DEPARTMENT OF INFORMATION TECHNOLOGY

RICHMOND, VIRGINIA

SERVICE ORGANIZATION REVIEW

REPORT ON POLICIES AND PROCEDURES PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS AS OF MARCH 31, 1999

EXECUTIVE SUMMARY

This report reviews the Department of Information Technology's (DIT) policies and procedures placed in operation as of March 31, 1999. We conducted our review using **Statement on Auditing Standards No.70, Reports on the Processing of Transactions by Service Organizations**, issued by the American Institute of Certified Public Accountants. We have defined the control objectives for this review from the Information Systems Audit and Control Foundation's work on "Control Objectives for Information and Related Technology" (COBIT). COBIT was developed as a generally applicable and accepted standard for good practices for information technology control.

This report should provide DIT customers, their independent auditors and report users with sufficient information about DIT's internal control structure policies and procedures. This report assesses the operating effectiveness of policies and procedures surrounding automated transactions processed or other services provided by DIT. This report, when combined with an understanding of the customer's internal control structure policies and procedures, is intended to assist auditors in planning the customer's audit and in assessing control risk for assertions in customer's financial statements that may be affected by policies and procedures at DIT. If customers do not have effective controls, DIT's control structure policies and procedures may not compensate for such weaknesses.

We found:

DIT's policies and procedures, as reported in Section III, are suitably designed and operating effectively to provide reasonable assurance that the specified control objectives have been achieved as of March 31, 1999. The reader should evaluate this information only with a concurrent assessment of the customer's internal control structure.

We recommend that DIT:

- Perform reviews of firewall trusted relationships.
- Modify router configurations.
- Coordinate responsibility for maintaining a secure network environment.
- Review Services Allowed on UNIX Web Page Server.
- Document testing and rollback procedures for system software changes.
- Establish frequency controls for updating business impact analysis.
- Enforce the policy requiring employees to visibly display picture ID badges.
- Limit data center access.
- Require vendor notification of employee terminations.
- Organize and maintain the agency policies and procedures manual.

-T A B L E OF C O N T E N T S -

Section I. FINDINGS SUMMARY

Perform a Review of Trusted Relationships

DIT does not perform security reviews of trusted agency firewalls to ensure adequate security. Four agencies have firewalls that have a trusted relationship with the DIT firewall. DIT's firewall does not authenticate these agencies before connecting them to the MVS or Unisys environments. Inadequate review of these trusted relationships could jeopardize the integrity of valuable information resources. In addition, DIT does not have a policy establishing why some agencies are exempt from authentication and what procedures the agency must follow to maintain its exemption. We recommend that DIT develop a policy that establishes exemption requirements, procedures that agencies must follow, and requires periodic security reviews.

Modify Router Configurations

The primary router that routes communication traffic between DIT, user agencies, and the Internet allows all sources to attempt to logon to the router via telnet. Additionally, DIT does not store the passwords used to protect the router's configuration in an encrypted format. This current configuration increases the chance of unauthorized changes to the router's configuration.

We recommend that DIT set the router configuration to accept telnet functions from a few trusted administrators' addresses. The passwords should also make use of Cisco's encryption feature.

Coordinate Responsibility for Maintaining a Secure Network Environment

DIT has no central division for its network services and the structure seems disjointed for network security. The agency has not issued an updated network diagram since September 1996 and no particular division has responsibility for handling this function. There are individual portions of the network diagram in the Unisys DataBase Division, Unisys System Support, Telecommunications, and Computer Operations Division.

We recommend that DIT assign oversight responsibility for their network environment to a department or individuals that understand the complete network structure. This will mitigate risk in providing continued reliable services to the agencies.

Review Services Allowed on UNIX Web Page Server

DIT does not have a policy regarding new server security set-up and maintenance. As a result, our review found numerous active network services present on the UNIX based web page server. Services such as these can allow unauthorized access to the web server. We recommend that all network services, except for FTP, should be reviewed and turned off unless there is a valid reason for allowing this security risk.

Document Testing and Rollback Procedures for System Software Changes

DIT does not consistently document testing and rollback procedures for system software changes as required by DIT Procedure-023. Lack of testing and rollback plans could adversely affect system performance and customer operations. We recommend that DIT have documented test results and rollback plans for all projects.

Establish Frequency Controls for Updating Business Impact Analysis

DIT performed a Business Impact Analysis in April 1999. Prior to this date, an analysis had not been completed since 1996. There have been critical system changes that have taken place over the past two years that were not included in the Business Impact Analysis until 1999.

We recommend that DIT should establish policies and procedures indicating a reasonable frequency for updating the Business Impact Analysis.

Enforce Policy Requiring Employees to Visibly Display Picture ID Badges

DIT does not enforce its policy requiring employees to visibly display picture ID badges at all times. We noted numerous instances of employees carrying their ID badge in their pocket or laying their ID badge down where someone else could easily pick it up. We recommend that DIT reinforce the importance of displaying ID badges to all employees. By enforcing this policy, DIT reduces the risk of current and terminated employees accessing unauthorized areas.

Limit Data Center Access

As of March 31, 1999, 259 individuals had access to DIT's data center, several of whom have no need for this access. Currently, there are no guidelines for area managers to follow when determining whether their employees need data center access. Individual area managers request physical access for employees under them. Additionally, the Center's management only annually reviews who has data center access.

DIT should develop written guidelines specifying which employees should have access to the data center. We recommend that supervisors regularly review the listing of employees with data center access and remove access for all employees whose job functions do not require them to enter the data center. Limiting physical access to employees who only have the need to enter the data center reduces the risk of theft and vandalism.

Require Vendor Notification of Employee Terminations

DIT does not have a policy that requires vendors to give notification when their employees with data center access terminate. Several of DIT's outside vendors have physical access to the data center. Physical security relies on the vendor to tell them when their employees terminate.

We recommend that DIT implement a policy that requires vendors to notify DIT of employee terminations when the employees have data center access. DIT could best enforce this policy by making it part of all new vendor contracts. This procedure would limit the risk of a disgruntled vendor employee returning to the data center after termination and causing damage.

Organize and Maintain the Agency Policies and Procedures Manual

DIT continues to work on updating its Policies and Procedures Manual. We recommend that DIT devote resources to finish the project of reviewing and updating the current policies and procedures manual and establish a procedure to regularly review policies and procedures to ensure they are still relevant.

Section II. OVERVIEW OF SERVICES PROVIDED

DIT provides state and local governments with a source for meeting their information technology needs. DIT manages the state's telecommunications contracts; provides state government with data processing services; assists agencies and local governments with designing and purchasing their information technology resources; and provides information technology solutions, such as audio and video conferencing.

The Department has two directorates: Finance and Administration, and Services. Finance and Administration organizes, manages, and provides internally the financial, human resources, information systems, technology resources, and acquisition services support. Services coordinates and supplies information technology resources to governmental entities located throughout the Commonwealth.

Service's divisions are described below.

MVS Database Division

The MVS Database Division provides database support services for customers. The Division uses the Department's two Hitachi GX-8824 mainframes to provide support for ADABAS, DB2, and IMS database management systems and related products.

MVS Systems Software Support Division

The **Operating Systems Software Section** manages the MVS operating system program products and related software for security, report writing, programming languages, and data sorting that customers require for their daily production. Some of these products include ACF2, FOCUS, SYNCSORT, EASYTRIEVE, COBOL II, and FORTRAN G1. This section also modifies the MVS software definitions to match changes in the hardware configuration for central processing units; disk allocation storage devices, tape, and other systems related hardware.

The **Teleprocessing Software Section** supports teleprocessing software products such as TCP/IP, VTAM, NCP, and CICS, which is the on-line monitor for several database products.

Both sections have responsibility for acquisition, installation, availability, maintenance, performance, problem and change management, disaster recovery, and evaluation of their software as well as system configuration management.

Unisys Systems Software Support Division

The **Operating Systems Software/Program Products Section** manages the operating system and its components, media storage, interactive processing, performance monitoring software, utility processors, and language processors such as COBOL. This section also provides software configuration to match the existing hardware platform.

The **Teleprocessing Software Section** supports all teleprocessing software that runs in the Department's four front-end processors and the host based software that provides data communications. Further, the section supports software associated with the router based network coming into the Data Center, as well as the software configurations for their customers remote based routers.

Unisys/UNIX Database Division

The Unisys/UNIX Database Division provides database support services for customers using the Department's Unisys 2200/9844 mainframe for MAPPER and DMS 1100. The Division also provides UNIX system administration, Internet services, domain name service, e-mail service, and news feed service. The Division also services the Department of Social Services' SUN E10000 by providing Oracle Database Management and MAPPER support.

Computer Operations Division

The **Systems Operations Branch** provides a customer service support center to assist customers with resolutions to processing problems and service requests. They also communicate with customers on job status and production problems as well as provide production support services such as coordination, delivery services, and protection of physical security. Additionally, this branch operates the computer systems, consoles, peripheral devices, printers, and the mounting and dismounting of tapes.

The **Technical Support Branch** coordinates vendor installation and maintenance of data processing hardware, performs data center environmental and equipment facilities management, as well as provides internal data communications and systems hardware support services. This branch also develops procurement documents for hardware and software.

Telecommunications Division

The Telecommunications Division administers local and long distance telephone and data communications services for State government. The Division competitively obtains most services from telecommunications vendors.

Information Engineering Division

The Information Engineering Division provides technology and database planning, data administration, desktop systems, and local area network planning and implementation. They offer Internet services, including Internet access and server space for sites, as well as Internet web page consulting, and marketing support services.

Automated Systems Division

The Automated Systems Division provides for the implementation and operation of automated operations software and storage management. They are responsible for all IBM DASD space allocations and the software implementation of various storage devices. The division is responsible for the evaluation, acquisition, availability, maintenance, performance, and disaster recovery of software. The Division also provides technical assistance to clients and problem, change, and system configuration management. The Automated Systems Division interfaces with DIT's Capacity Planning Group to relay current and projected DASD requirements based upon customer requests. They develop regular performance management reports to assist the Capacity Planning Group in their responsibilities.

Telemedia Division

The Telemedia Division provides audio and video teleconferencing services, and coordinates this service statewide. It also provides consultation and management services on video networks, capacity, and equipment.

Systems Development Division

The Systems Development Division provides personal computer local area network support, development, and procurement; assists the computer services division with the installation and configuration of software; develops applications; and provides support to the Governor's Office for its local area network and system operation.

Security Division

The Security Division provides centralized physical and data security for all of DIT's programs and oversees facilities management.

Technology Consulting Division

The Technology Consulting Division provides network planning, design, training, and implementation assistance. The Division provides these services for Local Area and Wide Area Networks, all types of micro to mainframe communications, Client/Server Technology, and Personal Computers.

Section III. CONTROL OBJECTIVES, POLICIES AND PROCEDURES AND TESTS OF OPERATING EFFECTIVENESS

The Auditor of Public Accounts determined the nature, timing, and extent of tests performed in order to obtain evidence about the operating effectiveness of the Department of Information Technology policies and procedures in meeting specified control objectives. The procedures used to test the operating effectiveness are listed next to the respective control objective and policies and procedures in the following matrix. The results of each test are listed next to the test procedures.

The following matrix represents testing as of March 31, 1999.

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing application systems and new systems under development.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Systems Development Division (SDD) has responsibility for changes to existing and new application systems. The SDD has established system maintenance standards to provide optimum service, ensure responsive systems, and manage SDD's resources. The other Divisions of DIT do not maintain application systems. The SDD provides assistance to DIT customers for all phases of application development and maintenance. The computing environment that SDD uses to develop application systems depends on the needs of the client. SDD may use the existing hardware/software at DIT or the client's computing environment. **New Systems Development** SDD has established and defined standard phases and tasks within the division to enhance project management of systems development/modification projects, special projects, monitor operations, maintenance, and administrative activities. SDD requires Project Agreement forms for all projects. A Project Leader does a preliminary project plan. SDD procedures require a pre-project review if the analysis to determine the project's scope and objectives finds that the project requires more than 500 man-hours. If the project might exceed 1000 hours, the SDD Deputy Director attends the review. Additionally, DIT's Internal Auditor must provide a written recommendation to proceed for all projects in excess of $100,000. After the SDD Director's approval, the customer receives the Project Agreement for signature and SDD opens the project in the Management and Control System (MACS). The MACS system tracks project assignments, project tasks and subtasks, estimated hours, and calendar start and completion dates. The system reflects the employee's worked hours charged and the status of the various project tasks. The system also tracks standard project task activity phases such as the project initiation phase, requirement definition phase,	**New Systems Development** Evaluate and document any project design tracking software that may currently be in use. Obtain a list of new application programs, implemented in the last year, from the System Development Division. From this list, judgmentally select six mainframe and client server programs, in total, from new systems and trace back to the initiating request. Evaluate whether new program development procedures are in accordance with proper project management standards and development changes are authorized and documented. **Changes to Existing Application Systems** Evaluate and document any change control tracking software that may currently be in use. Obtain from the Systems Development Division a list of application programs that have changed in the last year. From this list, judgmentally select six mainframe and client-server programs, in total, for maintenance of existing systems and trace back to the initiating request. Evaluate to determine whether application program change procedures are in accordance with management's specifications. Evaluate whether changes are properly authorized, tested, documented, and approved and whether only authorized programs are moved into production.	In response to last year's testwork and finding that SDD lacked a policy and procedure to document application development, DIT created a new policy. This policy went into effect February 15, 1999. Audit testing of work done by DIT after implementation of the policy could not be performed, as there was no work completed. Auditors performing agency audits should not rely on application change control at DIT for work done for their agency. The user agency should also monitor program movements into and out of production to ensure that all movements are authorized.

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing application systems and new systems under development.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
systems analysis phase, detail design phase, development phase, implementation, and evaluation. After project approval, the Project Manager assigns the project to a Project Leader and informs the Project Leader of any responsibilities and expectations. The Project Leader and Project Manager then meet with the assigned project team and review their duties and responsibilities. The Project Leader conducts a monthly one on one review with the Division Director. The Project Leader documents the review agenda and results in a Project Status Report. SDD structures the review so that one member of the project team acts as a reporter. SDD documents any changes from the initial project agreement in a Modification Agreement. **Changes to Existing Application Systems** Application system customers communicate any changes for application system maintenance in writing to the SDD Project Leader. The Project Leader assigns the work to an analyst who prepares the requirements. Each Project Leader will be responsible for obtaining approval for all production changes and ensuring that all changes are documented, tested, and reviewed by an individual other than the one making the change. During normal work hours, a programmer makes the change, tests the change, and signs off on the completion of all changes. Someone other than the programmer then reviews the change. The program is moved into production and the Project Leader makes sure all the documentation requirements above have been met. After normal work hours, the programmer on call receives all requests concerning critical emergency production problems. The programmer will fix the problem and move the changed program into production. The programmer must complete an "Operational System Maintenance Activity" form, which includes listing the problem,		

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing application systems and new systems under development.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
action taken, individuals involved, time required and the name of the customer who notified the programmer of the problem. The programmer must sign the form and have it signed by either the Project Manager or the Information Technology Manager who verifies the appropriateness of actions taken. For all systems that DIT supports completely, assigned DIT personnel have constant access. The user organization is responsible for authorizing DIT personnel access to their system because DIT is not allowed to act as the security officer for any user organization application system. For systems that DIT supports only occasionally, they must request access from the user organization each time they have a service request. Upon completion of each request, DIT's access is deleted. Programmers have access to the test and production programs for only those application systems that they work on or test. Although there are some situations where programmers have the capability to move changes into production, policies expressly forbid them moving changes into production without appropriate documentation except for critical production problems, which occur after normal business hours. The library shows the date the last 8 changes to any program occurred.		

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occurs for changes to existing operating system software and implementation of new systems.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The following divisions make changes in existing operating system software and new system software: Divisions with MVS Environment: Automated Systems Division MVS Database MVS System Software Support Divisions with Unisys and UNIX Environment: Unisys/UNIX Database Unisys Systems Software Support DIT has established and documented standard procedures for the installation, modification and/or removal of operating system software. The policy states common steps to follow in the installation, modification, or removal of system software. These steps are Receipt, Create Change Management Documentation, Analysis, Approval, Project Plan, Schedule/Coordination, Test Plan and Test Implementation, Back Out Plan, Production Implementation, Post Implementation Evaluation, and Closure. During emergencies, the procedures described below may be abbreviated and documentation completed after the emergency. The Chief Engineer or designee coordinates the analysis of the new product, version, maintenance, or removal of the operating system software. All changes to existing software and the implementation of new software involve the creation of a change management record in the Change Management System. Staff discuss all change request forms during the weekly Change Management Review meeting. System software changes require approval at the analysis, testing, and implementation phases. The Chief Engineer ensures the completion of the approval process by either accepting or rejecting the system software change. The Chief Engineer may escalate approval authorization to the Project Leader level for any change that does not have unanimous approval. Where circumstances warrant, the Project Leader may escalate approval to the	Evaluate and document any change control tracking software that may currently be in use. Obtain a list of existing system software changes from the MVS Systems Support Section, the Unisys/UNIX Database Division, the Unisys Systems Software, and Data Communications Division. From this list, judgmentally select twelve changes and trace back to the initiating request. Evaluate whether existing system software change procedures are in accordance with management's specifications. Determine whether changes are properly authorized, tested, documented, and approved and that only authorized programs are moved into production. Determine that a written rollback plan is present. Obtain a list of new version system software changes from the MVS Systems Support Section, the Unisys/UNIX Database Division, the Unisys Systems Software, and Data Communications Division. From this list, judgmentally select eight programs and trace back to the initiating request. Evaluate whether new systems software implementation procedures are in accordance with management specifications. Determine whether new versions are properly authorized, tested, documented, and approved and that only authorized programs are moved into production. Determine that a written rollback plan is present.	Documentation of testing and rollback procedures is inconsistent. Six of twelve (50%) existing software changes tested had rollback plans. One of twelve (8%) existing software changes tested had test documentation.

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occurs for changes to existing operating system software and implementation of new systems.***

Provided by the Department	**Provided by the Auditor of Public Accounts**	
Policies and Procedures	**Tests Performed**	**Results**
Division Director. During testing of software change implementation, the Chief Engineer takes precautions to protect the production libraries/systems files from loss or destruction. The Chief Engineer must review and determine if the plan adequately and thoroughly tests the change and documents the results. The engineering staff for the affected system communicates all problems or unexpected results to the Chief Engineer. Before production implementation, the Chief Engineer documents the back out plan. Back out plans will allow the staff to restore the system to its former production state should the implementation of the change fail. All impacted divisions review the back out plan and after implementation perform an assessment of the impact of the change, review the adequacy of the project, test plan, and provide input from lessons learned. After successful production implementation, the Chief Engineer resolves any problems or unexpected results and is responsible for closing the project.		

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, and documentation occurs for changes to existing hardware and the implementation of new hardware.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Computer Operations Division performs changes to the MVS and Unisys hardware in the Data Center and the Telemedia Division performs the changes for the PC Desk Top Video and PictureTel Videoconferencing hardware. Many colleges and universities use this hardware to broadcast classroom instruction to off-campus locations. Additionally, many state agencies use this service for teleconferencing. **Computer Operations Division** DIT has a policy to provide the framework for the implementation and tracking of all changes involving the Data Center. A change is any alteration and testing to any component of the Data Center's hardware, software, procedures, scheduling processes, application configuration changes, movement of databases between systems or any documentation needs. The Computer Operations Division performs all changes approved by the Computer Operations Manager. The Software Support Engineer, Facility Engineer Operations, and Operations Analysts submit a Change Request form to their manager/supervisor for approval through e-mail. Once the manager approves the change, he sends the request to the Operations Analyst Section (Unisys or MVS) for review. The Operations Analyst distributes the change to the appropriate personnel for review, addresses questions or concerns, and informs the requester of the time and date to schedule the change. The customer bulletin includes all changes. Emergency changes require immediate implementation to resolve mainframe software or hardware system outages. After the change and restoration of the system to normal operation, the manager or supervisor documents the action taken on a Change Request form marked "emergency." The Operations Analyst will review the changes and give them to the Operations Supervisor.	Evaluate and document any hardware change control/hardware inventory tracking software that may currently be in use. Obtain a list of hardware changes that have occurred, including at least one telemedia upgrade. From this list judgmentally select ten changes and trace back to the initiating request. Evaluate whether hardware change procedures are in accordance with management's specifications. Determine whether changes are properly authorized, tested, documented, and approved.	Documentation of testing is non-existent. Six out of six changes tested had no testing documentation. In response to last year's findings a new test field was added to the change management record in early March, 1999.

Objective: ***Policies and procedures provide reasonable assurance to limit physical access to computer equipment, storage media, and documentation to only properly authorized individuals.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Policies and procedures for physical access involve all DIT divisions and computing environments. The DIT Physical Security Section of the Security Division administers and maintains the physical security program. **Physical Access Security** DIT has established and documented policies and procedures regarding physical access security. The Personnel Department notifies the Physical Security Section of a new employee's starting date. The hiring division generates and forwards an Access Authorization Form to the Physical Security Officer. The hiring division manager determines employee's access considering their job classification/function. The Physical Security Officer assigns an access card, picture id number, the appropriate clearance codes and forwards the Access Form to the Security Manager for approval. Employees must sign, acknowledging receipt of their access card and ID badge. The Physical Security Officer maintains access card information on the Security Tracking System and keeps unassigned access cards in a locked file cabinet. An inactivated access card cannot open any doors until recorded on the Tracking System and assigned specific access points. The access card reader at each locked door reads the access card and only unlocks it if the Tracking System acknowledges access to the locked area. All DIT employees visibly display picture ID badges at all times and report any lost, missing, or stolen picture ID badges or access cards immediately to the Physical Security Section. If the discovery occurs after normal business hours, the employee contacts the Capitol Police station so they can take the proper steps to remove the card from the security system. Employees obtain a visitor's badge from the appropriate reception area or the security station if they forget their picture ID or access card. DIT employees do not allow unescorted	Tour DIT facilities and perform the following: a) Document where critical computer processing hardware (mainframes, servers), computer storage devices (disk packs, optical drives), telecommunication devices (modems, routers, gateways), backup devices (tape drives, mirrored servers), sensitive documentation, backup media (tapes), and Telemedia Equipment (PC desktop video and picture teleconferencing hardware) reside. b) Determine by observation, then document the current status of locked physical access points to the above listed devices. Be sure to notice doors or service windows that are propped open or have tape over lock mechanisms. c) Document all control points that must be passed through in order to get to the Data Center. Consider access from stairwells, front lobby, freight elevator and other entry points. d) Determine by observation that all people encountered in the secure areas have their picture ID displayed as required by DIT policy. Document reasons for exceptions. e) Obtain from Capitol Police, who enforce access control, a log of responses to emergency alarms over the past year. Determine and document whether proper responses and follow-up procedures were performed. f) Document and evaluate who has control over the access card database and hardware. g) Document and evaluate if a master key is available for the Data Center and other areas that contain secured devices, and if so who has a copy or access to these keys Obtain from the Physical Security Manager a computer generated file or printout that includes each employee's name, ID number, and approved physical access points. Using this information, judgmentally select ten employees who have	DIT does not enforce its policy requiring employees to visibly display picture ID badges at all times. Numerous instances of employees carrying their ID badges in their pocket or laying their ID badge down where someone else could easily pick it up were noted. As of March 31, 1999 there were 259 individuals with access to DIT's Data Center. Several individuals were identified who use their access approximately once a month, but due to a lack of written guidelines, it could not be determined if their access was appropriate. Physical Security relies upon vendor notification for information about vendor employee terminations. However, DIT does not have a policy to obtain notification from vendors of terminations of employees they are using to perform their contractual obligations at DIT.

Objective: ***Policies and procedures provide reasonable assurance to limit physical access to computer equipment, storage media, and documentation to only properly authorized individuals.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
visitors or vendors to follow behind them when entering a door requiring use of an access card. With the exception of those individuals using the DIT auditorium or classrooms, DIT requires visitors have escorts at all times while in areas requiring access cards unless the visitor has an access card. Employees must report any unidentified or unauthorized person to the Capitol Police or the DIT Physical Security Section. Capitol Police enforces access control through continuously manning the security station and observing all video monitors. After normal business hours, a Capitol Police Officer makes a periodic walk-through check of all DIT areas including all corridors and fire exits. Capitol Police respond immediately to panic alarms and treat every alarm as an emergency. They notify key personnel if emergencies occur and make decisions for evacuating the building. **Physical Access of Promoted, Transferred and Terminated Employees** DIT has established steps to promptly remove physical access for terminated employees and correctly allocate physical access to transferred and promoted employees. When a supervisor learns of an employee's termination, the supervisor immediately provides Personnel with a memorandum notifying them of the termination. Personnel immediately notifies the Security Division, which provides the supervisor with a Separation Checklist. The checklist serves to guide the supervisor in collecting all items related to physical access. For those employees terminating under abnormal circumstances (i.e., firing or death), the supervisor contacts Security immediately to remove physical access to DIT premises. The supervisor attempts to collect, at a minimum, the employee's ID card, door keys, and access card. For transferred and promoted employees,	access to the Data Center. Determine and document if these individuals have job functions that require such access. Obtain from Human Resources a list of new employees. From this list judgmentally select three employees and obtain their DIT-41 form. Request from the Physical Security Manager an access profile for each employee. Determine and document whether the profile matches the requested access on the DIT-41. Obtain from Human Resources a list of recently terminated employees. Judgmentally select three and determine that DIT's policy on terminated employees is being followed. Request memorandum from the user's supervisor to the Personnel Branch and memorandum from the Personnel Branch to the Security Office. Determine that both notifications were timely and that access denial was timely. Review the access list to determine that the terminated employees are no longer given access. Obtain a list of recently terminated contractors. Judgmentally select three contractors and verify that access has been terminated in a timely manner. Determine that the computer facility is reasonably secure from foreseeable and preventable threats to its physical continuity. Consider heating and cooling requirements, fire suppression and readiness, water detection and readiness, power supply, and whether personnel have been trained for emergency responses. Determine that storage media (sensitive tapes, disks, and printouts) are kept in a controlled and environmentally protected manner. Determine that sensitive forms (such as computer access forms) and manuals or documentation are kept in a controlled environment.	

Objective: ***Policies and procedures provide reasonable assurance to limit physical access to computer equipment, storage media, and documentation to only properly authorized individuals.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Personnel notifies Security of the change in status by providing them with a Payroll Transaction/Authorization Form. Security works with both the present and former supervisors to modify the employee's physical access to meet the needs of the new position. **PC & Local Area Network Security** DIT has established a security policy that will protect and safeguard information residing within the DIT Local Area Network (LAN) and PC environments. LAN administrators place file servers, related equipment such as gateways and wiring components, and original copies of LAN software in an environmentally safe and physically secure area. LAN equipment resides in locked rooms that require access cards to open. The card access computer system alerts Capitol Police to investigate if the equipment room door remains open. DIT employees lock (where possible) and terminate power to their PC when leaving the premises. Also, users store magnetic media (i.e. diskettes, tapes, etc.) in a secure container away from extreme temperature and sunlight. **Systems Development Division (SDD) PC Security** DIT has established PC security standards in order to protect and safeguard both the property and data associated with PCs assigned or in the custody of the SDD. Employees protect diskettes containing sensitive or confidential data by locking them in a secure place. The employee advises the SDD Security Officer of the nature of the data and its secure location. Employees do not store sensitive or confidential data/information on any PC hard disk. The LAN equipment and laptop computers are stored in a cubicle that is locked at night. All employees are encouraged to challenge anyone whom they do not recognize.		

Objective: ***Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Security Division has responsibility for logical access to programs and data. The policies and procedures cover the computing environments of MVS, Unisys, and access through firewalls. **All DIT Computing Environments** DIT has established a program to ensure the confidentiality, availability, and integrity of data DIT owns or serves as custodian. The program follows the Commonwealth of Virginia Information Technology Resource Management Standard 95-1 issued by the Council on Information Management (CIM). When customers request access to DIT systems, the procedures below are followed. **Logical Access to Programs** When customers request access, they receive access to all programs in either the MVS or Unisys systems by default. In the MVS system, ACF2 provides security to all programs, except some specific IMS databases, and users must prepare specific rules to allow user access to programs. In the Unisys system, customers must take security measures to ensure that another customer cannot access their data contained within a program. DIT cannot mandate that customers use Unisys security features, but only recommends their use. **Logical Access to Data** <u>MVS Computing Environment for DIT Employees and Customers</u> Each customer (including DIT) must appoint an Agency Security Officer (ASO), who establishes, maintains, updates, and deletes access for customer end-users. The customer must complete a form for each individual user and the ASO, DIT Security Officer, System Coordinator, and DASD Coordinator must sign the form indicating approval. DIT's Security Division keeps a copy of the approved form. DIT performs the following procedures after receiving the form. 1. Verify the ASO signature.	**MVS ENVIRONMENT** To obtain an understanding of the logical access controls surrounding the MVS IBM environment, document in detail the files, the file contents, and the mechanisms that are used by DIT to secure other agencies resources and access. Document how an Agency Security Officer is set up by DIT. Determine what flags this user as different than the other agency users and in what file(s) this occurs. Determine what features keep Agency Security Officers from writing in another agency's rules. Determine where the on-line user validation process receives its information. For instance, is the password stored under native TSO's User Attribute Data Set (UADS) or does TSO use the ACF2 Logon ID parameters or a shadow file? Determine that all users have a password. Using the SHOW ACF2 and SHOW STATE commands, determine that the system parameters are reasonable (MAXTRY should be between 1-3, and MINPSWD should be between 4-6). In addition verify that the following settings are set: • MODE=ABORT which kills logon attempts not authorized by access rules. • NOSORT=NO To determine that system access by DIT personnel is restricted to authorized individuals, obtain a computer-generated printout of the Logon ID File (for DIT) and perform the following: a) Judgmentally select ten users and determine that the Logon ID record is accurate for each user by reviewing the initial written request form (DIT03-001). b) From the above sample, evaluate reasonableness of the password expiration setting under 'Miscellaneous' MAX for each user. c) From the above sample, evaluate the 'Miscellaneous' STATISTICS, which shows the number of security violations. Investigate and document any large numbers reported. For the three terminated employees selected for	DIT does not perform security reviews of trusted agency firewalls to ensure adequate security. Four agencies (VDOT, DGS, DSS, and VDH) and the agencies that go through them to reach DIT (APA, etc.) are exempt from authenticating at the DIT firewall. These four agencies have firewalls of their own that DIT trusts as being secure. DIT does not have a policy as to who will be a trusted relationship and the requirements to maintain this relationship. DIT does not have a policy regarding the security set up and maintenance of servers. DIT has active network services on the UNIX based web server that are not needed and pose a security risk.

Objective: ***Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
2. Verify that the logon id is seven (7) alphanumeric characters and that the first three (3) characters are the agency qualifier. 3. List the logon id's to make sure ACF2 returns message that logon id does not exist. If the logon id does exist, contact ASO. <u>Unisys Computing Environment for Customers</u> Each customer must select a Unisys Sub-Administrator and send a letter to DIT indicating the sub-administrators name and to have the appropriate security features established. DIT does not set up access of customer's employees, only the sub-administrator. The individual customer implements procedures for setting up <u>end user</u> logon-id's and privileges. <u>Unisys Computing Environment for DIT Employees</u> All DIT end-users must fill out a Unisys logon-id request form with proper authorization and submit it to the Security Division when requesting access. DIT designated personnel receive all special requests with written justification and the signature of the end-user and their supervisor before setting up the logon-id in accordance with the request. **Logical Access to Programs and Data through DIT Firewalls** The security firewall is a combination of hardware and software designed to provide a security barrier by blocking external networks from accessing DIT's computer environment, including the MVS and Unisys systems. The ASO requests access to the DIT firewall by contacting the DIT Help Desk. The ASO completes and signs a Commonwealth Telecommunications Network (CTN) Security Firewall Access Form. The DIT Firewall Administrator establishes a user logon id and password. This password does not expire and users do	physical access test work, verify that Logon IDs were deleted in a timely manner. Obtain from DIT's ACF2 Officer, the names of all ACF2 Rules datasets. Determine that all DIT controlled Rules datasets are restricted to the security officer and an alternate. Using the Logon Id report, document and evaluate based on job function, those DIT employees that have one or more of the following privileges: ACCOUNT, SECURITY, AUDIT, CONSULT, LEADER, READALL, RESTRICT. Produce an ACF2 "decomp" listing of the access rules for system accounts (datasets) such as IMS, DB2, and ADABAS. Determine that the users in a judgmental sample of five programs or utilities are reasonable and appropriate. Contact three agencies using the MVS platform and get the names of their most recent user additions from their Security Officer. Obtain the DIT10-001 request form for each of the users. Determine that the Agency Security Officer, the DIT Security Officer, the System Coordinator, and the DASD Coordinator have signed the form. Determine: (1) what reports the security officer runs (2) how often the reports are run (3) how the reports are reviewed (4) what is done with the information and (5) their effectiveness in controlling access. **Unisys ENVIRONMENT** Obtain an understanding of the logical access controls surrounding the Unisys environment. Document in detail the files, the file contents, and the mechanisms that are used by DIT to secure other agencies resources and access. List features even if they are not in use by any agency. Review the Unisys Sub-Administrator request form (DIT10-001) for three agencies that use the Unisys. Determine that a request letter signed by the agencies MIS Director was sent with the request form and that the forms were filled out properly before access was given. Evaluate and document how many DIT personnel can access the User ID Maintenance screen by using the DIT SIMAN Administrator sign-on. This access allows for adding, deleting, or	

Objective: ***Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
not have the capacity to change their password. In addition to setting up access, the ASO can request additional firewall services such as monitoring the system, changing passwords and using TRACEROUTES that identify external traffic trying to access the network. DIT has established procedures for each of these additional services.	changing agencies' Sub Administrator's capabilities. Review the Unisys request form (DIT10-001) for three DIT users with Unisys access. Determine that the end-user and end-user's supervisor signed the request. Contact three agencies that rely on the Unisys to determine if DIT has informed them that access security is the responsibility of the agency. **FIREWALLS** Document in detail the firewalls used at DIT that control access from agencies and the outside world. Obtain a sample of the programming used in the Application Gateway Firewall. Determine that in fact the firewall is checking for proper system usage. Determine that the UNIX files have been configured properly on the firewall by performing the following: a) Obtain a listing of the root directory. Determine that no other applications are running on this server such as compilers, other application programs, Web services, etc. b) Obtain the /etc/passwd file and determine that only the root and one administration account are active. c) Determine that all standard network services in the /etc/inetd.cof file are commented out except for the console log. There should be no telnet, rlogin, ftp, tftp or other network logins, or file transfers. d) Determine that all trusted services are turned off. For example, there should be no /etc/hosts.equiv or /users/$HOME/.rhosts files. These files tell who is trusted by the mere fact that the user is trusted somewhere else. e) Inspect /etc/inittab and	

Objective: ***Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
	/var/spool/cron/crontab/root to determine what scripts and jobs are run at startup and other times. Determine that these jobs can not be written to except by owner. f) Obtain system file directory with permissions. Examine key directories for restricted permissions. Determine from interviews with key staff, what reports are generated from the firewall and how often they are reviewed. Obtain a computer-generated list of authorized users that can pass through the firewall. Trace three users back to their original CTN Security Firewall Access Form (DIT03-004). Determine that the form was filled in correctly with the proper authorizations. **LAN ENVIRONMENT** Document and evaluate the access security surrounding the LANs that are relied upon by DIT to support outside agencies. Review the password files for each critical server and evaluate and document the strength of its settings. Judgmentally select a sample of five DIT employees and review the LAN access request form for proper authorization and determine if access is reasonable based on job description. **WEB SERVERS** Determine that the UNIX based Web Servers are configured properly by: a) Obtain a listing of root directory. Determine that no other application is running on this server. b) Obtain the /etc/passwd file and determine that only one account has UID of "0," that a shadow password file is used with all accounts passworded or disabled, that application users are not given a shell, that only a few users know the superuser password. c) Obtain a listing of system files with	

Objective: ***Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
	permissions. Examine key directories for restricted permissions. d) Determine that all standard network services are commented out of the /etc/inetd.cof file. e) Examine /etc/inittab and /var/spool/crin/crontab/root to determine what scripts are run at startup and other times. Determine that these are restricted. f) Determine that all trusted services are turned off. Determine that the NT based Web Servers are configured properly by: a) Determining who has ADMIN account capability and that this is reasonable. b) Verify on-line that the GUEST account is not set up in the user domain. c) Determine that NTFS is used to protect system resources. d) Determine if any trusted relationships exist between domains. Obtain the name of the most recent terminated contractors. Determine what projects and platforms they were assigned to. Determine that access to these platforms was removed in a timely manner.	

Objective: ***Policies and procedures provide reasonable assurance that the Computer Operations Division schedules processing appropriately, and identifies and resolves deviations.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Computer Operations Division schedules processing, and identifies and resolves deviations in jobs. **MVS Computing Environment** Control-M is the program DIT uses to perform job scheduling and production control. Control-M is designated in the Job Control Language (JCL) and completely automates the JCL setup tasks, job scheduling and execution, processing analysis and problem resolution, workload optimization, and recovery processing. Control-M provides comprehensive tracking and control facilities and allows for projections and graphic presentations to further enhance data center productivity. When using Control-M, the customer submits a Scheduling Request Form for additions, deletions, or changes. A DIT scheduler inputs the information from the form into Control-M. Jobs can then run daily, weekly, monthly, on holidays, on workdays, etc. Control-M assembles a schedule outlining when jobs will be run based on the day and time requested and any prerequisites to the job. A daily scheduling report runs in the morning and lists any changes during the day affecting that day's processing. All DIT customers use Control-M exclusively, except for the Department of Health, which prints some reports independently of Control-M, and the Department of Accounts, which does not use Control-M at all. For the Department of Accounts, DIT performs manual scheduling of nightly production jobs rather than using Control-M. The Department of Health submits jobs themselves and calls to let DIT know the job name, hours to run, number of drives, prerequisites, and comments. If the job errors, the console operator notifies Health. DIT personnel ensure that jobs scheduled through Control-M or manually do not interfere with one another. DIT is currently working on getting all the customers to use Control-M exclusively. **Unisys Computing Environment**	**MVS ENVIRONMENT** Document the method and system (Control-M, Control-R) used for scheduling jobs for the various agencies. Determine if there is a method for identifying and resolving scheduling deviations. Consider both on-line application and batch program execution. Trace a current job back to its original request form (DIT-04) and perform the following: a) Determine that it is scheduled in Control-M for the time stated in the request form. b) Determine that all prerequisites as stated in the request form have been met before the scheduled run time. c) Determine that Control-R has the restart rules if they were noted in the request form. Document and evaluate the status of the Department of Accounts scheduling of jobs. Document and evaluate whether a policy has been written to give guidance when there are scheduling problems. Document and evaluate who is allowed to access the Control-M and Control-R functions for adding, deleting, or changing scheduling related information. Through inquiry of key operations personnel, determine and evaluate what procedures are followed when a customer wants to kill or change a job start. Review the Data Center's operations log. Investigate references to manually restarted jobs. Determine that they were restarted or killed in accordance with the agency guidelines. **Unisys ENVIRONMENT** Document the method and system (SAM Control) used for scheduling jobs for the various agencies. Determine if there is a method for identifying and resolving scheduling deviations. Consider both on-line application and batch program execution. Trace a current job back to its original request	No exceptions were noted.

Objective: ***Policies and procedures provide reasonable assurance that the Computer Operations Division schedules processing appropriately, and identifies and resolves deviations.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
SAM (Scheduling and Activity Monitor) Control is the automated scheduler for the Unisys system. All customers run jobs through SAM except the Board of Elections. DIT is currently working on setting up the Board of Elections on SAM Control. In SAM Control, a scheduler receives an approved scheduling change request on the SAM Automated Scheduling Change Request form. DIT personnel enter the change and the SAM Control arranges the schedule and the starting of jobs. The Board of Elections sends documentation for each job they want scheduled and DIT manually schedules the job. **Error Processing in MVS and Unisys Computing Environment** Control-M and SAM Control alert the console operator when there is a problem by highlighting the line of an error. Each job submitted to scheduling has instructions for when errors occur. If the error is an agency job, the customer contact person or programmer is contacted, whomever the documentation instructs to call. If the problem is with an application, an on call engineer is contacted. Operations keeps an on call list of engineers for both agencies and DIT. In all cases of an error, a problem resolution ticket is created (see the HELP DESK Control Objective for a description of Info/Sys Problem Management Database). This ticket often helps in solving recurring problems quicker. The console operator will fix the problem or contact the on-call engineer for the application. If a job does not run through Control-M, the customer monitors the job. The only exception is if a customer calls the console operator and makes a special request for him to monitor a job. In this case, the customer must provide the console operator with a contact person and instructions on what to do if an error occurs.	form (DIT-04) and perform the following: a) Determine that it is scheduled in SAM Control for the time stated in the request form. b) Determine that all prerequisites as stated in the request form have been met before the scheduled run time. Document and evaluate access to SAM Control, for adding, deleting, or changing scheduling related information.	

Objective: ***Policies and procedures provide reasonable assurance that a periodic monitoring of system performance/capacity occurs.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Capacity Planning Branch is part of the Technology Resource Management Division, which is under the Finance & Administration Directorate. Capacity planning covers the MVS and Unisys Environments and the Commonwealth Telecommunications Network. The Capacity Planning Branch prepares a capacity planning report monthly to be used for procurement planning. The report contains recommendations, based on the performance/capacity measures. There is a capacity planning meeting monthly. **MVS Performance/Capacity Monitoring Procedures** Several software packages monitor performance and capacity in the MVS computing environment. NetSpy by Computer Associates runs constantly and can intercept data and identify the kind of application (VTAM, CICS, TSO) in use. Additional software periodically analyzes the NetSpy data and produces performance and capacity reports. DIT is installing Omegamon software, from Candle Corporation, to do performance monitoring for the MVS environment on a continuous basis. Omegaview software will alert operators of possible problems. **Unisys Performance/Capacity Monitoring Procedures** A software package called PRISM monitors the Unisys lines. PRISM reports the transaction traffic on a line. DIT will eventually replace this software because it cannot monitor newer technologies like TCP/IP. DIT will provide the PRISM line summary report to customers who request it, such as DMV, DSS, VEC and TAX. Constant monitoring of the Unisys system occurs. TORCH/PMS software (Performance Management System) collects Unisys system statistics and downloads the data to VIEWPOINT software on a PC. VIEWPOINT constantly displays statistics about the Unisys system. When	Document and evaluate the effectiveness of the capacity planning meeting by reviewing notes and memos from the meetings. Determine that the following areas are reviewed for the MVS, Unisys, LAN, and PC environment at these meetings: a) Processor capacity and speeds. b) Storage capacity and access times. c) Communication traffic volume and speed. d) Memory capacity and speed. Document and evaluate the effectiveness of performance/capacity monitoring software that is run in the MVS environment. Obtain a printout of an MVS performance-monitoring report and judgmentally choose three messages that appear to be threatening. Determine what actions have been taken or will be taken. Document and evaluate the effectiveness of performance/capacity monitoring software that is run in the Unisys environment. Obtain a printout of a Unisys performance monitoring report and judgmentally choose three messages that appear to be threatening. Determine what actions have been taken or will be taken.	No exceptions were noted.

Objective: ***Policies and procedures provide reasonable assurance that a periodic monitoring of system performance/capacity occurs.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
VIEWPOINT encounters a problem, it flashes a red signal or produces an audible alarm. If a problem occurs, the Unisys Operator notifies the Help Desk or Unisys Systems Engineer. The same alarm also alerts a Unisys Systems Engineer on their PC.		

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, and documentation occurs for changes to existing hardware and the implementation of new hardware.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Computer Operations Division performs backups of the MVS and Unisys environment including all shared disk packs. It is the customer's responsibility to perform backups of all dedicated disk packs. It is the customer's responsibility to inform DIT of the information to store offsite. **MVS and Unisys Backups and Offsite Storage** Customers must notify DIT to store off-site all data files and application programs. DIT does backup all data files and application programs that reside on shared disk packs nightly (Sunday through Friday except holidays) at midnight. DIT uses SAM Control and Control-M to automatically perform the nightly backups for Unisys and MVS systems, respectively. A back up occurs nightly (Sunday through Friday except holidays) at midnight for all MVS operating system files, any sub-systems, and program products. There is a weekly back up of all dedicated IMS and ADABAS database files. The DIT scheduling group enters the back up, offsite storage, and retention time requests made by customers and in-house divisions into an automated system. DIT maintains the latest disk file backup tapes at the data center for on-request file restoration. As part of DIT's disaster recovery plan, the offsite storage facility has the next two (older) backup tapes. DIT has contracted with Data Base, Inc. for their off-site storage. Data Base, Inc. sends a courier to pick up new and return old tapes. Monthly, DIT personnel go to the off-site storage location and perform an inventory of the tapes. If there is a discrepancy, DIT personnel determine the cause for the discrepancy. A bar code on Unisys tapes helps to reduce discrepancies. During March 1997, the MVS librarians began using scanning equipment to pull the tapes. Also, later in calendar year 1997, DIT began using a robotics tape library for the MVS tapes. When this went into	Determine if DIT has backup procedures for the following. a) Shared and dedicated disk packs in the MVS ENVIRONMENT b) Shared and dedicated disk packs in the Unisys environment c) Dedicated database files d) System files e) Historical tapes f) Tape storage off-site along with the tape retention period g) Backup of individual microcomputers Visit the off-site storage area and perform the following: a) Review the facility for physical security (access, fire and water suppression etc). b) Match the tape inventory by tracing a judgmental sample of ten items from DIT's off-site storage list to the inventory at the off-site location. Obtain from DIT the scheduling printouts from Control-M and SAM Control to determine that a backup job routine is scheduled. Examine a copy of the backup jobs source code (JCL) to verify what is being backed up. Contact an agency and obtain a list of what they have requested DIT to back up and a list of what tapes they have requested that DIT store off-site. Determine that these backups are occurring and that the requested items are on DIT's off-site storage list. Determine, by reviewing DIT's off-site storage list, that LAN server backups are occurring and stored offsite (especially the IHRIS system) and that firewall and router configurations are stored offsite. Determine that for the Systems Development Division (SDD): a) That software under development for	No exceptions were noted

Objective: ***Policies and procedures provide reasonable assurance that proper authorization, testing, and documentation occurs for changes to existing hardware and the implementation of new hardware.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
operation, the "Rabbits" began pulling the tapes for off-site storage. Now the MVS librarians scan the tapes to verify the shipment of the correct tapes. **PC and LAN Backups** DIT employees regularly back up data on their PC hard drive. If the DIT employee created critical data files, the DIT employee has responsibility for storing the backup copy off-site for purposes of disaster recovery. The DIT LAN Administrator backs up data files stored on network directories nightly. **Systems Development Division (SDD)** SDD copies and stores offsite all systems and documents for SDD customers and internal management and administration. Offsite storage includes all SDD purchased software tools and packages and one copy of the Management and Control System (MACS) microfiche files. Every Friday night, there is an automatic back up of the SDD LAN project directory, and an automatic incremental tape backup runs Monday through Thursday night. SDD can use the last incremental tape and the Friday night backup tape for reconstruction of files. All backup tapes are stored in the DIT/MIS fireproof safe.	agencies and DIT is backed-up and included in DIT's offsite storage list. b) That a copy of the Management and Control System (MACS) is included on DIT's offsite storage list. c) That software purchased by SDD and not on the LAN servers, is backed-up and stored along with its documentation offsite. This can be determined by reviewing DIT's off-site storage list. Request a list of critical applications that are stored on microcomputers. Determine that they are backed-up properly.	

Objective: ***Policies and procedures provide reasonable assurance that data completeness, accuracy, and security occurs for data transmissions/communications between DIT and customers.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
DIT provides several modes of communications such as dial-up, dedicated lines, and a telecommunications network. Our focus for this objective is the Commonwealth Telecommunications Network (CTN) used as the backbone carrier by a customer for their private network. There are three areas that customers must understand when using the CTN. First, DIT provides routers and firewalls to protect systems that reside in the DIT data centers. Second, DIT does not provide the necessary security (firewalls and routers) to protect customer networks. This security is the responsibility of each CTN user. Finally, various telecommunication companies such as MCI, Bell Atlantic, and Sprint own and control the physical lines from the customer to DIT. The customer can use frame relay, PVC (Point Virtual Circuit), or a telephone line on the CTN to send data to DIT. The customer contacts DIT to establish the proper connection and DIT contracts with various communication companies to provide the telecommunication service. There are multiple ways agencies can access DIT. They can access through a direct connection using SNA architecture for legacy systems, through a router based frame relay network using TCP/IP, and various dial-up connections. There are multiple physical lines connecting the CTN to the DIT facility. When the data enters DIT, its first contact is the router. Traffic from the Internet hits an additional router. An access list is a security feature programmed into the router using Internet protocol (IP) addresses. Only customers using the specified IP address can gain access through the router. After the router, the raw TCP/IP data passes to the DIT Firewall; and again there is verification made to grant or deny access. Customers must request access to the DIT Firewall (see further explanation at the LOGICAL ACCESS Control Objective). DIT does not establish or configure	Document in detail the communications environment that surrounds the DIT to agency interface. Specifically account for: a) The Commonwealth Telecommunication Network (CTN) b) Frame relay circuits c) Point to Point dedicated circuits d) Analog dial-up lines Obtain the router table and perform the following: a) Determine that source and destination IP addresses are valid. Investigate any addresses that seem odd. The default should be to deny all traffic. b) Determine what filtering if any is being done at the router. Filtering should show up as "deny statements." c) Determine that Internet traffic that **originated** from outside of DIT is routed to a secure Web Page or the firewall. d) Determine that the router is using the two level password option so that the router table itself is secure. e) Determine that telnet services are not allowed on this router because this router interfaces with the Internet. All maintenance on this router should be done in person. f) Determine who is allowed to make changes to this router, who is responsible for reviewing the table, and how often. Tour the DIT offices and Data Center and look for analog lines that are connected to systems equipment. Determine the need of such lines and their security. Determine if DIT allows employees or agency employees to dial in from laptops or home PCs. Evaluate the method and security of this arrangement. Document instances of line down time and how DIT and the CTN handle such an event. Document how DIT provides incoming and	The Internet router allows all sources to attempt to logon to the router via telnet. The telnet and Enable passwords are not encrypted. This current configuration increases the chances of unauthorized changes to the router's configuration. Final approval of a router's security settings is done by each agency. Some agencies assume that when DIT configures the router, it is set up to be bulletproof. This is not necessarily so. This arrangement allows for an exposure that an agency security configuration could be deficient. **Auditors performing agency audits should review critical router configurations**. The Department has no central division for its network services. The structure seems to be disjointed in terms of network security. The Department has not issued an updated network diagram since September 1996. There are individual portions of the network diagram in the Unisys Database Division, Unisys System Support, Telecommunications, and Computer Operations Division. There are two individuals in the Unisys Database Division responsible for firewall security, and one individual in the Unisys System Support Division who is responsible for router security.

Objective: ***Policies and procedures provide reasonable assurance that data completeness, accuracy, and security occurs for data transmissions/communications between DIT and customers.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
customer routers unless requested. The request to have their router set up or worked on follows the procedures used for problem management (See procedures for the HELP DESK Control Objective). Various telecommunication companies own and control the physical lines between the customer and DIT. DIT has no security responsibility for these lines.	outgoing Internet services for other agencies. Determine if this function is secure for DIT and whether the DIT firewall protects agencies from any Internet based threats. Investigate and document the extent of cooperation between DIT and an agency when it comes to configuring the necessary communication lines and equipment (modem, routers). Determine if this provides a secure method of communications implementation.	

Objective: ***Policies and procedures provide reasonable assurance that Department of Information Technology conforms to CIM Standard 95-1 Information Technology Resource Management Standard as it relates to the following areas:***

- ***Business Impact Analysis***
- ***Risk Assessment***
- ***Contingency Management Plan***
- ***Security Awareness/Training Programming***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Security Division promotes information security awareness; provides security technical assistance to divisions; implements and administers security programs and procedures; performs risk analyses; investigates alleged security breaches; develops, maintains, and disseminates a contingency management plan; and trains users on proper methods of securing technology resources. **Business Impact Analysis** DIT has completed a Business Impact Analysis following CIM Standard 95-1. The Business Impact Analysis only covers systems that affect DIT's business, not customer applications. DIT sent a questionnaire to each DIT Division Director and DIT Project Leader requesting they identify their critical systems and the resulting impact if the system was not operational for a period of time. DIT compiled the information into the Business Impact Analysis and the DIT Director approved it. When adding new systems, a business impact analysis should determine if the system contains critical or confidential information and should be included in the overall Business Impact Analysis. **Risk Assessment** DIT uses a risk assessment software package called RISKWATCH. Risk assessments are conducted at least every two years or as major system changes occur to determine whether measures exist to counteract threats to assets under DIT's control.	Determine that a recent Business Impact Analysis exists. Review this analysis for reasonableness. Obtain the name of a new system addition over the last year. Determine that this new system has been added to the Business Impact Analysis. Obtain a copy of the last prepared formal risk assessment. Determine that it is no more than 2 years old and that it reflects major system changes that have occurred in the past year as DIT policy requires. Review the contingency plans for DIT and evaluate for reasonableness. Consider time frames, percentage of operations that could be brought on-line, and the effect on the state agencies that rely on it. Request of the Contingency Plan Administrator three of the DIT required quarterly division updates from the Disaster Recovery Coordinators. Determine that they exist or if no changes were needed that an e-mail was sent to the Contingency Plan Coordinator. Make an inquiry to SunGard (DIT's hot site vendor) and determine that they have been kept abreast of any critical changes to the contingency requirements. Obtain a schedule and proof that the "Hot Site" scenario has been tested for both the MVS and Unisys environment. Obtain the names of five recently hired DIT employees and request to see their signed Information Security Agreement. Obtain the training attendance logs for the DIT Systems Security personnel. Determine that they have taken courses in the last year on security related topics. Verify that all DIT employees have had security awareness training.	The Business Impact Analysis was updated in April 1999; however prior to this date, an analysis had not been completed since 1996. Critical system changes have taken place over the last two years that were not in the Business Impact Analysis until 1999.

Objective: ***Policies and procedures provide reasonable assurance that Department of Information Technology conforms to CIM Standard 95-1 Information Technology Resource Management Standard as it relates to the following areas:***

- ***Business Impact Analysis***
- ***Risk Assessment***
- ***Contingency Management Plan***
- ***Security Awareness/Training Programming***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
DIT's risk assessment procedures include: identifying the likelihood of an occurrence of a threat, investigating the factors that could affect the threat occurrence rate, determining the vulnerabilities of service areas to potential threat, estimating the loss potential of a service area, and developing proactive countermeasures to reduce business loss. **Contingency Management Plan** The Contingency Plan Administrator maintains DIT's contingency management plan. The critical divisions at DIT have a Contingency Management Plan. Each critical division has a Disaster Recovery Coordinator, who updates their division's portion of the plan. The disaster recovery coordinators review the divisional action plans quarterly to determine the status of the information. The entire plan is now kept on the L:\ drive and can be accessed by all DIT employees. A month before the end of each quarter, the Disaster Recovery Coordinator sends out e-mail to each Division Coordinator. The Division Coordinator will make the necessary changes directly to their plan located on the L:\ drive. If there are no changes, the Disaster Recovery Coordinators send e-mail to the Contingency Plan Administrator stating there are no changes. DIT has a contract with SunGard to provide a "hot site" for the restoration of the MVS system in the data center. Philadelphia, Pennsylvania is the hot site location and DIT tests the hot site regularly to verify that the system and data can be restored. DIT signed a contract on March 25, 1997 with SunGard to provide a hot site in Warminster, Pennsylvania for the Unisys system. As of the date of this report, DIT has not tested the Unisys hot site.		

Objective: ***Policies and procedures provide reasonable assurance that Department of Information Technology conforms to CIM Standard 95-1 Information Technology Resource Management Standard as it relates to the following areas:***

- ***Business Impact Analysis***
- ***Risk Assessment***
- ***Contingency Management Plan***
- ***Security Awareness/Training Programming***

Provided by the Department	**Provided by the Auditor of Public Accounts**	
Policies and Procedures	**Tests Performed**	**Results**
The Contingency Plan Administrator maintains a list of current processing requirements for the alternate processing site and the divisional action plans. The Administrator updates the divisional action plans with changes submitted from the Disaster Recovery Coordinators. SunGard, the hot site vendor, receives from the DIT Configuration Review Committee any plan changes. The Administrator requests annually from customers a list of critical applications processed by DIT and uses this information for capacity planning at the hot site. **Security Awareness/Training Program** Human Resources and Security require that new employees read DIT Directive 92-1 - System Access Control and sign an Information Security Access Agreement. This agreement details the proper use of employee access to DIT systems. If the new employee will have Internet access they must sign an Internet Use Form. DIT does not have any formal procedures for security awareness/training for existing employees. However, annually at the end of November, the Security Division sponsors a Computer Security Day. DIT places a notification in each employee's pay envelope letting the employee know the training date and there are posters displayed in the building. Closer to the Security Day, employees receive an e-mail as final notification. During Computer Security Day, employees attend a formal program and receive a packet of information on security awareness.		

Objective: ***Policies and procedures provide reasonable assurance that Help Desk personnel, hardware, and software supports the user agencies.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
All DIT personnel must follow the DIT Policies and Procedures Manual. Management uses the policies and procedures to direct the decision-making process, and ensures that all DIT employees know the approved policies and procedures. DIT also has a Customer Guide, which contains procedures for their customers. **Approval Process for New/Changes to Existing Policies and Procedures** A Director or Manager initiates a draft policy and/or procedure. The Manager/Director sends the draft, usually through e-mail, to the Division Directors and Managers for input. The initiating Director or Manager takes the input into consideration and then submits a final draft to Human Resources. Human Resources submits the draft to the Agency Director for approval. If the Agency Director approves the policy or procedure, there is a distribution to the Division Directors/Project Leaders, who have the responsibility of making all employees aware of approved policies and procedures. **Division Procedures** Divisions may develop procedures that apply only to their division. Procedures developed by divisions must comply with the DIT Computer Services Division Customer Guide and the Problem Management Guidelines and Procedures Manual. The Deputy Director of Services approves divisional procedures. The Branch/Division Manager reviews the DIT Computer Services Division Customer Guide every December and makes the appropriate changes. There is no periodic review of the Problem Management Guidelines and Procedures Manual. If a manager identifies a possible change to the manual, he will present the change in writing and management conducts an analysis of the request. Management discusses the change at the weekly management meeting. If approved, management issues the change and then evaluates the success or failure of the change.	Determine that policies are initiated and approved in the manner described by the DIT Policies and Procedures Manual. Choose one new policy or procedure and one policy or procedure update and follow it through these steps: a) Determine that wanted policy is drafted by Division or Branch. b) Draft is distributed to Agency Director, Deputy Director and Division Directors for comment. c) If approved, it is signed by the Agency Director and distributed to the Division Directors / Branch managers. d) Employees are made aware of the policy by management. Document and evaluate whether a process to review policies for effectiveness and relevancy occurs on a regular basis.	There is no policy for periodically reviewing policies and procedures. The Intranet site, the main source of information concerning policies and procedures for employees, is not kept up to date.

Objective: ***Policies and procedures provide reasonable assurance that Help Desk personnel, hardware, and software supports the user agencies.***

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Help Desk in the Computer Operations Division identifies, records, tracks and engages the appropriate resources to resolve customer and DIT system problems. DIT provides Help Desk service 24 hours a day. DIT uses an Automatic Call Distribution (ACD) software package that tracks and routes calls to either Help Desk or Network Communications Center personnel. Personnel log all problem calls into the IBM Info/Sys Problem Management database maintained in the MVS environment. Info/Sys records problems as tickets and automatically assigns a number and tracks the call. The Problem Management Guidelines and Procedures manual outlines procedures for creating, escalating, reviewing, dispatching, checking status, and closing tickets. When the MVS system is not operating, the Help Desk personnel manually record calls on a Problem Entry Reporter form, but do not assign a problem number. Once the system comes back up, personnel enter the manual ticket for logging and number assignment and then call the customer with the ticket number. The ACD system can track and report on calls answered, hung up before answering, and the wait times for calls. Management runs these reports daily and reviews them. Management reviews and discusses tickets open more than two weeks in Info/Sys at a weekly meeting.	Evaluate and document any Help Desk software that is used by DIT. Follow a sample of five recent help desk calls from the original call, then to the Automatic Call Distribution (ACD), and finally to problem resolution. Document and evaluate the response time and the following steps: a) Communication of the problem to proper DIT personnel b) Problem ticket creation c) Proper review and escalation if needed d) Method and speed of dispatching e) Reviewing of status of the problem resolution f) Closure of problem ticket	No exceptions were noted.

Section IV. OTHER INFORMATION PROVIDED BY THE SERVICE AUDITOR

The Year 2000 Issue

DIT's Information Resource Management Division began researching the potential impact of the Year 2000 issue on the Commonwealth in December 1995. DIT developed its general Year 2000 plan in October 1996. DIT's Year 2000 Internet homepage is the source for data center Year 2000 compliance information. This site provides detailed compliance information for the data center's hardware; IBM, Unisys, and UNIX software; and telecommunications equipment and service providers.

During this past year, DIT's Director coordinated with the Century Date Change Initiative (CDCI) Project Office Director to develop a reporting mechanism for the data center. In the May 1999 CDCI Agency Summary Year 2000 Progress Report shows the data center as 95 percent complete and telecommunications as 99 percent complete. Of the 5 percent not completed at the data center, testing and validation of the information systems and embedded systems makes up the largest part.

On behalf of the Century Date Change Initiative, an outside entity reviewed DIT's Year 2000 effort. This external verification, performed by CACI Inc., reported several findings. CACI states, "there is no specific analysis document to ensure uninterrupted services" from vendors. The report does state however, that DIT's personnel "are highly knowledgeable of Year 2000 compliance and methods and proactive in their pursuit of Year 2000 compliance."

DIT provides several tools that customer agencies can use to test their mainframe applications for Year 2000 compliance. A logically partitioned unit of the IBM mainframe, LPAR6, has Year 2000 "tools" for customers to use for development and testing with a simulated date. After testing their applications on LPAR6, customer agencies are ready to use the "Time Machine."

The Time Machine is a real Year 2000 environment consisting of two logically partitioned units totally isolated from production systems. The Time Machine loads and operates with a future date. The customers that use DIT the heaviest have used the Time Machine, but all mainframe customers should test their applications in the Time Machine. Customers currently testing in the Time Machine have discovered problems they could not detect using date simulation. DIT also has a Unisys Time Machine for customer testing. The major Unisys customers have used this time machine.

Section V. RESOLUTION OF PRIOR YEAR AUDIT FINDINGS

The Department of Information Technology has not taken adequate corrective action on these previously reported findings, which are also included in Section I. FINDINGS SUMMARY. The Department of Information Technology corrected all other previously reported findings and we have not included them in this report.

Limit Data Center Access

As of March 31, 1998, 259 individuals had access to DIT's data center, several of which have no need for this access. Currently, there are no guidelines for area managers to follow when determining whether their employees need data center access. Individual area managers request physical access for employees under them. Additionally, the Center's management only annually reviews who has data center access.

During our review, we found that DIT does not have policies and procedures in place to limit access to the data center. Therefore, we again make this recommendation in this year's finding, "Limit Data Center Access."

Require Vendor Notification of Employee Terminations

DIT does not have a policy that requires vendors to give notification when their employees with data center access terminate. Several of DIT's outside vendors have physical access to the data center. Physical security relies on the vendor to tell them when their employees terminate.

During our review, we found that DIT does not have policies and procedures in place to require vendor notification of employee terminations. Therefore, we again make this recommendation in this year's finding, "Require Vendor Notification of Employee Terminations."

Enforce Policy Requiring Employees to Visibly Display Picture ID Badges

DIT does not enforce its' policy requiring employees to visibly display picture ID badges at all times. We noted numerous instances of employees carrying their ID badge in their pocket or laying their ID badge down where someone else could easily pick it up.

During our review, we found that DIT does not enforce policies and procedures to require employees to visibly display picture ID badges. Therefore, we again make this recommendation in this year's finding, "Enforce Policy Requiring Employees to Visibly Display Picture ID Badges."

Modify Router Configurations

The primary routers that route communication traffic between DIT, user agencies, and the Internet allow all sources to attempt to logon to the router via telnet. Additionally, DIT does not store the passwords used to protect the router's configuration in an encrypted format. This current configuration increases the chance of unauthorized changes to the router's configuration.

DIT made the necessary corrections to the primary router. They have not made corrections to the Internet router. Therefore, we again make recommendations to modify the Internet router in this year's finding, "Modify Router Configuration."

Write a Policy for Updating and Reviewing Policies and Procedures

There is no formal policy for updating, revising, or regularly reviewing policies and procedures. This increases the risk that employees may follow outdated or incorrect versions of policies and procedures. We found one instance of an outdated policy rather than the most current version. In another case, we found an updated policy for documenting system software changes without its official release.

During our review, we found that DIT has not completed updating their policies and procedures manual. Therefore, we again make this recommendation in this year's finding, "Organize and Maintain the Agency Policies and Procedures Manual."

May 13, 1999

The Honorable James S. Gilmore, III
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Richard J. Holland
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

INDEPENDENT SERVICE AUDITOR'S REPORT

We have examined the accompanying description of the **Department of Information Technology's** (the Department) policies and procedures set forth in Section III of the accompanying report applicable to the automated data processing of transactions and other related services for the Commonwealth of Virginia. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's policies and procedures that may be relevant to the internal control structure of an organization (the Customer) using these services, (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if these policies and procedures were complied with satisfactorily, and (3) such policies and procedures had been placed in operation as of March 31, 1999. The accompanying description includes only those policies and procedures and related control objectives of the Department and does not include policies and procedures and related control objectives of any third party vendor. Our examination did not extend to policies and procedures of third party vendors. The control objectives were specified by the Auditor of Public Accounts. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned policies and procedures presents fairly, in all material respects, the relevant aspects of the Department's policies and procedures that have been placed in operation as of March 31, 1999. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified policies and procedures, included in Section III of this report, to obtain evidence about their effectiveness in meeting the control objectives described in Section III as of March 31, 1999. The specified policies and procedures and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user organizations of DIT and to their auditors to be taken into consideration, along with information about the internal control risk for user

organizations, when making assessments of control risk for user organizations. In our opinion, the policies and procedures that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved as of March 31, 1999.

The description of policies and procedures at the Department is as of March 31, 1999 and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the policies and procedures in existence. The potential effectiveness of specific policies and procedures at the Department is subject to inherent limitations and, accordingly, errors or irregularities 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.

The description of specific policies and procedures at the Department, as set forth in Section III, and their effect on assessments of control risk at customer organizations are dependent on their interaction with the policies, procedures, and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual customer organizations.

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

AUDITOR OF PUBLIC ACCOUNTS

KKH:jld
jld:58