



**REPORT ON CONTROLS  
PLACED IN OPERATION AND  
TESTS OF OPERATING EFFECTIVENESS  
FOR THE GOVERNOR'S OFFICE FOR TECHNOLOGY**

**For the Period July 1, 2001  
through June 30, 2002**

**EDWARD B. HATCHETT, JR.  
AUDITOR OF PUBLIC ACCOUNTS  
WWW.KYAUDITOR.NET**

**144 CAPITOL ANNEX  
FRANKFORT, KY 40601  
TELE. (502) 564-5841  
FAX (502) 564-2912**



Edward B. Hatchett, Jr.  
Auditor of Public Accounts

To the People of Kentucky  
Honorable Paul E. Patton, Governor  
Aldona Valicenti, Chief Information Officer  
Governor's Office for Technology

The enclosed report prepared by Crowe, Chizek and Company LLP, Certified Public Accountants, presents the report on controls placed in operation and tests of operating effectiveness for the Governor's Office for Technology for the period July 1, 2001 through June 30, 2002.

We engaged Crowe, Chizek and Company LLP to perform the SAS 70 audit of the Governor's Office for Technology. We worked closely with the firm during our report review process.

Respectfully submitted,

Edward B. Hatchett, Jr.  
Auditor of Public Accounts

Enclosure

---

# Commonwealth of Kentucky



---

## **REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS**

For the Period July 1, 2001  
Through June 30, 2002

Prepared by:



**Crowe, Chizek and Company LLP  
Information Risk Management Practice  
330 East Jefferson Boulevard  
South Bend, IN 46624  
<http://www.crowechizek.com>**

---



**Commonwealth of Kentucky  
Governor's Office for Technology  
Frankfort, Kentucky**

**REPORT ON CONTROLS  
PLACED IN OPERATION AND  
TESTS OF OPERATING EFFECTIVENESS**

**For the period July 1, 2001  
Through June 30, 2002**

**Table of Contents**

<b>REPORT OF INDEPENDENT ACCOUNTANTS</b> .....	1
<b>DESCRIPTION OF POLICIES AND PROCEDURES PLACED IN OPERATION Provided By the Governor's Office for Technology</b>	
<b>GENERAL CONTROLS</b> .....	3
Organizational Structure and Personnel.....	3
Application Maintenance and Documentation.....	10
System Software and Hardware.....	11
Physical Security.....	12
Back-up and Contingency Planning.....	14
Mainframe.....	16
UNIX.....	20
Windows NT.....	22
Infrastructure.....	24
<b>APPENDICES</b>	
Appendix A -- Test of Operating Effectiveness.....	31
Appendix B -- User Control Considerations.....	42
Appendix C -- Organizational Chart.....	45
Appendix D -- Network Information Highway.....	46



## REPORT OF INDEPENDENT ACCOUNTANTS

Commonwealth of Kentucky  
Governor's Office for Technology  
Frankfort, Kentucky

We have examined the accompanying description of controls related to the systems of the Governor's Office for Technology (GOT). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of GOT'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 user organizations applied the controls contemplated in the design of GOT's controls, and (3) such controls had been placed in operation as of June 30, 2002. The control objectives were specified by Auditor of Public Accounts in conjunction with the GOT. 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.

As discussed in the accompanying description, GOT has not designed procedures to formally assess the risk levels for contingencies, document the entire plan, implement, and test the recovery capabilities for all aspects of the Commonwealth of Kentucky as provided by the GOT processing center. These deficiencies result in the controls not being suitably designed to achieve Control Objective 7: "Controls provide reasonable assurance of continued operations in the event that systems become unavailable; and formal plans for recovery have been considered".

In our opinion, the accompanying description presents fairly, in all material respects, the relevant aspects of GOT's controls that had been placed in operation as of June 30, 2002. Also, in our opinion, except for the matters described in the preceding paragraph, 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 internal controls contemplated in the design of GOT's controls relating to the systems at GOT.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Appendix A, to obtain evidence about their effectiveness in meeting the control objectives, described in Appendix A, during the period from July 1, 2001 to June 30, 2002. The specific controls and the nature, timing, extent, and results of the tests are listed in Appendix A. This information has been provided to user organizations of GOT and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations.

GOT states in its description of controls over the application development control process that a formal signoff and controlled implementation of applications is provided for all platforms. These controls exist, but have been applied inconsistently across the certain platforms (NT and Unix-based systems) under the control of GOT. (See Control Objective 2: "Controls provide reasonable assurance that changes to

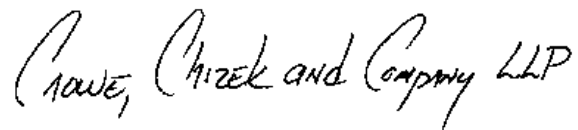
applications are authorized, tested, approved, properly implemented, and documented to provide an audit trail to facilitate future program changes.”)

Except for the matters noted in the paragraph above, in our opinion the controls that were tested, as described in Appendix A, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Appendix A were achieved during the period from July 1, 2001 to June 30, 2002. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Appendix A were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Appendix A.

The relative effectiveness and significance of specific controls at GOT 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 GOT is as of June 30, 2002 and information about tests of the operating effectiveness of specified controls covers the period from July 1, 2001 to June 30, 2002. 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 the GOT is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

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

A handwritten signature in black ink that reads "Crowe, Chizek and Company LLP". The signature is written in a cursive, flowing style.

Crowe, Chizek and Company LLP

South Bend, Indiana  
June 30, 2002

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for 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. These controls are divided into the following nine areas:

- Organization Structure and Personnel
- Application Maintenance and Documentation
- Systems Software and Hardware
- Physical Security
- Contingency Planning
- Operations and Scheduling
- Logical Security
- Output Distribution
- Backups and Recovery

It should be noted that, if these areas are not segregated, they can overlap to affect all information systems activities. As a result, the adequacy of these controls is considered fundamental to the effectiveness of specific applications and weaknesses within these General Controls can have pervasive effects that are detrimental to many applications.

### **Organization Structure and Personnel**

The Governor's Office for Technology is responsible for providing leadership, policy direction, and technical support to all executive agencies of state government in the application of information technology. The Governor's Office for Technology, under the direction of the Chief Information Officer, is composed of seven offices, two boards, and two advisory councils. These are outlined below.

The **Chief Information Officer** is responsible for policy direction and the general management of the Governor's Office for Technology. Our mission is to work in partnership with state agencies in meeting the needs of Kentucky's citizens by addressing business problems and opportunities through the effective use of information technology and services.

The **Office of Human Resources Management and Development** is responsible for personnel related issues including GOT employment opportunities, vacancy announcements, IT classifications, and the processing of internal personnel actions. This Office has the responsibility to seek employees who are adaptable to new processes/technology, who can develop flexible business models, and who are responsible to its customer's needs.

The **Office of Administrative Services** is composed of two divisions: *Division of Financial and Business Management* and the *Division of Asset Management*. This Office is responsible for the financial and business operations for the Governor's Office for Technology. These duties include the preparation of the biennial budget request, procurement assistance, fiscal administration and facilities support. Revenue for the Governor's Office for Technology is derived primarily from agency receipts. This office is responsible for establishing and maintaining a federally approved cost allocation plan in which each state agency shares in the cost of services provided by the Governor's Office for Technology.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

### Provided by the Governor's Office for Technology

The ***Office of Policy and Customer Relations*** is responsible for the statewide strategic information technology plan and development of the agency information resources planning model and plan review. This Office is composed of three divisions: *Division of Planning and Architecture*, *Division of Relationship Management*, and the *Division of IT Training*. Other responsibilities include the formation of Information Technology policy, enterprise architecture and standards, enterprise capacity planning and research and development. Customer relations activities include enterprise technical training, educational seminars, knowledge management and customer and vendor relationship management. Many of the policy and planning responsibilities, previously assigned to the Office of the Kentucky Information Resources Management (KIRM) Commission, have been assigned to this Office.

The ***Office of Infrastructure Services*** is responsible for the operation of the enterprise computing environment. This Office includes the daily operation of the Commonwealth Data Center (CDC), operation and maintenance of the Kentucky Information Highway, and all communications services, including data, voice, video and wireless. By Executive Order, the Governor has integrated the operation of the information technology infrastructure under a single agency. This Office is composed of five divisions: *Division of End User Support*, *Division of Security Services*, *Division of Computing Services*, *Division of Communication Services*, and the *Division of IT Operations*. The *Division of End User Support* is responsible for providing help desk assistance to end users in the Commonwealth of Kentucky. This Division provides support for hardware, mainframe system/applications, Internet issues, LAN/WAN or communication problems either directly or indirectly. The *Division of Security Services* is responsible for data security and charged with meeting the demands of tighter security of client information in the areas of electronic commerce and network computing. This Division is also responsible for the physical security of the Commonwealth Data Center, as well as four other GOT buildings, using the latest technology in electronic locking systems and badge access. Another responsibility for this Division is disaster recovery planning activities for the systems at the GOT. The *Division of Computing Services* is responsible for technical and operational support of the computing infrastructure located primarily at the Commonwealth Data Center. This support includes planning for the introduction of new technology, installing and maintaining system software, managing software contracts, managing equipment operations, coordinating the installation of equipment, maintaining data storage, resolving operational problems, and managing customer service levels. This Division is also responsible for providing server administration and technical support for CDC servers. This administration and support includes installing and maintaining systems software, providing systems programming support, managing the allocation and utilization of data storage, monitoring hardware and software performance, collecting usage and billing statistics, testing the data center disaster recovery plan, and resolving hardware and software problems. The *Division of Communication Services* has responsibilities that encompass all aspects of communications: data, voice, and video. This Division is responsible for network planning, network design, network management, systems administration, research and evaluation of desktop and departmental computer technologies, and support for end user computing. The Division also maintains all aspects of voice communications to state agencies. These responsibilities include consulting, installation, maintenance, moves, and changes of all telephone related equipment. Management of the Kentucky Information Highway (KIH) and the Kentucky Emergency Warning System (KEWS) also resides in this division. Finally, the *Division of IT Operations* is responsible for providing round-the-clock operational support for all computing equipment. This support includes console event monitoring and management, operation of peripheral equipment such as printers, coordinating computer equipment installation and maintenance, providing tape storage management, coordinating off-site storage of backup data, providing data control support, resolving operational problems, and managing the workflow to ensure that processing schedules are met.

The ***Office of Consulting and Project Management*** is responsible for providing comprehensive systems analysis, design, and development services, and applications consulting services to designated state



## DESCRIPTION OF CONTROLS PLACED IN OPERATION

### Provided by the Governor's Office for Technology

agencies. This Office provides cost-effective application systems support to state agencies for accomplishment of requirements defined in each agency's Information Resources plan. Successful attainment of agency service requirements necessitates utilization of a broad and variable spectrum of information systems technology, which includes: automation of new services, integration of diverse management systems, and enhancement of existing systems. This Office is composed of six divisions: *Division of Centers of Expertise*, *Division of Project Office and Integration*, *Division of Human Services Systems*, *Division of Financial Systems*, *Division of Transportation Systems*, *Division of Workforce Development and General Government Systems*. The *Division of Human Services Systems* is responsible for the analysis, design, development, and maintenance of: eligibility systems within state government related to public assistance; all systems related to the protection of both children and adults in Kentucky; all systems related to the establishment, collection, and enforcement of child support within the Commonwealth of Kentucky; and all systems related to public health and safety, including the collection and retrieval of vital statistics such as births, deaths, marriages, and divorces. The *Division of Financial Systems* is responsible for the analysis, design, development, and maintenance of: all systems pertaining to the administration and collection of Kentucky taxes; and all systems related to the management of state government, including personnel and financial management systems. The *Division of Transportation Systems* is responsible for the analysis, design, development and maintenance of: all systems related to a variety of activities within the Transportation Cabinet; all systems related to the registration and titling of vehicles and boats; and all systems related to the licensing of drivers within the Commonwealth of Kentucky. The *Division of Workforce Development and General Government Systems* is responsible for the analysis, design, development and maintenance of: all systems related to the education and training of adults, and all systems which support the business requirement of the Justice Cabinet, Labor Cabinet, Natural Resources and Environmental Protection Cabinet, Public Protection Cabinet, Tourism Cabinet and other agencies within the Executive Branch who request assistance.

The *Office of Geographic Information* is responsible for establishing a centralized statewide geographic information clearinghouse of map inventories, information on current and planned geographic information systems application, information of grants that are available for the acquisition or enhancement of geographic information resources, and a directory of geographic information resources available within the state or from the federal government. This Office also provides consulting and technical assistance, education and training on the application and use of geographic information technologies to state and local agencies. It is also responsible for providing staff support and technical assistance to the Geographic Information Advisory Council. Finally, this Office has the responsibility to assist and support geographic information systems services upon request.

The *Office of General Counsel* is responsible for providing all legal services for GOT and for advising the Chief Information Officer on the legal implications of information technology policy as it relates to government operations.

The *Geographic Information Advisory Council* is responsible for advising the Chief Information Officer on issues relating to geographic information and geographic information systems. The Council establishes and adopts policies and procedures that assist state and local jurisdictions in developing, deploying, and leveraging geographic information resources and geographic information systems technology for the purpose of improving public administration. The Council consists of twenty-six members and one legislative liaison. The Council is also responsible for overseeing the development of the adoption of policies and procedures, strategic planning, recommendation of standards, assessment of state agency plans, training and education plans, and sharing of data and data development of geographic information systems.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

The *Commercial Mobile Radio Service Emergency Telecommunication Board (CMRS)* is responsible for administrating the CMRS fund for the purpose of implementing wireless emergency 911 service throughout Kentucky in accordance with state and federal legislation and regulation.

The *Kentucky Information Technology Advisory Council* is responsible for advising the Chief Information Officer on approaches for coordinating information technology solutions among libraries, public schools, local governments, universities, and other public entities. Further, the Council provides a forum for the discussion of emerging technologies that enhances electronic accessibility to various publicly funded sources of information and services. The Council consists of members that are either appointed or serve by virtue of an office. No member receives compensation, but is reimbursed for actual and necessary expenditures in accordance with travel and subsistence requirements established by the Finance and Administration Cabinet.

The *Kentucky Telehealth Board* is responsible for the regulatory administration of establishing telehealth training centers across the state, the development of a telehealth network of rural sites, the establishment of protocols and standards to be followed by the training centers and rural sites, and the maintenance of the central link for the network with the Kentucky Information Highway. The training centers shall be established by the Board for the purpose of promoting telehealth and training practitioners and staff in its use. The Board is attached to GOT for administrative purposes.

*Policies and Procedures*

Employee Policies

Within the Governor's Office for Technology, executive directors and division directors are responsible for the development and maintenance of technical policies, procedures, standards and forms for the Governor's Office for Technology. The Office of Administrative Services, as stated in policy GOT-013 - Policy Development, Distribution, & Maintenance, is responsible for the development, maintenance, and publications of GOT internal administrative policies, procedures, standards and forms. The Office of Policy and Customer Relations is responsible for the development, maintenance and publications of the GOT enterprise administrative policies, procedures, standard and forms. All policies must comply with the Enterprise Architecture and Standards. Management personnel within the GOT must ensure that every employee is aware of and follows all GOT policies and procedures.

GOT Employees/contractors are required to complete and sign form GOT-F015 - Acknowledgement of Responsibility, which requires a GOT employee to accept the responsibility to protect the confidentiality 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 GOT employees abide by all GOT/Enterprise policies and procedures. Further, it requires all hardware, software and data that a GOT 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, GOT-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

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

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 GOT.

Other policies exist which set guidelines for purchasing (GOT-031 - Discretionary Purchases & Payments and GOT-061 - Procurement Card Program), asset management (GOT-024 - Acquisition of Surplus Property and GOT-055 - Shipping and Receiving), personnel (GOT-026 - Employee Time Reporting and GOT-043 - Employee Performance Evaluation), travel (GOT-021 - Travel & Travel/Training), consulting (GOT-016 - Task Order Agreement for Contractor Programming/Analyst Services and GOT-011 - Systems Life Cycle Methodology), customer relations (GOT-015 - Communications Standards and GOT-014 - Customer Request for Professional Services) , and end-user support (GOT-008 - Change Management Policy).

#### Security Policies

The Division of Security Services and the Office of Human Resources Management & Development developed GOT-F042 – Departing Employee Checklist (web-based system), for the purpose of ensuring that required tasks are performed as part of the exiting process for employees and contractors leaving the GOT. Of particular concern is the termination of logical and physical security access. This form is to be completed by management and states the official departure date of a GOT employee or contractor. Also included is a checklist of actions, required to be completed by GOT, which pertains to the user access of the departing employee or contractor. These actions include the revoking of the RACF (Resource Access Control Facility from IBM) user identification, building access, electronic mail, network access, KY-Net privileges, passwords, security badges, MARS access, enterprise server/database access, and specific access to electronic files and directories. Other cancellations include, procurement cards, gasoline cards, and telephone cards. Building keys, desk and file cabinet keys, laptop and computer workstations, pagers, cell phones and parking tags, are required to be returned prior to the exit.

Other policies pertaining to security are GOT-012 - Personal Computer Equipment Assignment; GOT-068 – Security Administrator Manual & Policy for Microsoft Windows NT; GOT-069 – Security Administrator Manual & Policy for UNIX (AIX); GOT-070 – Security Administrator Manual & Procedures for UNIX (Solaris); and GOT-067 – Security Policies & Procedures Manual (SPPM).

#### *Strategic Planning*

The Commonwealth of Kentucky Strategic Information Technology Plan (SITP) was adopted by the KIRM Commission July 1, 1997, which was originally supported by the EMPOWER Kentucky Initiative. The KIRM Commission has been abolished, and the responsibility for review and maintenance of the SITP has been transferred to the Governor's Office for Technology due to the Information Technology Transformation Initiative of the Office of the Chief Information Officer.

The Strategic Information Technology Plan for the Commonwealth of Kentucky has been developed to provide a framework for the effective management of Information Technology (IT) in the Commonwealth of Kentucky. The primary role of information technology is to support the business objectives of the Commonwealth of Kentucky and to facilitate agency efforts to provide efficient and effective services to the citizens of the Commonwealth of Kentucky. The plan will guide agencies in the development of their technology planning. Agency plans and ongoing activities will be reviewed for consistency with the strategic plan.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

The plan also provides a foundation for an enterprise wide approach to the management of information technology. The Commonwealth is in an organizational transition from functional silos to a process-oriented environment. Many future technology efforts will cross multiple cabinets with a single goal of providing services to the citizens of the Commonwealth of Kentucky. This environment requires technology that can communicate, inter-operate and share data and resources, while reducing the costs associated with training and support through the use of enterprise architecture and standards for IT.

The plan is not intended to limit department or agency creativity, but to provide a stable infrastructure and environment in which to solve common business problems faced by many agencies and to allow the agencies to collaborate on significant efforts. The plan is built on the assumption of an IT management model which utilizes the best features of both centralized and decentralized IT management, support and decision making.

The plan also provides a foundation for the development of the IT architecture and standards. The architecture and standards are critical to ensuring the ability of multiple cabinets or agencies to share resources including application and data. The standards provide for interoperability, consistency and more effective management of training and support costs. Exceptions may be necessary and these will be based on a business case analysis.

The following IT guiding principles are key statements of direction related to information technology and its ability to serve as an enabler to meet the needs and goals of the Commonwealth government. These guiding principles are intended to provide an environment in which the Commonwealth can achieve its objectives related to providing high-level customer service. The principles are interrelated and meant to provide a cohesive approach to IT. The plan includes five guiding principles for information technology:

- I. **Support the business objectives of the Commonwealth government** – Information technology can enable improvements in business processes including reduction of costs and cycle times. Technology has a limited value when not applied to the business objective and goals of the organization. IT planning, budgeting and management must be closely integrated with the business planning, development and management to ensure that IT is being applied effectively and efficiently.
- II. **Conduct Commonwealth business electronically** – Commonwealth business can frequently be transacted more efficiently and effectively utilizing information technology to support the process. Electronic commerce technologies including the World Wide Web (WWW), electronic data interchange (EDI) and electronic funds transfer (EFT) can speed the process of business transactions and reduce the amount of manual intervention required. Electronic mail is already in wide spread use within the Commonwealth, but can be used more effectively for communication.
- III. **Treat information as a strategic resource** – Information is a critical asset of, and owned by, the Commonwealth. It must be managed from an enterprise perspective to ensure accuracy, integrity and availability. This includes developing a methodology or structure for sharing data across functional, technical and organizational boundaries. Agencies and departments act as custodians or stewards of the data and facilitate the sharing and reuse of the data. Data should be collected once and used many times. The creation of standard data definitions, formats and values will require the participation of both IT professional and functional experts.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

- IV. **View technology investments from an enterprise perspective** – Technology investment decisions should be made from an enterprise perspective and not from the perspective of a single cabinet or agency. An enterprise wide focus is necessary to ensure that the Commonwealth's limited IT resources are being utilized in the most effective manner. A strong technology infrastructure is required to support both enterprise wide applications as well as cabinet or agency specific projects to ensure interoperability, compatibility and shared usage of technology resources. New IT projects must identify the impact on the enterprise and on the customer. The development of the architecture and standards along with a strong infrastructure (CDC, wide area network, and electronic mail) makes this principle the strongest.
- V. **Ensure electronic access to information and services while maintaining privacy** – Information is of little value if access to the information is not readily available. Providing efficient electronic access to information requires a strong infrastructure and a standard set of navigational methods and tools. The Commonwealth must balance the need for easy access to information against the privacy and security requirement of the information.

The successful implementation of this plan is dependant on (1) senior management's commitment to cross cabinet cooperation and coordination, sustained commitment to Business Process Reengineering and a willingness and commitment to share information and standardized data; (2) active agency participation in implementing the strategies defined in this plan in order to achieve the desired goals and objectives; (3) compliance and adherence to an IT architecture and a set of IT standards to ensure information can be transferred between different networks, or different hardware and software systems, with accuracy, reliability and security; (4) the recruitment and retention of top level information technology professionals; (5) managed expectations for IT initiatives; (6) cultural change in that organizational learning closely parallels user acceptance and training; and (7) education of IT users and customers must be an ongoing activity.

### *Training*

The Governor's Office for Technology strives to provide agencies not only with software and technology training, but also with a staff of individuals that are proficient in areas of technical development and support, communications, and programming and development expertise.

The Information Technology Training Division provides software and technical training opportunities for employees of the Commonwealth of Kentucky. GOT acts as consultants with agencies to establish training initiatives that address the business needs of each organization. GOT can develop training programs and customize training courses to meet the needs of the agencies. A wide array of training tools are offered such as (1) instructor-led, hands-on classroom training, (2) multi-media and computer based training in our training labs, (3) web-based desktop training and Commonwealth Integrated Network-based training, (4) vendor-supplied technical courses, (5) custom-developed training classes, and (6) video library resources for self-study.

To maintain the highest level of expertise necessary in the changing environment of today's technology and to provide agencies with staff that are skilled in program/applications development and maintenance, GOT personnel attend conferences, workshops, seminars, and training classes. The needs of the Commonwealth are ever changing, and GOT accepts the challenge to provide the Commonwealth with experienced staff to meet the demands of new technology.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

### **Application Maintenance and Documentation**

#### *Request for Services*

All requests for new applications or changes to existing applications are received on an appropriate request form. This is formal authorization for requesting work. Prioritization of the request is completed at the agency level. If GOT is unable to support a request or meet requested completion dates due to resource constraints, some prioritizing will be done in conjunction with the agencies.

#### *Estimate Level of Effort*

At the direction of the agency or based on GOT's risk assessment of the request, GOT may create a performance estimate based on the complexity of the request and transmit it to the agency. If an estimate is created, the agency approves the time and budget estimate before GOT acts on the request. Project plan information is entered into the Enterprise Project Management (EPM) program, which is used to monitor and track the status of the work request. GOT staff log their progress and time devoted to each task into EPM. GOT staff may use MS Project or other software to plan and manage projects.

#### *Perform and Validate Work*

Developers make software changes, noting a description of the modifications in comments within the source code. The comments include the date and request tracking number associated with the work being completed. Please refer to GOT System Life Cycle Manual for additional documentation requirements.

Developers test the software modifications. The complexity and the extent of the testing will depend on the nature of the software change, the importance of the modifications, the application environment and other factors. Some applications have quality assurance with a completely separate user acceptance test environment. The developer will review the test results with the user and GOT management. The developer will obtain written approval from the user before initiating the process to promote modifications into production.

#### *Promote to Production Environment(s)*

Mainframe - The developer initiates the process to move the software change into production by completing a production cutover form. The cutover form ties the software change to the request number. GOT management approves the movement of the software into production. The librarian moves the software to a staging library. Production control installs the software in the production environment from the staging library. GOT maintains version control of the software source. GOT notifies the user agency when the software is available in the production environment.

Web Development/Client Server – Three scenarios are utilized for the web development/client server development. Each scenario depends upon whether the server is agency-owned with technical support available at the agency, GOT-owned with shared services, or agency-owned without technical support available at the agency.

- For an agency-owned server with technical support available at the agency, GOT development staff will move the executable code and web pages to a staging library. The agency is responsible for moving the executable code to a production library. The GOT staff does not have access to the agency's production library.
- For a GOT-owned server with shared services, GOT development staff move the executable code and web pages to a staging library. The agency approves the application move to production and the

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

GOT production control staff moves the code to a production library. The GOT development staff does not have access to the production library.

- For an agency-owned server without technical support available at the agency, GOT development staff will move the executable code and web pages to a staging library. The agency approves the application move to production, and different members of the GOT development staff, independent of the original move, will move the code to the production library. This scenario is only implemented when the agency chooses to host their own servers, and the agency is without internal production support.

*Request Close Out*

Once all work has been completed under a professional service request, the request is closed in the EPM system. The request is signed by GOT management and returned to the user agency for sign off. The completed request is filed in GOT once it is returned from the user agency.

*Access to Production Files*

In order to resolve production problems, developers may need access to production files. This access will be approved, in writing for a specific duration, by GOT management and the user agency. Periodically, GOT management review staff access levels to production files and program cutover practices to ensure compliance with policy.

**System Software and Hardware**

*Changes/Implementation/Documentation*

Mainframe

The Server Administration 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 Server Administration staff. Upgrades, changes, and testing are scheduled through the change control process. The manager of the Server Administration Branch 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 of the Server Administration Branch. Testing of systems software is usually conducted in the Server Administration Branch Test LPAR (Logical PARTition) 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 Server Administration Branch using IBM's SMP software maintains all documentation regarding system software releases. This software stores detailed documentation regarding release levels and maintenance levels for system software. As new maintenance is installed, an assigned Server Administration employee updates a list of software titles and version numbers that is available to user agencies through the Server Administration Branch web site. Product manuals and documentation are usually stored online using IBM's BookManager product. The change control process also maintains a historical record of system changes.

NT

All system changes are implemented according to the GOT change control process wherein changes are submitted to change control by Wednesday morning and reviewed during the change control meeting on

<b>DESCRIPTION OF CONTROLS PLACED IN OPERATION</b> <b>Provided by the Governor's Office for Technology</b>
---

Wednesday afternoon. Emergency changes can circumvent this process but must be approved in advance by the Server Administration 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 Server Administration Branch and then processed through change control. Detailed documentation of changes made to each server is maintained within the Server Administration Branch. In addition, the change control process maintains a historical list of changes made.

### UNIX

All system changes are implemented according to the GOT change control process wherein changes are submitted to change control by Wednesday 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 Server Administration 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.

## **Physical Security**

### *Access*

#### Physical Entry Control

GOT issues a standardized identification badge/proximity card, which allows authorized employees/contractors access into GOT facilities. The badge should be prominently displayed by the employee/contractor while they are in a GOT 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 GOT-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., GOT employee, contractor, etc.). A corresponding policy has been implemented and is included in the Security Policies and Procedures Manual. Access rights to areas within GOT facilities, particularly the Commonwealth Data Center, are regularly reviewed and documented.

To ensure no one enters the CDC without appropriate access, a receptionist is always on-duty at the front desk during business hours Monday through Friday, 8:00 a.m. to 4:30 p.m. Visitors must sign in, are issued a visitor's badge, and must be escorted by appropriate GOT personnel. The receptionist maintains the visitors' log at the main entrance. All GOT employees have access to the front door Monday through Friday, 8:00 a.m. to 4:30 p.m. GOT employees who are located in one of the other GOT facilities must sign the visitor's log, but are not required to wear a visitor's badge, as they have valid GOT badges and are frequently required to attend meetings at the CDC. However, unless prior access has been approved, they may not access the third or fourth floors, or the two warehouse areas within the Commonwealth Data



**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

Center. During the past several months, we have heightened our security by restricting entrance via the back door. The door is still available as an exit in emergency situations.

The Commonwealth Data Center is currently equipped with video cameras that are located throughout the building at sensitive access points. A tape library is maintained and tapes are changed daily Monday - Friday, and one tape for the weekends. Tapes are recycled after approximately 1 1/2 months. A log is kept showing the tape number for each day and reviewed as necessary.

Badge readers are currently located at the front door, back door, east warehouse door, west warehouse door, third floor east, third floor west, fourth floor east and fourth floor west. Anyone who does not have a work area on the third and/or fourth floors must have supervisor approval in order to gain such access.

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 and/or alarms. Reports can be created for anything from all activity on a specific door, to a particular individual and all access attempts at any location. The physical security administrator reviews reports daily for these violations.

Currently, the CDC has "drive-by" security guard service. During the evening hours, a facilities security guard drives by and checks all outside doors to make sure that they are locked. As an added security feature, the door-locking system is connected to the State Police barracks from 6:30 p.m. - 6:30 a.m. If an incident occurs during that time, such as an outside door being opened too long, an alarm is sent and the State Police dispatch a vehicle immediately.

In addition to ensure badge access is kept up-to-date, a formal process for departing employees/contractors has also been implemented. This is accomplished by a web-based program, and is based on the form GOT-F042. This form not only helps assist that badges are disabled, but that all access to any computer resources is revoked. When all areas of access have been removed, the program sends an e-mail copy to the human resources division of GOT, and a copy is filed with the employee's personnel file.

#### Delivery/Loading Areas

The delivery and loading areas are controlled and isolated from information processing. Deliveries must be acknowledged by appropriate building maintenance staff or the receptionist before they can be accepted and the delivery door opened. The Office of Administrative Services (OAS) staff is responsible for inspecting the deliveries before they are unloaded and accepted.

Since other state agencies use our mainframe to complete many of their computing needs, GOT frequently must use tapes provided by the agency. It is the responsibility of the agency to pick up and/or drop off those tapes for GOT's use. The forms used are GOT-F082 (Authorization for release of reel tapes, cartridges and diskettes) and GOT-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.

#### *Security of Resources Off-Premises*

As more telecommuting from home is necessary, GOT does allow personal computers to be checked out as defined by GOT-012 (Personal Computer Equipment Assignment). A form (GOT-F018) must be

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

completed by each employee and signed by the branch manager, with specifics about the assignment. The form must be signed and dated by both individuals on the date the equipment is released, as well as the date it is returned.

*Environmental Protection*

The environmental protection is divided into three (3) areas of control: UPS, HVAC and fire protection.

UPS

An Uninterruptible Power Supply (UPS) services all critical electrical systems including the GOT computer systems. In June 2000, the UPS was upgraded for performance reasons. The new UPS is a redundant dual rotary system. Either side of the UPS is capable of supplying the CDC's electrical requirements. In the event of a utility outage, the Division of Mechanical Maintenance, Finance and Administration Cabinet, operates a 24-hour manned Central Utility Power System (CUPS) facility, which has diesel generators that will automatically start in the event of a power outage. There are two strings of batteries located in the CDC to provide power transition. The manufacturer of the UPS located in Middletown, NY is automatically notified of equipment fault status to the UPS. This is accomplished through a modem that is programmed to dial a specific telephone number and is also password protected. The UPS system is covered by a service contract with semi-annual service and inspection. The system is still under the original three-year warranty.

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.

Fire Protection and Halon

Five years ago a new fire alarm and notification system was installed. This new system has expanded detection for the elevator and has new visual and auditory alarms. The system on floors two, three and four is an air sampling system, which is extremely sensitive. The system has an automatic escalation, which will remove the likelihood of a halon release if the intensity of the danger increased. The halon suppression system covers floors two, three and four in the equipment areas, including the electrical and communication rooms. The main mechanical room on the first floor and the other areas are covered by a sprinkler system. The fire protection and Halon system is covered by a service contract, which has semi-annual inspections. The sprinkler system is also covered by service contract and is inspected quarterly. During many of these inspections and service calls, additional training for employees is given. One extensive day of training on the entire fire protection system and the scope of the halon suppression was held for employees this summer.

**Back-up and Contingency Planning**

*Backups and Recovery*

The mainframe disaster recovery strategy utilizes weekly full volume full data recovery backups of most of the DASD volumes attached to the IBM OS/390 server. The only volumes that are not backed up are the ones whose data changes too rapidly for a backup to be of any use and those that are more easily

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

created at the hot-site from scratch. These backup tapes are taken offsite to our secure storage facility for safekeeping and returned to us four weeks later. There are also daily backups of critical files that are taken offsite that include DB2 and IMS archive logs, some of the Information Management System (IMS) client nodes and selected application backups. This includes offsite backup copies of some of the TSM client nodes.

*GOT 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 an off-site location of system and application files (which reside on DASD) and a contracted hot-site location. Instructions in this manual include, but are not limited, to general information (statements, requirements, responsibilities), recovery preparations, recovery actions and return to normal processing procedures. A copy of the Disaster Recovery Manual and the instructions are also stored off-site at a secure underground storage facility. The agency responsible for each application also provides a designated representative who is responsible for the recovery or restoration of the application system.

GOT, recognizing the need to strengthen its ability to recover the Commonwealth's critical systems and functions in the event of a disaster, has written and issued a RFP to secure expertise for the purpose of developing and testing new disaster recovery plans. These plans will not only include systems running on the IBM OS/390 (mainframe computer), but also agency applications running on UNIX or NT servers that are maintained by GOT. The plans will also address networking and those functions running on enterprise servers (email, firewall, etc.) maintained by GOT. These critical systems and functions were selected by other state agencies and GOT through a Business Impact Analysis (BIA) process that also identified recovery timeframes, critical interfaces, and other information necessary for development of the plans. All applications that are deemed critical as part of our last Business Impact Analysis (BIA) are reviewed to ensure that the necessary backups are performed and taken off-site to the GOT underground storage facility.

Generally the RFP requires the vendor to:

- Develop plans for each critical system/function in the BIA, using a program/template that insures: clarity, standardization, and the ability to recover within the prescribed timeframe.
- Address security issues.
- Identify alternate approaches.
- Review and update the disaster recovery manual.
- Review and update changes that need to be made to GOT's current procedures, configurations, and DR organization to implement the new plans.
- Review and update the existing configuration with GOT's current hot-site provider.
- Identify and review all new and existing contracts that will be required to implement the new plans.
- Test the new plans as proof of concept.

GOT has added an additional Disaster Recovery (DR) staff member within the Division of Security Services to help support initiatives that can provide immediate improvement to its DR plan. These initiatives will also provide information and documentation for the successful RFP vendor. The initiatives include:

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

- Update the BIA immediately prior to awarding the contract.
- Collect and review existing documentation of the GOT's WAN/LAN infrastructure and their major service providers (i.e. Frankfort Plant Board, Sprint, etc.).
- Review and update DR plans in all facilities occupied by GOT. Designate coordinators, review space, review equipment and potential enhancements for alternate processing sites and establish communications procedures.
- Review and update areas of the DR manual that will accelerate the RFP planning process. Re-identify recovery management teams, their functions and responsibilities. Develop a contact list for recovery management teams, organizational entities, emergency personnel, vendor contacts, etc.

## **Mainframe**

### *Operations and Scheduling*

GOT operations are available/functional 24 hours per day, seven days per week and a supervisor is assigned to all shifts. The issues identified during a supervisor's shift are documented on a log sheet that is passed along to the next shift. This log includes the date, system changes, known communications problems, tape drives or disks drives off-line and other shift information. The shift turnover log is used in combination with a dry erase board in the Operations area to document equipment status issues on a daily basis. A Shift Procedures Manual is available to operators outlining the specific tasks to be performed and the approximate time of day that they should be performed.

The Division of IT Operations maintains an Operations Manual to provide instructions for operators on handling situations including system failures, restart procedures, and other emergency situations. All instructions provide primary contacts for the operators to discuss resolution actions and approval. Operators act to resolve system ABENDS as soon as possible. Agency application ABENDS are to be monitored by agency operators; however, GOT is aware of the ABENDS as they occur.

Most batch jobs are scheduled at the GOT using CA Scheduler, which is protected by RACF security. Only a few selected operators have access to add or modify the batch process schedules administered by GOT. GOT is also responsible for the administration and support of CA Scheduler. Most agencies are then responsible for their own batch operations and schedules. GOT Production Control is responsible for batch operations and scheduling of CFC, CHS, MARS, and Workforce Developments' UI (unemployment insurance) job streams. GOT operators have access to agency job schedules; however, they do not have access to agency job codes. GOT also runs a daily audit job that generates the GOT Scheduler Audit Report. This reports shows user changes to their job schedules. The job output is monitored daily on-line by the Systems Support Technician. This process is logged by the administrator and reviewed by operations management personnel.

### *Output Data Distribution*

GOT provides and supports two online report distribution products – IBM's RMDS, and MOBIUS' VIEWDIRECT for MVS. These 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 RACF. The owning agency of each report must authorize access to their reports – GOT administrators do not grant access to these reports without this authorization.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

*Security*

The Division of Security Services performs the Security Administration function. This division currently has three employees in the mainframe security group. This Division reports to the Office of Infrastructure Services.

Access to the IBM OS/390 Mainframe and its resources is controlled by the IBM package RACF, which is administrated by 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 days. After three unsuccessful logon attempts with a bad password, the user identification will be revoked and cannot be used again until a RACF 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 OS/390 Security Agreement. The Division of Security Services management must approve authorization of these functions.

Each agency is required to designate an IBM OS/390 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 Division of Security Services to become a security contact at an agency. The Division of Security Services 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 RACF and security administration
- Agencies that are able to reset their user's password only with all other administration being completed by GOT Security Administrators.
- Agencies that the GOT supports in all aspects of security administration.

The self-supported agencies will take care of their own administration but must follow GOT 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. GOT reviews the reports for those agencies that fall into the GOT supported category. A log is maintained to track the review of the violations. As an additional security precaution, multiple people review the logs.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

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

<b>Member Name</b>	<b>Description</b>
<b>CONNECTS</b>	This member contains a list of the agency's groups and what user ids are connected to those groups.
<b>DATASETS</b>	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).
<b>LASTUSED</b>	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
<b>RESOURCE</b>	This member contains a list of the agency's Resource profiles with the RACF class and what user ids / groups have access and at what level. (read, update, control, alter).
<b>UACC</b>	This member contains a list of the agency's profiles that have a UACC other than "NONE".
<b>USERGRPS</b>	This member contains a list of the agency's user ids with information about each user id.
<b>USERIDS</b>	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.
<b>USERTSO</b>	This member contains a list of the agency's user identifications that have TSO access.

User identification requests are assigned sequentially by the Division of Security Services and require a GOT-F181, RACF/Security User-ID Request form or an email from one of the agency contacts. The GOT-F181 form has recently been consolidated and is being used for all GOT type Security requests (Network, Mainframe, UNIX, NT, etc.).

As mainframe requests come in to the mainframe security group, they are entered into an MS Access Database and validated against the agency contact list to make sure the requestor is an authorized requestor. The requests with all the information are entered, given a unique tracking number and assigned to someone in the mainframe security group. When the request has been completed, the individual completing it updates the tracking system and the request by filling in the "date", "time" and "completed by" fields. Queries are available in MS Access to list the requests by request number, agency or requesting individual.

The Employee Departing Checklist (on-line web based system) notifies the Division of Security Services of any terminations or transfers of GOT employees/contractors. The Employee/Contractor Exit Request is sent to all of the mainframe security administrators to ensure that access is removed. When the

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

mainframe security group is notified of someone leaving, a query is run to check for a 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 GOT users change departments, their old user identification is put into REVOKE status. User identifications are then deleted and a new user identification is issued via the above procedure. User identifications with the prefix PS, only used for GOT, 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 GOT.

The Division of Security Services 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 GOT has developed several reports for agencies to use in order to assist them in identifying violations and reviewing access levels.
- RACF Administration - Several guidelines have been sent to the agencies suggesting the proper way to administer RACF, change a user's password, and add user identifications.

The Division of Security Services utilizes the Vanguard software suite to assist in security administration:

- Vanguard RACF Administrator - Allows cloning of user identifications and groups and allows reporting on RACF entities.
- Vanguard Advisor – Eases reporting on RACF Violations and System Management Facility (SMF) monitoring.
- Vanguard Analyzer – Produces many useful RACF system setup reports

A RACF Password Cracking utility to test the strength of the mainframe passwords is used periodically to 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. Reports are generated for internal GOT use also.

Access to DBMS databases is granted through RACF security software. Access must be authorized by the owner of the database and must be a written or electronic request to Division of Security Services.

The password for the System Emergency User Identification and the passwords for the RVAR Switch and RVAR Status have been sealed in envelopes and put in the GOT safe in the office area. In addition, dual control access is required. The password is split so that two individuals are required to use the user identification/password. The use of the password will be monitored and a log is also kept recording the use of the profile to ensure that it is restricted to emergency situations

In May 2001, the GOT enabled the cryptographic co-processor on the IBM OS/390 server, allowing the enhanced use of Secure Socket Layer (SSL) on this platform.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

## UNIX

### *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, rebooting servers, and notifying support personnel of problems and issues. However, operations does not reboot a server or restart any UNIX computers 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.

Batch-work processing in the UNIX environment is a manual process and these systems require monitoring during all phases of processing. Generally, batch-work processing starts at the same time that the batch-work for the mainframe is started for a particular software application. Most software applications require processes that coordinate between the UNIX system and the mainframe.

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 GOT 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.

### *Output data distribution*

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

### *Security*

A comprehensive Security Policies and Procedure 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 GOT's document management system.

An audit of user identifications was performed again this year. Some user identifications were reconfigured to be "su-only" (not loginable) 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



**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

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. GOT 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.

Virus scanning is being run daily on the Unix servers. A daily report is produced and reviewed every day. Also, staff is checking every day for DAT files.

Password restrictions are implemented so that all users must change passwords on a regular basis, have a 5-day grace period in which to change the password, will be locked out after 5 unsuccessful login attempts, and must use a password with at least 3 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 submitted to the Director of the Division of Security Services. A password cracking utility is used on a monthly basis to verify the strength of passwords. A final review of the user identifications will be conducted to verify that the restrictions put in place are being carried out. Most of the systems only have administrator, DBA, and developer user identifications and do not have user identifications for the end users of the systems.

The GOT-F181 is being used for user identifications creations and changes. Password resets and failed login count resets must be requested by email by the individual or the owner of a generic ID. Temporary passwords are sent by return email to the user and must be changed at next login. 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 GOT-F181.

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 and the Server Administration Branch Manager 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 via a web based system (GOT-F042 Departing Employee Checklist) to remove their user identification. 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 for AIX will be collected throughout the month. At the end of the month, the security patch information will be compiled and a list created for all system administrators to review. Solaris offers a "patchdiag" utility that will produce a similar list, and this utility is also run at the end of the month. At the beginning of the next month, security administrators will review the patches and those

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

that are required will be installed on test systems, with the owner's permission. After two weeks of evaluation, if no problems are found, patches will be rolled out to the remaining hosts according to the change control process. As patches are installed, they will be noted in a file on each host so that the monthly system information gathering process can include this information. Hard copy documentation supporting the change will also be filed. The exceptions to these procedures are the two KCCMS F50 servers and the Digital server. All three are running old versions of operating systems that are no longer supported.

Security administrators run Saint, a freeware utility that checks for system vulnerabilities, against each host, except for the older KCCMS F50 servers. This utility is run after a major release is installed. Security administrators fix problems that they can without causing problems in the application or the system. Security administrators will run Saint whenever a major change is made to the operating system or a newer version of Saint is obtained. Further, basic system auditing is activated and the output files produced are reviewed on a daily basis.

*Backups and Recovery*

Selected application data from the UNIX enterprise servers are backed up using the Tivoli Storage Manager (TSM) product, which is a client-server product. Most of the UNIX servers use the AIX TSM. 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 NT**

*Operations and Scheduling*

Windows NT 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 NT 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.

Batch-work processing in the Windows NT environment is a manual process. It requires monitoring during all phases of processing. Generally, batch-work processing starts at the same time the batch-work for the mainframe is started for a particular software application. Most software applications require processes that coordinate between the Windows NT system and the mainframe.

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 NT

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

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 GOT 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.

*Output Data Distribution*

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

*Security*

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

An NT security baseline is established for all NT enterprise servers. As each server is configured, a baseline script 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 NT team meets on the 1<sup>st</sup> and 15<sup>th</sup> day of the month to review all security vulnerabilities that have been identified. The team decides the impact of each vulnerability and makes a decision as to the implementation of a fix. Spreadsheets are maintained to track the testing and implementation of the fixes for each of the Windows NT servers. Documentation is maintained for each server that shows the security fixes that have been applied. Due to the large number of servers housed at GOT, tracking fixes from development, testing, and production can be cumbersome. The NT team stores and updates all documentation related to applied security fixes in a common location, which is accessible only to the security team. Each month all administrator passwords are changed and secured in a locked safe. These passwords can be retrieved by NT Team administrators in the event of an emergency.

Standards have been established for Windows NT 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.

Assignments have been made for the review of logs. On a daily basis, NT audit log alerts are reviewed. This review is logged and reviewed by the NT supervisor. Also, an in-house reporting application provides special reports for all servers. These reports include information, which show all users that have logged on to the system and the number times that a user logged on, users that log on to the system during unusual hours logon failures, and users that have been locked out of the system.

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

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

Additional password requirements are enforced for administrator passwords. In addition, password-cracking software is used on a regular basis for administrator passwords on the enterprise servers to ensure that password policies are being observed.

SSL certificates have been installed on Commonwealth IIS 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.

The Windows NT staff is notified when GOT staff members (contractors and employees) are terminated. A new web based notification system (GOT-F042 Departing Employee Checklist) is used to inform the appropriate individuals that the departing employee's security access can be removed. This process is initiated by an email from the Division of Security Services. An NT team member responds to the email by accessing and updating the web page.

NT staff regularly attends security training and conferences to stay abreast of new technologies. Two team members have attended SANS training, which is a recognized organization for information security. Also, a contractor is assigned to the GOT to assist in on the job training for security related issues.

STAT, a security vulnerability scanning software, is used on a regular basis to check for system vulnerabilities.

*Backups and Recovery*

Selected application data from the NT enterprise servers is backed up using the Tivoli Storage Manager (TSM) product, which is a client-server product. All of the NT servers use the IBM OS/390 TSM Server. Those TSM clients who participate in our offsite disaster recovery 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**

*Change Control*

The Governor's Office for Technology implemented a revised Change Management process effective April 1, 2001. The responsibility for this function lies within the Office of Infrastructure Services, Division of End User Support.

The process is outlined in GOT Policy Number GOT-008. The policy describes the responsibilities, policies, and procedures to be followed by GOT when making changes or recording events to the Commonwealth of Kentucky's IT infrastructure. The purpose of the Change Management process is to minimize service disruptions to our computing environment and promote system availability. This covers any and all changes to the 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).

GOT managers are responsible for pro-active planning in managing their environments. Change Requests should be submitted as soon as all planning has been completed, but no later than the mandatory deadline of 10:00 a.m. Wednesday. All Change Requests are submitted on the Change Request Form located at: <http://www.state.ky.us/got/ois/enduser/helpdesk/changcntl/ccform.html>. The Change Request must

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

include enough detail so that all areas know the relative impact of the change and how it may affect other areas.

Each request is discussed at the weekly Change Management meeting, which is 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 GOT customers. The Change Management Administrator or designee facilitates the meeting. Anyone submitting a change should be represented at the 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;
- 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.

The Change Control schedule is then posted each Thursday morning on the GOT Change Control website, and an email is sent out to the Change Control distribution list noting that a new schedule has been posted.

The primary participants of the Change Management process are the areas that affect the GOT infrastructure. GOT applications/development areas are to submit major events affecting production systems.

#### *Outage Review*

In January 2001, the Office of Infrastructure Service (OIS), Division of End User Support piloted an outage review process, where OIS formally reported on "unplanned" outages that had a major impact to GOT customers. The report identified the outage, the start and end dates and time, the trouble reported, the resolution, the action item(s), the person(s) responsible for the action item(s), the customers affected, the sequence of events from the time the problem is reported to the resolution, and the person(s) that provided the information. A spreadsheet is used to track all action items. Meetings are held with the OIS Directors each month to discuss status of the issues.

In the fall of 2001, this report was made available to all management within GOT. The intent is to provide the report within 36 hours of the resolution. The reports are available via GOTSsource, which is a GOT repository for documents. GOTSsource allows for keyword searches, which allows managers to do additional analysis and reporting. The next phase is to provide for trend analysis based on these outages. Reviewing the information should allow GOT to be more proactive in reducing these occurrences.

#### *Awareness Notification*

The GOT Help Desk will send the Awareness Report via email within 10 – 15 minutes, 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 Help Desk with a brief description of a problem and assessment of the services and users affected by the situation. A follow-up notification is

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

sent once the issue is resolved. If the issue is not resolved by 4:00 p.m., a status is sent to the Help Desk so it can be included in the Evening Report.

The Awareness Notification distribution list is made up of not only GOT personnel, but also many of the key individuals within the agencies. Anyone can be added/deleted to the list by contacting the GOT Help Desk.

*Evening Report*

A report is sent out to the Awareness group every evening at 5:30 p.m. This report is a listing of current outages or outages that occurred during the day that affect major sites/customers. Sites or systems that are totally down are identified on the report in red, and sites being monitored are identified in blue.

The information provided includes the:

- Remedy ticket number (this is the problem tracking number);
- Time problem started;
- Time problem is resolved;
- Site, area or system that is down or is having problems;
- Resolution that corrected the problem; and
- The support group that was assigned the problem.

This gives key personnel a consolidated list of the outage activity for a 24-hour period.

*Internet and Enterprise 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 HP Openview gather these logs.

The GOT Firewall team documents these attempts and completes a security incident report that is sent to the security division 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 we have communicated with management from that party. On Intranet attacks, the offending IP or entire IP subnet of the offending party is blocked. Communications will not be re-established until the offending entities' CIO responds as required by GOT policy. Network services will resume and continue as long as the offending party demonstrates they are in compliance with GOT network security policies.

The firewall also contains a Demilitarised Zone (DMZ) for resources that need visibility to the Internet. The DMZ was created to allow state agencies the opportunity to place WEB, FTP, and other servers that need this functionality to be on a separate subnet from the rest of the Intranet. This allows GOT to restrict unnecessary traffic from accessing agencies' internal networks and promote a more secure infrastructure.

*Intrusion Detection Systems (IDS)*

A joint decision was made within the Office of Infrastructure Services to make Internet Security Systems (ISS) the enterprise standard for network based IDS. GOT has been working on a pilot IDS system from ISS since September 2000. GOT's current platform has agents installed to detect security breaches from the Internet and at the MARS application server farm. This system interfaces with GOT's Checkpoint

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

Firewall-1's management console for alerts and automated actions based upon the rule sets established. When the IDS agents identify attack signatures, they will block the IP address at the firewall and then notify the GOT Firewall Team by email. Also, automatic pages are sent to the primary and backup pagers of the Firewall support staff that are on call.

GOT now has a security contract that provides product, maintenance, and professional services. Internet Security Systems (ISS), Systems Design Group (SDG), and Fishnet Security, Inc. hold the contract jointly.

GOT has installed an Intrusion Detection System (IDS) from ISS and is currently working on a pilot for server-based Intrusion Detection. The Technical Services Branch will manage the pilot that will involve various servers within the infrastructure including, Exchange messaging servers, PDC's, File Servers, and other devices as identified by staff personnel.

*Enterprise Applications / Cabinet Firewalls*

GOT provides firewall services for various state agency applications. (A detailed list is available upon request.) The customer owns the rules set for each firewall. GOT has been working 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.

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. All of the firewall consoles, servers, and other network hardware are maintained in a secure, physical access-controlled location.

*Agency Firewalls*

GOT has a firewall appliance solution that offers the same level of protection as the enterprise service offering. The service utilizes the Checkpoint Firewall-1 product and can provide VPN services. GOT currently has customers utilizing the service.

*Virtual Private Networking (VPN)*

A Virtual Private Network (VPN) is also available for clients wanting a secure connection from their access point to the GOT Firewall or to their own GOT administered firewall. All VPN users are required to enter a username and password to connect with the VPN client. Once the connection is accepted, a "secure tunnel" is created from their workstation to the firewall. This service is available upon request for all Internet and Intranet clients.

*Network*

All backbone routers and switches are monitored at all times and are configured to send an alert message upon failure of hardware or if security breaches have been attempted. These attempts are logged and reviewed every morning by the Internet team. GOT measures the performance of the WAN links with HP Openview, ServiceLink, and MRTG. These tools allow the ability to provide measurements for

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

customers and to take a more proactive approach in Network performance monitoring. GOT measures availability, response time, and error conditions. ServiceLink has a web interface that can be used to track these issues in real time and allows the ability to report problems and update trouble tickets. Senior engineers in both the Enterprise Services area and the WAN area perform capacity planning with the help of these tools.

*Virus Protection*

McAfee of NAI is the enterprise IT standard for virus scanning. GOT has Total Virus Defense (TVD) and Active Virus Defense (AVD) agreements with McAfee, which validates GOT's multi-tiered approach to virus protection.

TVD includes the following:

- VirusScan: Virus protection for desktops
- NetShield: Virus protection for servers

VirusScan's and NetShield's AutoUpdate feature uses pull technology to keep our virus protection current at all times. The agent checks daily for DAT updates and weekly for engine upgrades.

- GroupShield: Virus protection for Exchange servers
- WebShield: Virus protection for in-bound Internet mail

The combination of WebShield and GroupShield helps promote a nearly virus-free messaging environment.

AVD includes the following:

- All of the above products
- ePolicy Orchestrator (ePO)

ePO provides additional power in maintaining a complete virus security solution. It is designed to manage policies and deploy protection while generating detailed graphical reports on McAfee's anti-virus products. It has the ability to provide up-to-the-minute information that the virus signature and scan engines are up to date.

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

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

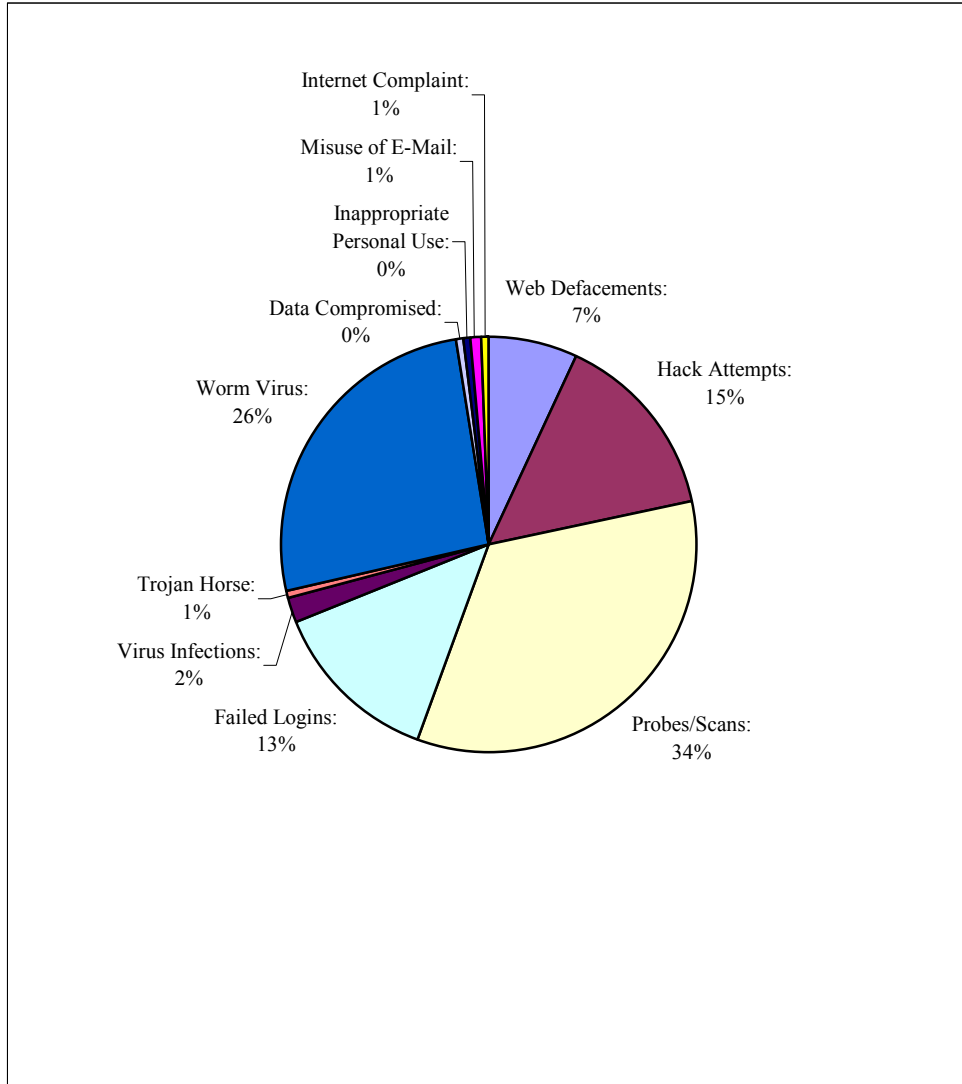
*Incident Reporting*

GOT implemented a security incident reporting policy that requires employees and/or contractors to report suspected security violations immediately. A security incident reporting form (GOT-F012) is made available for use in reporting security incidents. As incidents are reported, the Division of Security Services performs investigation and follows up as required. Monthly spreadsheets are prepared that



**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

provide statistics on the number of incidents being reported by type. The following summarizes the incidents for the calendar year 2001.



<i>Web Defacements:</i>	65
<i>Hack Attempts:</i>	136
<i>Probes/Scans:</i>	314
<i>Failed Logins:</i>	123
<i>Virus Infections:</i>	19
<i>Trojan Horse:</i>	5
<i>Worm Virus:</i>	243
<i>Data Compromised:</i>	4
<i>Inappropriate Personal Use:</i>	4
<i>Misuse of E-Mail:</i>	8
<i>Internet Complaint:</i>	6
<i>Total Primary:</i>	<b>927</b>

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
**Provided by the Governor's Office for Technology**

*Policies and Procedures*

A comprehensive Security Policies and Procedure Manual (SPPM) was implemented at the beginning of 2001. The manual includes logical security, managerial security, physical security, contingency planning, and security awareness. The manual was distributed to all GOT staff. In addition, several administrator manuals were implemented to provide guidelines to staff in the administration of the NT and UNIX environments. These include: (1) Administrator's Manual for NT; (2) Administrator's Manual for Solaris; and (3) Administrator's Manual for AIX. These manuals are available on GOT's document management system.

*Vulnerability Assessments*

The Division of Security Services has staff available to perform vulnerability assessments. These staff members have been working not only with GOT internal staff but also with agency staff to identifying vulnerabilities. An RFP currently resides within the Division of Purchases that will provide a contract mechanism to obtain additional resources for assessments and audits.

*Security Alerts*

The GOT Division of Security Services has purposed to provide guidelines for the handling and reporting of security alerts to those individuals charged with the security of the Commonwealth's computer and network resources. In doing this, GOT has begun to provide a structured, routine and timely service of announcing security alerts to proper personnel and distribution lists. It is the intent of GOT 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 Division of Security Services 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, GOT has recently entered into a contract with Security Focus to receive security alerts on a daily basis. Analysts within the division are charged with the responsibility to review these notifications as soon as they arrive. Once an alert has been determined to be critical to send out to agencies, the security analyst will supply the necessary information to other security staff members who are designated to craft the alert notification and post the detailed information of the alert on the GOT security alerts web page. The security alerts web page has been designed specifically to contain technical information on each alert. On a weekly basis, GOT produces a "Weekly Security Alert Recap." The recap attempts to cover all security alerts not deemed as an immediate threat to the Commonwealth of Kentucky computing environment, yet still important enough to be highlighted in a weekly communication. This weekly recap is emailed to the GOT regular security contacts and other appropriate distribution lists. This weekly information is posted and updated regularly on the security alerts web page.

*Secure E-mail*

GOT has begun an e-mail encryption pilot program using Entrust Technologies Express for Outlook product. Initially, more than 10 GOT employees installed and used the security software over a several month period. The pilot has been extended to about 100 selected participants in different agencies. Some of these agencies include: Finance, Transportation, Revenue, Workforce Development, Personnel, and Military Affairs / Homeland Security. The pilot is expected to end in late February or March 2002. A decision will be made at that time regarding implementation across the enterprise.

## **Organization and Administration**

### Control Objective 1

Controls provide reasonable assurance that GOT policies and procedures are documented and GOT functions and responsibilities are appropriately segregated.

#### *Tests of Operating Effectiveness Achieved*

- Inspected policies and procedures related to oversight and management of the organization.
- Reviewed the organizational chart for completion, accuracy and appropriateness to the situation.
- Reviewed the GOT organization chart noting the degree to which operations/programming functions are segregated.
- Interviewed computer operations management and programming management to determine adherence to policy.
- Reviewed the organization chart to verify existence of specific functions and departments.
- Reviewed the policies and procedures of the GOT to ensure that GOT personnel do not initiate or authorize transactions.
- Ascertained that personnel policies exist and reviewed them for inclusion of policies for hiring, termination, salary administration, performance evaluations, vacation, employee benefits, building and system security and emergency procedures.
- Reviewed policies related to GOT specific personnel, security, and administrative policies.
- Obtained and reviewed the strategic planning and major accomplishment documents.
- Discussed with management and reviewed documents regarding training provided to agency personnel.

## **Application Maintenance and Documentation**

### Control Objective 2

Controls provide reasonable assurance that changes to applications are authorized, tested, approved, properly implemented, and documented to provide an audit trail to facilitate future program changes.

#### *Tests of Operating Effectiveness Achieved*

##### **Mainframe**

- Reviewed program change control procedures with management noting detailed procedures for program implementation.
- Inspected a judgmental sample of program change requests from the “EPM Projects Requested Report” with a request date between July 1, 2001 and June 30, 2002 and traced the request from authorization, initial agency approval, and prioritization, to properly implemented program in the production directory. Projects not completed were inspected to ensure the current project status was identified as "active."

## APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inspected a judgmental sample of program executables from the production directories with a last modified date between July 1, 2001 and June 30, 2002 and verified that the System Life Cycle was followed, and supporting documentation was properly completed.
- Reviewed the Systems Life Cycle Manual (SLCM) for documented policies and procedures for development and maintenance of applications.
- Inspected SLCM to determine whether it outlines that certain deliverables are required for change requests.
- Inquired of management to determine whether the System Life Cycle Manual is followed for larger projects.
- Reviewed EPM reports and discussed with management to determine its use in documenting program change requests and the status of those requests.
- Inquired of Project Management to determine the types of testing performed by GOT.
- Inquired of Project Management to determine that Production Program Cutover Process was used to promote mainframe program changes.
- Inspected a judgmental sample of Production Program Cutover Forms for appropriate approval and authorization.
- Inquired of Project Management to determine user involvement in testing changes to programs.
- Inspected a judgmental sample of documentation maintained by GOT programmers for changes to programs.
- Inquired of Project Management to determine that documentation was provided to the agencies for changes that affect users.

### UNIX/Windows NT

- Reviewed program change control procedures with management noting detailed procedures for program implementation.
- Inspected a judgmental sample of program change requests from the “EPM Projects Requested Report” with a request date between July 1, 2001 and June 30, 2002 and traced the request from authorization, initial agency approval, and prioritization, to properly implemented program in the production directory. Projects not completed were inspected to ensure the current project status was identified as "active".
- Inquired of management to determine whether the System Life Cycle Manual is followed for larger projects.
- Reviewed EPM reports and discussed with management to determine its use in documenting program change requests and the status of those requests.
- Inquired of Project Management to determine the types of testing performed by GOT.
- Inquired of Project Management to determine user involvement in testing changes to programs.
- Inspected a judgmental sample of documentation maintained by GOT programmers for changes to programs.

- Inquired of Project Management to determine that documentation was provided to the agencies for changes that affect users.
- Inspected a judgmental sample of UNIX/Windows NT implementations.

*Tests of Operating Effectiveness Not Achieved*

**UNIX/Windows NT**

- Reviewed the Systems Life Cycle Manual (SLCM) for documented policies and procedures for development and maintenance of applications.
- Inspected SLCM to determine whether it outlines that certain deliverables are required for change requests.
- Inspected access to production directories for appropriateness for a judgmental sample of production directories.
- Inquired of Project Management to determine that appropriate implementation procedures are used for UNIX/Windows NT program changes.

Finding: As noted in prior years, application development controls over the mainframe processing environment appear to be well designed, while application development controls over the client/server applications that utilize the UNIX and Windows NT operating systems are not as mature. Management has made significant improvements in application development controls to ensure that GOT programmers are appropriately restricted and monitored. However, in four of the ten applications selected for testing on the UNIX and Windows NT, GOT programmers have access to the production libraries.

Recommendation: We recommend that management restrict programmer access to the development and staging libraries to help ensure that the proper segregation of duties exists. In the event that management has a business need to allow access to both the source code and to the production environment, procedures should be implemented to require the daily review of all items moved to the staging libraries by an individual independent of the process. This individual should verify that all items are supported by the originating request and are not source code that has been modified by the individual promoting items to the staging library.

Management Response: *POS - This situation has been corrected. The programmer(s) no longer have access to any production code. The Librarian moves the file to a staging area and contacts Operations Staff to move the file to Production.*

DHR – *New procedures have been put in place to correctly handle DHR. The cut over procedures call for the Librarian to place the appropriate files (.jar, jsp's , etc) in a staging folder and Production staff then deploy them to production.*

KCCMS - *is an application developed for CFC by a vendor several years ago. The platform is Oracle on UNIX. The application, due to a number of shortcomings with the original development, has already been targeted for redesign and platform migration by the customer agency. The 1st phase of the redesign is underway and targeted for completion during this calendar year. The 2nd phase is scheduled for calendar year 2003.*

*Security is deeply embedded into the application with id/passwords being coded in some programs and batch scripts. Changing security or permissions is therefore a much more complex task.*

*The following actions have been taken to facilitate tighter controls:*

- *Analysis indicates that the security design does not lend itself to an easy fix of the application. The agency CIO has been advised of this problem but since a replacement for the application is underway, we've not been authorized to correct the current problems. The replacement application will address the security problems.*
- *We've obtained written confirmation from the customer for the use of the kyprod id when necessary. Each use will require management and customer authorization.*
- *A log to track all kyprod authorizations has been implemented.*
- *A software tool that will facilitate monitoring of kyprod usage has been installed. Implementation and staff training currently underway. The manager & director on a monthly basis will monitor usage logs.*

*KEWES - the access noted for these two programmers has been deleted and they will rely on librarian resources from other areas as backup to their project librarian. Programmers will not be performing librarian functions.*

- Inspected a judgmental sample of program executables from the production directories with a last modified date between July 1, 2001 and June 30, 2002 and verified that the System Life Cycle was followed, and supporting documentation was properly completed.

Finding: A review of a sample of program changes taken from a population of programs completed or initiated during the current fiscal year revealed the following:

- The project number for two program change requests was not entered in the documentation in the source control software (MS Visual Source Safe).
- E-mails that are sent to users detailing time and cost estimates for programming change requests were not retained for one programming change request.
- A time and cost estimate was not given to the requesting party prior to the implementation and start of work for six programming change requests. However, the department has since implemented procedures for the notification of time and cost estimates.

Recommendation: We encourage management to reinforce the program change control standards and procedures included in the Systems Life Cycle Manual (SLCM) in order to ensure that all program changes are properly documented and time and cost estimates are approved. Documenting the project number in the source control software will provide management with an audit trail to trace changes to the request for the change thus providing a reason for each change. Providing time and cost estimates to agencies prior to starting a project will help facilitate management of each project and potential future billing.

Management Response: *The noted project numbers that were not entered in the documentation in the source control software have been entered and the existing policy for doing so has been reinforced. As noted within the bullets above, procedures have been implemented for such notification & retention of time and cost estimates.*

## System Software and Hardware

### Control Objective 3

Controls provide reasonable assurance that changes to system software and hardware are authorized, tested, approved, properly implemented and documented to provide an audit trail to facilitate future system changes.

#### *Tests of Operating Effectiveness Achieved*

- Inquired of the Server Administration Branch Manager to determine whether only the Server Administration Branch is responsible for implementing and maintaining system software in the Enterprise Application Domain at GOT.
- Inquired of the Server Administration Branch Manager and LAN Supervisor to determine how system software is selected and authorized.
- Inquired of the Server Administration Branch Manager and the LAN Supervisor to whether testing is performed in a test region.
- Inspected a judgmental sample of Change Control schedules to determine whether upgrades, changes, and tests were scheduled appropriately.
- Inquired of the Server Administration Branch Manager and the LAN Supervisor to determine that a full system backup is performed prior to implementation of any changes to system software.
- Inquired of the Systems Programming staff to determine that SMP is used to manage and monitor changes to system software.
- Inspected a judgmental sample of documentation for mainframe system software products, which included release, version, and vendor information.
- Inspected a judgmental sample of the on-line user documentation including product manuals and help files maintained in BookManager.
- Inquired of the LAN Supervisor to determine that the Technical Services Branch is responsible for implementing and maintaining system software on the file and print, email and Internet servers.

## Physical Security

### Control Objective 4

Controls provide reasonable assurance that safeguards and/or procedures are used to protect computer equipment, storage media, and program documentation against intrusions, fire, and other hazards.

#### *Tests of Operating Effectiveness Achieved*

- Discussed with management procedures revoking physical access for departing employees, contractors, vendors and others separated from active involvement with GOT.

- Discussed with management procedures for issuance of card keys to determine whether terminated or inappropriate personnel have access to the doors at the Commonwealth Data Center.
- Observed physical security procedures throughout the audit and verified the compliance with the Security Policies and Procedures Manual.
- Inspected a sample of card key access levels and discussed with management the appropriateness of the access levels.
- Verified card key access levels by selecting a sample of card keys and attempting to access doors and areas for which those keys should have been restricted.
- Inspected reports from the card key system to determine that invalid access attempts and other reports are reviewed on a daily basis and significant issues are reported to management.
- Observed the receptionist monitoring the building entry sign-in forms and access to the Commonwealth Data Center throughout the audit.
- Observed video cameras at the access points to the Commonwealth Data Center and computer rooms and discussed with management the procedures for reviewing and storing the tapes.
- Discussed procedures for admitting and escorting visitors in the Commonwealth Data Center and observed application of the procedure throughout the audit.
- Toured the Commonwealth Data Center building and the computer room and noted the presence and location of portable fire extinguishers (recent inspection), fire detection sensors and alarms, automatic fire extinguishing system, electrical power shut-off switch, telephone in the computer room that can dial directly outside, emergency lighting, and emergency exit signs.
- Toured the Commonwealth Data Center and computer room and noted the presence and location of a UPS system and generator.
- Toured the computer room and noted the presence and location of separate air conditioning units.

## **Logical Security**

### Control Objective 5

Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.

#### *Tests of Operating Effectiveness Achieved*

- Reviewed the Security Policies and Procedures Manual and other security policies and brochures to evaluate management direction of logical security of the GOT.
- Discussed with management the security policies for the various platforms at the GOT.
- Discussed with management the policies and procedures for modifying the agency security contact list to determine appropriateness.



- Discussed with management procedures for adding, deleting, and changing user identifications and inspected documents to determine whether procedures for granting access and issuing user identifications and passwords are followed.
- Discussed with management procedures for revoking users and use of the Departing Employee Checklist.
- Discussed with management procedures for reviewing violation reports and security logs on the NT and UNIX platforms at the GOT to determine appropriateness.
- Inspected documents and reports to determine that GOT security policies are implemented on the system settings for the various platforms at the GOT.
- Inspected documents and reports to determine whether access to source program libraries is properly restricted.
- Inspected documents and reports to determine whether access to production program libraries is properly restricted.
- Discussed with management procedures for implementing security patches and “hot-fixes” on the systems at the GOT.
- Discussed with management the procedures for individuals to gain dial-up access to system resources.
- Discussed with management procedures and responsibilities of staff to monitor the network security.
- Discussed with management procedures for reviewing violation reports and security logs on the mainframe platforms at the GOT to determine appropriateness.
- Discussed with management the RACF Security Administrator System Emergency user profile.

## **Contingency Planning**

### Control Objective 6

Controls provide reasonable assurance that system and application backup procedures are performed; significant files are stored off-site.

#### *Tests of Operating Effectiveness Achieved*

##### **Mainframe/UNIX/Windows NT**

- Discussed with management to verify that full system backups are created weekly and retained in the off-site storage facility.
- Reviewed procedures used to take daily backup tapes off-site to result in an adequate rotation schedule.
- Reviewed the log listing of the backup tapes, which are maintained off-site and verified that the tapes were present off-site.
- Observed the procedure of preparing the backup tapes for off-site delivery.

- Toured the off-site storage facility and noted that proper controls exist in the storage of backup tapes.
- Toured the off-site storage facility to determine whether a copy of the Disaster Recovery Manual and operations, systems and other reference materials are maintained off-site.
- Discussed with management the backup procedures in place for the systems at the GOT.
- Toured the GOT tape library and noted the organization of the tape-based media.
- Discussed tape labeling and logging procedures with management.
- Inquired of the Security and Recovery Branch Manager to determine the involvement of agencies in developing and testing back-up and recovery procedures.

**Infrastructure**

- Reviewed the log listing of the backup tapes, which are maintained off-site and verified that the tapes were present off-site.
- Discussed with management the backup procedures in place for the systems at the GOT.
- Discussed with management the backup procedures in place for configuration files (firewalls, routers, email, LAN).
- Reviewed checklists, which document the procedures for the backing up of the e-mail servers.
- Toured the GOT tape library and noted the organization of the tape-based media.
- Discussed tape labeling and logging procedures with management.
- Reviewed procedures used to take daily backup tapes off-site to result in an adequate rotation schedule.

Control Objective 7

Controls provide reasonable assurance of continued operations in the event that systems become unavailable; and formal plans for recovery have been considered.

*Tests of Operating Effectiveness Not Achieved*

- Discussed with management the availability of compatible systems at the hot-site location.
- Obtained a copy of the Disaster Recovery Manual and reviewed it for completeness and for being current.

Finding: The Disaster Recovery Manual includes only systems on the IBM OS/390 system but does not include the recovery procedures for applications running on UNIX or NT platforms. Except for the mainframe and hardware supporting critical MARS applications, compatible systems are not maintained for backup purposes (infrastructure, e-mail, enterprise servers, etc.). Based on the project to develop the Disaster Recovery Manual, specific rebuild instructions for all critical systems are being formalized. The omission of such procedures and systems creates the potential risk that the GOT will be unable to recover these systems in a timely manner in the event of a disaster. It is recognized that the GOT is in the process of

contracting with a consulting firm to gain assistance in the development of a comprehensive Disaster Recovery Manual that addresses all systems. We encourage management to continue with its efforts to include all critical systems in the Disaster Recovery Manual and to secure available equipment to support critical functions in the event of a disaster.

*Management Response:* The Finance and Administration Cabinet awarded the disaster recovery planning contract to LBL Technology Partners with an effective date of July 16, 2002. GOT has assembled a project team and work has already begun with LBL Technology Partners. The GOT Executive Steering Committee for this project has also met and reviewed deliverables and next steps. The current project plan indicates a completion date in late December, 2002.

- Reviewed the results of the most recent disaster recovery test.

Finding: Due to the current Request for Proposal (RFP) for the development of the Disaster Recovery Manual, a test of the plan is not scheduled for this year. Management has signed a contract with a consulting firm to assist in the development of the Disaster Recovery Manual with an anticipated start date of July 16, 2002 with completion scheduled for January 2003. Due to the timing of this project, testing has been tentatively scheduled for March 1, 2003.

Recommendation: We recommend that management evaluate options to ensure that adequate testing of the disaster recovery process is conducted. Testing of disaster recovery operations should include setting the test objectives, formalizing the test results, updating the plan for problems noted during testing, as well as procedures for retesting in the event of unsuccessful results. We also encourage management to conduct walkthroughs, simulations, and other tests as identified by the plan to ensure that disaster procedures are communicated and understood by GOT staff. Further, these tests of the disaster recovery process should be conducted on an on-going basis, and the results should be included and reflected within the Disaster Recovery Manual.

*Management Response:* The Finance and Administration Cabinet awarded the disaster recovery planning contract to LBL Technology Partners with an effective date of July 16, 2002. GOT has assembled a project team and work has already begun with LBL Technology Partners. The GOT Executive Steering Committee for this project has also met and reviewed deliverables and next steps. The current project plan indicates a completion date in late December, 2002. GOT currently has a contract with SunGard for testing. GOT has reserved a date of March 28, 2003 in Chicago for the next scheduled test. GOT has scheduled a walkthrough for December 16, 2002.

GOT has participated in two simulations during the past fiscal year. On December 6, 2001, GOT participated in a Small Pox contamination simulation exercise. The area of infection was Frankfort, Kentucky and resulting in citywide exposure and resulting disaster issues. This test involved contingency procedures for some GOT operations. The GOT Disaster Recovery Manual was updated after this exercise and redistributed to the appropriate staff and team members. On May 15, 2002, GOT participated in a chemical/biological simulation exercise that resulted in an extended evacuation of a GOT facility at the Fair Oaks Complex. Many of the support staff that manage major systems were affected by this disaster event. GOT staff at that complex are participating in follow-up discussions with other state agencies since the Fair Oaks Complex is a multi-agency facility. Enhancements will be made to the GOT Disaster Recovery Plan as a result of those activities.

## **Computer Operations**

### Control Objective 8

Controls provide reasonable assurance that processing is scheduled appropriately and deviations are identified and resolved.

#### *Tests of Operating Effectiveness Achieved*

- Discussed with management as to the procedures of scheduling batch jobs.
- Discussed with management as to the appropriateness of users with access to modify job schedules and reviewed access to the schedule by inspecting documents and reports.
- Discussed with management their review of audit reports, which show changes made to agency job schedules.
- Reviewed operations, console logs, and job scheduling manuals for completeness.
- Discussed with management to verify that job scheduling reports are produced, which specify the completion of mission critical processing jobs, along with any abends or problems that occurred.
- Discussed with management the procedures used to monitor system activity, downtime, or system outages.
- Inquired of the management to determine that operators were on duty during regular shifts.
- Inspected a judgmental sample of the shift turnover logs to determine their use by operators.
- Inspected the Shift Procedures Manual to determine that it identifies specific tasks and approximate times that they should be performed.
- Inspected the GOT Operator Manual to determine that the manual contained the following information:
  - Problem and Emergency Notification Contacts and phone numbers
  - System Service phone numbers
  - Problem Handling \ Escalation Procedures for the system as well as system applications
  - System and system application restart procedures
  - Weekly Maintenance Procedures
- Inspected a sample of daily console logs for system downtime documentation.
- Inspected a judgmental sample of the daily GOT Evening Reports for help desk service items and abend documentation.
- Inspected a judgmental sample of Monthly Availability Reports displayed on-line as Server Metrics to determine whether system downtime is published.
- Inspected a judgmental sample of Weekly Change Schedules to determine that scheduled changes were included on the Monthly Availability Reports.
- Inquired of the management to determine communication of the Weekly Change Schedule to the users.

## APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired of the management to determine what type of monitoring is performed in the LAN environment.
- Inquired of management to determine what tools were used by GOT employees to perform capacity planning in the LAN environment.
- Inspected a judgmental sample of Nightly Cycle Documents to determine their use in reporting key information to senior management.
- Inquired of the Production Control Manager to determine the monitoring of the GOT Scheduler Audit Report.

### Control Objective 9

Controls provide reasonable assurance that output data and documents are distributed to authorized recipients on a timely basis.

#### *Tests of Operating Effectiveness Achieved*

- Inquired of management as to the distribution methods for reports run by agencies.
- Inspected reports printed for agencies to determine banner pages included appropriate information.
- Inquired of management to determine that reports were being packaged and labeled for distribution to agencies.
- Inquired of the management to determine that RACF is used to control access to reports.
- Discussed print output distribution methods with operations management and personnel to determine adherence to standards.
- Discussed with management the use of schedules listing the reports to be provided to each agency.
- Toured the print operations room and noted that proper controls exist in limiting access to the room.
- Discussed with management the procedures in place to control the storage of outside vendor tapes.
- Reviewed agency forms used to control the storage and distribution of outside vendor tapes.

## **USER CONTROL CONSIDERATIONS**

This section outlines specific user control considerations, or issues each agency may want to consider and address for the purpose of monitoring the data processing done by the GOT. These considerations are not necessarily a comprehensive list of all internal accounting controls that should be employed by the user agency, nor do they represent procedures that may be necessary in all circumstances.

### **Organization Structure and Personnel**

- Controls should be established to ensure that agency employees are adhering to Enterprises Policies.
- 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.
- Controls should be established to ensure that agencies properly use GOT forms, policies, and procedures when interacting with or requesting items from the GOT.
- Controls should be established to ensure cost allocations from GOT services are appropriate.
- Controls should be established to ensure that employees are adequately trained.

### **Applications Maintenance and Documentation**

- Controls should be established to ensure that all requests sent to GOT are prioritized.
- Controls should be established to ensure that if time and budget estimates are presented by the GOT, the time and budget estimates are reviewed and approved by the appropriate individuals at the agencies.
- 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 GOT.
- Controls should be established to ensure that software supported by out-side vendors is properly tested prior to implementation of the software application or change.
- Controls should be established to ensure that the agencies, when responsible, make only approved, tested and documented changes to software when appropriate.

### **System Software and Hardware**

- Controls should be established to ensure that agencies, when responsible, install only appropriate system software in the their systems.
- Controls should be established to ensure that the agencies, when responsible, make only approved, tested, and documented changes to system software.

## APPENDIX B –USER CONTROL CONSIDERATIONS

- Controls should be established to ensure that the agencies participate or review change control documentation at the GOT for the weekly change control meetings.
- Controls should be established to ensure that agencies, when responsible, install only appropriate system software in the network environments.

### Logical Security

- Controls should be established at the agencies for reviewing the GOT Agency IBM OS/390 Security Agreement and ensuring compliance with the terms of the agreement.
- Controls should be established at the agencies for designating an IBM OS/390 authorized security contact.
- Controls should be established for those agencies that are responsible for their own RACF administration to restricting access to data sets and programs under the RACF Security software and for monitoring security reports provided by the GOT.
- Controls should be established for those agencies that are responsible for their own RACF administration to review and monitor the CA Scheduler listing to identify and remove users that are no longer required to have access to the system.
- Controls should be established for those agencies that are responsible for resetting their own passwords on the IBM OS/390 to ensure that this activity is appropriately restricted.
- 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.
- Controls should be established at the agencies for controlling access to IBM's RMDS and Mobius's View Direct for reports and assigning access to these in RACF.
- Controls should be established at the agencies to ensure that agency employees are using strong passwords and adhering to GOT recommended standards for passwords.
- Controls should be established at the agencies to ensure that agency employees are appropriately removed from the systems at the GOT upon termination of their employment or changes in responsibilities.
- Controls should be established at the agencies to ensure that agency employee access to applications and data are properly controlled.
- Controls should be established at the agencies to ensure that each generic user identification is assigned to the appropriate authorized individual.

### Back-up and Contingency Planning

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

## APPENDIX B –USER CONTROL CONSIDERATIONS

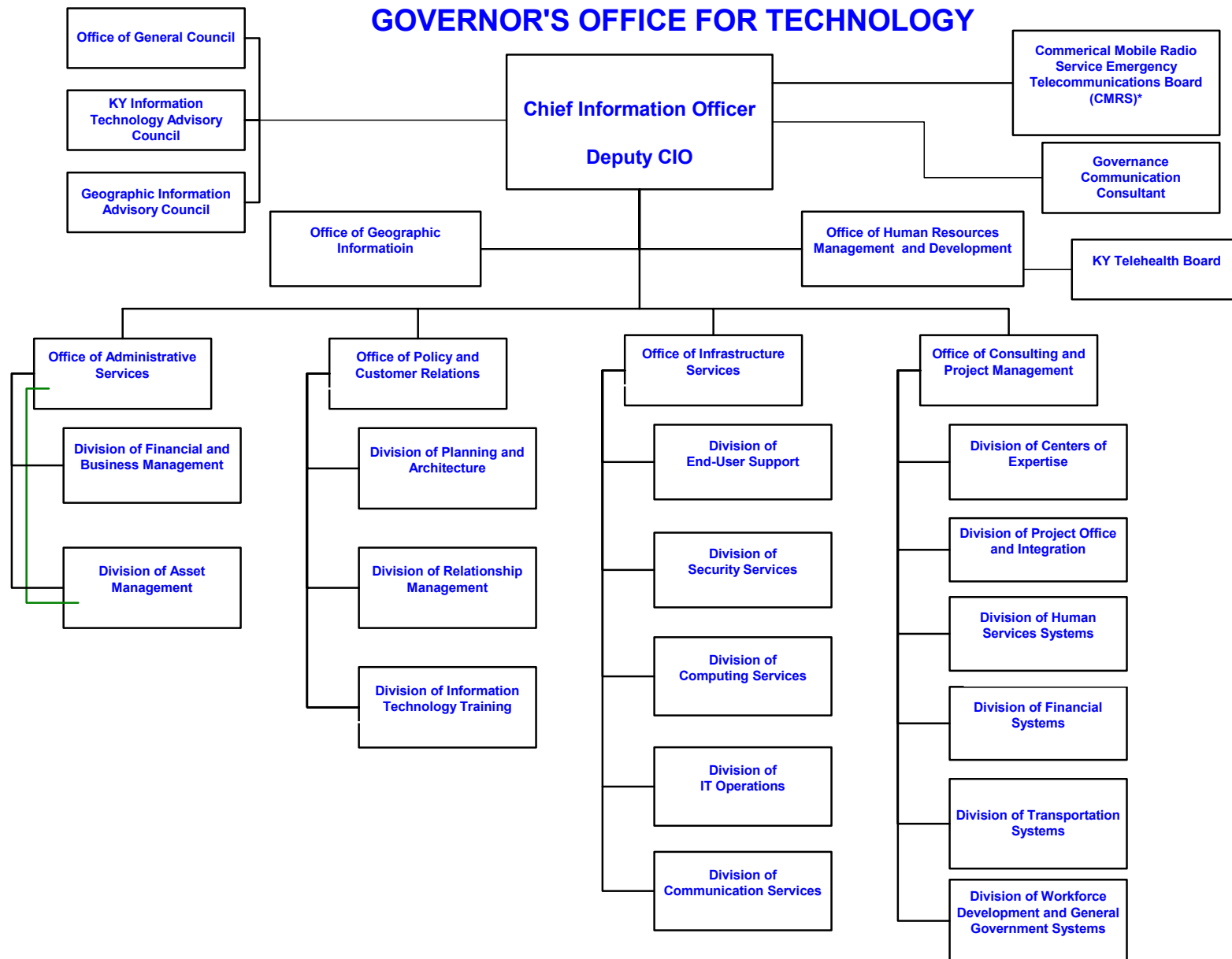
- Controls should be established to ensure that the agency informs the GOT of the criticality of the data, files, programs, etc. that should be backed up and the off-site rotation for these items.
- Controls should be established to ensure that the agency designates a disaster recovery coordinator that is responsible for coordination of recovery procedures with the GOT.
- Controls should be established to ensure that the agencies participate in business impact analysis with the GOT to determine risks and recovery priorities.
- Controls should be established to ensure that Agency Disaster Recovery procedures, critical applications, and critical circuits are identified and communicated to GOT.

### Computer Operations

- Controls should be established to ensure that agency batch jobs are properly scheduled and run in accordance with the schedule.
- Controls should be established to ensure that only properly authorized individuals have access to maintain batch job schedules and libraries.
- Controls should be established to ensure that agencies monitor and document abends that occur related to their applications and batch jobs.
- Controls should be established to ensure that reports generated at GOT are received and distributed to the appropriate individuals in a timely manner.
- 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.
- Controls should be established at the agencies to ensure that data transmissions are complete, accurate, and secure.
- Controls should be established to ensure that the agencies reconcile the number of records sent to GOT with the number of records actually received and processed by GOT.
- 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 GOT.
- Controls should be established to ensure that the agencies review the Awareness Reports as they are issued.
- Controls should be established to ensure that the agencies review the Evening Reports.
- Controls should be established to ensure that the agencies review the Change Control postings.



APPENDIX C – ORGANIZATIONAL CHART



# Kentucky Information Highway

