



**CITY OF CLEVELAND - CENTRAL COLLECTION AGENCY  
STATE REGION - ISA, CUYAHOGA COUNTY**

**SAS-70**

**JANUARY 1, 2008 THROUGH DECEMBER 31, 2008**



**Mary Taylor, CPA**  
Auditor of State



**TABLE OF CONTENTS**

**I INDEPENDENT ACCOUNTANTS' REPORT..... 1**

**II ORGANIZATION'S DESCRIPTION OF CONTROLS**

CONTROL OBJECTIVES AND RELATED CONTROLS..... 3

OVERVIEW OF OPERATIONS ..... 3

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING .....5

    Control Environment.....5

    Risk Assessment.....5

    Monitoring.....5

INFORMATION AND COMMUNICATION .....6

GENERAL EDP CONTROLS.....7

    Overall Operation of the IT Function ..... 7

    Development and Implementation of New Applications and Systems.....7

    Changes to Existing Applications or Hardware Systems ..... 8

    IT Security ..... 10

    IT Operations..... 12

FINANCIAL APPLICATION CONTROLS.....14

    Municipal Income Tax Information System (MITIS™)..... 14

USER CONTROL CONSIDERATIONS .....25

**III INFORMATION PROVIDED BY THE SERVICE AUDITOR**

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS..... 27

    Overall Operation of the IT Function ..... 27

    Development and Implementation of New Applications and Systems..... 28

    Changes to Existing Applications or Hardware Systems ..... 31

    IT Security ..... 36

    IT Operations..... 42

FINANCIAL APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS.....45

    Municipal Income Tax Information System (MITIS™)..... 45

**IV OTHER INFORMATION PROVIDED BY THE ORGANIZATION**

INFORMATION RELATED TO RACKSPACE AND THE CCA eFILE APPLICATION..... 56

HARDWARE AND SOFTWARE PROFILE ..... 58

LIST OF MEMBER TAXING AUTHORITIES ..... 61

**This Page Intentionally Left Blank**



# Mary Taylor, CPA

Auditor of State

## INDEPENDENT ACCOUNTANTS' REPORT

Members of the Advisory Board  
Central Collection Agency (CCA)  
205 W. St. Clair, 3<sup>rd</sup> Floor  
Cleveland, OH 44113

To Members of the Board:

We have examined the accompanying description of controls of the Central Collection Agency (CCA) applicable to the processing of transactions for users of the Municipal Income Tax Information System (MITIS™). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the CCA's controls that may be relevant to a member community's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and member communities applied the internal controls contemplated in the design of the CCA's controls; and (3) such controls had been placed in operation as of December 31, 2008. The CCA uses the lockbox services of Key Bank for receipt and deposit of some tax payments. The CCA also uses the processing, verification and collection services of Key Bank's affiliate Govolution for electronic payments. In addition, the CCA has contracted with Rackspace for managed web application hosting services. The accompanying description includes only those controls and related control objectives of the CCA, and does not include controls and related control objectives of Key Bank, Govolution, or Rackspace. Our examination did not extend to the controls of Key Bank, Govolution, or Rackspace. The control objectives were specified by the management of the CCA. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of the CCA's controls that had been placed in operation as of December 31, 2008. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance the specified control objectives would be achieved if the described controls were complied with satisfactorily and member communities applied the controls contemplated in the design of the CCA's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from January 1, 2008 to December 31, 2008. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to member communities of the CCA and to their auditors to be taken into consideration along with information about the internal control at member communities, when making assessments of control risk for member communities. In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from January 1, 2008 to December 31, 2008.

The relative effectiveness and significance of specific controls at the CCA and their effect on assessments of control risk at member communities are dependent on their interaction with the controls and other factors present at individual member communities. We have performed no procedures to evaluate the effectiveness of controls at individual member communities.

The information in Section IV is presented by the CCA to provide additional information and is not part of the CCA's description of controls that may be relevant to a member community's internal control. Such information has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for member communities and, accordingly, we express no opinion on it.

The description of controls at the CCA is as of December 31, 2008, and information about tests of the operating effectiveness of specified controls covers the period from January 1, 2008 to December 31, 2008. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the CCA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the CCA, its member communities, and the independent auditors of its member communities.

A handwritten signature in black ink that reads "Mary Taylor". The signature is written in a cursive, flowing style.

**Mary Taylor, CPA**  
Auditor of State

February 27, 2009

---

## SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

### CONTROL OBJECTIVES AND RELATED CONTROLS

The CCA's control objectives and related controls are included in section III of this report, "Information Provided by the Service Auditor," to eliminate the redundancy that would result from listing them here in section II and repeating them in section III. Although the control objectives and related controls are included in section III, they are, nevertheless, an integral part of the CCA's description of controls.

### OVERVIEW OF OPERATIONS

The CCA is an agency of the City of Cleveland which provides a full range of tax collection services for 47 member communities throughout 15 Ohio counties. The tax collection services include; mailing returns, processing payments, billing taxes due, assessing penalties and interest, issuing refunds, mailing delinquency notices, preparing court cases and distributing the taxes collected to the municipalities. The only function not performed by the CCA for their member communities, with the exception of the City of Cleveland, is the filing of court cases against delinquent taxpayers.

The CCA is governed by an advisory board and an executive committee. The tax administrator for each CCA member community serves on the advisory board. The executive committee is made up of five advisory board members, four of whom are elected. The City of Cleveland finance director is a permanent member of both the advisory board and the executive committee.

Senior management at the CCA includes the tax administrator, who is responsible for the administrative functions and reports directly to the city finance director, the assistant tax administrator, who is responsible for the daily operation of the CCA, and the controller, who is responsible for the daily, monthly, and yearly financial operations and reports.

The CCA employs more than 100 individuals to process more than one million returns, estimated payments, and tax assessments. During 2008, the CCA collected more than \$434 million at its location on West Saint Clair Avenue in Cleveland. Employees are aligned in one of three functional areas: audit and operations, legal or information systems support.

The functional area of audit and operations is managed by two administrative managers, one chief of accounts and collections, and between seven and eight supervisors. The administrative managers and the chief of accounts and collections report to the assistant tax administrator.

*Audit* - Audit is responsible for issuing refunds and verifying the accuracy of reported income. Audit is divided into the following three areas: corporate audit, individual audit, and special audit.

*Operations* - Operations is divided into four areas: data entry, records, collections, and taxpayer assistance. Data entry personnel enter tax return information and the records room personnel manage the physical income tax returns. The taxpayer assistance area directly assists taxpayers to collect tax payments and answer questions. Collections personnel are responsible for recording cash received.

The legal department consists of two attorneys, two paralegals, and support staff. They are responsible for research and court cases filed against taxpayers. The department also reviews pending or new taxation legislation to determine its impact on the operations at the CCA. The legal department reports to the assistant tax administrator.

Information Systems Support (ISS) is supported by five individuals, four of whom are consultants from Modis, an international IT recruitment company. The project leader/applications development is a CCA staff member who manages the daily activities of the four Modis consultants. The project leader also performs daily operational and programming tasks when necessary.

The following are the titles and responsibilities of the Modis consultants:

*Application specialist* - is responsible for support of the MITIS™ application software; for investigating, analyzing and implementing new software opportunities and techniques to enhance the MITIS™ system; and for assisting in end user support.

*Database specialist* - is responsible for the support and maintenance of the Sybase database used by the tax application. Support includes optimizing the database structure, and assisting the application specialist in supporting end user needs.

*Network/operations specialist* - is responsible for submission and tracking of batch processes. He also prepares system documentation and performs help desk and network administration functions.

*Web/Desktop Publishing (DTP) consultant* - is responsible for the maintenance and enhancement of CCA's Website and Web application.

The CCA uses the Municipal Income Tax Information System (MITIS™) to process tax data. The CCA has a diverse computing environment and uses three major operating systems and various types of hardware to deliver the services available from the primary client server application, MITIS™. Local and remote connectivity, user authentication, and application interface execution are delivered through the Windows 2003 operating system. Sybase database software controls data storage and access. Batch processing tasks are accomplished through programming developed for the Solaris operating system.

The CCA provides member communities with an option to perform remote inquiries on their historical tax data. Currently, 23 of the 47 member communities have dial-up access. CCA also provides standard reports, on a monthly and year end basis, to their member communities which include the following:

Monthly Reports:

- Recap of total dollars collected by form and period end for each community.
- Collections broken out by day and form.
- Report of withholding transactions by community and period end.

Annual Reports:

- Report listing of active taxpayers living in or doing business in the community.
- Report listing of all annual returns filed by both individual and business type.
- Report listing of delinquent taxpayers.
- Report of all companies filing withholding for the community.

In addition, CCA can provide a tracking report for the top withholders in a member community. This is normally the top 25-50 companies depending upon the size of the community.

---

## RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

### ***Control Environment***

The advisory board meets on a quarterly basis to inform, consult with, and advise the CCA tax administrator and the executive committee of common concerns of the member communities.

The executive committee is responsible for establishing policy and addressing significant staffing and budget issues. The executive committee meets only as needed.

The CCA uses the City of Cleveland personnel policies and procedures which are distributed to each new employee. Detailed job descriptions exist for all ISS staff positions and evaluations are conducted on an annual basis. All employees are required to sign a confidentiality agreement to protect the integrity of taxpayer data.

Additional information regarding the control environment can be found in section II of this report under, "Overall Operation of the Information Technology Function."

### ***Risk Assessment***

The CCA does not have a formal risk management process; however, the City of Cleveland's Risk Management Office is an available resource when necessary. The advisory board actively participates in the oversight of the CCA. The board and the CCA legal department track pending legislation and address the impact of new legislation on the CCA and its member communities. The tax administrator informs the board of key staff changes, improvements in services provided by the agency, current collection figures, and other administrative issues. When necessary, the executive board meets to establish policy or address major staffing or budget issues.

In addition, the CCA has identified operational risks resulting from the nature of services provided to the member communities. These risks are primarily associated with computerized information systems. These risks are monitored as described under "Monitoring" below and in additional detail throughout the "General EDP Control" section of this report.

### ***Monitoring***

The CCA organization is structured so that managers of each functional area report to the assistant tax administrator and the tax administrator. Many of the key management employees have worked for the CCA for several years and are experienced with the systems and controls at the CCA. The CCA project leader/applications development and the ISS staff monitor the quality of service to member communities and system performance as a routine part of their job duties. To assist them in this monitoring, the CCA uses a variety of reconciliation procedures and key indicator reports to monitor transaction processing for user organizations. Additionally, collection, refund, and service charge reports are provided to member communities each month along with the tax collection distribution.

Computer access is monitored on an ongoing basis by the ISS staff. Network, database, and hardware monitoring reports are reviewed daily or monthly. Exceptions to normal processing related to hardware, software, or procedural problems are resolved daily. Reconciliations that require

management approval are present throughout the CCA's income tax processing procedures. These reconciliations identify exceptions that may have occurred.

**INFORMATION AND COMMUNICATION**

The aspects of the information and communication component of internal control as they affect the services provided to user organizations are discussed within the General EDP and Application control sections.

## GENERAL EDP CONTROLS

### *Overall Operation of the IT Function*

The CCA Information Systems Support (ISS) staff consists of five individuals. The breakdown of individuals by position is as follows:

Project leader/applications development.	Database specialist.
Application specialist.	Network/operations specialist.
Web/DTP Consultant.	

The ISS staff is experienced with the CCA systems. Both the project leader/applications development and the application specialist have been on staff with the CCA for more than ten years. The project leader/applications development has direct control over the responsibilities of the consultants and is actively involved in the daily duties of the consultants. All four consultants report to the project leader/applications development who reports directly to the assistant tax administrator and the tax administrator.

An organizational chart and job descriptions are available for each member of the ISS staff. The ISS employees attend technical training when deemed necessary by the tax administrator.

The ISS staff is responsible for all areas of computer support which include:

- Maintenance and support of application software, database software, web application, CCA website, and operating systems.
- Resolution of hardware problems and general user concerns.
- Operational duties such as report generation, system backups, system monitoring, and disaster recovery preparation.

The ISS has developed an EDP long range plan. The plan includes long and short term goals for the MITIS™ database and the CCA applications. The plan is reviewed and updated on a periodic basis.

### *Development and Implementation of New Applications and Systems*

The CCA's current application, the Municipal Income Tax Information System (MITIS™), was developed by McHale US Connect in 1993 and was implemented at the CCA in September 1994. The ISS personnel maintain and support the MITIS™ application as well as investigate enhancements to the application using new technologies.

CCA is using a systems development methodology for the development of an eFile web application. CCA's eFile application allows individuals to file the following forms: Individual Exemption Certificate, Individual Annual Return, Individual Estimated Payments, and Assessment Payments. Businesses can file forms for Net Profit Estimated Payment, Employer's Return of Income Tax Withheld, and Assessment Payments. In addition, individuals and businesses can make payments online.

The database specialist prepares a project requirements document for new phases of the web filing application. The project requirements document includes an overview of the prospective project, hardware requirements, software requirements, and technical requirements. The Modis consultants report the project status to the database specialist who acts as the team leader and in turn communicates the status to the project leader/applications development.

To help ensure a new application will achieve CCA's business needs, an analysis of the project is performed. The goal of the analysis is to model the desired system. Design specifications, application flow charts, and architecture diagrams are also prepared when a new application is developed. New applications are tested by the user test teams and errors are corrected prior to placement of new code into production. Movement of new code into production is performed by the network/operations specialist who does not perform any MITIS™ or batch programming functions.

The CCA has designed a "Frequently Asked Questions" section for their website. This section serves as documentation to help the user register with CCA, file and pay their taxes online, submit and pay employer withholdings, file and pay estimates, file exemptions, and file and pay penalty and interest assessments.

### ***Changes to Existing Applications or Hardware Systems***

The CCA has implemented program change procedures for authorization, coding, testing, implementation, and documentation. There are two types of modifications based upon the type of code requiring modification: (1) client executable code, which is code executed on user PCs and (2) batch code, which is code executed on the Sun Solaris systems. Change procedures vary for each type of code.

#### *Approval Process*

MITIS™ application users may request modifications to the client executable code. Change requests are submitted by department supervisors to the assistant tax administrator for approval using a work request form. The requesting supervisor and the assistant tax administrator review the proposed change and determine if the change is advantageous to the organization. Requests are collected until a sufficient number or a sufficient need is present to warrant a new release of the software. Design meetings are held with the CCA management and the application specialist to help ensure proposed changes are acceptable by all departments.

Modifications to batch code programs are also requested using the work request form. These changes are requested by the department supervisors and are sent to the assistant tax administrator. The project leader/applications development and the assistant tax administrator approve the requests. The project leader/applications development then prioritizes and assigns the requests to the application specialist.

#### *Programming and Operating System Upgrades*

PowerBuilder® is the application development tool used by the CCA. Modis consultants perform all programming tasks and communicate the project status to the project leader/applications development. All program source code resides on the Windows 2003 server. Production object code is maintained in a production directory. Once the appropriate changes have been made to the source code by the application specialist, the source code is compiled in the test environment using PowerGen, a tool used to automate the building of PowerBuilder® applications. Application changes are tested by the user test team. The test team consists of a representative from each of the user departments and/or the department supervisor and the application specialist.

Upgrades to the operating system are performed by the Modis consultants. Installation instructions included with the upgrade are reviewed and followed to ensure proper installation. System documentation for the Windows 2003 operating system is available online, and Microsoft can be contacted for additional support.

### *Service Agreements*

The CCA has contracted with Modis, Inc. to provide on-site consultants who are responsible for support and program modification services. CCA has also contracted with Sybase, Inc. for database software support and has purchased an incident support plan that provides case-based technical support for PowerBuilder®. Contracts have been established with Sun Microsystems and Great Northern Consulting to provide support for the Sun Solaris operating system.

### *Testing*

The application specialist is responsible for the design of the client executable code while the test team is responsible for testing changes to client executable code. The application specialist develops test spreadsheets which define the areas to be tested by the user test team. After testing has been performed and the test team is satisfied the change is working as intended, the test team leader, test team members, and/or the assistant tax administrator sign off on the spreadsheets. If errors are detected, the application specialist corrects the errors and the program is tested again. If errors continue, the change will be delayed to be worked on for a subsequent MITIS™ release.

Users also test changes to the batch code. Test results from the modified batch programs are reviewed and discussed with the application specialist. Errors are corrected before new programs are introduced into the production system.

### *Implementation and Documentation*

Programs are moved into the production environment by the network/operations specialist. Windows Explorer is used to move programs into production for changes made to the client executable code. File Transfer Protocol (FTP) is used to move batch code changes into production. Access has been assigned to prevent the application specialist from accessing both the Windows 2003 and Solaris (UNIX) production environments.

Users acquire the new version of the client executable code (MITIS™) when they log into the Windows 2003 server. Each time the user logs into the network, a script located on the Windows 2003 server compares the version of MITIS™ running on the user's PC to the version of MITIS™ located on the Windows 2003 server. If the versions do not match, the PC is updated with the new version from the Windows 2003 server. Prior versions of the source code are stored in an archive directory and are named with a date extension.

Each batch program and client executable code change is documented and kept in a separate folder in the ISS department. A documentation checklist is used by ISS to ensure that all required documentation (print out of the batch program and/or script highlighting the code changes; programmer initials, change date, and brief description in the batch program header) is generated for each change. Production source code is included in the daily backup ensuring its availability, if required. User manuals are updated if the functionality of the application is altered as a result of the program change. Typically, new versions only include fixes and minor enhancements.

Users are notified of all revisions made to the MITIS™ application. Notices are either e-mailed to users or are posted throughout the building. The test team provides user training when necessary.

## ***IT Security***

The CCA has addressed internal, external, and physical computer security risks. Security procedures help to ensure access is provided to only authorized individuals and at access levels corresponding with their job responsibilities.

An Internet and e-mail usage policy is included in the personnel policies and procedures manual which is distributed to all employees when they are hired. The policy states that Internet and e-mail use is restricted for business use only and the city reserves the right to monitor and review documents on city computers. The policy also includes guidelines for usage and enforcement of the policy rules. Violators are subject to discipline including the possibility of discharge. Employees sign an acknowledgment form accepting the policy.

The MITIS™ security council was established by the CCA to develop security policies. The council consists of four members including the assistant tax administrator and the supervisors of individual audit, collections, and taxpayer assistance. The council also reviews the MITIS™ roles and their assigned permissions and requests changes in security due to promotions or re-assignments. These changes are e-mailed to the ISS staff so they can make the appropriate updates to the system.

Supervisors send new user access requests to the ISS project leader/applications development via e-mail. The ISS staff confirms the information with the supervisor and the MITIS™ security council. Network and application user IDs and passwords are established by the appropriate ISS staff member. The appropriate department supervisor is responsible for training the new employee and ensuring the initial password is changed. Application level security roles are assigned by mirroring the account of another employee with the same job position.

MITIS™ security reports are reviewed monthly by the application specialist. The report is compared to current employee listings and established security parameters. Deviations from expected results are investigated by the application specialist with assistance from the appropriate department supervisor. ISS also encourages supervisors to review user access through the user maintenance screen in the MITIS™ application.

The ISS staff receives notice of employee terminations from the department supervisor or administration via e-mail. Employee access is removed by an ISS staff member at the end of the final work day. If the terminated user had system privileges, system administration passwords are changed immediately.

Remote access is provided to current or previous member communities for inquiry of tax data. Currently, 23 communities have dial-in capabilities. Remote access users are restricted to their own community data by network and application level controls.

A firewall has been placed between the CCA and the larger City of Cleveland network to control network traffic. Traffic originating from within the CCA network is permitted to pass through the firewall based on the destination and individual network configuration.

The MITIS™ application is a client server based system with aspects of the system maintained on the Solaris (UNIX), Windows 2003, and Sybase software platforms. Access to the resources offered by these systems is controlled by specific features of these platforms. Security features of these platforms and the MITIS™ application are discussed below.

### *Solaris (UNIX) Environment*

The Solaris system is used for batch processing and storing MITIS™ application data. Primary logical access control to this system is provided by the security provisions of the Solaris operating system. This includes access to data, programs and system utilities. Users of the system are

required to have a valid user account to access the system, and the accounts are restricted to the ISS staff. All accounts on the system are password protected. Access to system administrative tools and system utilities is also limited. The password for the administrative account has been provided to only the ISS staff. No other accounts have been provided with access similar to this account. Sensitive security files, like the password, shadow password, and group files are protected to ensure they cannot be altered by unauthorized users. Access to batch source and object files is also protected to ensure unauthorized modifications cannot be made. Application data is housed within a Sybase database, and database files are only accessible to ISS staff.

Trusted hosts and trusted accounts, which simplify access by bypassing the password security check, have not been established on the application server.

#### *Windows Environment*

Windows systems, both client and server versions, are used to distribute and secure computer resources across the internal network at the CCA. Access to the network is controlled with a number of operating system security features. Users of workstation and network resources are provided with individually assigned, password-protected, user accounts. Password and login parameters have been set on the Windows domain to prevent unauthorized access of system resources. A minimum password length is required. The complexity of a user's password is also defined through parameter settings. The system requires a password contain three of the following four items: special characters, numbers, uppercase, and lowercase characters. These settings help ensure a password is complex enough to prevent successful guessing of the password. Login parameters have been set to discourage unauthorized users from attempting to log into valid accounts. The password for the administrative account has been provided to only the ISS staff and the tax administrator. No other accounts have been provided with access similar to this account. The CCA does not use trusts to allow single sign-on authentication across domains. Dial up access via the AS 5300 universal access server is available and is limited to an authorized group of member community users.

Network security events; including logon events, object access, policy changes, privilege use failures, and system events; are logged and monitored by ISS staff.

#### *Database Level Security and Application Level Security*

The Sybase database and the MITIS<sup>TM</sup> application work together to restrict user access to the tax data. When new users are added to the system, they are assigned roles within MITIS<sup>TM</sup> that are appropriate for their job position. MITIS<sup>TM</sup> then works with Sybase to access only the data which is permitted by the defined role. Only a limited number of accounts have been established in the Sybase database. Users do not have individual accounts for the Sybase database and all accounts are password protected. Only one account has been given system administration, site security officer, and operator properties. The database specialist is the only individual who knows the password to the administrative account; however, a central reference file for passwords is maintained and may be accessed by the project leader/applications development in an emergency situation.

Access at the application level is further restricted by an additional user ID and password. Password length and expiration controls have been incorporated into the MITIS<sup>TM</sup> application. MITIS<sup>TM</sup> passwords are not permitted to be reused. MITIS<sup>TM</sup> users are instructed not to share their password. Access to the application is segregated by groups. Users are assigned to the group with the appropriate level of access for their job responsibilities.

### *eFile Web Application*

In order to use the eFile web application, the taxpayer must register with CCA or have an existing taxpayer account. Users of the eFile application are authenticated through the use of a taxpayer ID number, password, and entry of a human verification code. Password length requirements have been incorporated into the eFile application.

Access to taxpayer data that resides in the database at Rackspace is restricted to CCA personnel through database accounts and passwords.

An eFile entry log is reviewed monthly by the database specialist for any errors that would indicate malicious activity. The eFile entry log is an activity log that captures HTTP activity on the eFile application server. When errors are found, the database specialist initiates a ticket with Rackspace to request they block the IP addresses at the firewall which is located at Rackspace. The number of errors indicating malicious activity has been very small.

### *Physical Environment Controls*

Physical access to the CCA's computer systems is also controlled. Security guards monitor the entrances to the building. Visitors are required to check in at one of the security desks and present a state issued photo ID. A visitor's badge is then provided which is to be returned when they leave the building for the day. The security guard records the visitor's arrival and departure times in the key card system. The main doors to the CCA building are locked after normal business hours. The computer room is locked at all times and is restricted to authorized personnel using a key card system.

The following items protect the computer room from adverse environmental conditions:

- Heat/smoke detectors.
- Building wide uninterrupted power supply.
- Building wide back generator.
- Air conditioner to control temperature and humidity.
- HFC fire suppression system.

The City of Cleveland is self-insured for computer losses.

### ***IT Operations***

The ISS staff performs the day-to-day operational functions. ISS personnel monitor key performance measures, such as disk space capacity, performance times of batch processes, and system usage. These performance measures are not reported to management, but they are monitored on a weekly basis by the network/operations specialist and the database specialist. ISS personnel attempt to resolve issues as they are identified. If the issues cannot be resolved in a timely manner, the software and/or hardware vendors are contacted for technical assistance. Hardware and software related problems are monitored through system messages and electronic pages to ISS personnel. Procedural and operating support manuals are retained to guide the ISS group when processes are run or support questions arise.

The MITIS™ application is an online, real time system; however, batch processing is also critical to system functionality. Batch processing procedures are documented in the MITIS™ Procedures/Operations manual. The manual is available on all end user PCs. The procedures include step-by-step instructions for batch processing.

A batch processing directory has been set up to include all regularly scheduled batch jobs, including daily batch processes. A master Excel spreadsheet is automatically generated and is available for review by ISS personnel for problem resolution. The spreadsheet indicates the name of the job, time and date run, and any exceptions, condition codes or system problems that occurred. Scripts scan the log directory and extract log information. The extracted information is inserted into a Sybase database table which is used to update the master Excel spreadsheet daily. System logs are reviewed online for monitoring the batch processes.

The CCA also processes transactions electronically received from Key Bank (income tax payments), Coleman Data Solutions (third party vendor used for data entry of non-cash returns, which are those returns where no tax is due or payment isn't made at the time of filing), and the State of Ohio (filing and payment of municipal income taxes by businesses through the Ohio Business Gateway (OBG)). The ISS staff loads this information into the MITIS™ system and produces reports that are used by other CCA staff to reconcile the data.

ISS is responsible for producing and distributing all reports for the CCA. Reports from production batch processing are distributed by ISS personnel to the appropriate department supervisor. End user personnel are responsible for distributing reports outside of the CCA main office.

The Windows network is used for routing and printing reports. Eight local and 23 network printers are available for end user departments to facilitate computer operations and processing.

Balancing and reconciliation procedures are performed by the application user to monitor application data. The controller's department performs a monthly reconciliation. The daily transaction reports from the collections department are compared to the monthly reports from the MITIS™ application, summarizing the monthly activity for tax remittances and refunds.

Modis consultants install vendor provided upgrades to system software. Upgrades are tested in a test environment before installation into the production environment. Full system backups are performed prior to implementing the upgrade.

### *Backups*

Documented procedures are available for performing backups. Backups for the Sybase database are performed via SQL Backtrack during daily scheduled processing for the Solaris (UNIX) server. SQL Backtrack stores three generations of backup files (hourly, daily, and full weekly backups) within the same root directory. SQL Backtrack backs up Sybase databases to flat files residing on Sun servers. ARCserve backup software is used in both the Windows 2003 and Solaris (UNIX) computer environments, and is initiated through the use of automated scripts. The hourly and daily backups are written to high density, 100 gigabyte tapes each night. In addition, full system backups of both computer environments are performed on a weekly basis.

The CCA backup tapes are rotated off-site. The CCA contracts with a records retention vendor to store all of the CCA's backup media. The drop-off/pick-up dates are typically scheduled at one-week intervals. During holidays the interval length may be as long as two weeks. Daily and weekly backup tapes are rotated off-site to the vendor's facility. The monthly full system backups are also rotated off-site and are retained for one year.

A system message is sent to ISS personnel regarding the status of the Sybase nightly backup or any errors that occurred. ISS personnel also receive system logs from both the SQL Backtrack and ARCserve backup programs that document backup completion. ISS personnel are responsible for resolving error conditions and ensuring backups are completed in a timely manner. Users notify ISS staff of application processing

problems. Hardware problems are monitored through system messages and electronic pages to ISS personnel. These pages are delivered via Q page, and briefly indicate the type of problem that is occurring.

Service agreements with Sun Microsystems and Great Northern Consulting Services cover technical support and maintenance on the CCA's computer hardware.

## **FINANCIAL APPLICATION CONTROLS**

### **Municipal Income Tax Information System (MITIS™)**

#### ***Overview of the Application System***

The Municipal Income Tax Information System (MITIS™) is a Windows based application. The primary function of MITIS™ is to record the collection of municipal income taxes and to distribute the tax revenue to the member communities. Users utilize an icon driven interface to enter or update information online. Taxpayer information is entered by authorized staff in the collections, audit, and administrative departments. A variety of batch processes are also executed to provide daily and monthly reports, print bills, issue refunds, and load lockbox and other data from external sources. Revenue collected includes employer withholdings and payments of municipal income taxes from taxpayers of member communities.

Residents of the CCA member communities receive annual tax forms after year end and may receive quarterly estimated billings. Likewise, businesses of the CCA member communities receive annual tax forms, may receive quarterly estimated bills, and monthly/quarterly withholding forms. The CCA uses several methods to ensure all taxpayers pay their tax obligation. For example, the CCA performs name and address matches of MITIS™ taxpayer records to state name and address files, obtains real estate transfer listings to identify new residents, and obtains W-2 information filed by employers.

Revenues are sent to member communities on a monthly basis. Monies held by the CCA are invested daily and interest earned is allocated to the member communities. Using a two-factor formula, all of the CCA expenses are allocated to the member communities. These overhead costs, up to five percent of taxes collected, are deducted from the monthly distribution.

#### ***Revenue Collection***

Taxpayers can pay by check, cash, credit card or Automated Clearing House (ACH) debit. While the majority of payments are received through the mail and are processed through the lock box services of Key Bank, payments are also received at the agency, either by direct mail to CCA or by taxpayer "walk-in", and are processed by the CCA collections department. Within the past few years, CCA has begun accepting electronic payments through the Ohio Business Gateway and eFile. These electronic payments are also processed through Key Bank.

#### ***Payments Received by Lock Box***

The CCA contracts with Key Bank for lock box services. Processed tax forms are grouped into batches of 30 by form type. Photo copies of the checks for each batch are received by the CCA from Key Bank.

Some forms, such as tax assessment and tax estimate forms contain information that can be scanned. A data tape is also generated for batches of forms with scannable information. Collection reports and transaction tapes are generated by Key Bank and are sent to the CCA electronically. The transaction detail file is loaded into the MITIS™ application by the ISS staff. Totals on the tape label are compared to totals generated by the MITIS™ application to ensure all data has been received from the tape. Balances, from the report sent with the data, are manually compared to MITIS™ totals to ensure all data was processed correctly. If errors in the data file are discovered, the data is removed from the system and a new tape is requested from the bank.

#### *Direct Payments*

Payments received at the CCA are opened and sorted by the mail openers. Mail is sorted by payment type (cash and check, or credit card), and by filing type (individual or corporate return, etc.).

The returns are collected in batches of 30. The cashiers separate the tax forms from the payments for further processing. Although the forms and the payments are separated, they remain in the same batch. Each tax form in the batch is entered into the MITIS™ system by a cashier who enters the taxpayer ID and verifies the taxpayer information. MITIS™ programming controls validate the taxpayer ID number, and will not allow posting of payments to taxpayers not on file. The tax year, payment date, and amount are entered by the cashier. A grand total of the total tax amount assessed for each payment batch is calculated.

Payments are then entered into the MITIS™ system by a second cashier, providing for a separation of duties. Payment totals are compared to the batch totals from the tax forms. The MITIS™ system automatically assigns a number to each batch for document tracking, and processing cannot continue until the payments and forms are in balance. If an imbalance exists, the entry error is identified and corrected by an income tax supervisor. These corrections can only be made by supervisory personnel who have been authenticated through a user name and password. If the imbalance is due to a discrepancy between the amount of the check and the tax form, the amount is noted on the return, and the taxpayer is either billed or notified of the overpayment. Only authorized individuals have the capability to change cash batch totals in MITIS™.

For tax returns received with credit card payment, the payments are pulled and placed into a separate process. The payments are treated as walk-in payments and are placed in a batch. A tax return is generated by the MITIS™ application and is compared to the return submitted with the payment. If the tax due is the same, staff will enter the credit card information into the credit card machine and attach an authorization form. One cashier enters the amount on the tax form and another cashier enters the amount on the authorization form. All documentation related to the credit card transaction is filed.

#### *Ohio Business Gateway (OBG)*

Payments and withholdings by businesses can be made online using OBG's ACH debit payment service. Users are required to supply banking information after creating and choosing to file report(s). In order to pay by ACH debit, the following information is needed: routing and transit number of the taxpayer's bank and the taxpayer's account number.

After filing, OBG automatically sends tax data, ACH debit payment instructions, and the OBG confirmation number directly to CCA. The OBG confirmation includes a time-stamp to validate the time and date of filing. Confirmations are issued only after the entire filing and payment process is completed.

The OBG ACH debit payment service generates files for download by the ISS department. ISS downloads the following OBG files available daily:

- NACHA file which is a file formatted according to the standards established by the National Automated Clearing House Association (NACHA). This file is only created if a payment is available.
- Withholding source files which include withholding returns.
- Net profit source files which include net profit, net profit estimate, and net profit extension returns.

ISS compares the NACHA file to the report of transactions for completeness and accuracy. ISS then generates reports for the fiscal department to verify accuracy and for reconciliation purposes. The NACHA file is then sent to the bank through an automatic process. The bank then sends a confirmation to the fiscal department indicating they received the file and it matches what was reported. A second confirmation is received when the money is deposited into CCA's account and the transaction is final. When the second confirmation is received, ISS processes the files and loads the data into MITIS™.

The collections department receives the tape edit (batch summary sheet) which includes the transaction amount and type of transaction. They also receive the detailed activity reports that are used to enter and verify the information in MITIS™ and to balance the batch. Finally, the net profit returns and extensions are given to the corporate audit department, and the corporate withholdings are given to the collections department to pre-audit and finalize the batch.

#### *CCA eFile*

CCA's eFile is a convenient and secure way for qualified taxpayers to file their CCA municipal income tax forms and make payments electronically. The following forms can be filed electronically through eFile:

##### Individual Tax Forms:

- Individual Exemption Certificates: used when a taxpayer resides in a CCA community and had no earned income for the entire year.
- Individual Annual Return: used when a taxpayer lives and works in a CCA community and taxes were withheld by the employer. If the tax form shows an overpayment or refund, eFile will not accept the form. Instead the taxpayer will need to mail the tax form to CCA.
- Individual Estimated Payment.
- Assessment Payment.

##### Business Tax Forms:

- Net Profit Estimated Payment.
- Employer's Return of Income Tax Withheld.
- Assessment Payment.

Taxpayers have the option to make a payment for each of the above forms with the exception of the Exemption Certificate. When taxpayers choose to make a payment, they are transferred to a KeyPay module (created and hosted by Key Bank and its affiliate Govolution). Key Bank and Govolution are responsible for the processing, verification, and collection of the payment whether it's an ACH payment or credit card. CCA eFile records the payment data communicated by Govolution in the eFile database. The payment received is sent to a lock box which is reconciled by CCA with the payments portion of the eFile database.

---

Payments accumulated within the eFile database are extracted daily by the CCA ISS staff and are loaded into MITIS™. All extracted eFile records are flagged and periodically archived into the eFile history tables located on the MITIS™ server.

#### *Deposit Process*

The principal cashier summarizes the cash received per the balanced batch totals and completes a daily deposit slip. Daily deposits include payments mailed directly to CCA and collected via walk-ins. All monies collected after the predetermined cut off time are applied to the following day. Deposits are taken to Key Bank by a courier, and the batches are marked as “deposited” in the MITIS™ system.

#### *Pre-Audit Review*

Nearly all forms go through a “pre-audit” process. In this process, the MITIS™ application recalculates the tax liability of the taxpayer. This calculated tax liability is compared to the prepared tax form. Documentation is reviewed to ensure all required information is included. If documentation is missing, the form is held in the pre-audit stage until all the information has been collected from the taxpayer. MITIS™ performs edit checks for valid city code, taxpayer city of residence, and employer ID number during this process. Processing cannot proceed until these items are entered.

Tax assessment forms are not included in the pre-audit process. These forms are generated by MITIS™ and therefore are not required to go through the comparison process. When the payment information is entered into the system, the original MITIS™ assessment information is retrieved and payments are applied to this assessment.

MITIS™ calculates the tax due from W-2 information. W-2 data is entered into the system via two methods. The primary method is through data files obtained from employers and a third party vendor, Coleman Data Solutions. The secondary method is through data entry by the CCA staff from the W-2 information provided by the taxpayer.

If sufficient information is not available to complete the pre-audit process, a letter is sent to the individual requesting the missing information. If the information is not supplied in a timely manner, the assessed tax is estimated and payments are applied. The taxpayer is billed for additional assessments resulting from errors identified in the pre-audit process. Payments received are applied to the current taxes. Errors which result in an overpayment of taxes are applied to future periods. Additionally, MITIS™ does not permit entry of an amount that does not match the actual amount collected. Once the pre-audit is complete, the status is changed, by appropriate supervisors and staff, from “pre-auditing” to “pre-audited.”

#### *Finalization Process*

All pre-audited tax forms are forwarded to the principal cashier or income tax collections supervisor. The system compares the batch total to the total of the pre-audited forms to identify inconsistencies. Batches without inconsistencies are marked as “finalized” within MITIS™. All other batches are adjusted for the payments received and marked as “estimated” payments within the MITIS™ system. These other batches can now be marked as finalized. Only authorized users have the MITIS™ privileges to mark batches as finalized.

### *Reconciliation Process*

At month end, all monies received from the lock box and the CCA deposits are reconciled to the total monies distributed within MITIS™. Differences are investigated and corrected by the controller or the principal cashier. In order to complete the month end closing procedures, tax forms must be finalized for all tax payments deposited since the prior reconciliation.

### **Refund Distribution**

#### *Return Sorting*

Tax returns that result in refunds are collected by the audit department via lock box, direct mail to the CCA, and through taxpayer “walk-in.” The following describes the initial handling of tax refund requests:

- *Refunds received through the lockbox service* - The collections department receives refund requests which are mailed to the CCA’s lockbox. Refund requests included in lockbox batches are treated the same as refund requests received through the mail.
- *Refunds received through direct mail to the CCA* - The collections department receives, opens, dates, and sorts all mail received by the CCA on a daily basis. Refund requests are pulled and sorted for distribution to the audit department.
- *Refunds received by “Walk-In Taxpayers”* - Requests personally submitted to the CCA by taxpayers are processed through a “walk-in” batch. Each CCA audit staff member has been assigned an individual “walk-in” batch number. These batch numbers are greater than 9799. An income tax audit supervisor then receives the batches for review.

Refund requests are separated from payments and are sent to the audit department for processing. Refund requests are sorted by type (individual, corporate, and W-3.)

#### *Batching*

Once sorted, the forms are grouped into temporary batches of 25 and are assigned a temporary batch number. Refund requests are transferred to permanent batches after all auditing procedures have been completed. The audit department staff enters the data from the refund request forms and the attached W-2s into MITIS™.

#### *Pre-Audit of Refunds*

To support segregation of duties, an audit department employee, other than the one who entered the refund request data, performs the audit procedures. MITIS™ recalculates the refund amount from the data entered. The amount from the refund request form is compared to the MITIS™ calculation. If additional documentation or information is required, the refund request remains in the pre-auditing status until the additional information is received. The pre-audit process requires the auditor to validate certain key fields and MITIS™ does not allow further processing of the refund until the fields are validated.

Once the pre-audit process is complete, the refund request is marked “pre-audited.” The conclusion of the pre-audit process results in one of the following actions:

1. A refund is processed for the same amount requested.
2. The refund is adjusted based upon the pre-audit results. Correspondence is sent to the taxpayer to explain the difference.
3. The refund is denied based upon pre-audit results. Correspondence is sent out to the taxpayer to explain the denial.
4. The taxpayer is billed for additional taxes based upon pre-audit results. Correspondence is sent to the taxpayer explaining the action.
5. Correspondence is sent to the taxpayer requesting additional information before the refund request can be processed further.

For all the preceding actions except number 5, the auditor marks the tax form “pre-audited” and processing continues. Approved refunds are then forwarded to an income tax audit supervisor, who compares the physical return to the data entered into the MITIS™ application. An income tax audit supervisor holds refund requests which are different from MITIS™ data for further review. All refunds for more than one thousand dollars must be reviewed and approved by an income tax audit supervisor, administrative manager, and income tax administrator. An income tax audit supervisor then assigns permanent batch numbers to approved tax return refunds. Only authorized users have the MITIS™ privileges to mark batches as pre-audited.

#### *Reconciliation Procedures*

After a group of refunds have been reviewed and assigned to permanent batches, an income tax audit supervisor, or a designee, runs an adding machine tape of each batch and marks the batch in MITIS™ as “finalized.” Once all permanent refund batches have been finalized, the ISS staff initiates a batch processing job that generates a “Voucher Generation Report” (VGR). The VGR collects and summarizes all the finalized batches. The VGR assigns a voucher number to each refund and sorts the refunds into “voucher batch number groups.” An income tax audit supervisor matches the total dollar amount of the refund group (per the VGR) to the adding machine tape batch totals. Then, an income tax audit supervisor compares the VGR with the MITIS™ total refund amount processed for that time period to ensure all finalized records (returns) have been included in the VGR.

The VGR also includes any interest owed to the taxpayer. An income tax audit supervisor, or designee, reviews the interest amounts and adjusts the VGR for any errors detected by deleting the erroneous refund or interest record from MITIS™. Only a limited number of authorized users can perform this function in MITIS™. The VGR report is not rerun. Hand written adjustments are made and are supported by an Excel spreadsheet (adjusted VGR).

After the VGR has been reviewed, ISS generates a FAMIS Interface Report which lists the voucher number, the refund amount, interest, if any, and other taxpayer information associated with the refund such as taxpayer ID, tax year, and city code. An income tax audit supervisor matches each approved refund batch tape total to the Voucher Report. Because refund adjustments cannot be made at this point, incorrect refund amounts must be removed from the batch. The interest amounts are also verified, and if necessary, adjusted by an income tax audit supervisor.

Once the VGR is verified as accurate or is adjusted to the correct amount, an income tax audit supervisor marks all the voucher batches as “approved.” Only a limited number of authorized users can perform this function in MITIS™. All refunds included on the VGR report must be set to “approved” before an income tax audit supervisor will release a refund for payment. An income tax audit supervisor prints the approved Refund Voucher Batch Status Screen, files a copy with the auditor’s documentation packet, and forwards a copy to an assistant income tax financial supervisor. An assistant income tax financial supervisor makes a deposit for the total amount of refunds and interest pending into the CCA refund account.

At the request of an income tax audit supervisor, ISS initiates a MITIS™ batch job to create the FAMIS Interface Report which identifies the final refund and interest payment information. An income tax audit supervisor then verifies the FAMIS Interface Report agrees with the total amount of funds deposited by an assistant income tax financial supervisor into the refund account from the MITIS™ Refund Voucher Batch Status Screen. Once the FAMIS Interface Report runs, all refund batch statuses are automatically changed to “sent” in MITIS™. An income tax audit supervisor instructs ISS to transfer the report, via diskette, to city hall where refund and payment information is entered into the city’s accounts payable system.

#### *Distribution of Refund Warrants*

During processing, the city prints an AP Trial Payment Register from the PeopleSoft Accounts Payable module. An income tax audit supervisor matches payee and check amounts from the MITIS™ FAMIS Interface Report to the AP Trial Payment Register. After these are reconciled, the CCA then asks the treasury to release the refund checks in that evening’s mail.

After the warrants have been printed, the CCA receives a Detailed Check Register from city hall. The Detailed Check Register is reconciled to the MITIS™ Refund Voucher Batch Status Window, and the batch status is changed from “sent” to “check cut.” An income tax audit supervisor also enters a “check cut date” for each refund batch from the date on the Detailed Check Register.

#### ***Distribution of Tax Revenues***

Collections are sent to member communities, with the exception of the City of Cleveland, via Automated Clearing House (ACH) on the Monday following the second Wednesday of each month. Remittance to the City of Cleveland is made on a daily basis. Because of contractual agreements to distribute collections on a monthly basis, member communities receive estimated amounts during peak filing periods. The estimated distributions are equal to the higher of the amounts which were actually generated during the same period of the previous year or the current balance in the MITIS™ system. Adjustments between the estimated and actual figures are made in the following month.

Receipts and refunds are processed through the end of the month. A monthly reconciliation of receipts, refunds, and adjustments is performed prior to distribution of revenues to the member communities. At month end, the books are closed and the controller’s office works with the collections department and the audit department to reconcile total receipts, refunds, and adjustments. When the final figures for the month are reconciled, settlement statements are run for each of the member communities which indicate the total receipts, refunds, adjustments, overhead, and the net payment that will be wired to the member community’s account. The controller’s office mails the settlement statement, which serves as the official remittance advice of the amount to be transferred, along with supporting MITIS™ reports to the individual member communities.

Prior to remittance day, the CCA prepares a wire transfer schedule. The schedule is generated by ISS staff. The schedule lists the member communities, their bank account information, and the net amount to be wired. After the schedule is approved by the income tax administrator, the city finance director, the city commissioner of accounts, and the city treasurer, the amounts are wired by the City of Cleveland treasury department to the appropriate bank accounts.

The CCA performs monthly bank reconciliations and compares the amounts transferred by the treasury department to the wire transfer schedule.

### *Overhead deductions*

Overhead rates charged to member communities are entered into the MITIS™ system. The CCA expenses are allocated to the member communities using a two-factor formula. The first factor is the community's percentage of dollar revenue collected to the total dollar revenue collected for all communities. The second factor is the community's percentage of transactions recorded to the total number of transactions recorded by the CCA for all communities. The percent average of these two factors is called a net-cost percentage. The cost allocated to the community is calculated by multiplying the net-cost percentage times the total CCA expenses. The net-cost percentage was initially calculated using actual data from the most recent audited fiscal year. The cost percentage will differ for each member community and is updated during the year upon completion of the city's next audit. In 2008, the amounts to be withheld from the distributions of the final three months, October, November and December collection amounts, were adjusted to ensure the year end recovery of all the estimated calculated costs. A net-cost estimate was calculated using audited 2006 data for the first nine months of 2008.

### ***Penalty and Interest***

Penalty and Interest amounts are automatically calculated by the MITIS™ system. The process is performed either through a batch job or online via the MITIS™ application.

### *Batch Process*

The batch job responsible for calculating penalty and interest is included in the monthly closing procedures. This batch job calls two programs which are responsible for the following functions:

Payment/Distribution Program – The purpose of this program is to apply finalized payment distributions entered online or through batch from lock box receipts to the corresponding assessment or payment plan records that originally created the bill. This process closes assessment record(s) or payment plans that meet the condition for closure. Any remaining amount owed is processed by the penalty, interest and payment plan billing process for additional billings.

Assessment Record Creation Program– This program goes through the current payment transactions. These transactions are checked for various penalty and interest conditions such as late payments and balances due. For transactions flagged by the program, an assessment record is created, the months late (difference between the filing date and the due date) will be calculated, and then interest and penalty are calculated based on the penalty and interest conditions including, but not limited to, the form type, first time filer, filing of an extension, or exempt filing status.

Although this batch job is run each month, individual assessment records whose assess status is initially set to 'Open Assessment,' are evaluated approximately every other month. If payment has not been made in full, a second notice is sent to the taxpayer and their status is changed to 'Delinquent.' In approximately another two months, if payment has still not been made in full, including the tax liability as well as any penalty and interest charges, a third and final notice is sent to the taxpayer. Upon sending the third notice, the taxpayer's account status is set to either "Final Tax Due (FNTAXD)" or "Final No Tax (FNNTAX)". "Final No Tax" means the taxes have been paid, but the taxpayer still owes penalty and/or interest.

An assessment record can be updated with an assess status of City Review (PPHOLD) at any time. PPHOLD (Payment Plan Hold) status is assigned when a payment plan has been set up for the taxpayer and further penalty and interest are not assessed unless the taxpayer defaults (missed two payments) on the payment plan.

#### Red Bill Procedures:

This procedure, also referred to as 'RB,' is automatically performed in October as part of the September month end procedures.

This procedure recalculates the 'Months Late' (difference between the due date and the current end of month) and penalty and interest due for the assessment record with an assess status of Final Tax Due, Final No Tax, or delinquent PPHOLD. However, if the recalculated penalty and interest is less than what is already owed, the penalty and interest will remain unchanged. Payments received are first applied to the tax owed. This is done to prevent the penalty and interest due from being recalculated at a lesser amount when the payment received is partial and does not cover the penalty and interest charges. This helps to ensure CCA the penalty and interest due is paid in full.

This 'RB' process also generates an additional notice. The wording and severity of this notice is determined by the individual member communities. At the request of the member community, this notice may also be pulled and not mailed.

#### Online Process

In addition to the batch process, an assessment record may be generated including the calculation of penalty and interest by the click of a button within the MITIS™ online application. When a taxpayer comes in for the first time to file and makes a payment for an overdue tax form, the CCA Auditor has the ability to calculate the penalty and interest by the click of a button. This online process actually runs the same program used in the batch process. Authority to generate the assessment record via online method (calculated by MITIS™) is permitted by most CCA staff with the exception of clerical positions. However; the authority to update the penalty and interest liability amounts based on manual recalculations or corrections is restricted to tax administrators, administrative managers, supervisors and their backups.

#### GASB

Penalty and Interest amounts may also be updated at the request of the CCA's external auditors. This is usually performed as of the end of a fiscal year and does not generate any notices. This program updates the assessment reason, billing date, months late, and penalty and interest amounts due on the assessment record. The GASB program is a batch program which can only be initiated by the ISS staff.

#### Assessment Record

The Assessment Register may include more than one assessment record, one for each form for each filing period in which the taxpayer is delinquent. Each assessment record documents several dates and figures which are updated at different times throughout the penalty and interest lifecycle. The dates within the assessment record are as follows:

Due Date: This is a system generated date and is based on the type of form and filing period.

Date Created: This is also a system date that documents the first time the Assessment Record Creation Program is run, either submitted by batch or selected from the online program. An assessment record is not created until after the tax form has been

processed.

- Billing Date:** This is a system generated date that documents the date the last notice was generated. This is updated by the Assessment Record Creation Program and the 'RB' process.
- First Notice:** This is a system date that reflects the date of the first notice (Status = OPEN). This is updated by Assessment Record Creation Program.
- Second Notice:** This is a system date that reflects the date of the second notice (Status = DELINQUENT). This is updated by the Assessment Record Creation Program.
- Final Notice:** This is a system date that reflects the date of the final notice (Status = FNNTAX, FNTAXD, or PPHOLD). This is updated by Assessment Record Creation Program.
- Filing Date:** This date is manually entered and reflects the date the form was actually received (per date stamp) by CCA.

The following information is also maintained on each assessment record:

- Assess Status:** This is updated with each notice that is given, and again when either the 'RB' process or GASB program is run.
- Months Late:** This is the number of months between the due date and the actual filing date. This is only updated when the 'RB' process is run.
- Original:** These amounts are system generated based on the tax due, and calculation of penalty and interest by either the Assessment Record Creation Program when the assessment record is originally generated; the 'RB' process; or if the GASB program is run.
- Liability:** These amounts are updated by the system the same as the original figures. However; they may also be manually updated by the following individuals: CCA tax administrators, administrative managers, supervisors and their backups. Changes are based on manual recalculations or corrections including additional taxes owed determined through the audit process. The system does not restrict changes to these figures outside of access rights. However; business rules require taxpayers to pay the original tax due and the interest. The individuals with the system privileges to make changes are given permission to work with the taxpayers in reducing or abating penalties owed.
- Actual Paid:** These are the payments that have been made through the month end process and are in history.
- Current Paid:** These are payments for the current month.
- Net Due:** This figure reflects the Liability minus any payments made on the assessment record (Actual or Current).

The system is not designed to maintain a history of key fields, including the liability figures that can be manually updated. Therefore, monitoring of changes is limited to who made the change and the date upon which the assessment record was last updated. The prior values are not readily available. However, the prior values would be available in the form of prior billing reports from previous months or from the backup tapes if necessary.

#### ***Update of Taxpayer and Tax Rate Information***

Taxpayer name and address changes are obtained from either the taxpayers (on the submitted forms), or lists received from third party sources. Information supplied by taxpayers is input by the CCA staff. Selected third-party information received electronically is loaded directly into the MITIS™ application. In this case, ISS staff loads the data and prints reports for the CCA staff who verify the accuracy of the data. Third party information not loaded directly into the MITIS™ application may be used to verify data, generate taxpayer notices, or generate delinquencies.

Tax rates, tax credits, and penalty and interest rates vary among the member communities. The CCA changes the tax tables through a MITIS™ screen after receipt of an official copy of the adopted ordinance establishing the new rates. Access to the tax rate maintenance screen is limited to the ISS staff, the tax administrator, assistant tax administrator, controller, and one assistant. Upon completion of the update, tax rate accuracy is verified by a second staff member.

#### ***Rate Confirmations***

Tax rates and tax credit rates are confirmed yearly by CCA staff. Once elections have been held, a report is generated by the IT staff that lists the current rates in the system for each community. The individual communities are then contacted by CCA staff to confirm there were no changes to the tax rate or tax credit rate. The results are tracked on a spreadsheet. If CCA staff is unable to contact a particular community's tax administrator, they follow-up with e-mails or attempt to verify the rates by researching board of election web sites, city web sites or county web sites to ensure the rates have not changed.

---

## USER CONTROL CONSIDERATIONS

The CCA's MITIS™ application was designed with the assumption that certain controls would be implemented by member communities. This section describes additional controls that should be in operation at the member communities to complement the controls at the CCA. User auditors should consider whether the following controls have been placed in operation at user organizations:

- Member communities should verify the amount of revenue distributed to their organization per the statement sent by the CCA equals the amount wired to their account.
- Member communities should review reports supplied to them by CCA to follow up on delinquent accounts.

The user organization control consideration presented above does not represent a comprehensive set of all the controls that should be employed by member communities. Other controls may be required at member communities.

### **SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR**

*This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the CCA's internal control that may be relevant to member community's internal control, and reduce the assessed level of control risk below the maximum for certain financial statement assertions.*

*The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system for example procedures performed at the CCA and procedures performed at member communities which utilize the CCA.*

*For each of the control objectives listed below, only those controls which contribute to the attainment of the related control objective are described and were tested.*

## GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

### Overall Operation of the IT Function

<b>Overall Operation of the IT Function - Control Objective:</b> <b>IT Personnel</b> - IT personnel should have the appropriate knowledge and experience for the complexity of the IT environment.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
An organization chart and job descriptions have been developed to communicate the responsibilities and segregation of duties for the CCA Information System Support (ISS) staff.	Inspected the CCA organizational chart and job descriptions.	No exceptions noted.
The CCA uses the personnel policies and procedures manual of the City of Cleveland to guide employees in the performance of their duties. The manual addresses issues related to employee benefits, conduct and terminations.	Inspected the City of Cleveland personnel policies and procedures manual.	No exceptions noted.
Trade periodicals and Internet resources are used by ISS staff to maintain an understanding of technology changes in the industry.	Inspected the listing of trade periodicals used by the ISS team for research purposes.  Observed trade periodicals, books, and journals on-site in the ISS department.  Confirmed with each member of the ISS staff they are using the listed resources to stay current on information relevant to their job duties.	No exceptions noted.

<b>Overall Operation of the IT Function - Control Objective:</b> <b>IT Planning</b> - IT strategy should be consistent with the overall strategy of the organization		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
An advisory board meets on a periodic basis to inform, consult with, and advise the CCA tax administrator and the executive committee of issues of common and mutual interest to the member communities.	Inspected the CCA advisory board meeting minutes for the audit period to confirm meeting occurrence and content.	No exceptions noted.
The Information System Support (ISS) staff has developed long term goals and objectives. The document addresses long and short term goals for the MITIS™ application software and database.	Inspected the ISS long term goals and objectives of the ISS Department as well as the individual goals and objectives of ISS staff members.	No exceptions noted.

#### **Development and Implementation of New Applications and Systems**

<b>Development and Implementation of New Applications and Systems - Control Objective:</b> <b>Project Management</b> - Project management should ensure appropriate control over the design and implementation of new applications or systems.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
CCA uses a systems development methodology to steer development of new applications.	Inspected the system development methodology document and confirmed it was followed by CCA in developing their web filing application through independent inquiry with the project leader/applications development and the database specialist.	No exceptions noted.
The database specialist prepares a project requirements document for new phases of the web filing application to help ensure applications are implemented as management intends. The project requirements document included an overview of the prospective project, hardware requirements, software requirements, and technical requirements.	Inspected the project requirements document to confirm hardware, software and technical requirements were considered when developing new applications.	No exceptions noted.

<b>Development and Implementation of New Applications and Systems - Control Objective:</b> <b>Project Management</b> - Project management should ensure appropriate control over the design and implementation of new applications or systems.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Projects are monitored by CCA management, ISS Personnel, and users throughout the development process to help ensure all aspects of the project plan are considered.	Inspected correspondence, including project status meeting notes and e-mails, to confirm ISS, CCA management and users are involved throughout the project.	No exceptions noted.

<b>Development and Implementation of New Applications and Systems - Control Objective:</b> <b>Design/Selection of Applications and Hardware Systems:</b> - Applications and Hardware Systems should be appropriately designed/selected to achieve business and application control requirements (including access security).		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
ISS creates design specifications and requirements for each phase of the eFile web filing application to help ensure business and application needs are met.	Inspected the design specifications and requirements for the phases of the eFile web filing application developed during the audit period (phase 5 and phase 5 rev 2).	No exceptions noted.

<b>Development and Implementation of New Applications and Systems - Control Objective:</b> <b>Testing of Applications/Systems:</b> - Testing should ensure that the new application or hardware system delivered achieve the necessary business and application control requirements.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The test team is responsible for testing new applications to help ensure they are performing as intended. If errors are detected, the application specialist corrects the errors and the program is tested again prior to placement of code into production. Test documentation is maintained on file for future reference.	Inspected test documentation and sign-offs to confirm testing was performed prior to implementing phase 5 and phase 5 rev 2 of the web filing application.	No relevant exceptions noted.

<b>Development and Implementation of New Applications and Systems - Control Objective:</b> <b>Transfer into the Live Environment:</b> - Transfers into the live environment should be authorized and coordinated.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Programmers are restricted from access to the production environment.	<p>Confirmed the application specialist does not have access to the production environment through independent inquiry with the application specialist, network/operations specialist, database specialist, and project leader/applications development.</p> <p>Inspected the following documentation to confirm the application specialist is restricted from the production environment:</p> <p><u>MITIS™ programs</u></p> <ul style="list-style-type: none"> <li>• Program change flow charts and procedures.</li> <li>• Production directory share information and file permissions.</li> <li>• Windows group membership listings to confirm the application specialist is not a member of any group with file permissions above read and execute.</li> </ul> <p><u>Batch programs</u></p> <ul style="list-style-type: none"> <li>• Program change flow charts and procedures.</li> <li>• Solaris (UNIX) password file – to confirm the application specialist does not have an account.</li> <li>• Solaris (UNIX) Group file – to confirm the application specialist is not a member of the system administration groups.</li> </ul>	No exceptions noted.
The assistant tax administrator, administrative manager, and bureau of collections chief are required to approve phases of the eFile web applications development prior to being moved to production.	Inspected the phase 5 and phase 5 rev 2 sign-off sheets to confirm transfer to the production environment was authorized.	No relevant exceptions noted.

<b>Development and Implementation of New Applications and Systems - Control Objective:</b> <b>Training and Documentation:</b> - Users and IT staff receive appropriate training when their responsibilities are impacted by application development and implementation. In addition, technical documentation should be provided to support ongoing operations, problem resolution and future application maintenance.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Documentation, for the taxpayer who uses the new web filing application, was prepared in the form of "Frequently Asked Questions" (FAQs) which are available on CCA's website.	Inspected the CCA website on 02/02/09 to confirm detailed information was available in the FAQ section of the website including updates for phase 5 and phase 5 rev 2 which were developed in 2008.	No exceptions noted.

### **Changes to Existing Applications or Hardware Systems**

<b>Changes to Existing Applications or Hardware Systems - Control Objective:</b> <b>Change Requests</b> - Requests for application program changes or system upgrades should be appropriately considered and processed.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Program change procedures are documented to guide programmers through the program change process. Procedures describe the approval process, test procedures, transfer to production, and documentation. The program change procedures are categorized as follows: <ul style="list-style-type: none"> <li>• Batch program development/change procedures – applications.</li> <li>• Notes on creating a new production MITIS™ executable.</li> </ul>	Inspected the documentation related to program change procedures.	No exceptions noted.
Program changes to client executable code (MITIS™ online system) are requested via a CCA/ISS Work Request Form and are approved by the assistant tax administrator.	Inspected a directory listing of the current production version of client executable code to identify changes made during the audit period.  Inspected the corresponding work request forms for approval by the assistant tax administrator.	No exceptions noted.

<b>Changes to Existing Applications or Hardware Systems - Control Objective:</b> <b>Change Requests</b> - Requests for application program changes or system upgrades should be appropriately considered and processed.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Changes to production batch programs and newly created non-production ad-hoc reports are requested via a CCA/ISS Work Request Form and are authorized by CCA management.	<p>Inspected the directory listing of batch program files and confirmed with the application specialist and project leader/applications development, which programs were actually in production. Identified 41 production programs that were changed during the audit period.</p> <p>Inspected the corresponding work request forms for approval by the assistant tax administrator.</p>	No exceptions noted.
CCA has contracted with Modis, Inc. for on-site consultants to provide support and program modification services.	<p>Inspected the Modis, Inc. service agreement, contract renewal, and related payment information to confirm the agreement is current.</p> <p>Observed the presence of Modis consultants working on-site.</p>	No exceptions noted.
CCA has contracted with Sybase, Inc. for software support and maintenance of the Sybase database software. They have also purchased an incident support plan that provides case-based technical support for PowerBuilder® which is used by the MITIS™ application.	Inspected the Sybase Inc. support agreements, incident support packs, and related payment information to confirm the agreements are current.	No exceptions noted.
CCA has contracted with Sun Microsystems, Inc. through Great Northern Consulting to provide software support for the Solaris operating system which includes all patches and upgrades.	<p>Inspected the support agreement between the City of Cleveland and Great Northern Consulting Services.</p> <p>Inspected billing and payment documentation to evidence CCA purchased operating system software support for the audit period.</p>	No exceptions noted.

<b>Changes to Existing Applications or Hardware Systems - Control Objective:</b> <b>Testing of Program Changes or Hardware System Upgrades</b> - Program changes and hardware system upgrades should be tested to ensure that they achieve the business' requirements and do not negatively impact existing processing.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Testing of altered client executable code is performed by a test team which includes the application user, department supervisor, and the application specialist. Once testing has been completed, a "Checklist for Changes Made to the MITIS™ System" is signed by the test team leader, test team, and/or the assistant tax administrator.	Inspected the program change documentation folder and the "Checklist for Changes Made to the MITIS™ System" for evidence testing was completed for <u>executable code</u> program changes made during the audit period.	No exceptions noted.
Batch programs are tested for accuracy and documentation is maintained and tracked on the "Checklist of Documentation for MITIS™ Batch Programs and Scripts."	Inspected the program change documentation for evidence that testing was completed for batch program changes made during the audit period. Referenced the "Checklist of Documentation for MITIS™ Batch Programs and Scripts" for the changes where testing documentation was not available.	No exceptions noted.

<b>Changes to Existing Applications or Hardware Systems - Control Objective:</b> <b>Transfer into the Live Environment</b> - The transfer of programs or system upgrades into the live environment should be appropriately controlled.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Programmers are restricted from access to the production environment.	<p>Confirmed the application specialist does not have access to the production environment through independent inquiry with the application specialist, network/operations specialist, database specialist, and project leader/applications development.</p> <p>Inspected the following documentation to confirm the application specialist is restricted from the production environment:</p> <p><u>MITIS™ programs</u></p> <ul style="list-style-type: none"> <li>• Program change flow charts and procedures.</li> <li>• Production directory share information and file permissions.</li> <li>• Windows group membership listings to confirm the application specialist is not a member of any group with file permissions above read and execute.</li> </ul> <p><u>Batch programs</u></p> <ul style="list-style-type: none"> <li>• Program change flow charts and procedures.</li> <li>• Solaris (UNIX) password file – to confirm the application specialist does not have an account.</li> <li>• Solaris (UNIX) Group file – to confirm the application specialist is not a member of the system administration groups.</li> </ul>	No exceptions noted.
Client executable code updates are migrated throughout the network via an automated script.	<p>Inspected the automated script used to migrate version updates to each user's workstation.</p> <p>Compared the version of MITIS™ running in production to the version of MITIS™ running on a user workstation to confirm the user had the most recent version of MITIS™.</p>	No exceptions noted.

<p><b>Changes to Existing Applications or Hardware Systems - Control Objective:</b>  <b>Transfer into the Live Environment</b> - The transfer of programs or system upgrades into the live environment should be appropriately controlled.</p>		<p><b>Control Objective Has Been Met</b></p>
<p><b>Control Procedures:</b></p> <p>Transfer instructions are prepared by the application specialist to assist the network/operations specialist with implementing, into production, changes made to client <u>executable code</u>, batch programs, scripts and reports.</p>	<p><b>Test Descriptions:</b></p> <p>Confirmed with the network/operations specialist that transfer instructions are used to implement changes in production.</p> <p>Inspected the transfer instructions for changes made during the audit period.</p>	<p><b>Test Results:</b></p> <p>No exceptions noted.</p>

<p><b>Changes to Existing Applications or Hardware Systems - Control Objective:</b>  <b>Documentation and Training</b> - Technical documentation should be updated to reflect program changes and system upgrades. When changes to applications and system upgrades affect user procedures, documentation should be updated accordingly. Likewise, users and IT staff should receive appropriate training when their responsibilities are impacted by application changes or system upgrades.</p>		<p><b>Control Objective Has Been Met</b></p>
<p><b>Control Procedures:</b></p> <p>The application specialist uses a checklist to ensure technical documentation for changes to client executable code, batch programs and scripts is produced. The application specialist maintains a folder with the technical documentation for each change.</p> <p>Technical documentation includes a print out of the program and/or script highlighting the code differences between the current and prior versions, difference reports of the current and prior versions, and transfer instructions to the network/operations specialist. Documentation within the batch program includes programmer's initials, change date, and a brief description of the change in the header of the batch program.</p>	<p><b>Test Descriptions:</b></p> <p>Inspected the following to confirm technical documentation was created and maintained by the application specialist:</p> <ul style="list-style-type: none"> <li>• Program change documentation folders.</li> <li>• "Checklist of Documentation for MITIS™ Batch Programs and Scripts for batch program changes made during the audit period.</li> <li>• "Checklist for Changes made to the MITIS™ System" for the client executable code program changes made during the audit period.</li> </ul>	<p><b>Test Results:</b></p> <p>No exceptions noted.</p>

**IT Security**

<p><b>IT Security - Control Objective:</b>  <b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</p>		<p><b>Control Objective Has Been Met</b></p>
<p><b>Control Procedures:</b></p> <p>The city's e-mail and Internet use policy, which is included in the personnel policies and procedures manual, is distributed to all employees when they are hired. Employees sign a form acknowledging their acceptance of the policy.</p> <p>The computer usage policy is divided into five sections: purpose, use and misuse of internet or e-mail systems, limits of privacy, e-mail etiquette and best practices, and enforcement and consent.</p>	<p><b>Test Descriptions:</b></p> <p>Inspected the e-mail and Internet use policy.</p> <p>Inspected the policy acknowledgement forms for all CCA employees.</p>	<p><b>Test Results:</b></p> <p>No relevant exceptions noted.</p>
<p>MITIS™ security reports are generated and reviewed on a monthly basis by the application specialist to help ensure all accounts are active and changes in access are appropriate.</p> <p>The security report includes listings of active users, inactive users, active users with last access date greater than 30 days, active users who have not changed their passwords in 90 days, and changes in the user master file.</p>	<p>Inspected the monthly security reports reviewed by the application specialist throughout the audit period to confirm they included user account activity and evidence of review.</p> <p>Confirmed the security report review procedure through independent inquiry of the project leader/applications development and the application specialist.</p>	<p>No exceptions noted.</p>
<p>Access requests (new accounts, changes, and terminations) are sent to the project leader/applications development via e-mail to ensure access is authorized and only current employees have access. Requests must be submitted by supervisory level positions.</p>	<p>Inspected the access requests for 2008 to confirm requests were sent by a department supervisor or an administrator and were maintained for the audit period.</p> <p>Identified changes made during the audit period to users with read-write access to significant objects within the MITIS™ application and confirmed an access request was on file.</p>	<p>No exceptions noted.</p>

<b>IT Security - Control Objective:</b> <b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Notification of employee terminations are received by the Information Services Support staff from either a department head or an administrator. ISS staff then inactivate the user account within the MITIS™ application to ensure only current employees have access to the MITIS™ application.	Inspected the access requests for 2008 and identified any termination requests. Inspected the MITIS™ security report for December 2008 to confirm terminated employee accounts were inactive.	No exceptions noted.
<p>Network security events are logged and monitored by Information Systems Support (ISS) staff for unauthorized changes or access requests.</p> <p>Network level audit policies have been established to log the following events:</p> <ul style="list-style-type: none"> <li>• Logon events.</li> <li>• Object access.</li> <li>• Policy change.</li> <li>• Privilege use failures.</li> <li>• System events.</li> </ul>	Inspected the audit policies in the domain controller security settings under the local policies group. In addition, inspected the security log maintained in the event viewer and confirmed the logs are reviewed weekly by the network/operations specialist. Also confirmed the logs are not being cleared manually.	No exceptions noted.
The database specialist reviews the eFile entry log monthly for errors indicating malicious activity. The database specialist initiates a ticket with Rackspace to request they block IP addresses causing errors in the firewall located at Rackspace.	<p>Observed the database specialist review the eFile entry log on 02/04/09.</p> <p>Confirmed the monthly review of the eFile entry log with the database specialist, Inspected CCA's Rackspace tickets to confirm tickets requesting changes to the Rackspace firewall were placed throughout the audit period and included a response from Rackspace the ticket had been closed.</p>	Control operating as described.

<b>IT Security - Control Objective:</b> <b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
<b>Solaris (UNIX) Server:</b> System level access to the application server is restricted to a limited number of ISS personnel through the use of individual user IDs and passwords.	<p>Inspected the password files to confirm all accounts had unique user IDs and were password protected.</p> <p>Calculated the number of days since the date of the last password change to determine whether the passwords were changed during the audit period.</p>	<p>Passwords were not changed during the audit period. However, there were only six accounts on this system which are either system accounts, application accounts, or ISS staff accounts. Access to the UNIX server is further limited through network access and emulation software.</p> <p>No other relevant exceptions noted.</p>
<p><b>Solaris (UNIX) Server:</b> Trusted hosts and trusted accounts have not been established on the application server.</p> <p>Trust relationships simplify access by bypassing the password security check otherwise required on the server.</p>	<p>Inspected a listing of trust relationships to confirm trusts have not been established on the application server.</p> <p>On 02/04/09, observed online with the database specialist that trust files do not exist.</p>	No exceptions noted.
<b>Solaris (UNIX) Server:</b> Access to batch source and object programs is restricted to system level accounts on the application server.	Inspected the password, shadow password, and group files to confirm only ISS staff have accounts on the Solaris (UNIX) server.	No exceptions noted.
<p><b>Windows Active Directory:</b> Active Directory is used to control access to the network. Password parameters are enforced at the network level to aid in the authentication of users to the system. User accounts are locked out after a limited number of invalid logon attempts.</p>	<p>Inspected the password, account lockout, and Kerberos policies in the default domain security settings.</p> <p>Inspected the account policies at the user level to confirm system policies were not overridden.</p>	No exceptions noted.
<p><b>Windows Active Directory:</b> Access to connect to the MITIS™ application from outside CCA has been limited to member communities through the AS5300 universal access server.</p> <p>Member community accounts on the AS5300 are password protected.</p>	<p>Inspected the listing of users on the AS5300 to confirm access was limited to member communities or previous member communities who access historical data.</p> <p>Inspected the listing of users on the AS5300 to confirm the presence of encrypted passwords.</p>	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
A firewall is in place between CCA and the City of Cleveland networks. The firewall permits a limited number of individual outbound privileges and denies all incoming traffic.	Observed the existence of a firewall within the computer room. Inspected the CCA network diagram and firewall parameters with the network/operations specialist.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Application Level Access Controls</b> - Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
MITIS™ application level access controls include a password minimum length, password history, and password expiration interval.  Error messages are received by the user when they attempt to use a password not in agreement with the minimum length parameter or a password that has been used previously. The password expiration interval has been set in the MITIS™ application to require users to change their passwords on a periodic basis.	Inspected the MITIS™ parameter maintenance screen and observed error messages received when passwords do not meet coded MITIS™ password requirements.	No exceptions noted.
Access within the MITIS™ application is controlled by group membership. Each group is assigned access to specific transactions and functions.	Inspected the MITIS™ user audit report for evidence of segregation of access and limited access to system administration functions.	No exceptions noted.
Access to the database is limited to only a few accounts. None of the accounts are assigned to users and each account is password protected.	Inspected the database user listing to confirm the number of accounts is limited and all accounts are password protected.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Application Level Access Controls</b> - Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
<p>eFile users are authenticated through the use of a taxpayer ID number, password and entry of a human verification code.</p> <p>The taxpayer must register with CCA or have an existing taxpayer account before they can use the eFile application.</p> <p>Password length requirements have been incorporated into the eFile application.</p>	<p>Observed the resulting error messages and confirmed users were unable to proceed when attempting to login to eFile with:</p> <ul style="list-style-type: none"> <li>• A blank taxpayer ID and password and/or the incorrect entry of a human verification code.</li> <li>• A taxpayer ID that had not completed the sign-up process.</li> <li>• A taxpayer ID that had not registered with CCA.</li> </ul> <p>Inspected the password length requirement message to confirm a password minimum length requirement is enforced.</p>	No exceptions noted.
<p>Access to taxpayer data that resides in the database at Rackspace is restricted to CCA personnel through database accounts and passwords.</p>	<p>Inspected the eFile database user listing to confirm the number and authority of accounts is limited and all accounts are password protected.</p>	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Sensitive Facilities</b> - Use of sensitive facilities, such as, master passwords, powerful utilities, and system manager facilities, should be appropriately controlled.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
<b>Solaris (UNIX) Server:</b> Users are not permitted administrative (root) capabilities on the application server through their user account or group membership.	Inspected the group listing to confirm users are not included in the root group.  Inspected the password listing to confirm users do not share the same GID (group ID) as root which would give them root capabilities.	No exceptions noted.
<b>Solaris (UNIX) Server:</b> Users do not have the ability to update sensitive security files.	Inspected the password and group file protections and confirmed that WORLD write access is not provided to users.  Inspected the ownership and group membership of the password, shadow password and group files to confirm they are not accessible by a user account.	No exceptions noted.
<b>Windows Active Directory:</b> System administration accounts are restricted to the tax administrator and ISS personnel.	Inspected the administrator group to confirm only ISS and CCA administrators have access.	No exceptions noted.
<b>Windows Active Directory:</b> The CCA does not use trusts to all allow single sign-on authentication across domains.	Inspected the Active Directory Domains and Trusts listing to confirm no trust relationships have been defined.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Physical Security</b> - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Computer equipment is protected from physical and environmental hazards through the following devices: <ul style="list-style-type: none"> <li>• Key card access.</li> <li>• Heat/smoke detectors.</li> <li>• Building wide uninterrupted power supply and generator.</li> <li>• Air conditioner which controls temperature and humidity.</li> <li>• HFC fire suppression system.</li> </ul>	Inspected the computer room on 01/15/09 and observed the existence of the physical and environmental controls.	No exceptions noted.
Physical access to the CCA computer room is restricted to authorized personnel using a key card system.	Inspected a list of individuals with access to the CCA computer room. Confirmed with the project leader/applications development that access was limited to ISS staff and authorized individuals.	No exceptions noted.

**IT Operations**

<b>IT Operations - Control Objective:</b> <b>System Administration and Maintenance</b> - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Key performance measures, such as disk space capacity, performance times, and system usage are recorded in a system usage log which is reviewed by the database specialist on a daily basis.	Inspected 30 system usage logs from a population of 300 logs generated during the audit period to confirm review by the database specialist.	Four of the 30 system usage logs selected for testing showed no indication of review by the database specialist, or his backup, the applications specialist.  No other relevant exceptions noted.

<b>IT Operations - Control Objective: System Administration and Maintenance</b> - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
<p>A batch log table is updated daily to help ensure successful completion of each job. The table tracks job name, start date and time, finish date and time, batch date, and total run time.</p> <p>Scripts are used to extract information from the batch log tables. The extracted information is inserted into a Sybase database which updates a master Excel spreadsheet. The Excel spreadsheet is reviewed online for problem resolution.</p>	<p>Inspected the scripts run against the batch log tables.</p> <p>Independently discussed review procedures with the project leader/applications development and the network/operations specialist.</p>	No exceptions noted.
<p>System batch logs are created and monitored by ISS staff for the successful completion of daily and monthly batch jobs.</p>	<p>Confirmed the monthly review procedures with the project leader/applications development and the network/operations specialist. Inspected a listing of monthly batch jobs. Observed the online directory listing of batch job logs and selected one batch job log for inspection.</p>	No exceptions noted.
<p>Collection reports and transaction tapes are received electronically from Key Bank for the collection of taxes via lock box.</p> <p>The transaction data file is loaded into the MITIS™ application by ISS staff and a reconciliation process is performed on this data by CCA personnel.</p>	<p>Using the master Excel spreadsheet of batch jobs, selected 60 batch jobs from a total of 508 lockbox related batch jobs run throughout the audit period. Inspected the reconciliations for existence and re-performed the reconciliation.</p>	No exceptions noted.
<p>Service agreements with Sun Microsystems and Great Northern Consulting Services cover technical support and maintenance on the computer hardware.</p>	<p>Inspected the Sun Microsystems and Great Northern support agreements for services provided and periods of coverage. In addition, inspected the related payment documentation.</p>	No exceptions noted.

<b>IT Operations - Control Objective:</b> <b>Backup</b> – Up-to-date backups of programs and data should be available in emergencies.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Documented procedures are available for performing backups. Hourly, daily, and weekly backups are automated and ISS staff is notified if problems occur during the backup process.	Inspected the backup procedures and automated backup scripts used to generate backups and error alerts.	No exceptions noted.
Daily, weekly, and monthly backup tapes are rotated off-site on a consistent basis. The tapes are maintained off-site by a third party vendor.	<p>Inspected the offsite storage procedures.</p> <p>Confirmed the backup process through independent inquiry with the database specialist and the network/operations specialist.</p> <p>Inspected a file of back-up tape work-order (transfer) forms created during the audit period. Inspected the documents for the presence of authorization signatures from both CCA and vendor staff. Scanned to confirm the transfer forms indicated a consistent rotation, and to confirm corresponding vendor summary sheets were present. Observed the third party data retention vendor pick-up and return backup tapes on 02/04/09.</p> <p>Selected and confirmed one date of tape bar-codes between the work-order form and summary tape.</p>	No relevant exceptions noted.

**FINANCIAL APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS**

***Municipal Income Tax Information System (MITIS™)***

<p><b>Municipal Income Tax Information System - Control Objective:</b>  <b>Authorization:</b> - Recorded transactions represent actual taxes imposed at rates established by the entity's governing body and are approved. Receipts (remittances) represent valid payments by assessed taxpayers. Non-cash adjustments are valid and approved.</p>		<p><b>Control Objective Has Been Met</b></p>
<p><b>Control Procedures:</b></p> <p>Tax rates, tax credit rates, and penalty and interest rates in the MITIS™ system and on the 2008 tax form are supported by ordinances from the member communities.</p>	<p><b>Test Descriptions:</b></p> <p>Inspected the ordinances for all 47 member communities of CCA. Compared the tax rates, tax credit rates, and penalty and interest rates on the ordinances to the CCA 2008 tax form and the rates in the MITIS™ application.</p>	<p><b>Test Results:</b></p> <p>The rates in the MITIS™ system did not reflect the current ordinances for three communities. The communities and the rates that were in error are as follows:</p> <ul style="list-style-type: none"> <li>• Village of Oakwood – withholding penalty rate.</li> <li>• Russells Point – penalty rate, interest rate, and withholding penalty rate.</li> <li>• Seville – penalty rate, interest rate, minimum penalty, and withholding interest rate.</li> </ul> <p>CCA corrected the rates in the MITIS™ application during fieldwork. They are in the process of reviewing taxpayer returns which may have been affected by the errors. It is the intent of CCA to either collect from or reimburse the taxpayers affected by the errors.</p> <p>No other exceptions noted</p>
<p>The authority to update the penalty and interest liability amounts based on manual recalculations or corrections is limited to tax administrators, administrative managers, supervisors and their backups.</p>	<p>Inquired with the applications specialist to identify the security objects with the authority to update or delete penalty and interest amounts.</p> <p>Inspected the MITIS™ security access information to identify users with update</p>	<p>No exceptions noted.</p>

<p><b>Municipal Income Tax Information System - Control Objective:</b>  <b>Authorization:</b> - Recorded transactions represent actual taxes imposed at rates established by the entity's governing body and are approved. Receipts (remittances) represent valid payments by assessed taxpayers. Non-cash adjustments are valid and approved.</p>		<p><b>Control Objective Has Been Met</b></p>
<p><b>Control Procedures:</b></p>	<p><b>Test Descriptions:</b></p> <p>access to the identified security objects.</p> <p>Confirmed access was appropriate with the chief of accounts and collections.</p> <p>Observed that staff without access to the identified security objects could not alter the penalty and interest liability amounts due.</p>	<p><b>Test Results:</b></p>

<p><b>Municipal Income Tax Information System - Control Objective:</b>  <b>Completeness of Input:</b> - Authorized tax filings and cash receipts are input and accepted for processing.</p>		<p><b>Control Objective Has Been Met</b></p>
<p><b>Control Procedures:</b></p> <p>Collection reports and transaction tapes are received electronically from Key Bank for the collection of taxes via lock box.</p> <p>The transaction data file is loaded into the MITIS™ application by ISS staff and a reconciliation process is performed on this data by CCA personnel.</p> <p>Mail is sorted into returns and payments and is entered into the system in batches. Batch numbers are automatically assigned by MITIS™ for document tracking purposes.</p> <p>MITIS™ balances the total of all checks distributed (payments entered) to the total tax due from the income tax returns. Processing cannot continue until the payments and forms are in balance.</p>	<p><b>Test Descriptions:</b></p> <p>Using the master Excel spreadsheet of batch jobs, selected 60 batch jobs from a total of 508 lockbox related batch jobs run throughout the audit period. Inspected the reconciliations for existence and re-performed the reconciliations.</p> <p>Inspected 60 batches to confirm MITIS™ automatically assigned a batch number.</p> <p>Inspected the program logic for the selected edit checks and observed the resulting error message when an amount is entered (distributed) that is not equal to the amount owed.</p>	<p><b>Test Results:</b></p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Accuracy of Input:</b> - Tax remittances are accurately recorded as to amounts, dates, taxpayer and type of tax.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
In the audit process, MITIS™ performs edit checks for valid city code, taxpayer city of residence, and employer ID number.	Inspected the program logic for the existence of the selected edits and observed code online.  Confirmed the functioning of the edits by observing the resulting error messages from the entry of erroneous data for city code, taxpayer city of residence, and employer ID number.	No exceptions noted.
The MITIS™ system performs edit checks to confirm the amount entered matches the amount collected for residence tax, employment tax, and tax owed.	Inspected program logic for selected edits and observed code online.  Confirmed the functioning of the edits by observing the resulting error message from an attempt to apply amounts not equal to the actual check amount.	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Cutoff of Transactions</b> – What assures that tax cash receipts are recorded in the proper period?		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Tax forms are reviewed before month end procedures are completed to ensure the accuracy of the tax liabilities for the filed returns. The MITIS™ system prevents further processing of returns until they have been marked as “pre-audited.”	Inspected program logic for the selected edit and observed code online.  Confirmed the functioning of the edit by observing the resulting errors from an attempt to continue processing (finalize) tax return batches before all individual returns were marked within the computer system as “pre-audited.”	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Cutoff of Transactions</b> – What assures that tax cash receipts are recorded in the proper period?		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
A monthly reconciliation of receipts, refunds, and adjustments is performed prior to distribution of revenues to the member communities.	<p>Inspected the log used to record review of the monthly reports to confirm the reports were reviewed regularly.</p> <p>Confirmed the reconciliation process was performed, prior to distribution, with the controller and assistant income tax financial supervisor.</p> <p>From a population of 660 distribution transactions, selected 60 distributions to member communities and performed the following:</p> <ul style="list-style-type: none"> <li>Traced “gross” collection amounts from the Report of Distribution Payments to Communities to the Monthly Distribution Reports.</li> <li>Traced the total distribution amount for the first 11 months of the year to corresponding bank statements.</li> </ul>	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Transaction Occurrence:</b> - What assures that the cash receipts recorded occurred and are not fictitious?		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
<p>Collection reports and transaction tapes are received electronically from Key Bank for the collection of taxes via lock box.</p> <p>The transaction data file is loaded into the MITIS™ application by ISS staff and a reconciliation process is performed on this data by CCA personnel.</p>	Using the master Excel spreadsheet of batch jobs, selected 60 batch jobs from a total of 508 lockbox related batch jobs run throughout the audit period. Inspected the reconciliations for existence and re-performed the reconciliation for evidence of reconciliation.	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Transaction Occurrence:</b> - What assures that the cash receipts recorded occurred and are not fictitious?		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
<p>Mail is sorted into returns and payments and is entered into the system in batches. Batch numbers are automatically assigned by MITIS™ for document tracking purposes.</p> <p>MITIS™ balances the total of all checks distributed (payments entered) to the total tax due from the income tax returns. Processing cannot continue until the payments and forms are in balance.</p>	<p>Inspected 60 batches to confirm MITIS™ automatically assigned a batch number.</p> <p>Inspected the program logic for the selected edits and observed the resulting error message when an amount is entered (distributed) that is not equal to the amount owed.</p>	<p>No exceptions noted.</p>

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Integrity of Standing Data - Changes to standing data are authorized and accurately input.</b>		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Tax rates, tax credit rates, and penalty and interest in the MITIS™ system and on the 2008 tax form are supported by ordinances from the member communities.	Inspected the ordinances for all 47 member communities of CCA. Compared the tax rates, tax credit rates, and penalty and interest rates on the ordinances to the CCA 2008 tax form and the tax rates in the MITIS™ application.	<p>The rates in the MITIS™ system did not reflect the current ordinances for three communities. The communities and the rates that were in error are as follows:</p> <ul style="list-style-type: none"> <li>• Village of Oakwood – withholding penalty rate.</li> <li>• Russells Point – penalty rate, interest rate, and withholding penalty rate.</li> <li>• Seville – penalty rate, interest rate, minimum penalty, and withholding interest rate.</li> </ul> <p>CCA corrected the rates in the MITIS™ application during fieldwork. They are in the process of reviewing taxpayer returns which may have been affected by the errors. It is the intent of CCA to either collect from or reimburse the taxpayers affected by the errors.</p> <p>No other relevant exceptions noted.</p>
Taxpayer information is accurately entered by authorized collections, audit, and administrative staff.	Selected 60 tax filing batches created during the audit period. From each batch, selected one form and confirmed the data contained in the MITIS™ system matched the source document.	No exceptions noted.
Overhead rates charged to member communities are accurately calculated and applied within the MITIS™ system.	Selected 60 of 582 distributions to member communities and recalculated the overhead amounts for comparison to the actual overhead allocations entered in the MITIS™ system.	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Integrity of Standing Data</b> - Changes to standing data are authorized and accurately input.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
CCA confirms tax rates and tax credit rates with their member communities on an annual basis to determine whether there has been any change in legislation which would affect the rates in the MITIS™ application for their member communities.	Inspected the “City Tax Rates Confirmation Tracking” spreadsheet for evidence of a yearly confirmation of both the tax rate and tax credit rate.	The confirmation process does not confirm the actual rates currently in use by the MITIS™ application.  No other relevant exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Completeness and Accuracy of Updating</b> - Taxpayer remittances are accurately updated to the taxpayer and cash receipts databases.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Tax forms are reviewed before month end procedures are completed to ensure the accuracy of the tax liabilities for the filed returns. The MITIS™ system prevents further processing of returns until they have been marked as “pre-audited.”	Inspected program logic for the selected edit and observed code online.  Confirmed with the chief of accounts and collections that all returns are reviewed prior to month end procedures.  Confirmed the functioning of the edit by observing the resulting errors from an attempt to continue processing (finalize) tax return batches before all individual returns had been marked within the computer system as “pre-audited.”	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Completeness and Accuracy of Updating</b> - Taxpayer remittances are accurately updated to the taxpayer and cash receipts databases.		<b>Control Objective Has Been Met</b>
<b>Control Procedures:</b>	<b>Test Descriptions:</b>	<b>Test Results:</b>
Two staff members review tax forms for which a refund is owed. MITIS™ recalculates the refund amount and will not allow further processing until the "pre-audit" process is complete.	<p>Inspected program logic for the selected edit and observed code online.</p> <p>Confirmed with the supervisor of corporate audit that all refund requests are reviewed by two staff members.</p> <p>Confirmed the functioning of the edit by observing the resulting error after an attempt to continue processing (finalize) a refund batch while the batch status was marked within the computer system as "pre-auditing."</p>	No exceptions noted.
Penalty and interest is automatically calculated by the MITIS™ system. The process is performed in one of two ways, through a batch job or via the online MITIS™ application.	<p>Obtained and inspected the MITIS™ programs responsible for the penalty and interest calculations.</p> <p>Reviewed the program code for the penalty and interest calculations, within the online MITIS™ application, with the project leader/applications development, applications specialist, and chief of accounts and collections.</p> <p>Selected a population of 25 Assessment Registers from the 2008 Monthly Billing Reports. Re-performed the calculation of the penalty and interest amounts on the 25 assessment records selected for testing.</p>	No exceptions noted.
The penalty and interest batch job is included in the monthly closing procedures. The ISS department of the CCA has instructions and a worksheet to steer and define their month end procedures.	<p>Inspected the ISS Worksheet of Monthly Processes and Monthly Procedures for the inclusion of the penalty and interest job.</p> <p>Inspected the batch job log to confirm the monthly penalty and interest batch was run monthly throughout the audit period.</p>	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Completeness and Accuracy of Accumulated Data</b> – The integrity of individual taxpayer accounts in the taxpayer database and the tax revenue and cash accounts in the accounting system, after tax collection transactions have been accumulated in them, is preserved.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
A monthly reconciliation of receipts, refunds, and adjustments is performed prior to distribution of revenues to the member communities.	<p>Inspected the log used to record review of the monthly reports to confirm the reports are reviewed regularly.</p> <p>Confirmed the reconciliation process is performed, prior to distribution, with the controller and assistant income tax financial supervisor.</p> <p>From a population of 660 distribution transactions, selected 60 distributions to member communities and performed the following:</p> <ul style="list-style-type: none"> <li>Traced “gross” collection amounts from the Report of Distribution Payments to Communities to the Monthly Distribution Reports.</li> <li>Traced the total distribution amount for the first 11 months of the year to corresponding bank statements.</li> </ul>	No exceptions noted.
The Voucher Generation Report (VGR), FAMIS Interface Report, and Check Register are reconciled by the audit staff for each run date to ensure all refund amounts are distributed appropriately.	<p>Inspected the Voucher Generation Report, FAMIS Interface Report, and the Check Register for 12 of the 48 run dates within the audit period.</p> <p>Traced the total refund amount from the initial VGR generated from MITIS™ to the adjusted MITIS™ FAMIS Interface Report to the auditor’s adjustment spreadsheet. Then reconciled the AP Trial Register to the Check Register generated from the city’s PeopleSoft financial application.</p>	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Restricted Access to Assets and Records - Only authorized personnel have access to the MITIS™ data.</b>		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
There is a proper segregation of duties for mail-in tax payments (cash batches), between the receipt and entry of tax payments and the entry of tax assessment data from the tax form.	Confirmed departmental procedures through independent inquiry of a tax auditor in the collections department and the chief of accounts and collections.  Selected 60 dates during the audit period and obtained the batch status reports (GNRDTD02). Traced one batch from each report to confirm the batch processing cover sheets indicate the separation of duties between the processing of returns and submitted payments.	No exceptions noted.
Only CCA management and ISS staff have access to update tax rates, tax credit rates, and penalty and interest rates in the MITIS™ application.	Identified the security objects with the ability to update tax rates.  Inspected the MITIS™ security report to identify users with update access to the identified security objects.  Confirmed access was appropriate with the controller.	No exceptions noted.
Only authorized users have access to update taxpayer standing data, such as identification number, name, address, and employer information.	Identified the security objects with the ability to update taxpayer standing data.  Inspected the MITIS™ security report to identify users with update access to the identified security objects.  Confirmed access was appropriate with the controller	No exceptions noted.

<b>Municipal Income Tax Information System - Control Objective:</b> <b>Restricted Access to Assets and Records - Only authorized personnel have access to the MITIS™ data.</b>		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The ability to alter application security, password parameters, or change application passwords is limited to members of management and the technical staff.	Identified the security objects with the ability to alter application level security, password parameters or change application passwords.  Inspected the MITIS™ security access information to identify users with update access to the identified security objects.  Confirmed access was appropriate with the administrative manager.	No exceptions noted.
Access to mark tax forms as “pre-audited” and the access to mark new and revised batches as “finalized” is limited to authorized supervisors and staff of CCA.	Identified the security objects with the ability to mark tax forms as “pre-audited” and the access to mark new and revised batches as “finalized”.  Inspected the MITIS™ security access information to identify users with update access to the identified security objects.  Confirmed access was appropriate with the administrative manager and chief of accounts and collections.	No exceptions noted.
Access to the following supervisor cashiering functions is limited to members of management and supervisory staff: <ul style="list-style-type: none"> <li>• Alter cash batch totals.</li> <li>• Alter cash amounts.</li> <li>• Alter processing dates.</li> <li>• Alter daily batch totals.</li> </ul>	Identified the security objects with the ability to alter cash batch totals, cash amounts, processing dates and daily batch totals.  Inspected the MITIS™ security access information to identify users with update access to the identified security objects.  Confirmed access was appropriate with the administrative manager and chief of accounts and collections.	No exceptions noted.

## SECTION IV - OTHER INFORMATION PROVIDED BY THE ORGANIZATION

### Information related to Rackspace and the CCA eFile Application:

Taxpayers can file their CCA Municipal Income Tax forms electronically using eFile. The eFile application was written in-house with the assistance of the Modis consultants. CCA has contracted with Rackspace to host their eFile application. The application server located at Rackspace is three tiered including Web server function, application server function, and database function. The database includes taxpayer information which is refreshed daily from the MITIS™ database housed at CCA.

An executable is initiated by the ISS staff to automatically pull the data from the eFile database. The following files are downloaded each day: taxpayer file, taxpayer address file, taxpayer relationship file, note file, document file, W-2 file and 1099 file. An additional file for payment data is also downloaded by the executable file. A second executable is used to refresh the files from the MITIS™ application to the eFile application daily. Both of these executables are subject to the change procedures established for batch programs. A script is run daily which reconciles the payment file with the document file and creates a reconciliation report for the controller to reconcile with the KeyPay reports. Finally, another script is run to process (post to MITIS™) those payments that have been batched and reconciled and generate reports for the chief of accounts and collections, supervisor of collections, supervisor of data entry, and head cashier. They are notified via e-mail that these reports have been generated and their location.

Only the executable programs reside on the application server, source code does not. Taxpayer data that resides in the database at Rackspace is secured through database security. All data transfers between the CCA and Rackspace are encrypted.

Taxpayers are required to register or create an account which must have a match in CCA's MITIS™ database table of active taxpayers. The taxpayer's account is verified with the taxpayer information tables in the eFile database that resides at Rackspace. If the taxpayer is a new CCA user and needs an account, they may register through the eFile application; in which case the user is added to the eFile tables and later on to the MITIS™ tables

In order to sign-in, taxpayers must agree to CCA's web filing agreement and they must meet the following qualifications:

- The taxpayer must be a registered CCA taxpayer. This means the taxpayer filed a tax return with CCA in the last 5 years or registered with CCA within the last year (either by mail or through the Internet).
- The taxpayer did not change their name, address or filing status from January 1 through December 31 of the tax year for which they are filing.
- The taxpayer is filing for the current tax year.

Users of the eFile application are authenticated through the use of a taxpayer ID number, password, and entry of a human verification code. In addition, password length requirements have been incorporated into the eFile application.

An eFile entry log is used to record all HTTP (hypertext transfer protocol) activity on the eFile application server. The following information is included in the log:

- Server variables or server system configuration parameters.
- HTTP start-up configuration.

- 
- All HTTP activity including “Get” requests, “Post” requests” and errors. Errors are recorded when:
    - “Page not found” errors occur.
    - Trusted information does not come from other CCA pages. CCA controls the flow through the eFile application and when information deviates from the flow, an error is logged.
    - Programming errors occur.

The log is reviewed monthly by the database specialist. The consultant scans the log for errors indicating malicious activity. Errors are investigated and when necessary the database specialist creates a ticket, which is sent to Rackspace, to block the site to prevent future attacks.

HARDWARE DATA

## Central Processors and Peripheral Equipment

<u>Manufacture / Model Number</u>	<u>Random Access Memory</u>	<u>Disk Storage</u>	
Sun Microsystems / V480R	16 GB	146 GB	
Sun Microsystems / V280R	2 GB	146 GB	
Sun Microsystems / StorEdge 3510	N/A	436 GB	
Sun Microsystems / Sun Ultra 5	128 MB	9 GB	
Sun Microsystem / Tape Drive 6250	N/A	N/A	
Dell PowerEdge 2600	2048 MB	68 GB	(Disk 1)
		204 GB	(Disk 2)
Dell PowerEdge 2800	2048 MB	22 GB	(Disk 1)
		546 GB	(Disk 2)
Dell PowerEdge 2900	4096MB	67 GB	

MISCELLANEOUS EQUIPMENT

<u>Equipment Type / Manufacturer and Model</u>	<u>Units in total</u>
Universal Gateway / Cisco / AS 5300/3560	1
Network Printer / Data Products LM 1600 Line Printer	1
Network Printer / HP Laserjet IV Laser Printer	13
Network Printer / HP Laserjet V Laser Printer	2
Network Printer / HP Laserjet 4000N Laser Printer	3
Network Printer / HP Laserjet III	1
Network Printer / HP 930 Color Printer	3
Workstations / Dell Optiplex	132
Workstations / NEC Powermate	5
Workstations / Dell Dimension	4
External Modem / US Robotics 14.4 KBPS	1
HP 960 Color Printer	1
HP 940 Color Printer	1
HP Scanjet 7490	1
Switch / 3COM 16 Port	1
Switch / IOGear KVM 8 Port	1
Switch / IOGear KVM 4 Port	1
HP Laserjet 6122	6
Kyocera Mita Printer	6
HP 1600 Printer	6
Tape Library / Sony D81	1
Tape Library / Dell ML6000	1
SAN / Dell AX150	1

SOFTWARE

<u>Type</u>	<u>Name/Manufacturer</u>	<u>Version Number</u>
Operating System (Domain Controller)	Windows 2003 Server / Microsoft	2003 SP 2
Operating System	Windows 2003 R2 Server / Microsoft	2003 SP 2
Operating System	Windows 2000 Server / Microsoft	2000 SP 4
Operating System (Workstation)	Windows NT Client / Microsoft	4.0 SP 6
Operating System (Workstation)	Windows XP	SP2 or SP3
Operating System	Solaris (UNIX) / Sun Microsystems	9.0
Database	ASE / Sybase Inc.	12.0.0.8/P/ EBF 12162 ESD3
Database	SQL Server	SQL Server 2005
Application Development	PowerBuilder® / Sybase Inc.	8.0.4 Build 10501
Application Software	MITIS™ / Modis, Inc.	8.0.4
Production Software	PowerBuilder® / Sybase Inc.	8.0.4 Build 10501
Backup Software	ARCserve / BrightStor	11.x or 12.x
Backup Software	SQL Backtrack / BMC Software	5.0.21
Image Retrieval	OnBase	6.x
AntiVirus	eTrust Threat Management	8.x
AntiVirus	eTrust AntiVirus	7.x

**MEMBER TAXING AUTHORITIES**

<b><u>MEMBER COMMUNITY</u></b>	<b><u>COUNTY</u></b>	<b><u>MEMBER COMMUNITY</u></b>	<b><u>COUNTY</u></b>
Village of Cairo	Allen	City of Painesville	Lake
Village of Elida	Allen	City of Willoughby Hills	Lake
Village of Andover	Ashtabula	Village of Grand River	Lake
Village of Geneva-on-the-Lake	Ashtabula	Village of Madison	Lake
Village of Orwell	Ashtabula	Village of North Perry	Lake
Village of Cridersville	Auglaize	Village of Perry	Lake
Village of Waynesfield	Auglaize	Village of Timberlake	Lake
City of Cleveland	Cuyahoga	Village of Russells Point	Logan
City of Rocky River	Cuyahoga	City of Medina	Medina
City of Warrensville Heights	Cuyahoga	City of Wadsworth	Medina
Village of Bratenahl	Cuyahoga	Village of Seville	Medina
Village of Gates Mills	Cuyahoga	Village of Antwerp	Paulding
Village of Highland Hills	Cuyahoga	Village of Oakwood	Paulding
Village of Linndale	Cuyahoga	Village of Paulding	Paulding
Village of North Randall	Cuyahoga	City of Barberton	Summit
Village of Metamora	Fulton	City of Munroe Falls	Summit
Village of Burton	Geauga	City of Norton	Summit
Village of Chardon	Geauga	Village of Northfield	Summit
Village of Middlefield	Geauga	Village of Peninsula	Summit
Village of South Russell	Geauga	Village of Creston	Wayne
Village of Ada	Hardin	Village of Bradner	Wood
Village of Alger	Hardin	Village of Grand Rapids	Wood
Village of Liberty Center	Henry	Village of North Baltimore	Wood
City of Mentor-on-the-Lake	Lake		





**Mary Taylor, CPA**  
Auditor of State

**CITY OF CLEVELAND-CENTRAL COLLECTION AGENCY**  
**CUYAHOGA COUNTY**

**CLERK'S CERTIFICATION**

This is a true and correct copy of the report which is required to be filed in the Office of the Auditor of State pursuant to Section 117.26, Revised Code, and which is filed in Columbus, Ohio.

*Susan Babbitt*

**CLERK OF THE BUREAU**

**CERTIFIED**  
**JUNE 23, 2009**