unapproved system access has been adequately minimized.

Do note that all iNovah activity is tracked in the system's audit log. The Audit Division is welcome to review the audit log at any time.

The final determination of whether or not the iNovah vendor, System Innovators, will be able to produce a system generated iNovah user access security violation control log report over all iNovah user access is planned for completion on June 30, 2016. The Treasurer's Office will continue to retain all supporting inquiry documentation. Estimated completion date: June 30, 2016.

If such a log report can be produced by the iNovah vendor System Administrators, the implementation date for the Treasurer's Office staff to review the user access security violation control log report security is estimated to be September 30, 2016. Estimated completion date: September 30, 2016.

Recommendation 5 – Configure all passwords to comply with the City's Password Policy.

While the current iNovah application does not have the same password requirements as dictated by City policy, the Treasurer's Office users have been required to create a password that is in compliance with the City's password policy since its adoption. The Treasurer's Office has forwarded the City's password policy to System Innovators for their consideration in future versions of iNovah and System Innovators has stated that they would make the change.

The final determination of whether or not the iNovah vendor, System Innovators, will be able to accomplish compliance with City Password Policy, by implementing an increase in password length, is estimated for September 30, 2016. Estimated completion date: September 30, 2016.

Recommendation 6 – Develop and document policies and procedures over the iNovah application's key processes and controls.

The Treasurer's Office has numerous documented policies and procedures covering the iNovah application and added the formalized procedures regarding system access reviews and the user access change processes recommended on 02/02/2016.

The completion date for adding the security violation reporting use, monitoring, and follow-up and escalation processes to the department policies and procedures is estimated for completion no later than September 30, 2016. It is understood that this recommendation is contingent upon the final disposition of Recommendation 4.

Sincerely,

SPENCER COGGS
City Treasurer

SC/JFK/RLM/BHD/jk

Ref: K:\USERS\FINSERV\AUDIT\Audit of iNovah Application Controls-Audit Response 2016-02-12.docx