REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS FOR THE COMMONWEALTH OFFICE OF TECHNOLOGY

For the Period July 1, 2008 through June 30, 2009

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS
www.auditor.ky.gov

209 ST. CLAIR STREET
FRANKFORT, KY 40601-1817
TELEPHONE (502) 564-5841
FACSIMILE (502) 564-2912

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Jonathan Miller, Secretary
Finance and Administration Cabinet
Phil Baughn, Commissioner
Commonwealth Office of Technology

The enclosed report prepared by Potter & Company, LLP presents the report on controls placed in operation and tests of operating effectiveness for the Commonwealth Office of Technology for the period July 1, 2008 through June 30, 2009.

We engaged Potter & Company, LLP to perform the SAS 70 audit of the Commonwealth Office of Technology. We worked closely with the firm and the Commonwealth Office of Technology during the audit and reporting process.

Respectfully submitted,

Crit Luallen
Auditor of Public Accounts

209 ST. CLAIR STREET
FRANKFORT, KY 40601-1817

TELEPHONE 502.564.5841
FACSIMILE 502.564.2912
WWW.AUDITOR.KY.GOV

THE COMMONWEALTH OFFICE OF TECHNOLOGY

SAS 70 Type 2 Report on Controls Placed in Operation
And Tests of Operating Effectiveness

July 1, 2008 to June 30, 2009

July 15, 2009

THE COMMONWEALTH OFFICE OF TECHNOLOGY

Report of Controls Placed in Operation
and Tests of Operating Effectiveness

Table of Contents

SECTION I

Independent Service Auditors' Report Provided
by Potter & Company LLP

POTTER
POTTER & COMPANY LLP
CERTIFIED PUBLIC ACCOUNTANTS ▪ CONSULTANTS

301 East Main Street, Suite 1100 ▪ Lexington, KY 40507 ▪ 859.253.1100 ▪ 859.253.1384 fax ▪ **www.mspotter.com**
Offices in Lexington and Louisville

Independent Service Auditors' Report

The Board of Directors
The Commonwealth Office of Technology
Frankfort, Kentucky

We have examined the accompanying description of the information technology general controls of The Commonwealth Office of Technology (COT). Our examination included procedures to obtain reasonable assurance about whether: (1) the accompanying description presents fairly, in all material respects, the aspects of COT's controls that may be relevant to a user organization'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 if the user organizations applied the controls contemplated in the design of COT's controls and (3) such controls had been placed in operation as of June 30, 2009. The control objectives were specified by the management of COT. 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.

The COT states that it has implemented controls to logically secure Mainframe, UNIX, and Windows servers as well as databases supported by COT. In addition, the COT states that it has implemented controls to ensure system changes are authorized, approved and appropriately tested. Our test of operating effectiveness noted that the configuration of the mainframe, Windows, UNIX, and database security settings were not in accordance with COT standards or were not adequately secure to restrict unauthorized users access to COT systems and data. In addition, user account management procedures were not sufficient to provide reasonable assurance that terminated employees had access removed and that access for current employees was based on the "rule of least privilege". Additionally, change control processes could be bypassed by developers with direct access to the production environment and changes were not being consistently approved by management prior to implementation. This resulted in the non-achievement of the following control objectives:

- "Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data."
- "Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data."
- "Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production."

In our opinion, except for the matters described in the preceding paragraph, the controls tested as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the controls objectives specified in Section III were achieved during the period from July 1, 2008 to June 30, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of COT'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 to obtain evidence about their effectiveness in meeting the control objectives during the period from July 1, 2008 to June 30, 2009. The specific controls, related control objectives, and the nature, timing, extent and results of the tests are listed in Section III.

This information has been provided to user organizations of COT and to their auditors to be taken into consideration, along with information about the internal controls at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness, except as identified above, to provide reasonable, but not absolute assurance that the control objectives specified in Section III were achieved during the period July 1, 2008 to June 30, 2009.

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

The description of controls at COT is as of June 30, 2009 and information about tests of the operating effectiveness of specified controls covers the period from July 1, 2008 to June 30, 2009. 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 specified controls at COT is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of conclusions, based on our findings, to future periods is subject to the risk that (1) changes 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.

The information in Section IV of this report is presented by COT to provide additional information to user organizations and is not part of the COT's description of controls placed in operation. The information in Section IV has not been subjected to the procedures applied in the examination of the description of the controls related to the information technology general controls and accordingly express no opinion on it.

This report is intended solely for the use by the management of COT, its customers and the independent auditors of its customers.

Potter + Company, LLP

July 15, 2009

SECTION II

Description of Relevant Controls Provided
by the Commonwealth Office of Technology

Overview of Operations

The Commonwealth Office of Technology (COT) is an office in the executive branch of state government within the Finance and Administration Cabinet. COT's mission is to provide leadership in the use of information technology to enhance government services, improve decision making, promote efficiency and eliminate waste in government. According to the Kentucky Revised statutes, COT has the sole responsibility for IT operations in the Executive Branch. COT provides the leadership, policy direction and technical support to all executive branch agencies of state government in the application of information technology (IT) and the delivery of information services. This broad statement of responsibility encompasses major information resource functions such as: data center operations and hosting, data and voice communications, application development, data administration, desktop support, networking, project management, security, printing and related end-user and customer support services.

COT must ensure that these operations are conducted in the most efficient and effective way. The goal is to transform the Commonwealth's use of information technology to improve the efficiency of state government and delivery of services.

COT carries out the functions necessary for the efficient, effective and economical administration of information technology and resources within the executive branch. These duties include:

- Overseeing shared IT infrastructure resources and services;
- Performing strategic and tactical planning for information technology;
- Assessing, recommending and implementing IT governance and organization design;
- Identifying IT applications that should be statewide in scope and ensuring that these applications are not developed independently or duplicated by individual agencies of the executive branch;
- Establishing partnerships and alliances for effective implementation of statewide IT projects;
- Establishing IT policy and standards.

Description of Computerized Information System Environment

The information system processing environment within COT involves an array of hardware, operating systems and application systems. State and agency data and communications are transacted and stored on a proprietary local area network utilizing servers with Mainframe, Windows and UNIX operating systems. COT employees utilize Windows XP workstations.

COT has constructed a well secured wide area network with dedicated firewalls throughout the network. Firewall rules are well constructed to restrict access for each individual only to those areas based upon business need. Firewall access logs and Intrusion Protection System (IPS) logs are detailed and archived for historical purposes. In addition, configuration settings for the firewall and IPS are backed up as part of the regularly scheduled backups.

Remote access is available to select employees with management approval. All remote access users are required to authenticate prior to be granted access to COT's IT resources. Detailed log reports are archived for historic purposes. All activities are encrypted to secure confidential information.

Relevant Aspects of Internal Control Environment

Control Environment

The COT control environment reflects the overall attitude, awareness and actions of management, driven primarily by the members of COT senior management concerning the importance and emphasis given to controls in COT's policies, procedures, methods and organizational structure. The following is a description of COT's control environment elements:

Organizational Structure

Effective June 16, 2008, an Executive Order was signed by Governor Beshear reorganizing the Finance and Administration Cabinet. The majority of changes within COT consist of name changes for existing divisions and the movement of functions to different divisions better suited to perform that function. The complete text of the Executive Order 2008-056 is available at:
http://apps.sos.ky.gov/Executive/Journal/EJimages/2008-MISC-2008-0506-195888.pdf.
An updated COT organization chart is available at
http://gotsource.ky.gov/docushare/dsweb/Get/Document-178493.

Commissioner's Office
COT is headed by a Commissioner, appointed by the Secretary of the Finance and Administration Cabinet. The Commissioner also serves as the state's Commonwealth Chief Information Officer (CIO)**.** The Deputy Secretary of the Finance and Administration Cabinet currently serves as Acting Commissioner. Two Deputy Commissioners assist the Commissioner in managing COT. The Deputies oversee the business aspects of COT and focuses on some of the major challenges such as Infrastructure Consolidation, upgrade of the Kentucky Emergency Warning System (KEWS), and the wireless interoperability program.

The position of *Chief Information Security Officer (CISO)* was created in December of 2006 and reports directly to the Commissioner. The CISO's mission is to provide leadership with respect to the security of information technology within the Commonwealth and assist state government in establishing IT security best practices, standards and policies. Effective under the Executive Order, the *Office of Chief Information Security Officer (CISO)* was created within the Commissioner's office and overseen by the CISO. The Security Administration Branch was moved to this office in the reorganization.

The *Kentucky Wireless Interoperability Executive Committee* was established in 2004. The Kentucky Wireless Interoperability Executive Committee was created to address communications interoperability. The committee advises and makes recommendations regarding strategic wireless initiatives to achieve public safety voice and data communications interoperability.

The *Kentucky Geographic Information Advisory Council* advises the Commissioner of Technology on issues relating to geographic information. It establishes policies and procedures to assist state and local jurisdictions in leveraging geographic information and technology for improving public administration.

COT has approximately 460 employees and over 100 contractors to assist in its mission of supporting government services. COT is organized with three subordinate offices:

- *Office of Infrastructure Services*
- *Office of Enterprise Technology and*
- *Office of Application Development*

The *Office of Infrastructure Services* is responsible for day-to-day technical support and operation of executive branch IT resources. This includes overseeing shared IT infrastructure resources and services, including large-scale computing, server hosting, IT security, data and voice communication networks, and phone systems. The Office of Infrastructure Services consists of five (5) divisions:

- The **Division of Communications** maintains network and telecommunications services.
- The **Division of IT Operations** coordinates change management, service Desk support, and day-to-day operations of existing infrastructure services.
- The **Division of Field Services** manages enterprise-wide customer support.
- The **Division of Technical Services** is responsible for system software, operating system support, and data management.
- The **Division of Printing Services** manages copy and print services for the Commonwealth.

Additionally, this Office has the responsibility for maintaining the state's Kentucky Emergency Warning System (KEWS), which is a completely redundant microwave network with over 150 towers that span the Commonwealth.

The *Office of Enterprise Technology* is responsible for coordinating enterprise IT governance activities, oversight of large IT projects and long-term IT capital planning within the Executive Branch. The office is also responsible for the coordination of all Geographic Information Systems (GIS) activities within state government. The *Office of Enterprise Technology* consists of two divisions:

- The **Division of IT Governance** supports Enterprise IT Policies, Architecture and Standards, and IT capital planning activities.
- The **Division of Geographic Information** collects, compiles, and facilitates the production of geospatial data for the Commonwealth.

The *Office of Application Development* is responsible for IT project management, consulting, and IT development for Executive branch applications. COT provides comprehensive systems analysis, design, and development services, and applications consulting services. These services are provided within the structure of COT's Product Development Process (PDP) which is based on the Project Management Institute's "Project Management Body of Knowledge" (PMBOK),

and follows industry standard Project Management Lifecycle and System Development Lifecycle methods. The Office of Application Development consists of three (3) divisions:

- The **Division of Software Engineering** is responsible for the Commonwealth's IT application development.
- The **Division of Consulting & Project Management** is responsible for gathering of requirements, business and technical analysis, prioritization, co-ordination and management of system application projects.
- The **Division of Support Services** is responsible for quality control and assurance and quality testing.

IT Consolidation

On June 16, 2005 Governor Fletcher signed Executive Order #2005-562 to streamline the information technology (IT) resources of the Commonwealth's Executive Branch. The order directed the Secretary of the Finance and Administration Cabinet to review each Executive Branch agency's IT infrastructure and to consolidate operational control under the Commonwealth Office of Technology (COT) when it was found to be in the best interest of the Commonwealth. Combining IT resources across the Commonwealth provides economies of scale in purchasing and greater negotiating advantages.

As part of the Executive Order, the Customer Service Branch was created within the Office of Infrastructure Services (OIS). The primary goal of this branch is to serve as a ***single point of contact*** (Enterprise Service Desk) to request all types of products and/or services from COT. The purpose of the single point of contact process is to ensure that all requests are properly recorded and to ensure that there are no lost or misplaced requests.

In addition to the Enterprise Service Desk, Kentucky's IT consolidation project included the reengineering of all IT support processes to conform to ITIL best practices. It also included redesigned processes for IT procurement and financing, new IT purchasing contracts and significantly improved volume discount pricing. In addition, rates for IT shared services were greatly simplified and restructured, and COT's website was completely redesigned to highlight the changes. Inventories of IT vendor contracts in use were created and the responsibility for those contracts was transferred to the Finance Cabinet.

To ensure that all parties are aware of the objectives in the consolidation effort, a Memorandum of Agreement (MOA) was created and formally signed by the Cabinet Secretary of each cabinet whose IT infrastructure is consolidated. This helps to make sure that IT objectives are aligned with agency business objectives.

New Service Level Agreements (SLAs) were created for all consolidated agencies that identify each IT service and the service delivery targets to be met. Critical applications were also identified so escalation can occur for any systems that are deemed to be critical to the agency.

The state agencies involved in the consolidation effort include the Commerce Cabinet, Finance and Administration Cabinet, Revenue Department, Transportation Cabinet and the Governor's Office for Local Development (GOLD). Full time IT staff positions in each agency were either absorbed back into non-IT positions or were transferred to COT. Application development staff

was not affected by the consolidation effort and those not already in COT were allowed to remain in the business units.

Personnel Policies and Practices

Finance & Administration Cabinet Standard Procedures

The Office of Enterprise Technology acts as a focal point within COT to coordinate the development, review and approval of Finance Cabinet IT-related standard procedures and serves as a liaison to the Finance Cabinet Standard Procedures Coordinator. Finance Cabinet standard procedures are available to Cabinet employees on the Cabinet's intranet.

Enterprise IT Policies

Enterprise IT Policies articulate the rules and regulations of state government regarding information technology. These policies determine the type of activities that are approved for both agencies and employees. The Office of Enterprise Technology coordinates the development; review and approval process for enterprise IT policies as well as the enterprise architecture and standards. Enterprise IT policies are presented to the Commonwealth Technology Council for compliance by all appropriate agencies. A complete list of Enterprise policies are located at: http://technology.ky.gov/epmo/enterprise_policies.htm#

IT Security Policies

IT Security policies for COT, as well as Enterprise IT policies, are developed within COT. The Security Standard and Procedures Manual (SSPM), COT-067, (formerly the SPPM) was revised in July, 2008. The manual is available on COT's Website at http://technology.ky.gov/security/sspm_toc.htm. This document has been reformatted into sections to allow for easy updating and distribution. The formatting also allows for selected sections to be extracted and distributed to COT customers. The SSPM addresses security concerns such as policy settings, file system security, etc. in Windows, UNIX and Mainframe environments. In addition, security policy tip documents were prepared providing a summary of many COT security policies. The policy tip documents were customized for three different audiences: COT All, COT Managers, and the COT Application Developers. The following documents also contain information related to IT security. These documents can be found in COT's document management repository or on COT's IT Security Standard Procedures webpage.

- Data Breach Determination Standard Procedure (COT-107)
- Security Policies & Procedures - Frequently Asked Questions

COT Standard Procedures and Forms

The Office of Enterprise Technology establishes, maintains, and coordinates the process for review, approval, publication and announcement of COT customer agency and internal forms and internal standard procedures. COT customer forms are available from the COT home page.

To view the forms, select the following link: http://technology.ky.gov/support/cot_forms.htm. A complete collection of COT standard procedures and forms are available to COT employees in COT's document management repository and the COT intranet.

Employee Policies

COT Employees/contractors are required to complete and sign form COT-F015 - Acknowledgement of Responsibility, which requires a COT employee to accept the responsibility to protect the confidentially and integrity of all Commonwealth of Kentucky data. This responsibility is inclusive of systems and software that the Commonwealth owns, develops or acquires from third parties. This policy requires that COT employees abide by all COT/Enterprise policies and procedures. Further, it requires all hardware, software and data that a COT employee accesses to be used in the performance of assigned job duties. Any violation to the above statements is subject to disciplinary or legal action by the Commonwealth of Kentucky under KRS Chapter 434.840-855.

For contracted personnel, COT-F011 – Acknowledgement of Confidentiality Agreement outlines the responsibility of the contractor/vendor regarding the confidential nature of access to the Commonwealth of Kentucky's data resources. All contracted personnel are required to read and sign this form. The contractor shall be granted access to agency documents, records, programs, files, and any pertinent data resources as needed and shall maintain confidentiality and data integrity of these data resources. The contractor agrees that all developments made and works created by him/her shall be the sole and complete property of the Commonwealth of Kentucky and all copyright and other proprietary interest shall belong to the Commonwealth of Kentucky. Violations of this agreement will result in immediate termination of the contractor/vendor. Upon termination of the contractor/vendor, all forms of data resources and any copies will remain with COT.

Miscellaneous Policies

A listing of all other COT policies/procedures can be found at: https://gotsource.ky.gov/docushare/dsweb/View/Collection-207. These policies set the guidelines for consulting, customer requests for support, and end-user support to cite some examples. Other types of policies/procedures listed include Administrative, Purchasing, and Asset Management.

Security Forms

COT has various types of forms used for security-related requests. To see the complete list go to: http://technology.ky.gov/security/security_forms.htm.

Risk Assessment

The COT risk assessment process includes identification, analysis and management of risks relevant to the processing of data. The risk assessment addresses the current control structure as well as identification of changed conditions that may impact the structure.

Information and Communication

Communication involves providing an understanding of individual roles and responsibilities pertaining to security of data and communications. This communication is accomplished through various standardized policies and procedures within the organization. The information system components relevant to services provided to user organizations are described in various sections of this report.

Monitoring

Monitoring of the internal control systems is a process that assesses the quality of the internal control system's performance over time. This is accomplished primarily by ongoing monitoring activities conducted by management for data security and communication. Ongoing monitoring occurs in the course of operations and includes regular management and supervisory activities, and other actions personnel take in performing their duties.

Control Activities

COT's control activities include the policies and procedures in place to ensure management's directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of COT's objectives. Control activities occur throughout COT, at all levels and in all functions. They include a range of activities such as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Control activities as they relate to the purpose of this report are included in the process description portions of Section II below. The key control activities that support COT control objectives have been identified in Section III, "Information Provided by **Potter & Company LLP**," and tested.

Description of Information Technology General Controls

General Controls are those policies, procedures, and safeguards that relate to all internal information system activities. Their purpose is to ensure the continued, consistent, and proper functioning of information systems by controlling, protecting, and maintaining application software and computer operations.

Strategic Planning

The Commonwealth of Kentucky's Strategic IT Plan: *Interim Update: 2008 – 2010 Biennium* explains the IT strategies that the Commonwealth is using to transform the business of government. The Commonwealth's most mission–critical technology initiatives, which are introduced in the strategic plan, describe how Kentucky government is changing to use technology in alignment with the investment priorities of government, deliver increased value from those investments, better manage risk, control costs, and ensure a marked improvement in

service, both in terms of what is offered to employees and citizens and the quality of the delivery.

IT Governance

Kentucky seeks to make technology investment decisions from an enterprise perspective and not that of a single cabinet or agency. It provides a way to ensure that the Commonwealth's limited IT resources are being utilized in the most effective manner for serving Kentucky's citizens, businesses and other constituencies.

The Commonwealth has the foundation for an enterprise approach to IT with a relatively strong shared infrastructure (e.g., enterprise architecture and standards, Kentucky Information Highway, consolidated data center, enterprise electronic mail, virus protection), but policy, planning and budgeting issues must also be resolved to address cost-effective and non-duplicating investments in IT. The governance model for IT therefore relies on numerous groups to provide Kentucky's Commissioner of Technology and Kentucky legislative bodies with particular insight.

The **Commonwealth Technology Council** (CTC), formed from cabinet and agency information technology officers (ITOs), assists the Commonwealth Commissioner of Technology in targeting and delivering IT resources for maximum business value for the Commonwealth. It provides comments and recommendations on policy, direction, planning and legislation; works to identify opportunities and conduct joint planning for shared services implementation, sourcing, investments, and cost recovery; and provides stewardship for other state IT programs and projects.

Training

COT does not currently provide IT training services. The previous contracts that covered IT training have expired and will be reviewed and reissued. When available, information about new IT training contracts will be posted on COT's web site.

Application Maintenance and Documentation

A. Request for Services

Current Process as of 7/1/2008:

All requests for COT services, including all Office of Application Development (OAD) requests, are sent to the Commonwealth Service Desk (CSD) to be logged and routed to the appropriate area for response. OAD provides three levels of support work for agency systems – Emergency Break/Fix, Maintenance/Support, and Project work. See COT-140 *COT System Development Lifecycle Standard Procedure* for a more descriptive explanation and process flow. Agency requests for new or enhanced application development services (or Projects) are documented on an appropriate request form, the Customer Request for Professional Services form (COT-F001) and forwarded to the CSD. The use of this form is defined in COT's *Customer Requests for Professional Services Standard Procedure* (COT-014). Once the CSD receives a request for service from the customer, an Incident ticket is generated and sent to OAD. A unique number is assigned to each Incident ticket and used for tracking purposes.

Exception to above Process

On July 1, 2008, the Executive Director of the Office of Application Development (OAD) granted an exception to the process defined in COT-014 "Customer Requests for Professional Services" through the creation of a Support Service Level Agreement (SSLA) and approved by the Executive Director of OAD and the Commissioner of the Department of Revenue. The SSLA serves as authorization to provide Emergency Support for critical DOR applications and provides billing information to COT and eliminates the need to submit F001 documents. Tracking and reporting on all of the service requests made via the SSLA will be utilizing COT's IT service management application and the Commonwealth Service Desk. COT is also working on a similar exemption with the Transportation Cabinet; however no agreement has been reached at this time.

Update of COT-014 effective 1/9/2009

On January 9, 2009 COT revised its Customer Requests for Professional Services Standard Procedure (COT-014). The revision, which applies to all customers who request Application Development Services from COT, eliminates the requirement to submit the request on the Customer Request for Professional Services form (F001) which has been rescinded. All the information contained in the F001 form is currently provided to the Customer Services Desk at the time a request is made. COT will continued to accept F001's submitted however the information will be extracted from the document and placed in the Incident ticket and the form itself will not be used for tracking.

B. Perform Request Work

OAD follows the development process as defined in *COT-140 System Development Lifecycle Process Standard Procedure* for completing all Application Development work. Once work is complete OAD follows the *OAD Production Implementation Process*, *OAD-DPM-BP-001*, developed to distinguish it from the higher level *COT-009 Change Management* document, of which it is a part. OAD's application development production implementation process is much more specific than COT-009 and includes detailed steps to be performed when new or revised code needs to be moved onto a COT Production System. A summary of information contained in the Production Cutover Process is described in Section D below.

There are seven phases to the Product Development Process:

- Defining Scope
- Gather Requirements
- Design
- Build/Construction
- Testing
- Implementation (production)
- Closeout

Developers make software changes, noting a description of the modifications in comments within the source code or as a separate "Read Me" document when appropriate. The comments include the date and request tracking number associated with the work being completed.

C. *Validate Requested Work*

Developers unit test the software modifications. The complexity and the extent of system testing will depend on the nature of the software change, the importance of the modifications, the application environment and other factors. In all cases the user agency is involved in User Acceptance Testing (UAT), and their written approval of acceptance is required prior to the change being promoted to production. If the request is for yearly maintenance, however, there is no final agency signoff since there was no actual change completed, and the final action is to close out the F001 form for the previous fiscal year.

D. Promote to Production Environment(s)

The Production Implementation process is triggered when there is a need to promote code to the production environment. Routine implementations are triggered by schedules associated with projects or deadlines associated with requests for maintenance. Break/fix and emergency break/fix implementations are triggered by critical issues documented in Incident Cases in the IT service management system.

- Routine/Scheduled: A project or a support change request that is scheduled for deployment.
- Emergency: An urgent support change request that requires immediate deployment outside of the regular support release schedule because of a critical impact on the user's business. This type of deployment is permitted only if it does not in any way negatively impact other sponsor systems.

No new or changed code may be moved into production until a code walkthrough (zSeries or distributed platform) is performed. Exceptions to this require the approval of the Director of Software Engineering (DSE) or the Executive Director of OAD. Routine distributed and mainframe online deployments are scheduled to occur on a two-week support release schedule on the second and fourth weekend of any given month. Routine mainframe batch deployments are scheduled to occur on a two-week support release schedule on the Friday proceeding the second and fourth weekend of any given month.

Routine Implementation

A routine implementation is a project or support change request that is scheduled for promotion to the production environment. Routine implementations follow this process:

1. The Project Manager (PM) or Development Lead identifies the necessary steps and personnel involved for successful implementation and opens a Change Request in the IT service management system at least two weeks (two CAB meetings) prior to the date of implementation.
2. The IT service management system notifies the appropriate approvers; depending upon the configuration item and combination of the category, type, and item identified in the request, the approvers may include the following roles:
   Change Advisory Board (CAB), Change Manager, Development Branch Manager.

Note: While the approvers review the Change Request, the Development Lead submits an email to the Development Branch Manager. The Development Branch Manager reviews the request and approves, needs more information or rejects.

3. The appropriate approvers approve or reject the Change Request in the IT service management system.
4. Prior to implementation, the Development Lead facilitates an Implementation Walkthrough with key roles involved in the implementation, if necessary based on the complexity or scope of the implementation.
5. The Development Lead finalizes the Change Request in the IT service management system by creating and assigning necessary tasks, attaching the approval email and any attachments, and initiating the tasks on the change requests associated with implementation.
6. The PCO Librarian verifies that all required documentation is attached to the Change Request. If documentation is complete--The PCO Librarian proceeds to Step 7. If documentation is missing—The PCO Librarian informs the Development Lead about the missing documentation; the Development Lead attaches required documentation to the Change Request.
7. The PCO Librarian extracts the PCO documentation from the IT service management system and archives it in COT's document management repository by date and state agency. Once scheduled, the librarian can deploy the change to the staging area.
8. All assigned roles complete the assigned tasks according to the schedule for implementation identified in the Change Request.
9. The IT service management system notifies the Development Lead when all tasks associated with the Change Request have been completed.
10. The Development Lead validates the implementation and enters a closure code on the Change Request.

Emergency Break/Fix Implementation

An emergency break/fix is an urgent support change request that must be implemented immediately and cannot be scheduled because of a critical impact to the user's business. This type of implementation is permitted only if it does not in any way negatively affect other systems. In order to be approved, emergency implementations must meet the following criteria:

- **Priority: Critical**—the change requires immediate action where a major system or application is not available and *no work around exists*. It involves potential impact to the highest percentage of users or a mission-critical system. Immediate action is required and resources are allocated immediately to build the change.
- **Urgency: Emergency**—Immediate action is warranted to restore functionality. Corrective action must be taken as soon as a fix is available.

Emergency Break/Fix implementations follow this process:

1. As soon as the need to request the change is known, the Development Lead submits an email to the Development Branch Manager with the following attachments:
    - Sponsor approval (obtained by PM or Development Lead)
    - Production Cutover Document for Mainframe
    - Production Cutover Document for Distributed Systems
    - Implementation Approval Form
    - Code Walkthrough Verification
2. The Development Branch Manager reviews the request and either approves, rejects or needs more information.
3. The Development Lead or PM creates an "Urgency:1, Impact:1" Emergency Change Request from the Incident Case in the IT service management system which requires at least the following:
    - Describing the requested change
    - Defining the proposed implementation timeline
    - Identifying the system(s) affected
    - Inserting a task for each group involved in the implementation
    - Attaching the approval email, with attachments, from the Development Branch Manager
    - Attaching the finalized Implementation Plan
    - Changing the status of the ticket to initiate the approval process
4. The IT service management system initiates the approval process and notifies the Change Manager. **Note:** To verify receipt of the emergency request, the Development Lead or Development Branch Manager should also contact the Change Manager via phone or email after opening the Change Request.
5. The Change Manager approves or rejects the Change Request in the IT service management system.
6. Prior to implementation, the Development Lead facilitates an Implementation Walkthrough with key roles involved in the implementation, if necessary based on the complexity or scope of the implementation.
7. The Development Lead changes the status of the Change Request to initiate the tasks associated with implementation.
8. The PCO Librarian verifies that all required documentation is attached to the Change Request. If documentation is complete--The PCO Librarian proceeds to Step 9. If documentation is missing—The PCO Librarian informs the Development Lead about the missing documentation; the Development Lead attaches required documentation to the Change Request.
9. The PCO Librarian extracts the PCO documentation from the IT service management system and archives it in COT's document management repository by date and state agency. Once scheduled, the librarian can deploy the change to the staging area.

10. All assigned roles complete the assigned tasks according to the schedule for implementation identified in the Change Request.
11. The IT service management system notifies the Development Lead when all tasks associated with the Change Request have been completed.
12. The Development Lead validates the implementation and enters a closure code on the Change Request.

Mainframe

Systems Software and Hardware

Changes/Implementation/Documentation

The Mainframe Team, Production Services Branch, is responsible for all system software upgrades and ongoing maintenance of system software. Systems programmers follow System Support Software Life Cycle procedures maintained online by mainframe support staff. Upgrades, changes, and testing are scheduled through the change control process. The manager assigns software products to the selected individuals who maintain each product. Local modifications of system software by technical staff are not permitted unless specifically authorized by the manager. Testing of systems software is usually conducted by the Mainframe Team in Test LPAR (Logical Partitions) region rather than in one of the two production LPARs. A full system backup is performed prior to any changes to system software being moved to production. The Mainframe Team maintains all documentation regarding system software releases, including detailed documentation regarding release levels and maintenance levels for system software. Product manuals and documentation is usually stored online. The change control process also maintains a historical record of system changes.

Operations and Scheduling

COT Operations provides monitoring and support from the Main Console 24 hours per day, seven days per week. A supervisor is assigned to each shift. Activities performed and issues identified during each shift are documented via a newly implemented Electronic Message Board that is maintained and updated by each shift. Entries to the log are posted in predefined topics for routine procedures and monitoring or in specific topics defined as events occur. Each posting contains the time, date, and name of the operator posting the reply as well as a brief description and any associated incident/change ticket number. Standard topics are created by 1st or 4th shifts, depending on the day of the week. Topics for the previous 24 hours are then printed by 3rd or 5th shifts, again depending on the day of the week.

Each shift also completes a checklist that includes all of the standard activities for that shift. They are still undergoing development and will include the date, time, and initials of the operator completing each item on the checklist. The shift supervisor ensures that the checklist is printed out at the beginning of each shift. The 3rd or 5th shift supervisors collect all checklists for the 24-hour period and have them available for review in the morning. These are reviewed by the Operations Supervisor and filed at the Main Console.

Documentation is available online to operators outlining the specific tasks to be performed during their shifts and the approximate time of day that they should be performed. On-line documentation also includes instructions for operators on handling ad-hoc situations including system failures, restart procedures, and other emergency situations. Documentation is maintained in COT's documentation repository, although hard copy manuals are also maintained in the event the documentation repository server fails. Unless specifically requested, only Operations staff can access Operations documentation in COT's documentation repository.

Ad hoc requests require a change request approved by a director, per COT Policy or an incident/change ticket. Operators create problem tickets at the request of authorized support staff. Operations is in the process of building a contacts database that lists for each piece of equipment on the fourth floor authorized support staff as identified by the agency.

Most batch jobs are scheduled using a 3rd-party scheduling product, which is protected by mainframe security. Only a few selected operators have access to add or modify the batch process schedules administered by COT. COT is also responsible for the administration and support of the job scheduling software. Most agencies are then responsible for their own batch operations and schedules. COT Production Services Branch is responsible for batch operations and scheduling CHFS, MARS, Revenue and Workforce Development's UI (unemployment insurance) job streams. In addition to Batch processing, the COT Production Services Branch is responsible for Production Cut-Over (PCO) processes for all COT Batch supported Job Control Language (JCL), Documentation, and Programs. COT operators have access to agency job schedules; however, they do not have access to agency job codes. COT also runs a daily audit job that generates the COT Scheduler Audit Report. This reports shows user changes to their job schedules. The job output is reviewed upon Agency request by the Scheduler Administrator and the agency is forwarded the results of the report.

Security

Access to the mainframe and its resources is controlled by a mainframe security product, which is administrated by the Security Administration Branch, mainframe security group. This application controls all user identifications and access to datasets or resources. There are password restrictions regarding length, composition and frequency of expiration. Passwords expire every thirty-one days. After three unsuccessful logon attempts with a bad password, the user identification will be revoked and cannot be used again until a mainframe Security Administrator resets the user identification.

User identifications are revoked after sixty days of inactivity. The use of common names is discouraged, writing down and taping of passwords to terminals is prohibited, and storing a password in a batch job is prohibited.

Limited security administration functions may be assigned at the agency level if defined in the Agency Mainframe Security Agreement. The Manager of the Security Administration Branch must approve authorization of these functions.

Each agency is required to designate a mainframe security contact. The request for agency security permissions (Agency contact) must be in a written or electronic form in order to request authorization from the Manager of the Security Administration Branch to become a security

contact at an agency. The Security Administration Branch maintains a list of each agency and who is authorized to request mainframe security changes from those agencies.

Each agency will fall into one of the following three classes of support:

- Agencies that are self supported for day-to-day mainframe security administration
- Agencies that are able to reset their user's password only with all other administration being completed by COT Security Administrators.
- Agencies that the COT supports in all aspects of security administration.

The self-supported agencies will take care of their own administration but must follow COT guidelines and procedures. Each self-supporting agency is provided daily violation reports that show any of their users trying to access the mainframe and having problems. Another daily report shows those trying to access data sets or resources that are denied.

The Logon Violation Reports are broken into three data sets, which show the following information:

- Detail Logon information showing a line for each attempted logon.
- Summary information showing a line for each user with the total count for each type violation.
- Threshold information showing only those users having more than three violations.

The last violation report shows violations against the agency data sets or resources. Each agency has been made aware of these reports and encouraged to review the reports. COT reviews the reports for those agencies that fall into the COT supported category. A log is maintained to track the review of the violations. As an additional security precaution, multiple people review the logs.

Every Sunday night (for each self-supporting agency prefix), a data set is created giving the agency the following weekly reports:

Member Name	Description
CONNECTS	This member contains a list of the agency's groups and what user ids are connected to those groups.
DATASETS	This member contains a list of the agency's data set profiles and what user ids & groups have access and at what level (read**, update, control, alter).**
LASTUSED	This member contains a list of the agency's user identification sorted in last used order. A user identification that has never been used will show up as Blanks which sort to the top followed by the user identification that has not been used in the longest time. (Sorted Date/Time)
RESOURCE	This member contains a list of the agency's Resource profiles with the mainframe security class and what user ids / groups have access and at what level. (read, update, control, alter).
UACC	This member contains a list of the agency's profiles that have a UACC other than "NONE".
USERGRPS	This member contains a list of the agency's user ids with information about each user id.
USERIDS	This member contains a list of the agency's user identifications with information about each user id. This report is sorted by the user identification and then within user identification by Default Group.
USERTSO	This member contains a list of the agency's user identifications **that have TSO access.**

User identification requests are sent to the Commonwealth Service Desk for assignment of a Tracking Number by COT's IT service management software. All requests for userIDs require a COT-F181, Employee Service Request Form from one of the agency security contacts. The COT-F181 form has recently been consolidated and is being used for all COT type Security requests.

As mainframe requests tickets come in to the mainframe security group, they are validated against the agency contact list to make sure the requestor is an authorized requestor and then assigned to someone in the mainframe security group. When the request has been completed, the individual completing it updates the IT service management tracking system.

A ticket generated by the IT service management system notifies the Security Administration Branch of any terminations or transfers of COT employees/contractors. The Employee/Contractor Exit Request is sent to all of the mainframe security administrators to ensure that access is removed. When the mainframe security group is notified of someone leaving, a query is run to check for mainframe user identification. Any user identifications owned by the individual will be revoked on their last day or when notified. These user identifications will be left on the system while management ensures that data set cleanup is performed, and then removed.

When COT users change departments, their old user identification is put into REVOKE status. User identifications are then deleted and new user identification is issued via the above procedure. User identifications with the prefix PS, only used for COT, are not deleted, but remain in REVOKE status until it can be determined that the information to which the IDs have access is no longer needed by COT. The Security Administration Branch has been regularly communicating with customer agencies to promote the importance of mainframe security. Listed below are examples:

- Cleanup of user identifications – Reports related to these cleanup procedures have been produced for each agency.
- Password Strengthening - Password cracking software has been utilized to produce a list of mainframe passwords that need to be strengthened. This list has been distributed to agency security contacts.
- Reports – The COT has developed several reports for agencies to use in order to assist them in identifying violations and reviewing access levels.
- Mainframe Security Administration - Several guidelines have been sent to the agencies suggesting the proper way to administer mainframe security, change a user's password, and add user identifications.

The Security Administration Branch utilizes a 3rd-party security software suite to assist in security administration. This security product suite has three components:

- Administration component - Allows cloning of user identifications and groups and allows reporting on mainframe security entities.
- Reporting component – Eases reporting on mainframe security violations and other mainframe monitoring.
- Analysis component – Produces many useful mainframe security system setup reports.

With the implementation of the Enterprise Password Auditing Policy, password audits are required on a quarterly basis. A mainframe Password Cracking utility is used to test the strength of the mainframe passwords and identify those user identifications with weak passwords. Reports are then sent to the agency contacts so that they may take steps to ensure the passwords are strengthened. The cracking utility is run at least once during the fiscal year. Reports are also generated for COT internal use.

With the implementation of the Enterprise UserID/Password Policy, non-expiring passwords must be approved by the COT. COT is now responsible for these passwords and ensures that the password composition meets the enterprise standard. Agencies must identify the need for requiring a non-expiring password and must identify special security precautions put in place to minimize the risk of having a non-expiring password.

Access to DBMS databases is granted through mainframe security groups. Access must be authorized by the owner of the database and must be a written or electronic request to Security Administration Branch.

The password for the System Emergency User Identification and other critical passwords have been sealed in envelopes and put in the COT storage safe. The use of the password will be monitored and a log is kept recording the use of the profile to ensure that it is restricted to emergencies. The password is periodically changed.

In October 2002, COT implemented the mainframe security option, Erase on Scratch. This option will prevent sensitive and/or confidential data from being recovered from a deleted dataset. Agencies were notified of the option change and were provided instructions as to how to implement this option for selected datasets.

In May 2001, the COT enabled the cryptographic co-processor on the mainframe enterprise server, allowing the enhanced use of Secure Socket Layer (SSL) on this platform.

Output Data Distribution

COT provides and supports two online report distribution products. Both products are for electronic report storage and retrieval on tape and/or optical disk for viewing and printing by customers. Security for both products is provided by the mainframe security management software. The owning agency of each report must authorize access to their reports. The COT Security Contact List that is maintained by the COT Mainframe Security Group is used as a list of individuals that may request or authorize access to agency reports. A form is currently being developed that will be used for formalize the request process.

Backups and Recovery

The disaster recovery strategy insures that all critical data files are backed up and taken offsite for storage. The mainframe strategy utilizes weekly full volume, full data recovery backups of most of the DASD volumes attached to the mainframe. The only mainframe volumes that are not backed up weekly are the ones whose data changes too rapidly for a backup to be of any use and

those that are more easily created at the hot-site from scratch. There are also daily backups of critical files that are taken offsite that include database archive logs, some of the database client nodes and selected application backups. Critical data files and enterprise functions residing on servers are backed up daily or weekly and sent to the offsite storage facility. The backup tapes are returned four weeks later.

UNIX

Systems Software and Hardware

Changes/Implementation/Documentation

All system changes are implemented according to the COT change control process. Changes are submitted to change control by Tuesday morning and reviewed during the change control meeting on Wednesday afternoon. Emergency changes can circumvent this process, but must be approved in advance by the Operating Systems Branch Manager and change control staff. Changes are applied (not committed) when possible so that they can be backed out if necessary. System changes are, except in emergencies, made by the system administrator responsible for a particular UNIX host. In an emergency any available system administrator may make the required change.

System changes are documented in the change control request. Patches are also documented briefly in a text file on each server so that a list of patches applied can be included in each month's collection of system information.

Operations and Scheduling

UNIX Operations support is provided 24 hours by seven days a week from the same staff that operates the mainframe systems. This support consists of monitoring the UNIX servers, restarting applications, occasional UNIX userID and password resets, rebooting servers, and notifying support personnel of problems and issues. However, Operations does not reboot a server or restart any UNIX computers OR reset any UNIX userID and password unless a request is sent via e-mail from a person on an authorized contact list, and the request is followed up with a phone call from the requestor.

A server manual is available at the main console in the operations area outlining responsibilities of individuals, procedures to follow and includes a list of support personnel. Server user identifications and passwords are kept in a padlocked metal box for which only the shift supervisors and server administrators have a key. Shift Supervisory personnel log any access to the metal box.

Issues identified during a particular shift are documented in a Production Control log each day, and the log is reviewed by the next shift during a shift turnover time period. The log includes the date, known problems, production migrations, special requests or runs, and other shift information. A Nightly Cycle document is also used by the Production Control Analysts, which is updated with statistics and other pertinent information regarding the cycle. Any problems

affecting availability of the UNIX environment are explained at the top of the document. The Nightly Cycle document also contains primary contact names and numbers for system ABENDS and resolutions for each cycle. The analysts discuss resolution actions and confer with the individual that is on-call prior to any changes or course of action.

On the business day following each cycle, further statistics are gathered, and the Nightly Cycle document is updated and sent to senior COT and agency management personnel for review. This provides them with explanations of problems from the previous night and any resolutions taken during the day to help prevent further problems.

Security-UNIX

A comprehensive Security Procedures Manual is available on-line that addresses mainframe, UNIX and NT concerns. In addition, a UNIX (Solaris and AIX) administrator's manual is available that includes topics such as policy settings, file system security, etc. These policies are available in COT's document management system.

An audit of user identifications is performed at least once a year. Some user identifications were reconfigured to be "su-only" (not login able) so that their use could be tracked through available logging mechanisms. Agencies are required to designate an owner for each generic user identification and the owner who would be responsible for everything that is performed with the specific unique user identification as well as being the only person authorized to ask for a password reset. Any generic user identifications that require login capability must have documentation from the owner of the identification as to why the identification requires this capability. COT security personnel periodically verifies with the agencies the particular hosts that each user identification should be able to access and ensures that the user identifications can access only those particular hosts.

Password restrictions are implemented so that all users must change passwords on a regular basis, have a five-day grace period in which to change the password, will be locked out after five unsuccessful login attempts, and must use a password with at least three non-alpha characters. Administrator passwords are stored in a locked box and access to the safe is restricted, logged and reviewed. A few generic user identifications are not required to have passwords that expire on a monthly basis. In these cases, written justification is prepared by the owner of the identification and a request for a security exemption is submitted to the Security Administration Branch, Office of Chief Information Security Officer. This request is submitted by completing the COT-F085, Security Exemption Request form.

The COT-F181 is being used for user identifications creations and changes. Password resets and failed login count resets are performed by the Division of IT Operations. The KCCMS help desk has "sudo" capabilities to add new users, reset passwords, and reset failed login counts and they define their own method of requesting changes.

Requests to lock/unlock user identifications must also be sent using the change management system.

A daily report of security log files is generated and emailed to all system administrators. In addition, a system administrator reviews log files once a day, Monday through Friday. These logs include the error report, “wtmp,” “sulog,” “sudo.log,” “syslog,” messages and the login log (depending on the particular operating system). Any anomalies will be reviewed with the UNIX team leader before filing a Security Incident Report. The daily check of these logs will be documented on a checklist and filed daily in a binder. In addition, Operations staff also monitors these logs on a shift-by-shift basis, thereby expanding coverage.

As employees depart, the security administrators are notified to remove their user identification via a ticket from the IT service management system with the F181 form attached. The security administrators deactivate the user identification and produce a list of files owned by that user identification. If the user identification does not own any files other than standard system files, security administrators delete the user identification immediately. If the user identification owns files other than the standard system files, security administrators email this list to the system owner and give him/her 30 days to determine what should happen to these files. At the end of 30 days, security administrators remove the user identification and files in the home directory. Security administrators do not remove files in shared directories as group ownership may provide access to other users.

Security patch information will be analyzed as patches are identified. Those security patches that are deemed critical are applied as soon as the outage can be scheduled. Patches that are less critical are collected and reviewed. The security patch information will be compiled and a list created for review. The Security Administrator will review the patches and those that are required will be installed on test systems, with the owner’s permission. After a week of evaluation, if no problems are found, patches will be rolled out to the remaining hosts according to the change control process.

Output Data Distribution-UNIX

There are no special output distribution procedures since reports are available on-line to those that have appropriate access.

Backups and Recovery-UNIX

Selected application data from the UNIX enterprise servers are backed up using the Tivoli Storage Manager (TSM) product, which is a client-server product. Those TSM clients who participate in our offsite disaster recovery process have copies of their data taken offsite daily and stored at our secure storage facility for safekeeping. (Backups for systems that have been deemed critical for disaster recovery are being taken off-site to underground storage.)

Windows

Systems Software and Hardware

Changes/Implementation/Documentation

All system changes are implemented according to the COT change control process. Changes are submitted to change control by Tuesday morning and reviewed during the change control meeting on Wednesday afternoon. Emergency changes can circumvent this process but must be approved in advance by the Operating Systems Branch Manager and change control staff. When possible, all changes must be applied to test servers and given the appropriate time for the users to test. Security changes, unless emergencies will be applied to the test servers between the 15th and 20th, and applied to the production servers on the first weekend of the month. Users will be notified and are encouraged to test changes after the fixes have been applied. "Emergency changes" must be approved by the manager of the Operating Systems Branch and then processed through change control. Detailed documentation of changes made to each server is maintained within the Operating Systems Branch. In addition, the change control process maintains a historical list of changes made.

Operations and Scheduling

Windows operations support is provided 24 hours by seven days a week by the same staff that operates the mainframe. This support consists of monitoring the Windows-based servers, restarting applications, rebooting servers, and notifying support personnel of problems and issues. However, operations does not reboot a server or restart any Windows servers unless a request is send via e-mail from a person on an authorized contact list, and the request is followed up with a phone call from the requestor.

A server manual is available at the main console in the operations area outlining responsibilities of individuals, procedures to follow and includes a list of support personnel. Server user identifications and passwords are kept in a padlocked metal box for which only the shift supervisors and server administrators have a key. Shift Supervisory personnel log any access to the metal box.

Issues identified during a particular shift are documented in a Production Control log each day and the log is reviewed by the next shift during the shift turnover time period. The log includes the date, known problems, production migrations, special requests or runs and other shift information. A Nightly Cycle document is also used by the Production Control Analysts, which is updated with statistics and other pertinent information regarding the cycle. Any problems affecting availability of the Windows environment are explained at the top of the document. The Nightly Cycle document also contains primary contact names and numbers for system ABENDS and resolutions for each cycle. The analysts discuss resolution actions and confer with the individual that is on-call, prior to completing any changes or undertaking a course of corrective action.

The business day following each cycle, further statistics are gathered, and the Nightly Cycle document is updated and sent to senior COT and agency management personnel for review. This provides them with explanations of problems from the previous night and any resolutions taken during the day to help prevent further problems.

Security

A comprehensive Security Standards Procedure Manual is available to address both UNIX and Windows security considerations. In addition, an administrator's manual is available to outline topics such as policy settings, file system security, etc. These policies are available in COT's document management system.

A security baseline is established for all enterprise servers. As each server is configured, a baseline GPO is applied to the server to ensure that adequate security settings are established. This script has also been applied to all existing servers.

Security hot fixes are reviewed on a regular basis. The team decides the impact of each vulnerability and makes a decision as to the implementation of a fix. Documentation is maintained that shows the security fixes that have been applied. Due to the large number of servers housed at COT, tracking fixes from development, testing, and production can be cumbersome. Each month all administrator passwords are changed and secured in a locked safe. Team administrators and/or management in the event of an emergency can retrieve these passwords.

Standards have been established for Windows audit settings. The required audit settings have been identified and each administrator is responsible to ensure that these settings are used on the server for which they are responsible.

COT utilizes Windows monitoring software to provide notification of problems with security, server hardware, and system services. Alerts are generated based upon thresholds established within the monitoring application. Automatic emails are sent to administrative staff when designated thresholds are reached.

SSL certificates have been installed on Commonwealth web servers where secure client/server communications is required. Certificate administration has been centralized and a list of certificates/servers is maintained on a server for documentation.

Output Data Distribution

There are no special output distribution procedures since reports are available on-line to those that have appropriate access.

Backups and Recovery

Selected application data from the NT enterprise servers is backed up using a storage management product. The storage management clients have copies of their data taken offsite daily and stored at our secure storage facility for safekeeping. (Backups for systems that have been deemed critical for disaster recovery are being taken off-site to underground storage.)

Infrastructure Support

Change Control

The Commonwealth Office of Technology implemented a Change Management process effective April 2001, with revisions to the process in August 2004. The purpose of the Change Management process is to minimize service disruptions to our computing environment and promote system availability. This process is designed to provide an orderly method in which changes to the IT environment are requested and approved prior to the installation or implementation. The responsibility for this function lies within the Office of Infrastructure Services, Change Management Branch.

The process is outlined in COT Standard Procedure Number COT-009. The document describes the responsibilities, policies, and procedures to be followed by COT when making changes or recording events to the Commonwealth of Kentucky's IT infrastructure. This covers any and all changes to hardware, software or applications. This process also includes modifications, additions or changes to the LAN/WAN, Network or Server hardware and software, and any other environmental shutdowns (i.e. electrical).

Effective July 2006, all new Change Requests were recorded in the COT ticket tracking system. Change Requests should be submitted to the Commonwealth Service Desk by email or by phoning the Commonwealth Service Desk. Change Requests are be submitted as soon as all planning has been completed, but no later than the mandatory deadline of 10:00 a.m. Tuesday in order to be added to the agenda for the weekly Change Advisory Board. The Change Request must include enough detail so that all areas know the relative impact of the change and how it may affect other COT areas. If not properly completed, the form will be rejected and returned to the Requester for additional information.

All Major changes will be discussed in the Change Advisory Board meetings, held each Wednesday at 3:00 p.m. The purpose of the weekly meeting is to share information, concerns, and comments in a cooperative environment in order to eliminate potential disruptions of service to COT customers. The Change Manager or a designee facilitates the meeting. Any area submitting a change should have proper representation attend the CAB meeting. Items discussed at the meeting include:

- Reviewing the last changes implemented and any pertinent issues/problems encountered;
- Reviewing the proposed changes for the upcoming week;
- Identifying conflicts and plan for resolution;
- Identifying customers affected and notification requirements to those customers;

- Schedule a time frame to implement a change, while considering application restrictions upcoming events such as month-end, year-end, heavy business days, holiday, or any justified business need.
- Ensuring availability of a back-out or fallback plan;
- Ensuring support is defined in the event of a back out; and
- Finalizing and approving changes.

If approved, the change will be added to the Forward Schedule of Change. This schedule is available for all Commonwealth exchange user to view and is located in the public folders region under "All Public Folders\Information Systems\COT Forward Schedule of Change".

Awareness Notification

The COT Service Desk will send an Awareness Report via email within ½ hour, if they are aware or notified of an occurrence affecting the production IT environment. It is the responsibility of the support group working on the problem to send an email to the Service Desk with a brief description of a problem and assessment of the services and users affected by the situation. A follow-up notification is sent once the issue is resolved. The Awareness Notification distribution list is made up of not only COT personnel, but also many of the key individuals within the agencies. Anyone can be added/deleted to the list by contacting the COT Service Desk.

Internet and Intranet Firewalls

Access to the Internet is controlled and monitored by the firewall. Firewall and router logs are reviewed for suspicious activity including any known attack signatures, SNMP attempts to the Firewalls, unauthorized Telnet sessions, IP spoofing, unusual packet routing, port scanning, and other suspicious activities. The Firewall, backbone routers, and network management system gather these logs.

The COT Firewall administers the Internet firewall and IDS sensors. The COT managed security vendor documents these attempts and completes a security incident report that is sent to the Security Administration Branch for follow-up. On attacks originating from the Internet, the offending IP addresses are filtered at various points in the infrastructure until the attacks have ceased, or COT has communicated with management from that party. On Intranet attacks, the offending IP or entire IP subnet of the offending party is blocked at the nearest routing point to the offending IP. Communications will not be re-established until the offending entities' ITO responds as required by COT policy. Restoration of services is at the discretion of COT since COT may conduct protocol analysis at multiple points throughout the infrastructure to determine if the agency has corrected the situation. Network services will resume and continue as long as the offending party demonstrates they are in compliance with COT network security policies.

A security architecture was designed and approved by the Commonwealth Technology Council (CTC) in 2002. COT has created an enterprise e-government zone and has added additional firewalls to separate the Intranet from the e-government zone. The e-government zone has multiple DMZ's to help protect services and customers. All agencies are required to move all

publicly visible services such as web servers, FTP servers, SMTP servers, etc., to the e-government zone. The goal is to create a "block all, allow few" approach on the Intranet firewalls. COT is working with agencies to reduce the protocols allowed. Until the "block all, allow few" rule is applied, COT is auditing all protocols. COT is capturing the traffic and reviewing the logs files for future enhancements and blocking. Both the Internet and Intranet firewalls are Tier 1. (Refer to Enterprise CIO-076, Firewall and Virtual Private Network Administration Policy). Agency/cabinet firewalls are Tier 1 or Tier 2. Tier 1 firewalls are managed and administered by COT. The logs from Tier 1 firewalls are correlated to the IDS. Tier 2 firewalls are also managed and administered by COT. These logs are not correlated to the IDS.

Agency/Cabinet Firewalls

COT provides firewall services for various state agency applications. The customer owns the rules set for each firewall. COT works with customers to strengthen each agency's firewall rule sets. The application requirements and the degree of security the application owners wish to implement determine how strict to make the rules base.

The firewall software is kept current with the latest releases, vendor-recommended patches, and enhancements. Modifications to firewall configurations can only be performed from the firewall's console. As such, COT's Firewall team performs the maintenance with the agency's approval and following the COT change management process.

The firewall requires a user identification and password to access or to change configuration settings. Only authorized persons have access to the password to change firewall information. Access is also restricted to certain IP addresses. All of the firewall consoles, servers, and other network hardware are maintained in a secure, physical access-controlled location.

The product for VPN and firewall is available for Tier II firewalls. COT recommends Tier II for network protection and agency firewalls not protecting enterprise class material and/or sensitive data that could result in loss of life or financial repercussions.

Intrusion Detection Systems (IDS)

COT utilizes a network based IDS. This system interfaces with COT's firewall management console for alerts and actions based upon the rule sets established. When the IDS agents identify attack signatures that are critical, a page is sent to the firewall team to determine of the IP address should be blocked. COT has greatly enhanced the number of sensors at strategic locations throughout the infrastructure.

COT's managed security vendor manages the IDS as well as the Tier 1 firewalls. This will provide 24x7 coverage at various points throughout the network. COT has a security contract that provides product, maintenance, and professional services. Three vendors hold the contract jointly.

A Layer 4-7 switch has been placed at the perimeter that allows COT to filter on content a well as port numbers.

Virtual Private Networking (VPN)

A Virtual Private Network (VPN) is also available for clients wanting a secure connection from their access point to the VPN Server or to their own COT administered firewall. All VPN users are required to enter a username and password to connect. Once the connection is accepted, a "secure tunnel" is created from their workstation to the VPN server. COT has also implemented two VPN appliances that restrict access to specific applications for specific servers. Finally, COT provides mobile VPN as a service offering for those users who connect from multiple (many different) networks during a short period of time. This service is available upon request for all KIH users.

COT also provides a site-to-site IPSec VPN solution in order to provide a secure link to KIH for all agencies participating. Placing a switch at each agency remote location and establishing a secure connection back to the agency's VPN bridgehead located at the COT data center accomplishes this. All other communications are shut off to the participants and each communication must pass through a common firewall and be approved before it is routed to the end node. The only allowed protocol and communications to each node is through the firewall and via the branch office tunnel. This eliminates all unsolicited traffic that is not approved to reach agency nodes.

Web Access to Email

Encryption for web access to email utilizing the SSL option is available. This service provides confidentiality for COT clients using web services to obtain email while traveling or not having access to the standard email client.

Network

COT's network management system monitors routers and switches and identifies potential problems. COT measures the performance of the WAN links with various network tools. These tools allow the ability to provide measurements for customers and to take a more proactive approach in Network performance monitoring. COT measures availability, response time, and error conditions. A web interface is used to track these issues and allows the ability to report problems and update trouble tickets. Senior engineers in both the Enterprise Services area and the Network Engineering area perform capacity planning with the help of these tools. COT has implemented network "sniffers" to help manage and protect the network. Protocol analysis can be performed at multiple points throughout the infrastructure. The protocol analysis deployment helps COT to determine where internal security issues are such as virus infection, mischievous behaviors, and other types of unwanted traffic. The goal is to have the ability to isolate traffic anywhere on the entire COT backbone (MPLS, Switched Ethernet, Server Farms, and Frankfort MAN).

Kentucky Information Highway (KIH)

An RFP was issued to establish a method for COT to obtain cost effective connectivity solutions for KIH eligible entities throughout the state. The contract was awarded in February 2005 and COT is in the process of planning the transition to the new infrastructure.

Virus Protection

COT has established enterprise standards and contracts for antivirus, anti-malware, intrusion prevention and endpoint protection software.

The majority of the Commonwealth makes use of a management console to manage and enforce anti-virus policies, automate updating of virus definition files, and perform regularly scheduled on-demand virus scans of computing equipment.

Agencies that do not make use of a central management console rely on the AutoUpdate feature of the anti-virus software to automate updating of virus definition files and performing regularly scheduled on-demand virus scans of computing equipment.

The Commonwealth's email servers are protected from malware by software that scans incoming and outgoing email for viruses and malware.

The anti-virus software vendor provides timely virus warnings and software updates as well as DAT files during emergency outbreak situations, at which time COT will alert our anti-virus enterprise clients. The vendor's DAT updates and/or engine upgrades are provided and posted to the dedicated FTP anti-virus server, and notification is provided to our clients.

Enterprise support from the anti-virus software vendor is available for each anti-virus contact in each cabinet that participates in the agreement.

Incident Reporting

COT implemented a security incident reporting policy that requires employees and/or contractors to report suspected security violations immediately to the Commonwealth Service Desk either by phone to 502-564-7576, or by email to CommonwealthServiceDesk@ky.gov. As incidents are reported, the Security Administration Branch performs investigation and follows up as required. An incident is anything logical or physical that compromises or may compromise the state network or facilities under the responsibility of COT.

Commonwealth Data Center Assessment

The Commonwealth Office of Technology contracted with Microsoft to conduct an operations assessment of the Commonwealth Data Center. The objective of the assessment was to review the IT management processes involved in operating and supporting the Microsoft based client/server technologies. The scope of the processes included change management, configuration management, release management, service monitoring and control, incident

management and problem management. Prioritized recommendations by service function were provided as part of the deliverable of this assessment.

Security Alerts

COT provides a structured, routine, and timely service of announcing security alerts to appropriate personnel by email using distribution lists, and posting the alerts on the Security Services web page. The COT Security Administration Branch will be responsible for providing notifications of security alerts. When acted upon, these alerts will assist in keeping the networking resources of the Commonwealth free from intrusion and viruses. It is the intent of COT to be the clearinghouse for the identification, collection, analysis, and dissemination of information to other Commonwealth Agencies to save each of them the effort of performing the same tasks.

It is important to note that the Security Administration Branch and the System/Network Administrators, who are responsible for implementing security measures, must continue to stay updated of the latest security threats, vulnerabilities, software patches, etc. For this reason, COT obtains notices of computer viruses and security alerts from a variety of sources including vendor subscription services.

Analysts will review the notifications as soon as they arrive for potential impact. Once an alert has been determined to be critical for supported products and systems, the security analyst will supply the necessary value-added information to other security staff members who finalize and publish the alert notification to selected email groups. When these damages or measures warrant immediate reaction(s) they will be sent with the subject, "COT Security Alert: ", with a brief explanatory title following the colon. When the damages or measures warrant only timely reactions, or when they are precautionary in nature, they will be sent with the subject, "COT Security Notification: ", with a brief explanatory title following the colon.

The alerts are posted on the COT Security Administration website as soon as possible after it has been distributed to the COT contacts. Postings will be to http://technology.ky.gov/security/security_alerts.htm. The alerts will be posted by links arranged chronologically beginning with the most recent and with no distinction between critical and informational alerts.

Homeland Security

In response to the development of the Homeland Security Advisory System created by the National Homeland Security Office, COT developed strategy and implementation procedures for each of the advisory levels.

Enterprise Directory

The Commonwealth of Kentucky has chosen a single enterprise directory as the database for users and objects within the Commonwealth. Previously, the Commonwealth had a variety of sources which contained the users and objects. The largest repository of user information in a directory today is the enterprise email address list. The Commonwealth's directory of users and objects are contained within the enterprise directory. Currently, the enterprise directory consists of an empty root domain and one level of child domains. The "foster domain" is the default domain in which users would be brought into the enterprise directory. A cabinet may choose to submit an exception request to ask that their cabinet be brought into the enterprise directory as a child domain under the root domain. COT's migration is complete and several cabinets have completed the migration process. As cabinets were migrated into the enterprise directory, their previous system was decommissioned. Moving forward, the Commonwealth will leverage the directory for such applications as enhanced enterprise email.

Secure E-mail

COT offers encryption software for customers that require encrypted email. As of August 2008, there are approximately 2,200 employees that use encrypted email. The encryption software allows customers using COT provided email services to enable secure email with other participating customers, or with any external email address that supports S/MIME compliant encryption.

Content Management

In April 2004, COT implemented a Content Security Management (CSM) solution. The CSM software provides website filtering and some anti-malware protection to the Commonwealth's executive branch agencies. COT is evaluating products to replace the Content Security Management solution. The expected implementation date for a new solution would be September 2008.

In July of 2007, COT upgraded the software used to help prevent unwanted spam and anti-malware in our messaging environment. The current solution is a two-tiered approach that relies upon 1) a reputation service that COT pays an annual subscription to utilize and 2) a combination of 22 configurable filters that scan the contents and header of electronic mail.

Physical Security

COT issues a standardized identification badge/proximity card which allows authorized employees/contractors access into COT facilities. The badge should be prominently displayed by the employee/contractor while they are in a COT facility. All employees are encouraged to challenge unescorted strangers and anyone not wearing visible identification. Requests for badge access and/or changes are completed via the form COT-F019 and signed by both the employee and the supervisor of the employee. All badges are required to include the employee's photo and are color coded in respect to their status (e.g., COT employee, contractor, vendor, etc.). A corresponding policy has been implemented and is included in the Security Standard Procedures

Manual (SSPM). Access rights to areas within COT facilities, particularly the Commonwealth Data Center (CDC), are regularly reviewed.

To ensure no one enters the CDC without appropriate access, a facilities security guard is stationed at the front desk 24 x 7 each day. Visitors must sign in, are issued a visitor's badge, and must be escorted by appropriate COT personnel. The front desk visitors' log is archived for one year and then shredded.

COT employees who are located in one of the other COT facilities are not required to wear a visitor's badge, as they have valid COT badges and are frequently required to attend meetings at the CDC.

The Commonwealth Data Center is currently equipped with video cameras that are located throughout the building at sensitive access points. A camera surveillance system has been installed at the guard station and a backup library of surveillance footage is maintained for a year. Outside cameras have also been added for enhanced security. The building is partially surrounded by bollards to protect access to the building, the parking area is access controlled, the entrance to the building has additional safeguards, and interior doors have been added on the first floor to reduce access to the computing facility.

Badge readers are located at the front door, back door, east warehouse door, west warehouse door, second floor east, second floor west, second floor service closet, third floor east, third floor west, fourth floor east, fourth floor west, elevator glass doors east, elevator glass doors west, maintenance room, and third floor server room. Access to any area other than an employee's assigned work area must be approved via the COT-F019 form.

The software controlling the doors is equipped to monitor all activity concerning physical entry, doors open for significant periods of time, invalid badge attempts and other activities. Reports can be created for anything from all activity on a specific door, to a particular individual and all access attempts at any location.

To help ensure badge access is kept up-to-date, a formal process exists for entering/departing employees/contractors/vendors. Effective 4/13/09, all employee entrances, exits and modifications will be requested through the IT service management application. This is accomplished by incorporating the Employee Entrance/Exit form into the existing F181 form. This not only helps assist that badges are disabled, but that all access to any computer resources assigned via the COT-065 is revoked.

Delivery/Loading Areas

The delivery and loading areas are controlled and isolated from information processing. Deliveries must be acknowledged by appropriate building maintenance staff before they can be accepted and the delivery door opened.

Since other state agencies use the mainframe for many of their computing needs, COT frequently must use tapes provided by that agency. It is the responsibility of the agency to pick up and/or

drop off those tapes for COT's use. The forms used are COT-F082 (Authorization for release of reel tapes, cartridges and diskettes) and COT-F033 (Tape Library Storage Request). The tapes cannot be left on the front desk for quick pickup. The agency must wait for an operator to bring the tape down, and also must wait for the operator to come pick it up. The forms are signed by the person from the agency picking up/dropping off the tapes. It is not necessary for this person to sign the visitor's log, as they never leave the front desk area.

Environmental Protection

The environmental protection is divided into three (3) areas of control: UPS, HVAC and Fire Protection/Halon.

UPS

An Uninterruptible Power Supply (UPS) services all critical electrical systems including the COT computer systems. The UPS system was improved recently. The CDC is now split between two parallel UPS systems; one is a redundant dual rotary system and the other is two static UPS units. Either side of the UPS is capable of supplying the CDC's electrical requirements.

HVAC

The temperature control for the building is also provided by the CUPS facility. It is a dual deck system providing a mixture of heated, fresh, and chilled air. The system was designed to operate in a building facility of computer equipment. Over the last couple of years, the HVAC controls have been updated to meet standards, including humidity control. The two large control boxes for each air handling unit were upgraded. There is 24/7 monitoring of air handlers by Capecon through the automated logic program. The system is monitored 24/7 for any changes the environmental controls. This is checked out and compared with a temperature gun every 6 months under a control PM. If something does not look right, it is investigated as well as the PM.

Fire Protection/Suppression System/Halon

The Commonwealth Office of Technology (COT) facility located at 101 Cold Harbor Drive, Frankfort, Kentucky is protected by a combination of automatic fire detection and suppression systems. The main fire alarm control panel (FACP) provides the systems central processor unit and houses the main user interface controls and text alarm and signal display (system was upgraded about 1 year ago). The FACP device include 37 smoke detectors, 2 duct detectors, 7 manual pull stations, 27 audio/visual devices, and 12 visual only devices. There is a remote annouciator located at the security officer's desk and a remote computer-based annouciator at the data center's command console. Both of these units display events in real time; the annouciator at the security desk also provides automatic and manual door control for the emergency exits. The FACP also provides the automatic local, central station, and proprietary signal notifications: 1) the local audio-visual devices are located throughout the facility; 2) the internal digital fire alarm communicator transmitter (DACT) transmits alarm to the contracted central fire alarm monitoring service via two (primary and secondary) dedicated phone lines; and 3) the internal data interface communications card provided automatic electronic mail notification to key

facility and process managers. The FACP communicates and or controls both elevators for fire recall and operations, provides zoned tamper and flow signals for the water based sprinkler system, provides signal integration and reporting for the multiple chemical based (Halon) suppression systems, and provides system interface for air-hander and environmental control systems. The wet sprinkler system provided protection for the first and second floor administrative and storage areas, as well as the two exit stair cores (there are zoned shut off valves for each of the 4 floor). There are 10 Halon 1301 suppression system located in the facility. One is located on the first floor's main electrical/UPS/mechanical rooms, which protects four zones with 2428 pounds of halon agent. The second through fourth floors each have three systems each, protecting the main data area and the separate electrical and communication (phone) rooms with 2820 pounds of agent each. The electrical and telephone communication areas are monitored with cross-zoned heat and/or smoke detectors. The main data rooms use a central air sampling system piped throughout the protection area to monitor for smoke particulates. The air sampling system is set for two separate escalating thresholds to sound the pre-alarm and system "dump" notifications. Each system has a "dead-man" style abort switch. All systems are maintained in accordance with prescribed codes and standards. The fire alarm system is inspected on a quarterly schedule. The chemical special hazards systems (Halon) are inspected and tested semi-annually under the umbrella of the maintenance agreement as well. Annual inspection and testing of the water based sprinkler system is also conducted. Under separate provisions, annual inspection of the installed hand portable fire extinguishers within the facility is also carried out.

COT Contingency Planning

Documented procedures for re-establishing computer operations and critical applications in the event of disaster are detailed in the Disaster Recovery Manual. These procedures include off-site storage of system and application files at a contracted off-site location. Instructions in this manual include, but are not limited to, general information (statements, requirements, and responsibilities), recovery preparations, recovery actions and return to normal processing procedures. A copy of the Disaster Recovery Manual and the instructions are stored off-site at a secure underground storage facility and can be accessed via a secure web site. The agency responsible for each application also provides a designated representative who is responsible for the recovery or restoration of the application system.

The DR Coordinator, with designated COT staff and independent auditors, visit the Commonwealth's offsite storage vendor at least once during the fiscal year. The Director of Business Development at the offsite location leads the tour and usually includes the document and electronic media storage areas, as well as other facilities.

COT, recognizing the need to strengthen its ability to recover the Commonwealth's critical systems and functions in the event of a disaster, contracted with a knowledgeable vendor to assist in the initial development of a disaster recovery plan. This project was started in July 2002, and was completed in February 2003. The plans include systems running on the mainframe computer, and agency applications running on UNIX or Windows based servers that are maintained by COT. The plans also address networking and those functions running on

enterprise servers (email, firewall, etc.) maintained by COT. The agencies/business owners identify their critical systems and functions for inclusion in the DR Plan.

In July 2003, COT contracted with a new vendor to provide hot/cold site services in the event of a disaster. The contract was expanded from previous contracts in that recovery for distributed systems is now available at the hot site. Previously, only critical applications residing on the mainframe platform were included in a hot-site contract. This new contract significantly expanded COT's ability to recover all critical systems in the event of a disaster. The contract includes services for Intel servers, UNIX servers, mainframe, and data circuits to a COT building to be used for testing purposes. After a review of the monthly cost required to provide hot site services for network equipment; i.e., hubs, routers, firewalls, etc., a management decision was made to exclude network equipment from the hot site contract. The savings from not including this in the new contract could be better spent in building the infrastructure required to provide network redundancy (See section on KIH for more detail).

COT conducts Disaster Recovery tests biannually, rotating the test between distributed systems and mainframe systems. In November 2004, distributed systems were tested at the hot-site location. The backup management server, which is critical to the recovery of many systems, was also included as part of this test. In June 2005, distributed systems were again tested. The TSM server was also included. Another DR test was conducted in December 2005, this time on critical mainframe systems. Distributed systems and the backup management server were recovered within the 48-hour allotted recovery timeframe in February 2006. This was the first *remote* recovery of distributed systems from the Plain City Recovery Center. In July 2006, mainframe applications were again tested. A DR test was conducted in February 2007 covering COT's distributed systems. The last test dates were:

November 2007 – Mainframe System	March 2008 – Open Systems
September 2008 – Mainframe Systems	April 2009 – Open Systems

Control Objectives and Related Controls

COT's control objectives and their related controls are included in Section III, "Information Provided by Potter & Company LLP," to eliminate the redundancy that would result from listing them in this section 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 COT's description of controls.

User Control Considerations

COT's internal controls are designed with the assumption that certain internal controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at COT. User auditors should consider whether the following controls have been placed in operation at user organizations:

1. Controls should be established to ensure that agency employees are adhering to Enterprises Policies.

2. Controls should be established to ensure agencies are maintaining appropriate separation of duties.

3. Controls should be established to ensure that the agency strategic planning documents follow the SITP and agencies actively participate in implementing the strategies defined in the SITP.

4. Controls should be established to ensure that agencies properly use COT forms, policies, and procedures when interacting with or requesting items from the COT.

5. Controls should be established to ensure that employees are adequately trained.

6. Controls should be established to ensure that all requests sent to COT are prioritized.

7. Controls should be established to ensure that if time and budget estimates are presented by the COT, the time and budget estimates are reviewed and approved by the appropriate individuals at the agencies.

8. Controls should be established to ensure that agencies properly test application changes prior to implementing changes or actively participate in user acceptance testing with the COT.

9. Controls should be established to ensure that agencies creating and forwarding changes to COT for promotion into production, control the movement of changes to COT.

10. Controls should be established to ensure that software supported by outside vendors is properly tested prior to implementation of the software application or change.

11. Controls should be established to ensure that the agencies, when responsible, make only approved, tested and documented changes to software when appropriate.

12. Controls should be established to ensure that the agencies, when responsible, determine and authorize access to programming source and programming load libraries/directories to ensure proper segregation of duties between development and change control.

13. Controls should be established to ensure that agencies, when responsible, install only appropriate system software.

14. Controls should be established to ensure that the agencies, when responsible, make only approved, tested, and documented changes to system software.

15. Controls should be established to ensure that the agencies participate or review change control documentation at the COT for the weekly change control meetings.

16. Controls should be established to ensure that agencies, when responsible, install only appropriate system software in the network environments.

17. Controls should be established at the agencies for reviewing the COT Agency Mainframe Security Agreement and ensuring compliance with the terms of the agreement.

18. Controls should be established at the agencies for designating an authorized security contact for the mainframe.

19. Controls should be established for those agencies that are responsible for their own mainframe security administration to restricting access to data sets and programs and for monitoring security reports provided by the COT.

20. Controls should be established for those agencies that are responsible for their own mainframe security administration to review and monitor the mainframe job schedule listing to identify and remove users that are no longer required to have access to the system.

21. Controls should be established for those agencies that are responsible for resetting their own passwords on the mainframe to ensure that this activity is appropriately restricted.

22. Controls should be established at the agencies to ensure that only authorized individuals have access to their programs and data in both the mainframe and client/server environment.

23. Controls should be established at the agencies to ensure that agency employees are using strong passwords and adhering to COT recommended standards for passwords.

24. Controls should be established at the agencies to ensure that agency employees are appropriately approved to access systems at COT.

25. Controls should be established at the agencies to ensure that agency employees are appropriately removed from the systems at the COT upon termination of their employment or changes in responsibilities.

26. Controls should be established at the agencies to ensure that agency employee access to applications and data are properly controlled by performing periodic user access review.

27. Controls should be established at the agencies to ensure that each generic user identifier is assigned to the appropriate authorized individual.

28. Controls should be established at the agencies to ensure that the agencies are adhering to COT enterprise security standards.

29. Controls should be established at the agencies to ensure that proper firewall rule sets are in place to protect the agency network from malicious content that may originate from within the KIH intranet.

30. Controls should be established at the agencies to ensure that proper controls exist to only permit authorized individuals VPN access.

31. Controls should be established at the agencies to ensure that vendor default accounts are removed or properly secured.

32. Controls should be established to ensure that agency data residing on tapes or cartridges is backed up by the agency and communicated to COT for off-site storage.

33. Controls should be established to ensure that the agency informs the COT of the criticality of the data, files, programs, etc. that should be backed up and the off-site rotation for these items.

34. Controls should be established to ensure that the agency designates a disaster recovery coordinator that is responsible for coordination of recovery procedures with the COT.

35. Controls should be established to ensure that the agencies participate in business impact analysis with the COT to determine risks and recovery priorities.

36. Controls should be established to ensure that agency batch jobs are properly scheduled and run in accordance with the schedule.

37. Controls should be established to ensure that only properly authorized individuals have access to maintain batch job schedules and libraries.

38. Controls should be established to ensure that agencies monitor and document ABENDs that occur related to their applications and batch jobs.

39. Controls should be established to ensure that reports generated by COT are received and distributed to the appropriate individuals in a timely manner.

40. Controls should be established at the agencies to ensure that only authorized individuals have access to their programs and data in both the mainframe and client/server environment.

41. Controls should be established at the agencies to ensure that data transmissions are complete, accurate, and secure.

42. Controls should be established to ensure that the agencies reconcile the number of records sent to COT with the number of records actually received and processed by COT.

43. Controls should be established to ensure that the agencies reconcile the number of records received at the agency with the number of records actually sent by COT.

SECTION III

Information Provided by Potter & Company LLP

Control Objectives, Related Controls and Service Auditor's Tests of Operating Effectiveness

This section presents the following information provided by the Commonwealth Office of Technology.

- Control objectives specified by the management of the Commonwealth Office of Technology.

- Controls established and specified by the Commonwealth Office of Technology to achieve the specified control objectives.

Also included in this section is the following information provided by the service auditor, Potter & Company LLP:

- A description of the testing performed by the service auditor to determine whether the Commonwealth Office of Technology controls were operating with sufficient effectiveness to achieve the specified control objectives. The service auditor determined the nature, timing and extent of the testing performed.

- The results of the service auditor's tests of operating effectiveness.

General Computer Controls

Manage IT Activities			
Control Objective 1: Controls provide reasonable assurance that the Commonwealth Office of Technology (COT) provides policies and procedures, adequate supervision and proper segregation of duties to support the State's IT environment.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
1.01	Strategic planning and major accomplishment documents are updated periodically.	Inspected the Information Technology strategic plan to determine existence and that it is current.	No exceptions noted.
1.02	The organization's policies and procedures have been documented and are provided to COT personnel.	Inspected the Commonwealth of Kentucky Employee Handbook and the Security Standard Procedures Manual to determine that policies and procedures exist and employees are required to read these and sign an acknowledgement upon hire.	No exceptions noted.
1.03	Employees are required to sign an acknowledgement confirming they have received, understand and accept relevant Information Technology (IT) policies, standards and procedures.	Inspected signed acknowledgement of responsibility forms for a sample of new hires to determine that personnel are being informed of policies.	**Exception noted.** 8 of 18 (44%) new hires sampled did not have signed acknowledgement of responsibility forms. **Management's response:** **Finance & Administration Cabinet, Division of Human Resources, realizes there may be a delay in receiving the personnel documents and placing them within the personnel files. Corrective measures, such as process mapping and the proposal of checklists, are being reviewed to assure compliance.**
1.04	Standards have been established to enforce and ensure appropriate segregation of	Inspected the organization charts to determine that responsibilities are defined and that the organizational	No exceptions noted.

Manage IT Activities			
Control Objective 1: Controls provide reasonable assurance that the Commonwealth Office of Technology (COT) provides policies and procedures, adequate supervision and proper segregation of duties to support the State's IT environment.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
	duties in assigning roles and responsibilities.	structure supports segregation of duties.	
1.05	Responsibilities have been allocated to appropriately skilled and experienced staff members under the direction of the Commonwealth Office of Technology Commissioner.	Inspected a sample of job descriptions to determine that the job descriptions identified the responsibilities of each position and required an appropriate set of skills and experience to perform the assigned responsibilities.	No exceptions noted.
1.06	Job descriptions are provided to ensure that staff members have a complete and appropriate description of required skills, competencies and qualifications.	Inspected a sample of job descriptions to determine that the job descriptions identified the responsibilities of each position and required an appropriate set of skills and experience to perform the assigned responsibilities.	No exceptions noted.
1.07	Adequate supervisory practices have been implemented within the IT function to ensure roles and responsibilities have been properly executed.	Inspected a sample of COT employee personnel files to determine that annual performance evaluations were completed noting roles and responsibilities were properly executed.	**Exception noted.** 2 of 15 (13%) personnel files sampled did not have a performance evaluation in the personnel file. **Management's response:** **COT, Human Resources, will ensure all evaluations are placed within COT personnel files by initiating a new checklist process. A spreadsheet has been developed containing the names of all COT employees and the responsible party for their evaluations. This spreadsheet will be used to keep track of evaluations turned in for EACH/EVERY**

Manage IT Activities			
Control Objective 1: Controls provide reasonable assurance that the Commonwealth Office of Technology (COT) provides policies and procedures, adequate supervision and proper segregation of duties to support the State's IT environment.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			evaluation period to ensure compliance to the control.
1.08	Employees are provided with ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational controls.	Inquired of the System Consultant - IT to determine that continuous training and career development is provided.	No exceptions noted.
1.09	Job performance evaluations are provided to employees to ensure core competencies, company values and skills required for each role are being satisfactorily met.	Inspected the Employee Evaluation Handbook to verify that personnel are subject to annual performance evaluations. Inspected a sample of COT employee personnel files to determine that performance evaluations were completed annually.	**Exception noted.** 2 of 15 (13%) personnel files sampled did not have a performance evaluation in the personnel file. **Management's response:** **COT, Human Resources, will ensure all evaluations are placed within the COT personnel file by initiating a new checklist process. A spreadsheet has been developed containing the names of all COT employees and the responsible party for their evaluations. This spreadsheet will be used to keep track of evaluations turned in for EACH/EVERY evaluation period to ensure compliance to the control.**
1.10	Procedures for termination of employment are documented and contain required	Inspected the COT Exiting Employee Procedure Memo to determine that there is a defined process for notification of	**Exception noted.** 1 of 5 (20%) employees

Manage IT Activities			
Control Objective 1: Controls provide reasonable assurance that the Commonwealth Office of Technology (COT) provides policies and procedures, adequate supervision and proper segregation of duties to support the State's IT environment.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
	elements.	terminated employees. In addition, inspected termination procedures implemented on April 13, 2009 to determine that formal terminations procedures had been implemented. Inspected a sample of termination forms to determine that notification of termination was processed in accordance with the policy.	terminated after April 13, 2009 did not have a completed termination form. **Management's response:** **COT management recognizes the importance of following all established procedures regarding departing employees. A new Employee Entrance/Exit process has been initiated to ensure compliance.**

Manage Facilities			
Control Objective 2: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals and that assets are appropriately safeguarded from environmental hazards.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
2.01	Policies and procedures are in place to govern requesting and granting access to the data center.	Inspected the Security Standard Procedures Manual and inquired of the Security Administration Branch Manager and the System Engineer – IT to determine policies and procedures are in place to govern requesting and granting access to the data center.	No exceptions noted.
2.02	Formal access requests are completed and authorized by management.	Inspected a sample of new hire employees and transfers to determine that access request forms were completed and authorized by a Branch Manager and/or the employee's Division Director.	No exceptions noted.
2.03	Access to sensitive IT locations is restricted through key cards on interior and exterior entries to current COT employees.	Observed that access to sensitive IT facilities is restricted through key cards on interior and exterior entries. Compared the key card access list to the current employee listing to determine that interior and exterior entries are restricted to current COT employees.	**Exception noted.** Five terminated employees with active badges to the COT data center facility. **Management's response:** **COT, Security Administration Branch, recognizes the importance of deactivating badge access for all departing employees. To meet that goal, a new Employee Entrance/Exit process has been initiated and will be used for all COT employees.**
2.04	A periodic review is performed to assess and recertify users' access and authorities.	Inspected the Security Standard Procedures Manual to determine that procedures exist to review badges that are inactive over 90 days. Inquired of the System Engineer – IT to determine that	**Exception noted.** There was no periodic review performed of inactive badges for two of the four quarters

Manage Facilities			
Control Objective 2: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals and that assets are appropriately safeguarded from environmental hazards.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
		quarterly badge reviews of inactive badges is performed.	within the period. **Management's response:** **COT, Security Administration Branch, agrees with the importance of periodic reviews of inactive badges. It is important to note that the control specifically states in section 13.2.2 of the SSPM that the audit will be conducted on restricted areas access. COT will continue the periodic audit of inactive badges with access to sensitive areas not used in over 90 days. COT will also be revising the timeframe required for the audits as stated in 13.2.2.**
2.05	Policies and procedures are in place for recording, monitoring, reporting and resolving physical security incidents.	Inspected the Security Standard Procedures Manual to determine that policies and procedures exist related to the recording, monitoring, reporting and resolving of physical security incidents. Observed the badge access monitoring system to determine that the security system records the badge and employee name when cards are used. Inquired of Security personnel to determine that system reports are reviewed for physical security incidents and that incidents are documented and resolved timely.	No exceptions noted.
2.06	The data center is protected by defined security perimeters coupled with	Observed the data center is protected by a defined security parameter.	No exceptions noted.

Manage Facilities			
Control Objective 2: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals and that assets are appropriately safeguarded from environmental hazards.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
	appropriate surveillance.	Observed that cameras are placed on the interior and exterior of the data center facility to provide monitoring of building entrances and sensitive areas. Observed that cameras are located on platforms that are stable and secure. Observed Security Administration personnel to determine that onsite monitoring of cameras is taking place and images are recorded.	
2.07	Policy requires visitors to sign a visitor log and be escorted at all times by a member of COT while onsite.	Inspected the Security Standard Procedures Manual to determine that visitors are required to be escorted at all times by a member of COT while onsite. Observed that individuals granted temporary access were escorted and activities monitored. Inspected the Visitor Daily Log to determine the log was utilized.	No exceptions noted.
2.08	Uninterruptible power supplies (UPSs) are utilized for power fluctuations and outages.	Observed the existence of UPS systems and a backup generator for the data center, which provide electrical power in the event of a power interruption.	No exceptions noted.
2.09	Fire protection and detection equipment and systems are in place to detect environmental threats.	Observed the existence of fire detection and suppression systems throughout the data center which are designed to detect early stages of a fire.	No exceptions noted.
2.10	Environmental controls are tested on a regular basis.	Inspected environmental system inspection reports to determine they are tested regularly.	No exceptions noted.
2.11	HVAC devices are in place and monitored to detect environmental changes.	Observed HVAC systems to determine that devices have been implemented within the data center. Inspected a sample of Temperature and Humidity Log Sheets to determine that environmental changes are being monitored.	No exceptions noted.

Manage Facilities			
Control Objective 2: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals and that assets are appropriately safeguarded from environmental hazards.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
2.12	Policies and procedures are in place to require personnel to display visible identification and prevent the issuance of identity cards or badges without proper authorization.	Inspected the Security Standard Procedures Manual to determine that personnel are required to display visible identification at all times and to obtain authorization for the issuance of identity cards or badges.	No exceptions noted.
2.13	Homeland Security procedures are updated periodically and are provided to employees.	Inspected the COT's Response to the Homeland Security Initiative and an internal website to determine that Homeland Security procedures exist and are provided to employees.	No exceptions noted.

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
3.01	Configuration baselines for hardware and software components are defined and documented.	Inquired of Security Administration Branch personnel and UNIX and Windows Administrators to determine configuration baselines are defined and documented. Inspected UNIX configuration files to determine systems were configured in accordance to defined standards.	**Exceptions noted.** Configuration baselines have not been developed for Windows, Mainframe and UNIX systems. All of the 4 sampled UNIX servers were running insecure and unnecessary services such as UUCP, Telnet, TFTP, FTP and Finger. **Management's response:** **COT, Operating Systems, recognizes the need to make the operating environment as secure as possible. Therefore, the servers listed, as well as the remainder servers in the environment, will have those ports reviewed. Any servers without a valid business need will have those services turned off.**
3.02	Security design features enforce password rules (e.g., maximum length, characters, expiration and reuse).	Inspected mainframe system security reports to determine security design features enforce password rules on mainframe systems. Inspected UNIX and Windows security parameters for a sample of COT servers to determine security design features enforce password rules.	**Exception noted.** Password parameters on the sampled Mainframe, Windows and UNIX servers were not set in accordance with documented policy.

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			In addition, four individuals were identified with access to switch to the administrator (root) account without using a password on the sampled UNIX servers. Furthermore, the following issues were noted with the sampled Windows servers: - 17,095 accounts have never been logged into - 1,576 accounts did not have a password expiration - 2,521 accounts had not changed their password within the past 31 days. **Management's response:** **Mainframe Security, Security Administration Branch, recognizes the importance of keeping password parameters in align with policy and procedures. In prior releases of mainframe security management software, changing password parameters on the mainframe was not available. Now that the current version supports this option, COT will be changing the Minimum**

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			Password Interval in accordance with the documented policies and standards. **COT's Operating Systems: For Windows those domains will be reviewed and brought into compliance with the current policy. For Unix, some reconciliation will need to be made as Unix passwords operate on a week rather than day basis. OS will research on how best to implement.**
3.03	System settings are configured to disable inactive users after 60 days on mainframe systems.	Inspected mainframe system security reports for a sample of agencies to determine that inactive user accounts over 60 days are automatically disabled by system software.	No exceptions noted.
3.04	User account management procedures address requesting, establishing, issuing, suspending, modifying and closing user accounts and documentation of related user privileges.	Inspected the COT Entrance and Exiting Employee Procedure Memos to determine that there is a defined process for requesting, establishing, issuing, suspending, modifying and closing user accounts. Inspected mainframe system security reports for a sample of agencies and compared it to the terminated user listing to determine that user accounts were suspended or closed timely. Inspected UNIX and Windows user access listing for a sample of servers and compared them to the terminated user listing to determine that user account management procedures are in place to address suspending and closing user accounts and related user privileges in a timely manner.	**Exception noted.** 18 of 75 (24%) terminated employees were identified with active accounts on the sampled Windows servers. 7 of 75 (9%) terminated employees were identified with active accounts on the sampled UNIX servers. **Management's response:** **With the establishment of the new Employee Entrance/Exit**

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			System, COT management recognizes the importance of following all procedures regarding departing employees. This tool will enhance communications regarding the notification to terminate activate accounts on all COT platforms. COT will also work with customer agencies to improve their notification of agency staffing changes, allowing COT to make updates in a timely manner. A periodic cleanup of accounts will also be implemented to benefit the server environment.
3.05	Access is authorized by management.	Inspected a sample of user access request forms to Mainframe, UNIX and Windows systems to determine that new user accounts were approved by management.	**Exception noted.** New hire access request forms were not maintained for sampled new hires from July 1, 2008 through February 1, 2009. Six of eight (75%) employees hired after February 1, 2009 did not have new hire access request forms completed. **Management's response:** **COT management recognizes the importance of following all**

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			established procedures regarding new employees. To meet that goal, a new Employee Entrance/Exit process has been put in place. Included in the new process is the completion of the COT-F181. Enforcing this process throughout COT will ensure all necessary documentation is included for a new hire.
3.06	Administrator accounts are limited to personnel approved by management.	Inspected mainframe system security reports for a sample of agencies to determine that administrator access was consistent job responsibilities. Inspected UNIX and Windows configuration files and user access listing for a sample of servers to determine that administrator access was consistent with job responsibilities.	No exceptions noted.
3.07	A periodic review is performed to assess and certify the appropriateness of user access and authorities.	Inquired of Security Group personnel to determine that an annual access review of Mainframe users was performed. Inquired of UNIX and Windows Administrators to determine that an annual access review of users was performed.	**Exception noted.** There was no periodic access review of users on the sampled Mainframe, UNIX and Windows systems. **Management's response:** **User access review is defined as a role of the data custodian in section 2.2 of the SSPM. COT recognizes the validity of these reviews. Therefore, we will initiate a new process for**

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			agency user reviews. These procedures will require the business owners to work closely with COT. A baseline review will be done at the start of this process. A list of accounts will be provided to the business owner(s) of the machine, with a given deadline to get back with COT regarding any changes. Quarterly runs will be done to keep the accounts up to date.
3.08	System user accounts are required to be uniquely identifiable.	Inspected mainframe system security reports to determine that system user accounts are uniquely identifiable. Inspected UNIX and Windows user access listing for a sample of servers to determine that user accounts are required to be uniquely identifiable.	No exceptions noted.
3.09	Approved roles delineate user access based upon rule of least privileges.	Inspected mainframe system security reports for a sample of agencies to determine that access is based upon rule of least privilege. Inspected UNIX and Windows group configuration for a sample of servers to determine that roles delineate access based upon rule of least privilege.	No exceptions noted.
3.10	Vendor-supplied accounts, including the guest account, has been appropriately safeguarded or removed.	Inspected mainframe system security reports for a sample of agencies to determine that unnecessary vendor-supplied accounts have been safeguarded. Inspected UNIX and Windows user access listing for a sample of servers to determine that vendor-supplied accounts have	No exceptions noted.

Ensure Systems Security – Systems			
Control Objective 3: Controls provide reasonable assurance that systems (Mainframe, UNIX, Windows) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
		been safeguarded or removed.	
3.11	Audit trails capture specific transaction information such as user identification, type of event, date and time, success or failure indication and affected object.	Inspected mainframe system security reports for a sample of agencies to determine that audit trails capture transaction information. Inspected UNIX and Windows audit results for a sample of servers to determine whether these capture administrative level activity, including date and time and success or failure of specified events.	**Exception noted.** While logging was enabled, none of the 13 Windows servers sampled were configured in accordance with the COT Security Department recommended settings. **Management's response:** **COT recognizes the need for adequate logging and audit trails. COT has reviewed several products for event log management and has submitted a request for funding to purchase the tools needed. Due to the current budgetary restrictions, the funding may not be available.**
3.12	Access control software (ACF2, RACF and TopSecret) is installed and operational on the Mainframe.	Inspected mainframe system security reports to determine that access control software is being utilized.	No exceptions noted.

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
4.01	Database configuration baselines are defined and documented.	Inquired of the Information Systems Manager for the Database Management group to determine whether configuration baselines are defined and documented.	**Exceptions noted.** Database configuration baselines have not been developed. **Management's response:** **To remediate the lack of documentation concerning Database configuration baselines, COT will be scheduling meetings with the database owners and documenting baselines of each major COT-supported database technology. The documentation will then be available on the enterprise collaboration portal.**
4.02	Security design features facilitate password rules (e.g., maximum length, characters, expiration and reuse).	Inquired of Database management to determine that Oracle password management functions are enforced by the UNIX systems. Inquired of Database management to determine that SQL password management functions are enforced by the Windows systems. Inquired of Database management to determine that Online database password management functions are enforced by the mainframe security software. Inspected UNIX and Windows security parameters for a sample of COT servers to determine security design features	No exceptions noted.

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
		enforce password rules. Inspected mainframe system security reports to determine security design features enforce password rules on mainframe systems.	
4.03	User account management procedures address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges have been documented.	Inspected the COT Entrance and Exiting Employee Procedure Memos to determine that there is a defined process for requesting, establishing, issuing, suspending, modifying and closing user accounts. Inspected database user access listings for a sample of various databases and compared it to the terminated user listing to determine that user account management procedures are in place to address suspending and closing user accounts and related user privileges in a timely manner.	**Exception noted.** One account was identified for a terminated database administrator on the sampled SQL databases. **Management's response:** **With the establishment of the new Employee Entrance/Exit System, COT management recognizes the importance of following all procedures regarding departing employees. This tool will enhance communications regarding the notification to terminate activate accounts on all COT platforms. COT will also work with customer agencies to improve their notification of agency staffing changes, allowing COT to make updates in a timely manner.**
4.04	Access is authorized and appropriately approved by management.	Inspected a sample of user access request forms to databases to determine that new user accounts were formally approved by management.	**Exception noted.** New hire access request forms were not maintained

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			for sampled new hires from July 1, 2008 through February 1, 2009. Six of eight (75%) employees hired after February 1, 2009 did not have adequate hire access request forms completed. **Management's response:** **COT management recognizes the importance of following all established procedures regarding new employees. To meet that goal, a new Employee Entrance/Exit process has been put in place. Included in the new process is the completion of the COT-F181. Enforcing this process throughout COT will ensure all necessary documentation is included for a new hire.**
4.05	Database Administrator (DBA) accounts are limited to personnel approved by management.	Inspected a sample of DBA account listings to determine that access is limited to authorized personnel based on job responsibilities.	**Exception noted.** Of the 27 DBA accounts, 14 (52%) employees had DBA rights to a database, which was not consistent with their job responsibilities. In addition, three out of 10 (30%) individuals were

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			identified with duplicate accounts on one sampled database. **Management's response:** **Inappropriate COT staff was shown to have DBA rights on the production database. COT took the following actions in order to correct this finding. A request was submitted to the Commonwealth Service Desk to revoke access to this database for the inappropriate COT staff. Research was conducted to show if appropriate requests and approvals were obtained and OAD management was not able to identify the actual request for access or approval.** **It has been discovered that because of the way database permissions are grouped, COT staff has been granted access to certain databases without management request or approval. For example, a request may be submitted for access to one dataset and as a result of the request, permissions are granted for the entire group.** **As a result, OAD has over the**

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			last few months conducted extensive reviews of production databases to insure that developers do not have access to production data, unless an exception has been identified and proper paperwork has been submitted. Ongoing diligence and research will continue to ensure proper policies are enforced. If there is an access issue, multiple areas within COT will work together to determine who authorized the permissions.
4.06	A periodic review is performed to assess and certify the appropriateness of user access and authorities.	Inquired of Database Management to determine that an annual access review of users was performed for all databases.	**Exception noted.** There was no periodic access review of users on the sampled databases. **Management's response:** **The new COT entrance/exit process will be amended to include the review of database access. If an employee is entering/exiting COT, the appropriate section of the entrance/exit form will be completed to grant or deny database access.**
4.07	System user accounts are required to be	Inquired of the Information Systems Manager for the Database	No exceptions noted.

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
	uniquely identifiable.	Management group to determine that Oracle user ID management functions are performed by the UNIX systems. Inquired of the Information Systems Manager for the Database Management group to determine that SQL user ID management functions are performed by the Windows systems. Inquired of the Database Management group to determine that database user ID management functions are performed by the external security software. Inspected mainframe system security reports to determine that system user accounts are uniquely identifiable. Inspected UNIX and Windows user access listing for a sample of servers to determine that user accounts are required to be uniquely identifiable.	
4.08	Vendor-supplied accounts, including the guest account, has been appropriately safeguarded or removed.	Inquired of the Database Management group to determine that database user ID management functions are performed by the UNIX systems. Inquired of the Database Management group to determine that database user ID management functions are performed by the Windows systems. Inquired of the Database Management group to determine that mainframe database user ID management functions are performed by the external security software. Inspected mainframe system security reports for a sample of agencies to determine that unnecessary vendor-supplied accounts have been safeguarded. Inspected UNIX and Windows user access listing for a sample of servers to determine that vendor-supplied accounts have	No exceptions noted.

Ensure Systems Security – Database			
Control Objective 4: Controls provide reasonable assurance that databases are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
		been safeguarded or removed.	

Ensure Systems Security – Network Components			
Control Objective 5: Controls provide reasonable assurance that network components are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
5.01	Design and architecture of the network environment is adequately documented.	Inspected the network diagrams obtained from the Network Administrator to determine that design and architecture of the network environment is documented.	No exceptions noted.
5.02	Firewall management of infrastructure is centralized and data security functions are segregated with regard to operations and control.	Inspected organizational charts to determine that security functions are segregated with regard to operations and control. Inspected user access list for the sampled firewall configurations to determine that access was consistent with job responsibilities.	No exceptions noted.
5.03	Complete and current network "Rules Based" policies are maintained in order to ensure network integrity, security and on-going maintenance.	Inspected firewall rules configuration for a sample of firewalls to determine that comprehensive and current network "Rules Based" policies are documented and maintained.	No exceptions noted.
5.04	Firewalls are adequately configured in compliance with security policies and standards.	Inspected the Firewall and Virtual Private Network Policy to determine that policies and standards have been documented to guide firewall configuration. Inspected firewall rule configurations for a sample of firewalls to determine they were maintained in accordance with policies and standards.	No exceptions noted.
5.05	Firewall rules have been established to properly restrict inbound access to the COT network.	Inspected firewall rule configurations for a sample of firewalls to determine that rules have been established to restrict inbound access to the COT network.	No exceptions noted.
5.06	VPN policies and procedures are in place to restrict and control user access.	Inspected security policies and procedures to determine that they have been documented, maintained, and include provisions related to VPN. Inspected VPN user access list to determine that access was consistent with job responsibilities.	No exceptions noted.

Ensure Systems Security – Network Components			
Control Objective 5: Controls provide reasonable assurance that network components are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
5.07	Encryption is utilized for non-console administrative access such as VPN.	Inspected VPN configuration settings to determine that encryption is utilized for non-console administrative access.	No exceptions noted.
5.08	VPN/dial-up logs and reports user activity.	Inspected a sample of VPN logs to determine that user activity is being automatically logged and reported.	**Exception noted.** A process for monitoring invalid login attempts and investigation of these attempts has not been put in place. **Management's response:** **Both failed and successful VPN login attempts are captured. They can be viewed via "RVAC". Commonwealth Service Desk monitors this tool. It is noted that the tool is not always available. Other VPN options exist that operate under a standard Windows based environment which could provide the required automated monitoring and alerting. The potential exists to write a stored procedure to inspect the database for multiple failed attempts. This activity would be a DBA responsibility. This issue involves several areas within COT besides NetOps. The Service Desk and DBA teams could also be involved.**

Ensure Systems Security – Network Components			
Control Objective 5: Controls provide reasonable assurance that network components are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
5.09	Intrusion detection system(s) are in place to actively monitor the network.	Inspected a sample of monitoring reports to determine that intrusion detection system(s) are in place to actively monitor the network.	No exceptions noted.
5.10	Wireless access points have established settings to restrict inbound access to the COT network.	Inspected wireless access point configuration settings to determine access to the COT network is properly restricted.	No exceptions noted.

Manage Backup and Recovery			
Control Objective 6: Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
6.01	Policies and procedures are in place to guide the backup of systems, applications, data and documentation.	Inspected documented procedures for backup and retention of data files to determine these provide guidance for backing up systems, applications, data and documentation. Inspected backup parameters for a sample of systems via the job scheduling software to determine that backups are configured in accordance with requirements.	**Exception noted.** Procedures related to backup processes for Windows, Mainframe and UNIX systems have not been formally documented and approved by management. **Management Responses:** **COT is in agreement that it is vital to document the backup processes for Windows, Mainframe and UNIX systems. To remediate COT's non-compliance, meetings with the various server managers (windows, unix, mainframe) will occur to document COT's backup baseline, strategy and guidelines. The documentation will then be placed on the enterprise collaboration portal. This and the database guidelines should be in place by October 31, 2009.**
6.02	A schedule exists for taking backups offsite in accordance with established policies and procedures.	Inspected Media Pull Lists, Tape Ejection Reports, Tape Work Orders, and Offsite Storage Shipment notices for a sample of systems to determine that COT is sending tapes to an offsite location and the offsite location was appropriately shipping tapes back to COT.	No exception noted.

Manage Backup and Recovery			
Control Objective 6: Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
		Inspected job scheduling software to determine that COT replicates agency backup in accordance with the frequency and requirements documented in the policies and procedures.	
6.03	Backup logs are reviewed to confirm that infrastructure data and software are successfully backed up.	Observed backup software on mainframe and midrange systems to determine that backup successes and failures are logged. Inspected email notification and checklists to determine that individuals are automatically notified of the status of backup jobs.	No exceptions noted.
6.04	Regular testing of tapes is performed to ensure the quality of backups and media.	Inquired of the Storage Management team to determine that annual testing of tapes occurs during the disaster recovery process. Inspected the results of the disaster recovery test to determine that the test was performed as scheduled and that testing of tapes is performed.	No exceptions noted.
6.05	Backup data is protected when taken offsite and while in transport.	Observed pickup/delivery of offsite tapes by third party vendors to determine that backup data is protected while in transport.	No exceptions noted.
6.06	An inventory of backups is maintained.	Inspected a listing of offsite backups to determine that an inventory of tapes stored offsite is being maintained.	No exceptions noted.
6.07	Tape management software is used to prevent the use of incorrect data files or the accidental erasure of data files.	Observed the tape management software to determine that the system is used to prevent the use of incorrect data files or accidental erasure of data files.	No exceptions noted.

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
7.01	A service desk function exists to register, communicate, dispatch and analyze calls, reported incidents, service requests and information demands.	Inquired of the Help Desk Manager to determine that procedures are in place to record and address reported problems. Observed the Help Desk system to determine that tickets are opened and tracked for problems and reported to the responsible COT party.	**Exception noted.** There are no documented policies or procedures for service desk functions. **Management's response:** **COT recognizes the importance of having formalized documentation in regards to the Service Desk processes and procedures. Therefore, COT is in the process of formalizing written Service Desk procedures. Draft documentation has been completed & must now go through management review and approval. The drafts are contained in COT-FSS-Commonwealth Service Desk-M file.**
7.02	Incidents are documented in a trouble ticket, prioritized and handled in a timely manner.	Observed the Help Desk system to determine that ticket logs are maintained and analyzed, and resolution times are monitored for customers. Inspected a sample of incidents to determine there was a timely resolution in accordance with priority established within the Help Desk system. Inspected monthly reports to determine that open tickets are being reviewed and closed in a timely manner.	**Exception noted.** 3 of 50 (6%) sampled incident tickets should have been handled as a change ticket or were not filled out completely. **Management's response:** **COT recognizes that an occasional error can occur**

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			within the Change Management Procedures. However, COT adheres to Change Mgt processes and procedures in a highly efficient manner in order to minimize the impact of incidents upon service quality and to improve day-to-day operations as stated in COT-009.
7.03	Procedures for handling change requests (including maintenance and patches) apply to applications, processes, system and service parameters, and the underlying platform.	Inspected COT's Change Management and System Development Life Cycle policies to determine there are formal policies and procedures related to the approval and implementation of changes to applications, processes, system and service parameters, and the underlying platform.	**Exception noted.** Procedures for database changes are not included in the policies. **Management's response:** **COT agrees there should be formal policies and procedures related to the approval of database changes. Therefore, database change request procedures will be updated within Change Management Procedure, COT-009.**
7.04	Changes are formally documented in a standardized manner.	Inquired of the Help Desk Manager to determine that change control request forms are required for database, system software and computer hardware changes. Inspected a sample of changes to determine whether change request forms were completed.	**Exception noted.** Database changes are not documented within the IT service management system. **Management's response:** **Database changes will now be**

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			documented within the Change Mgt system as each change is implemented.
7.05	Requested changes are formally approved by the business process owners and IT technical stakeholders.	Inspected a sample of change management request forms to determine the Change Control Group requires an authorization from the business process owner and IT stakeholder before proceeding with a requested change. Inspected COT's Change Management Policy to determine that the policy requires Change Advisory Board (CAB) approval for 'Major' changes.	**Exception noted.** The following was noted for the 43 sampled changes: - 18 (42%) tickets did not have required approvals. - 1 (2%) ticket had DBA sign off as the approver and implementer. Segregation of duties was not followed. **Management's response:** **Change Coordinators will place an additional task in the RFC ticket for process owner's approval. COT-009 will be changed to reflect the new process. RFC's received by the Change Coordinators will be reviewed to determine if the RFC should be marked as a "Major" change and require CAB approval. If RFC does not meet the criteria for "Major" change, the status will be changed to the appropriate type. The procedure for removing the check from the CAB box will be changed.**

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
7.06	Test plans are developed and documented for changes made to the COT environment.	Inspected a sample of change management request forms to determine the Change Control Group requires testing of changes prior to implementation.	No exceptions noted.
7.07	Testing of changes is conducted in a test environment that mirrors the production environment. The test environment segregated from the production environment.	Inspected a system listing to determine that test environments are separate and segregated from the production environment. Inquired of the Windows Server Support Team Lead, the Security Analyst, and the Systems Technical Specialist determine that the test environments are segregated from the production environment.	**Exception noted.** An accurate inventory of systems is not maintained. **Management's response:** **COT acknowledges it's weakness in maintaining an accurate inventory between all components of our information systems. To correct this, a Configuration Management Database (CMDB) project is in the planning and research stage and will be implemented in COT at a future date. (Approximate Implementation date is in 18 months).** **A repository of this kind will help COT understand the relationships between all COT components and track their configuration. The CMDB will contain details of the elements that our IT Services are dependant upon, including hardware, software, & personnel. CMDB will also help us address how the data will be kept up-to-date & give**

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			COT the ability to control change and manage the impact of our business in the event of a disaster.
7.08	Source program libraries have the capability to retain prior versions and access to such libraries is restricted to authorized personnel.	Observed the version control software to determine that prior versions were maintained and access is restricted to authorized personnel based on job responsibilities.	No exceptions noted.
7.09	Request for compilation and move into production is approved by IT management, account representative and/or customers.	Inspected a sample of completed change tickets to determine that changes being migrated into production were approved in accordance with requirements. Inspected listing of pre-approved changes to determine whether the change was listed on the list of pre-approved changes.	**Exception noted.** 1 of 43 (2%) sampled change tickets which should have followed the normal change process was pre-approved. **Management's response: Currently a weekly report is generated by the Service Desk Manager to review all pre-approved changes. This report was implemented in March 09. Changes are reviewed for appropriate labels.**
7.10	Computer programmers do not have access to production data or write directly to media.	Inspected a listing of individuals with the ability to migrate changes into production or write directly to media to determine access is limited to individuals based upon job responsibilities.	**Exception noted.** The following was noted regarding developer access to production environments. - Two developers were identified with production access on FOXPRO. - Three developers were

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			identified with production access to UNIX servers - Thirty developers were identified with production access on the Mainframe. No additional monitoring of developer access to production environments is taking place. **Management's response:** **COT/OAD management not only understands the importance of controlling access to production data but also the necessity for management to periodically review those instances where access has been granted and to remove that access once the need is no longer necessary. To that end, the management team in COT/OAD, with the Office of the CISO, will develop a plan to further identify and validate all instances of access to production data. This shall be set as a high priority. Access not validated as required for business needs will be terminated.** **Over the past two years**

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
			COT/OAD management has periodically requested lists of production level access granted to staff. These lists are used to identify area of concern, and result in either requests to revoke access deemed inappropriate, or the submission of an F085 Security Exemption to document and justify the needs for this access. **Finally, COT/OAD management understands the need to refine the process not only for granting access to production data but also includes the ability to audit backward (as in the case of this review) and to verify whose authority authorized these individuals access to production data.**
7.11	Emergency change procedures are included in the overall change management procedure. These procedures include defining, raising, testing, documenting, assessing and authorizing emergency changes.	Inspected change management procedures to determine that COT maintains policies and procedures to govern the performance of "emergency" processing of change requests.	No exceptions noted.
7.12	Changes are closed in a timely manner, in accordance with the established priority.	Inspected a sample of change tickets to determine that changes were completed within the required timeframe based on	No exceptions noted.

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
		priority.	
7.13	Documentation is provided to the agencies for changes that affect users.	Inquired of the Application Development Manager to determine that documentation is provided to agencies that are affected by the implemented changes.	**Exception noted.** There is not a process in place to provide change documentation to affected end users. **Management's response:** **A 'Forward Schedule of Change (FSC)' notification is currently under development. The Schedule will be available to agencies via the COT web page. FSC will contain relevant information of scheduled changes.**
7.14	A standardized process is in place to select and authorize system software.	Inspected policies and procedures to select and authorize system software.	**Exception noted.** A formal policy for selecting and authorizing system software was not put in place until March 2009. **Management's response:** **In recognition of the need for formalized policies in selecting and authorizing system software, COT redeveloped the formal policy and implemented on 3/10/2009.**
7.15	On-line user documentation including product manuals and help files is	Observed the document management repository website to determine that agency documentation has been uploaded to	No exceptions noted.

Manage Problems and Changes			
Control Objective 7: Controls provide reasonable assurance that problems and/or incidents are properly identified, recorded, and resolved and system changes are documented, authorized and appropriately tested before being moved to production.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
	maintained.	assist end users.	

Manage Operations			
Control Objective 8: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
8.01	Malicious software prevention policy is established, documented and communicated throughout the organization.	Inspected the Anti-Virus Policy to determine that it has been documented and communicated throughout the organization.	No exceptions noted.
8.02	A virus protection tool has been installed, which includes virus definition files and the last time the definitions were updated.	Inspected antivirus configuration settings and reports to determine that an anti-virus protection tool has been installed, updates to personal computers and servers are automatic and the latest antivirus definitions are installed daily.	**Exception noted.** There are no procedures in place to identify systems without anti-virus installed. **Management's response:** **COT utilizes the synchronization feature of its antivirus management console which ensures that any new COT-managed devices added to the enterprise directory domains receive a client agent and Antivirus software. COT realizes that unprotected computer systems that do not join our enterprise directory might present a risk if added to our network. COT is currently investigating potential solutions to this problem. A decision about what solution COT intends to move forward with is expected to be made and implemented by October 31st, 2009.**
8.03	Mainframe performance reports have been	Inspected a sample of monthly performance reports and daily	No exceptions noted.

Manage Operations			
Control Objective 8: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.			
Ref	**Controls Provided by the Commonwealth Office of Technology**	**Tests performed by Potter & Company LLP**	**Results of Tests**
	developed and are published on a regular basis.	ABEND reports to determine performance of the mainframe is being monitored.	
8.04	System software is maintained, kept current and updated with vendor system maintenance activities.	Inspected a sample of domain controller and non-domain controller WSUS reports and Patch status spreadsheet reports to determine that COT maintains current versions of system software.	No exceptions noted.
8.05	Procedures, including duties and responsibilities, are documented for each computer operator shift.	Observed the document management repository website to determine that checklists and procedures are documented for each computer shift.	No exceptions noted.
8.06	Non-routine operations occurrences and the corrective actions performed are documented.	Inspected a sample of shift check sheets and associated issue logs to determine that non-routine occurrences and corrective actions are performed, documented and approved by management.	No exceptions noted.
8.07	An automated job scheduling and execution system is used to set up, automatically submit, and monitor recurring production jobs for processing.	Observed the automated job scheduling and execution systems to determine that the system is used for automatically submitting recurring jobs.	No exceptions noted.
8.08	The ability to set up and submit jobs is limited to job scheduling and operations personnel.	Inspected listings of users with the ability to setup and submit jobs in the job scheduling systems to determine whether user access is restricted in accordance with job responsibilities.	No exceptions noted.
8.09	Procedures are in place for distribution of reports run by agencies.	Inspected a sample of emails to determine that system job reports are emailed to the appropriate team or individuals. Inspected a sample of ABEND reports to determine that Non-Revenue system job reports are reviewed by the Production Services Team and are available to agencies.	No exceptions noted.
8.10	Schedules are maintained of reports to be provided to each agency.	Inspected a sample of schedules from the Revenue and Non-Revenue systems to determine they are maintained and reports are provided to agencies.	No exceptions noted.

SECTION IV

Information Provided by the Commonwealth Office of Technology

Disaster Recovery Planning

Unexpected events can affect the availability of resources supporting mission critical business functions and cause an interruption in business services. Disaster Recovery Planning (DRP) covers the provisions specifically for the reinstatement of the technology infrastructure. The specific processes focus on the recovery, continuance and eventual return of business functions to their pre-outage condition.

An organization's ability to successfully manage the disaster recovery processes can directly impact its survival in the event of an unplanned service interruption. A plan, to be utilized in the case of an event which renders part or all of the system unusable and/or inaccessible, has been developed and is maintained.

A comprehensive enterprise-wide disaster recovery planning methodology exists and is under constant review, enhancement and development. Backup and offsite storage processes are in place, as described elsewhere in this document. All critical contact information for customers, vendors, and support team is retained in the disaster recovery document. A third party vendor has been contracted to provide a disaster recovery hot site which would allow for rapid recovery of critical systems in the event of a disaster. In addition, COT performs quarterly tests to validate that critical systems can be recovered timely.