SOUTH CENTRAL OHIO COMPUTER ASSOCIATION (SCOCA)
STATE REGION - ISA, PIKE COUNTY

SAS - 70

JUNE 30, 2007 THROUGH AUGUST 8, 2008

Mary Taylor, CPA
Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Mary Taylor, CPA
Auditor of State

INDEPENDENT ACCOUNTANTS' REPORT

Board of Directors
South Central Ohio Computer Association (SCOCA)
175 Beavercreek Rd.
Piketon, OH 45661

To Members of the Board:

We have examined the accompanying description of controls of the South Central Ohio Computer Association (SCOCA) applicable to the processing of transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS), and Education Management Information System (EMIS). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the SCOCA 's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the internal controls contemplated in the design of the SCOCA's controls; and (3) such controls had been placed in operation as of August 8, 2008. The SCOCA uses the services of the Northwest Ohio Computer Association (NWOCA) for systems development and maintenance of the USAS, USPS, SAAS/EIS and EMIS. The accompanying description includes only those controls and related control objectives of the SCOCA, and does not include controls and related control objectives of NWOCA. Our examination did not extend to controls of NWOCA. The control objectives were specified by the SCOCA management for the processing of USAS, USPS, SAAS/EIS, and EMIS with the assistance of the Ohio Department of Education. 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 controls presents fairly, in all material respects, the relevant aspects of the SCOCA's controls that had been placed in operation as of August 8, 2008. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the SCOCA's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from June 30, 2007 to August 8, 2008. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user organizations of the SCOCA and to their auditors to be taken into consideration along with information about the internal control at user organizations, when making assessments of control risk for user organizations.

88 E. Broad St. / Tenth Floor / Columbus, OH 43215-3506
Telephone: (614) 466-3402 (800) 443-9275 Fax: (614) 728-7199
www.auditor.state.oh.us

In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from June 30, 2007 to August 8, 2008.

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

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

The description of controls at the SCOCA is as of August 8, 2008, and information about tests of the operating effectiveness of specified controls covers the period from June 30, 2007 to August 8, 2008. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the SCOCA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the SCOCA, its user organizations, and the independent auditors of its user organizations.

Mary Taylor

Mary Taylor, CPA
Auditor of State

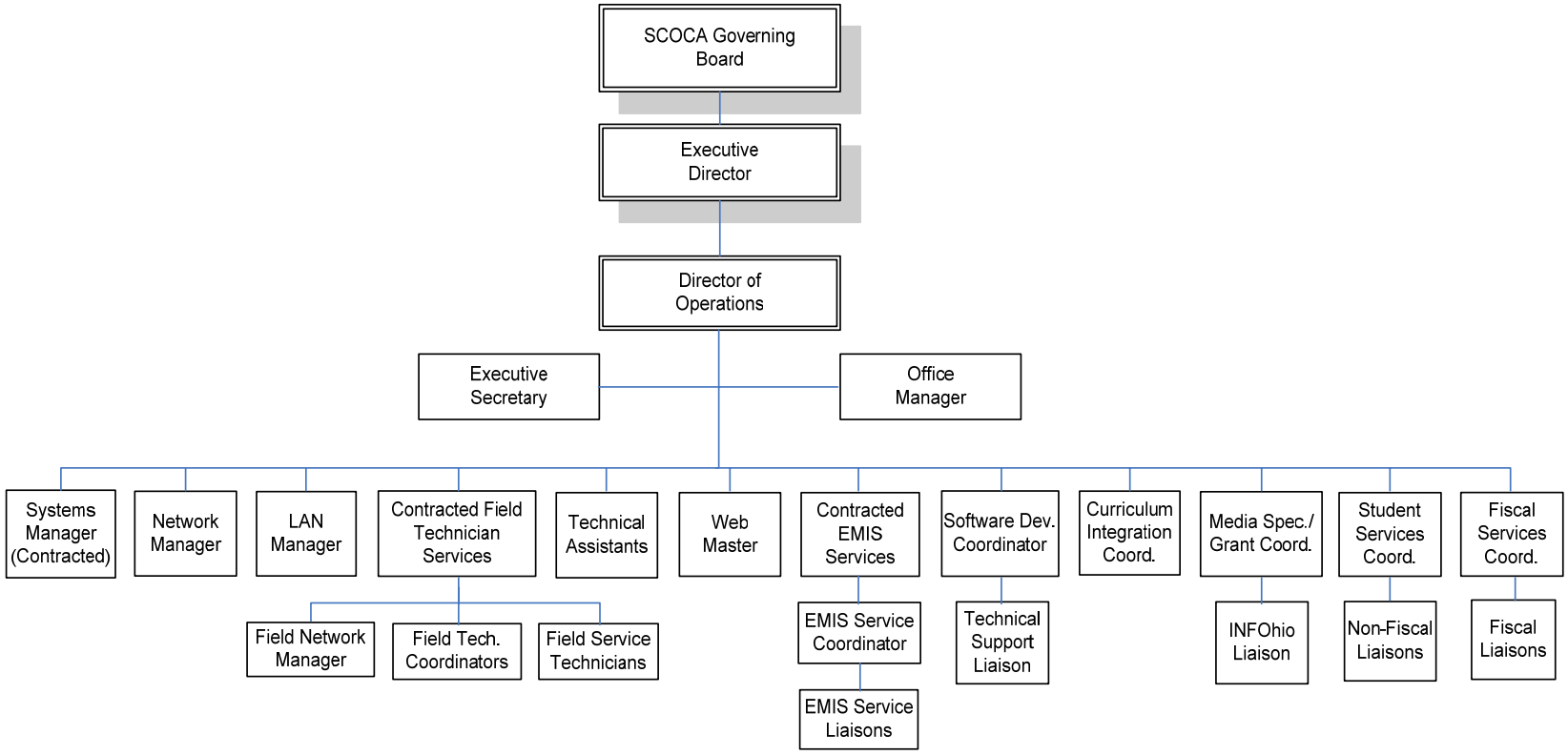
August 8, 2008

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

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

OVERVIEW OF OPERATIONS



The SCOCA is one of 23 not-for-profit computer service organizations serving more than 740 educational entities and 1.2 million students in the state of Ohio. These service organizations, known as Information Technology Centers (ITCs), and their users make up the Ohio Education Computer Network (OECN) authorized pursuant to Section 3301.075 of the Revised Code. Such sites, in conjunction with the Ohio Department of Education (ODE), comprise a statewide delivery system to provide comprehensive, cost-efficient accounting and other administrative and instructional computer services for participating Ohio entities. Funding for this network and for the (SCOCA) is derived from the state of Ohio and from user fees.

ITCs provide information technology services to school districts, community (charter) schools, JVS/career & technical, educational service centers (ESCs) and parochial schools; however, not all entities subscribe to the same services. Throughout the remainder of the report, the term "user organization" will be used to describe an entity which uses one or more of the following applications:

- Uniform School Accounting System (USAS).
- Uniform Staff Payroll System (USPS).
- School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS).
- Education Management Information System (EMIS).
- Community School Average Daily Membership (CSADM).

ITCs are organized as either consortia under ORC 3313.92 or Council of Governments (COG) under ORC 167. ORC 3313.92 allows for school districts to create a partnership (a consortia) to resolve mutual needs. One of the members of the consortia is designated as fiscal agent. The fiscal agent provides all accounting, purchasing, and personnel services for the consortia. A "COG" under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. The SCOCA is organized under ORC 3313.92 and the Pike County JVSD serves as their fiscal agent.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the governing board. The governing board is the legislative and managerial body of the SCOCA and is composed of 22 members; the fiscal agent superintendent, two representatives from each county and two treasurers. The governing board is responsible for supervising and administering operations of the SCOCA, setting overall policies, appointing sub-committees, and supervising staff and setting salary schedules. The governing board meets bi-monthly.

In addition, a six-member executive committee exists to review and make recommendations on pressing issues as defined by the executive director and the governing board. The committee consists of the governing board chairman, governing board vice-chairman, previous year's governing board chairman, fiscal agent superintendent, and two at-large members. The chairman appoints the at-large members. The governing board, the executive committee and the sub-committees work with the executive director to provide oversight and planning for the organization.

The SCOCA employs a staff of 51 individuals and is supported by the following functional areas:

Fiscal Services:	Provides support to end users for all fiscal services applications. Fills in for vacancies in the business offices when there is a change of staff, vacations, maternity leave, or a district needs additional assistance

	for a period of time.
Student Services:	Supports end users in all aspects of the student service applications with a focus on EMIS and assists in the software development of the EMIS.
INFOhio Services:	Supports end users in all aspects, from the day to day training and support of library automation to the electronic resources through INFOhio.
Network/Systems Support:	Supports the SCOCA computer systems and its networked communication system. Provides training and support to the users.
Video/Curriculum Integration:	Provides video scheduling and support as well as integration of technology in curriculum.
Field EMIS Services:	Districts may contract with SCOCA to act as their EMIS Coordinator and maintain the EMIS database as well as submit EMIS data to ODE.
Field Technical Services:	Districts may contract with SCOCA for a technician to work in their district or they may contract with SCOCA to act as their tech coordinator.

The managers of each of the functional areas report to the director of operations who reports to the executive director.

The SCOCA is generally limited to recording user organization transactions and processing the related data. User organizations are responsible for authorization and initiation of all transactions. SCOCA's management reinforces this segregation of duties as a part of its new employees' orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced SCOCA employees may alter user data and only at the request of the user organization.

The SCOCA follows the same personnel policies and procedures as their fiscal agent, the Pike County Joint Vocational School District. When necessary, additional policies will be developed and approved by the SCOCA governing board to address concerns of the SCOCA. Detailed job descriptions exist for all positions. The SCOCA is constantly re-evaluating its need for personnel to provide for the increasing range of services provided. The reporting structure and job descriptions are periodically updated to create a more effective organization.

The SCOCA hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree or experience in a computer-related field, and all the SCOCA staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must attend at least 15 hours of approved professional development training annually, and at least 80 hours of approved training every four years. All the SCOCA staff members are permitted and encouraged to attend professional training as deemed necessary. Staff evaluations are conducted annually by the executive director. The governing board is in charge of the annual evaluation for the executive director.

Risk Assessment

The SCOCA does not have a formal risk management process; however, the governing board actively participates in the oversight of the organization. As a regular part of its activity, the governing board addresses:

- New technology.
- Realignment of the SCOCA organization to provide better service.
- Oversight and supervision of the overall operation of the SCOCA.
- Personnel issues, including hiring, termination, and evaluations.
- Additional charges and services provided to user organizations and other entities.
- Changes in the operating environment as a result of ODE requirements, Auditor of State (AOS) and other accounting pronouncements, and legislative issues.

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

Monitoring

The SCOCA organization is structured so that department managers report directly to the director of operations who will then report to the executive director. Key management employees have worked here for many years and are experienced with the systems and controls at the SCOCA. The SCOCA executive director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, SCOCA uses a variety of ”key indicator” reports to monitor the processes involved in processing transactions for user organizations.

Hardware, software, network, database integrity, Internet usage, computer security and user help desk reports are monitored on an ongoing basis by departmental management. Some of these reports are automatically run through a scheduler program and sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the systems manager receives the same reports and monitors for interrelated and recurring problems.

INFORMATION AND COMMUNICATION

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

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The SCOCA staff members do not perform system development activities. Instead, the SCOCA utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the Northwest Ohio Computer Association (NWOCA), another ITC of the OECN. The Ohio Department of Education (ODE) determines the scope of software development for state-supported systems. Tactical means of accomplishing software development priorities are determined by the Software Advisory Committee (SAC), which consists of members from the Management Council of the OECN (MC OECN), the Ohio Association of School Business Officials (OASBO), the ODE and the SSDT. The SAC meets four times per year to discuss the status of proposed and ongoing projects.

Changes to Existing Applications and Systems

End-users participate in the program development/change process via the Software Performance Report/Request (SPR) tracking procedure, which is maintained by the SSDT. The SPR system utilizes SiteScape Forum, which is used for electronic conferencing, to accept and discuss proposed software enhancements in a public forum. Each major software package (USAS, USPS, SAAS, EMIS) has its own public and ITC forum which is monitored by the SSDT system analysts. All OECN ITC's and a majority of user organizations have access to forum conferences, providing end-user participation in the program development/change process.

The SCOCA personnel do not perform program maintenance activities. Instead, they utilize the applications supplied to them by the SSDT. The OECN requires the ITC to keep the version of each application current based on the provider's standard for continued support. Procedures are in place to ensure the SSDT developed applications are used as distributed. The SSDT, at NWOCA, copies zipped files containing the quarterly updates to the ITC's systems. The source code is not distributed with these files. Release notes are contained within these files and explain the changes, enhancements and problems corrected. User and system manager manuals are also distributed with these releases and are also available through the SSDT website. The SSDT informs the ITC's they will support only the latest release of the state software beginning 30 days following the software release date.

The SCOCA uses a software utility called OECN_INSTALL to unpack these zipped files and install each individual package into its proper OECN directory. The OECN_INSTALL utility has two options which will either install the new release on the system or install a patch for a current release. This utility ensures that all required components are installed properly and consistently.

Only vendor supplied changes are made to the operating system or system software documentation. The Northern Buckeye Education Council (NBEC), who acts as the fiscal agent for this and other participating ITC, has entered into a licensing agreement under the Campuswide Software License Grant Program (CSLG) through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of HP software packages.

The services acquired and/or provided by the NBEC under the agreement include the following:

- Provide for the acquisition and distribution of software media to the participating ITC for a limited series of HP software packages as approved by the board of trustees of the MCOECN.

- Provide telephone technical support to the participating ITC's technical staff for a limited series of HP software packages approved by the board of trustees of the MCOECN.

- Track and maintain an accurate listing of all HP hardware and software covered under the agreement.

- Provide periodic training and update sessions covering the policies and regulations governing this program as well as updating the ITC's technical staff on the latest releases of HP software packages covered under the agreement.

As a participating member of the program of the MCOECN the participating ITC's agree to the following:

- Read, sign, and comply with the rules and regulations of the CSLG Program and the Education Software Library (ESL) Program as operated by the NBEC on behalf of the MCOECN.

- Provide unrestricted privileged access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems of distributed software.

- Provide HP or MCOECN representatives, upon prior written notice, with physical access to computer facilities at reasonable times during normal business hours to inspect centers and system records for compliance with the terms of the CSLG and ESL Programs.

- Make payments to NBEC for services under the agreement within 30 days of the receipt of an invoice for said services.

Before new releases are installed at the SCOCA, a backup of the application or operating system affected by the change is prepared to ensure retention of the existing application or operating system in case of an error stemming from the upgrade process.

Documentation for the current version of the operating system and new releases are provided on the HP web site. New releases include documented changes to the operating system and implementation procedures. Since the SCOCA's system was still under the manufacturer's warranty, they were able to obtain their operating system disks and documentation free of charge. In addition, the MCOECN provides all ITC's with purchasing discounts on hardware and software through the Technology Solutions Group program under the MCOECN (MC TSC).

Beginning with FY2009, the SCOCA put in place Service Level Agreements (SLA) with their user organizations for certain computer, data processing, and applications services. The user organizations agree to pay a fee based upon a fee schedule set forth by the governing board and they agree to abide by the security policies implemented by the SCOCA. These SLA's are in effect beginning July 1, 2008, and will be in effect until terminated in writing by either the district or the SCOCA.

IT Security

The SCOCA has a security policy that outlines the responsibilities of user organization personnel, the SCOCA personnel, and any individual or group not belonging to the user organization or the SCOCA. These responsibilities include the use of the computer system, data access, outside access, and password guidelines. In addition to the security policy, the SCOCA utilizes banner screens that are displayed prior to a user login and after a user successfully logs on to the system. The screen informs the user that unauthorized access of the system is prohibited.

The SCOCA staff is granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. Access is established, granted and reviewed by the executive director.

An automated procedure is used to handle all requests for user accounts from the user organizations. Only authorized user organization management and SCOCA staff have access to this procedure via a menu option. The user organization management enters basic information about the user. Once an hour, DECScheduler runs a program to create new accounts, using the information provided by the requestor and the default template. This program assigns the user ID, district code, and UIC. It also makes sure the group number is correct and the member number is unique. This program creates the account on the system with the normal privileges and no identifiers. If a user needs additional access, such as access to an application, the authorized user organization management must submit a written (e-mail or fax) request to the SCOCA. All accounts are created by the SCOCA staff after receiving an authorized request.

A listing that indicates user access and privileges within the user organization is sent annually to the respective organization management to verify the present users on the system were properly authorized. In addition, the systems manager periodically runs a procedure to automatically "DISUSER" all users who have not logged in within the past 120 days and have pre-expired passwords. This procedure was not utilized during most of this period because users of the FISCweb system were getting flagged as not having logged in to the system even though they had. Procedures that were once in place to update the user authorization file for FISCweb users are no longer possible due to a reverse-proxy implementation of SSL secured web data. Instead, it is the user organization treasurer's responsibility to assure that old accounts are requested to be removed in a timely manner.

Access to the Internet has been provided to the user organizations through the Ohio Education Computer Network. The SCOCA relies on the user organizations to establish their own Internet and e-mail policies and to maintain all related documentation at the local districts.

Security alarm messages are sent to an operator terminal that has been enabled to receive security event messages. Security audit messages are sent to the audit log file; alarms are sent to the operator log file. Access to the operator log and audit log is limited to data processing personnel. Critical events should be reported as both alarms and audits; less critical events can be written to a log file for later examination. The following security alarms and security audits have been enabled through the operating system to monitor any security violations on the SCOCA system:

ACL:	Gives file owners the option to selectively alarm certain files and events. READ, WRITE, EXECUTE, DELETE, or CONTROL modes can be audited. This alarm is valid only if an ALARM_JOURNAL ACE is added to each ACL. The SCOCA uses ACLs on the data files.
AUTHORIZATION:	Enables monitoring of changes made to the system user authorization file, UAF, or network proxy authorization file in addition to changes to the rights database.
AUDIT:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
BREAK-IN:	Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, and DETACHED break-in types can be monitored.
LOGFAILURE:	Provides a record of logon failures. The BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS, and DETACHED logon failure types can be monitored.

A batch processed command procedure executes each night to extract any security violations from the audit journal and creates a summary report and a detail report which contains information on unsuccessful logon attempts and any use of the AUTHORIZE command. These security monitoring reports are e-mailed to the systems manager and reviewed daily. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed. The systems manager maintains approximately one month of these reports.

The SCOCA utilizes a pair of Barracuda Network appliances to scan all inbound and outbound e-mail for viruses. If a virus is found, the e-mail is rejected outright. Updates are provided hourly automatically by Barracuda and occasional firmware upgrades are performed to enhance performance.

Primary logical access control to the HP computers is provided by security provisions of the operating system. This includes access to data, programs and system utilities. When a user logs in to use the operating system interactively, or when a batch or network job starts, the operating system creates a process which includes the identity of the user. The operating system manages access to the process information using its authorization data and internal security mechanisms.

The SCOCA utilizes proxy logins. A proxy login enables a user logged in at a remote node to be logged in automatically to a specific account at the local node, without having to supply access control information. A proxy login differs from an interactive login because an interactive login requires a user to supply a user name and password before the user can perform interactive operations.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the SCOCA. For user organizations that use the SCOCA system, UICs are for the most part, functionally assigned and therefore, multiple district users may share an individual UIC. UICs are assigned at the user organization's request. UIC based protection controls access to objects such as files, directories, and volumes.

Certain limited-access accounts require a less restrictive environment than captive accounts. Accounts, under which network objects run, for example, require temporary access to DCL. Such accounts must be set up as restricted accounts, not captive accounts. User accounts should be set with the RESTRICTED flag instead of the CAPTIVE flag if they need to use network applications like MAIL or network proxy accounts. The RESTRICTED flag is used for all user accounts not belonging to the SCOCA or the system.

The system forces users to periodically change their passwords. The systems manager sets passwords to expire when a new user identification code is issued. New users must log in "interactively" to change their passwords. Notification of password expiration for existing users occurs automatically prior to the password expiration date. The SCOCA has established minimum password lengths for all user accounts.

The operating system has system parameters which, when set appropriately, control and monitor sign-on attempts. There are parameters in place to control certain aspects of the sign-on procedure, which include the following:

- The terminal name is part of the association string for the terminal mode of break-in detection.
- The user is restricted on the length of time they have to correctly enter a password on a terminal on which the system password is in effect.
- The number of times a user can try to log in over a phone line or network connection. Once the specified number of attempts has been made without success, the user loses the carrier.

- The length of time allowed between login retry attempts after each login failure.
- The length of time a user terminal, or node, is permitted to attempt a logon before the system assumes that a break-in attempt is occurring and evasive action is taken.
- The period for which evasive action is taken is variable and will grow as further logon failures are detected from the suspect source.
- The number of retry attempts allowed for users attempting to logon before evasive action consists of refusing to allow any logons during a designated period of time.

A timeout program, HITMAN, is used to monitor terminal inactivity and log-off inactive users after a predetermined period of time of non-use. The use of this program helps to reduce the risk of an unattended terminal being used to enter unauthorized transactions. Also, timeout programs aid in efficient use of system resources by maintaining connectivity with only active system users.

Associated with each object recognized by the operating system may be an Access Control List (ACL). When an access request is made to an object, ACLs are always checked first. An ACL may either grant or deny access to the user requesting it. When an ACL fails to specifically grant access, the system then defaults to UIC-based protection.

The system directory contains security files that control the security parameters for the system. When a user attempts to gain access to an object, such as a file or directory, the system compares the user's User Identification Code (UIC) to the owner's UIC for that object. In UIC-based protection, the relationship between the user's UIC and the object's UIC determines whether access is granted. Owner relationships are divided into four categories:

SYSTEM: Any of the following: (1) Users with a UIC group number between 1 and SYSGEN parameter MAXSYSGROUP (default decimal 8, octal 10). (2) Users with system privileges (SYSPRV). (3) Users with group privileges (GRPPRV) whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

OWNER: Users with the same UIC as the object's owner.

GROUP: Users with the same UIC group number as the object's owner.

WORLD: All users, including those in SYSTEM, OWNER, and GROUP.

Through the protection code, each category of users can be allowed or denied read, write, execute, and delete access. The default file protection is for (1) SYSTEM having read, write, execute, and delete capabilities; (2) OWNER having read, write, execute, and delete capabilities; (3) GROUP having read and execute capabilities; and (4) WORLD having no access capabilities.

Certain privileges can override all UIC-based and ACL protection. The operating system analyzes privileges included in the user's UAF record and places the user in one of seven categories depending on which privileges have been granted to the user. Default privileges are those authorized

privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login, and must be enabled or disabled by the user. All user organization users have NORMAL privileges.

The write and delete access capabilities are not activated for WORLD access to the files in the system directory. The UIC associated with each of these files is within the MAXSYSGROUP number. To limit access to security files, the SCOCA has limited the WORLD access for the user authorization file, which contains account information to identify which users are allowed access to accounts on the system; the proxy file, which contains proxy account information to identify which remote users are allowed access to proxy accounts on the system; and the rights file, which contains names of the reserved system identifiers and identifiers for each user.

User organizations have been set up with sub-networks that have addresses not recognizable to the Internet. This is called a private internal network. A firewall separates the private internal network from the public Internet. Outbound requests are redirected by the firewall to a filter server using IFP (Internet Filtering Protocol). The Internet filter service allows or denies defined content from the Internet for the typical user. Permission to bypass the filter server requires management authorization. The firewall equipment and additional routing devices deny all incoming traffic access to the inside servers and nodes unless the request originated from the sub-network, thus preventing all outside connections (traffic) from accessing inside hosts or servers, unless the IP address originated from inside the network. In addition, the SCOCA is relying on operating system security, including UICs, and the RESTRICTED flag to ensure that only proper access is granted to the Alpha.

Wireless access at the SCOCA is restricted to web and e-mail services through secure shell (SSH). In addition, an access control list is used to restrict access to the wireless network. Users need to be on the control list to be granted access.

Districts connect to the system through E-Term or Reflections emulation software, which is based on a Telnet session. Users are permitted three logon attempts before their account is locked, requiring appropriate SCOCA staff to unlock the account. Access inside the network would require a physical connection to a switch. Connection through Telnet outside the districts required Secure Socket Layer (SSL).

All users at SCOCA boot up to Windows XP and are automatically authenticated to the Windows 2000 network. Each user has an ID and password. Once on the network, users can access the system server either by using E-Term emulation software or accessing the command line and entering the server's IP address. The SCOCA maintains license agreements for all users of E-term.

Access to the OECN software packages is controlled at the ITC level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate operating system identifiers to authorized users. Each application package has a set of unique identifiers that permit access to programs. In addition to the standard identifiers for each package, a pass through identifier can be used to further customize access. OSA is used in conjunction with the OECN menu processor utility thus allowing the users to see only the items they are authorized to execute. UIC-based protection prevents WORLD write or delete access to USAS, USPS, SAAS/EIS and EMIS application data files.

The firewall has been configured for remote operation. Alteration of the configuration files requires that an individual know the proper IP address and a series of passwords before remote access is possible. Only the network manager and network engineer have been provided the passwords for the firewall. Alteration of the configuration files of the equipment is performed by the network manager.

The data center is secured by locked doors, security cameras, and an alarm system. The receptionist and executive director have security monitors that display views of all entry ways and outside parking areas via the security cameras. Individuals need both a key to unlock the door

and a security card to gain access to the data center. All entries via the security cards are logged showing who entered and when they entered. In addition, the computer room doors are equipped with a combination keypad, the code is known only to the SCOCA personnel.

The following items assist in controlling the computer room to protect it from adverse environmental conditions.

- Smoke and heat detectors.
- Temperature and humidity sensors.
- Liebert system.
- CO2 fire extinguishers.
- Uninterruptible power supply (UPS).
- Power kill switch.
- Power distribution device used to prevent power surges to any of the equipment in the computer room.

The smoke detectors, humidity and heat alarms are connected to the alarm system to alert the executive director.

IT Operations

Traditional computer operations procedures are minimal since users at the user organizations initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. The SCOCA staff has privileges that permit them to assist participating user organizations in performing data entry transactions. This is necessary so staff can respond to participating districts' requests and assist in resolving data entry errors. User organizations are responsible for changes to their own data. Occasionally SCOCA will assist the user organizations with data changes upon receipt of an e-mail. Periodically, SCOCA will assist the district using Datatrieve or other SSDT supplied software per request of the district via phone call or e-mail. Information is transferred from the e-mail account fiscal_help into the CA Unicenter Help Desk and documentation is maintained by SCOCA staff. All data changes are done in a test environment called Fiscal_Scratch. Once the district is satisfied with the changes, it is moved into the live environment. In addition, user organizations are encouraged to review the "AUDIT" report, which shows activity changes to their data files.

Certain routine jobs are initiated at the SCOCA for system maintenance. The SCOCA is responsible for operational maintenance tasks, such as: system backups, file rebuilds, file integrity testing, log reports, and other maintenance directed at the system as a whole. These tasks are scheduled to run automatically through DECScheduler.

The SCOCA helps to prevent failures or file corruption through the use of a program called ANALYZE. When data file errors occur, the systems manager runs the ANALYZE program on the system. A report is generated about each data file and it is reviewed by the systems manager to help determine what files were affected and what caused the error. Any problems found are corrected by SCOCA staff, if possible. Data integrity is maintained by the software through validity checks of all input.

Common problems that arise daily, such as terminal lockups and program crashes are usually handled by the SCOCA service representatives over the phone and may not be documented if the problem is minor. However, most problems are logged in the statewide helpdesk, CA Unicenter. CA-Unicenter is a protected web-based on-line utility that is accessible to all SCOCA employees via their website. Up until July 1, 2007, e-mail accounts were set-up for the districts that include fiscal_help, student_help, and tech_help. These e-mails were automatically put into the help desk directory. As of July 1, 2007, e-mail submission of tickets was no long being accepted by CA-Unicenter. User organizations may also log in to a special web site to submit

tickets. Each call is assigned a ticket number and a representative from SCOCA will work on the problem and document the resolution in the ticket.

Critical problem aspects from the console log, such as system failures, are reviewed periodically by the executive director and systems manager. A message is sent to the executive director and systems manager when there is a problem.

The SCOCA has a Storage Area Network (SAN) that is continuously monitored by the vendor (HP). In the event of any problem, the monitoring software e-mails the SCOCA systems support team as well as the vendor. The vendor then makes a phone call to the SCOCA to alert them of a possible problem and if necessary immediately dispatches a support technician.

Network performance is monitored through the use of SolarWinds. Pings are sent to each network device to determine if it is active. If a device is not active it will be highlighted on screen in red. Appropriate personnel will investigate why the equipment is not responding and decide what needs to be done to remedy the situation.

The SCOCA follows the guidelines of the OECN for backing up system programs, data, and related documentation. The SCOCA performs full system backups daily Monday through Sunday through a network connection from the system to an IBM StorServer backup appliance. The Storserver and tape library are located in the Adult Basic Literacy Education (ABLE) building located next to SCOCA. Data retention is controlled by policies set within the Storserver. The system retains 90 versions of 90 days worth of changes. The backup job resubmits itself to the backup queue upon completion.

A backup log is automatically printed each day and is reviewed by the technical support liaison or office manager to determine if a successful backup occurred. If the backup is not successful, errors are investigated and a new backup is run. The backup log is retained and filed.

All windows servers are backed up to the same StorServer appliance. The standard policies for all other servers are to retain 45 days worth of 45 versions worth of changes. The backups are checked daily by the LAN manager to ensure they were successful. If backups are not successful, they are investigated for the problem and resolved. All data is required by law to be maintained for a specific duration by the SCOCA.

The IBM StorServer rack is raised off the floor with legs to help prevent water damage. The ABLE building is open during business hours and the computer room is also open for access by ABLE staff and students. No separate air conditioning unit is used for the room. The temperature is controlled through the building's air condition system. A fire extinguisher is located in the room and was last serviced in June 2007.

The SCOCA has a hardware maintenance agreement with Service Express. The SCOCA has a Protect-All Service agreement with HP for business recovery purposes. In addition, all data processing equipment is covered under an insurance policy.

SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR

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

The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system, for example procedures performed at the SCOCA and procedures performed at user organizations that utilize the SCOCA.

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications and Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Applications developed and maintained by the SSDT at the NWOCA are the same as those distributed to and utilized by SCOCA. The most recent application updates are distributed by the SSDT and SCOCA is required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the object files for USAS, USPS, SAAS, and EMIS at SCOCA was compared to the CRC of the object files at SSDT. Inspected procedures SCOCA uses to install state software.	No relevant exceptions noted.
The SSDT distributes release notes and updated manuals to the SCOCA when application updates are released. Updated manuals are also provided on the SSDT web site.	Inspected the release notes and updated manuals for the most recent release to confirm that installation procedures, explanation of changes, enhancements, and/or corrections are documented and communicated to the SCOCA. Inspected the SSDT web-site for availability of updated manuals.	No exceptions noted.
The SCOCA participates in the CSLG/ESL program in order to maintain a licensing agreement for the operating system software and technical support.	Inspected a copy of the SCOCA's CSLG licensing agreement with the NBEC and payment information to confirm it is current.	No exceptions noted.
In order to maintain continued support of their application software provided by the SSDT, the SCOCA is required to install new releases of the operating system.	Discussed upgrade procedures with the systems manager. Inspected an email confirming their copy of the operating system upgrade.	No exceptions noted.

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The SCOCA maintains Service Level Agreements (SLA) with the user organizations for IT services.	Inspected the SLAs between the SCOCA and their user organizations to confirm it documented services are provided to the user organizations and user organization responsibilities. Inspected the SLAs for signatures from both the SCOCA and the user organizations.	No relevant exceptions noted.

IT Security

IT Security - *Control Objective:* **Security Management** - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The SCOCA has established policies and procedures regarding computer security and access for its staff and user organizations. Policies are communicated to users.	Inspected the Data Security Policy and confirmed its distribution to staff and user organizations.	No relevant exceptions noted.
An automated procedure runs hourly to process new Alpha account requests that are submitted on-line by authorized user organization management.	A batch file was created using security analysis tools to extract "new" user information from the user authorization file. From a population of 188 new user accounts, selected 40 user accounts to confirm the request was in the account request log and requested by authorized personnel from the district. Also inspected the account and program request command procedure that creates the accounts, and identified the program request command in DECScheduler.	No exceptions noted.
User organizations are required to confirm user accounts and associated access privileges annually with a positive confirmation to SCOCA, which is tracked and followed up as needed to facilitate a response from the user organization.	Confirmed procedures for positive confirmation of users and inspected a copy of the memo distributed to user organizations. Inspected returned listings from the user organizations to confirm the reports were signed and dated.	Responses were received from 51 of the 55 districts. Reminders were sent to the following unresponsive districts. • Minford LSD • South Point LSD • Rock Hill LSD • Westfall LSD
Tracking of security related events, such as break-in attempts and excessive login failures, is enabled through the operating system. The events are logged to audit journals for monitoring of potential security violations.	Inspected the security audits to confirm they were enabled.	No exceptions noted.

IT Security - *Control Objective:* **Security Management** - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Security violations are extracted, compiled into summary and detailed security reports, and e-mailed to the systems manager and technical support liaison daily through command procedures on the system.	With the systems manager, confirmed security monitoring procedures, including the process for monitoring reports and the frequency of review. Inspected the following relating to the security monitor reports to confirm these reports are produced daily and forwarded to the appropriate personnel: • Example of a security monitoring report. • Command procedure utilized to generate the report. • Scheduler command procedure and listing.	No exceptions noted.
A pair of network appliances are used to scan all inbound and outbound e-mail for viruses. Definitions are updated hourly.	Confirmed measures for protecting the servers from viruses. Inspected system documentation from the server indicating anti-virus software and the update schedule.	No exceptions noted
User Control Considerations: User organization management should make users aware of the confidential nature of passwords and that users should take precautions to ensure passwords are not compromised. User organization management should immediately request the ITC to revoke the access privileges of district personnel when they leave or are otherwise terminated. User organization personnel should respond to account confirmation requests from their ITC.		

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Individual user profiles are used to grant access rights and privileges in accordance with SCOCA policy.	Extracted information from the user authorization file to identify user accounts with elevated privilege and inspected the listed accounts.	No relevant exceptions noted.
The user profiles on the system do not consist of an excessive number of unused or inactive profiles.	Using security analysis tools, extracted and inspected the following information from the system authorization file: • User accounts that have never logged into the system. • User accounts that have not been logged into within 180 days.	No relevant exceptions noted.
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to not allow blanket access.	Inspected the proxy listing for use of wild card characters.	No exceptions noted.
Access to the operating system command line is restricted to authorized users.	Using security analysis tools, identified user accounts that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER or RESTRICTED flags set. Inquired with the systems manager regarding the appropriateness of these accounts.	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Password parameters are in place to aid in the authentication of user access to the system. Passwords used by individual profiles agree to password policies established by the SCOCA and the number of profiles with pre-expired passwords is limited.	Utilized security analysis tools to extract the following information from the system user authorization file and inspected the listed accounts: • User accounts with password minimum lengths less than SCOCA's established value. • User accounts with a password lifetime greater than SCOCA's established value. • User accounts with pre-expired passwords.	No exceptions noted for password minimum lengths. No relevant exceptions noted for user accounts with a password lifetime greater than SCOCA's established value. No relevant exceptions noted for user accounts with pre-expired passwords.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the login parameter settings. Confirmed settings have not been changed from suggested vendor settings.	No exceptions noted.
A program constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at system startup.	Inspected the HITMAN parameters to confirm parameters were set for idle time and action to be taken against inactive users. In addition, identified protected accounts and processes. Inspected the system startup file to confirm the HITMAN utility is part of the startup process.	No exceptions noted.
Access to production data files and programs is restricted to authorized users.	Inspected the directory listing of executable files for the USAS, USPS, EMIS and SAAS/EIS application programs to confirm WORLD access was limited to read and/or execute. Inspected a listing of user organization data files to confirm there were no files having WORLD access.	No relevant exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user organizations by restricting inbound and outbound IP traffic.	Inspected the network diagram to confirm components of the network which control Internet access. Inspected the firewall configuration to verify • All Internet traffic was switched to/from the firewall. • Inbound and outbound IP traffic is restricted through the firewall. • The existence of a private internal network.	No exceptions noted.
An access control list is used to restrict access through the wireless access points.	Inquired about the configuration of the wireless network to confirm how the wireless network is set up. Confirmed that access was available. Inspected the configuration of the network and reviewed restrictions.	No exceptions noted.
Connection to the system from the user organizations is restricted through emulation software installed on each authorized user's computer.	Confirmed user organization access restrictions to the system with the systems manager. Inspected logon procedures for connecting to the system.	No relevant exceptions noted.

IT Security - *Control Objective:* **Application Level Access Controls** - Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Users are restricted to predefined logical access identifiers that grant varying access privileges based upon requests from user management.	Using operating system commands, extracted all users with at least one USAS, USPS, SAAS/EIS, or EMIS identifier. From a selection of 40 new accounts, compared the requested identifiers to those on the system.	No relevant exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized users.	Utilizing security analysis tools, generated reports identifying active accounts with an OECN_SYSMAN identifier Inspected the listing of all users having the OECN_SYSMAN identifier to confirm only appropriate users were assigned the identifier. Confirmed the functionality of the identifier with the systems manager.	No exceptions noted.
User Control Considerations: User Identification Codes (UICs), passwords and associated access privileges should only be issued to authorized users who need access to computer resources to perform their job function.		

IT Security - *Control Objective:* **System Software and Utilities Access Controls** - Use of master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
WORLD access to “key” system and security files is restricted.	Inspected the system file directory listing for WORLD write and/or delete access. Inspected the file protection masks on the security files.	No exceptions noted.
System level user identification codes are restricted to authorized personnel.	Identified the maximum system group number. Used security analysis tools to identify a listing of all accounts with a UIC less than the maximum system group number. Confirmed the appropriateness of identified accounts with the systems manager.	No exceptions noted.
A user authorization alternate file is not permitted to be used and does not exist.	Inspected the value of the alternate user authorization alternate parameter to determine whether an alternate file is permitted. Inspected the system directory listings to determine if a user authorization alternate file existed.	No exceptions noted.
Remote access to the firewall and router configurations used to control Internet access is restricted through password protection.	Inspected the firewall configuration to confirm remote access is allowed and passwords are required to access the routing equipment used to control Internet access.	No exceptions noted.

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Physical access to the building, computer room, and the room housing the tape library is restricted to authorized personnel.	Inspected key locks, key pad entry devices, access cards, and observed use of the devices throughout the period of field work to confirm that these devices are in place and work properly. Inspected the off-site location where the data is housed on a HP Storageworks MSL 5000 tape library.	No exceptions noted.
Environmental controls are in place to protect against and or detect data loss and damage as well as to detect fire, water, humidity and/or changes in temperature.	Observed, with the systems manager, the existence of environmental controls over the computer room and the room housing the tape library.	No relevant exceptions noted.
User Control Considerations: PCs and terminals should be protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.		

IT Operations

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Routine system maintenance programs, such as file rebuilds, file cleanups and disk space management, run daily through DECScheduler.	Inspected the jobs that are run through the DECScheduler and discussed the various jobs with the systems manager to confirm routine system maintenance is performed. Inspected the startup script that includes DECScheduler to confirm it is initiated at system startup.	No exceptions noted.
SolarWinds software monitors network performance and alerts staff of hardware failures and system problems.	Inspected documentation showing the equipment status and indicating monitoring of the network.	No exceptions noted.
A service agreement with Service Express covers maintenance and failures on the computer hardware.	Inspected the service agreement and payment documentation for the audit period.	No exceptions noted.
Requests for changes to user organization data files are submitted via phone call or e-mail and are documented by SCOCA staff.	Confirmed the process for making changes to user organization data. Inspected help desk reports for completed changes to data.	No exceptions noted.
The system does not consist of an excessive number of Disusered user profiles.	Using security analysis tools, extracted information from the system authorization file to identify user accounts that have been DISUSERed. Inspected the listed accounts.	No relevant exceptions noted.
All data center equipment is covered by insurance in case of loss or damage.	Inspected the insurance policy and invoice to confirm the computer equipment is covered by insurance and the policy was in effect during the audit period.	No exceptions noted.

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The SCOCA maintains a Protect All service agreement for their hardware systems to be used in the event of a disaster, accident or environmental hazard.	Inspected the agreement and payment for the Protect All service to confirm it existed during the audit period.	No exceptions noted.
The SCOCA has a generator and an Un-Interruptible Power Supply (UPS) to maintain power in the event of a power outage.	Inquired about the use of the generator and the UPS to confirm how long power could be supplied to keep the system running in the event of a power outage. Observed the UPS in the computer room and the generator outside the SCOCA facility. Inspected the maintenance agreement and payment documentation.	No relevant exceptions noted.

IT Operations - *Control Objective:* **Backup** - Up-to-date backups of programs and data should be available in emergencies.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Full system backups of programs and data are performed nightly. The status of the backups is reviewed daily by the technical support liaison.	Confirmed the procedures for backups with the systems manager. Inspected the following documentation to confirm all application and system data is backed up regularly: • The backup command procedure. • The backup submission program. • Backup queue. • Backup logs.	No exceptions noted.
Incremental backups are performed daily and full backups are performed weekly for the Windows network.	Confirmed backup procedures with the LAN manager and inspected the Windows job log and backup log to confirm backups are completed daily.	No exceptions noted.
Archive data is backed up nightly and kept in the Storage Area Network (SAN).	Confirmed archive data backup with the systems manager and observed the archive tapes in the SAN. Inspected the archive backup program to confirm user organization data is backed up nightly.	No exceptions noted.
Backup tapes are stored off-site in a physically and environmentally secure location.	Confirmed backup storage procedures with the systems manager and inspected the storage of off-site backup tapes to confirm the backups are adequately secured.	No relevant exceptions noted.
The retention and rotation of tapes is managed by the StorServer based on policies defined by SCOCA.	Inspected the retention policies on the StorServer.	No exceptions noted.

IT Operations - *Control Objective:* **Backup** - Up-to-date backups of programs and data should be available in emergencies.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
User Control Considerations: The user organization should retain source documents for an adequate period to ensure data can be re-entered in the event that data files are destroyed prior to being backed up and rotated off-site. The user organization should establish and enforce a formal data retention schedule with SCOCA for the various application data files.		

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

CENTER DATA

Name:	South Central Ohio Computer Association (SCOCA)
Number:	15
Node Name:	SCOCA
Chairperson:	Robert Ralstin Superintendent Manchester Local School District
Fiscal Agent District:	Pike County Joint Vocational School District
Administrator:	Shawn Clemmons Executive director SCOCA
Address:	175 Beaver Creek Rd. Piketon, OH 45661
Telephone:	740-289-2908
FAX:	740-289-2082
Website:	www.scoca-k12.org

OTHER CENTER STAFF

Ron Morgan	Director of operations	John Rappold	Webmaster
Norm Brabson	Network manager	Eddie Butcher	Field network manager
Ryan McClay*	Systems manager	Ryan Hawk	Field technical coordinator
Brian Rittenour	LAN manager	Michael Layman	Field technical coordinator
Debbie Davis	Fiscal services coordinator	Luke Stevenson	Field technical coordinator
Linda Latham	Fiscal liaison	Holly Wagoner	Field technical coordinator
Alyssa Pflaumer	Fiscal liaison	Troy Pekkala	Field technical coordinator
Diana Shaffer	Student service liaison	Josh Montgomery	Field technical coordinator
Terry Claxton	Student service liaison	Ron Johnson	Field technical coordinator
Missy Merrit	Student service liaison (Part-time)	Justin MacCrae	Field service technician
Jamie Tuggle	Student service liaison	Kenneth Wigginton	Field service technician
Ryan Satterfield	Student service liaison	Brian Kirkendall	Field service technician
Karen Lawhun	Student service liaison	Donnie Curtis	Field service technician
Craig Haney	EMIS services coordinator	Nicholas Kongos	Field service technician
Patricia Cluxton	EMIS service liaison	Matt Klepper	Field service technician
Rhonda Palmer	EMIS service liaison	Johnathon Bowman	Field service technician
Rhonda Birkhimer	EMIS service liaison	James Unger	Field service technician
Kim Davis	EMIS service liaison	Ryan Saunders	Field service technician
Brian Birkhimer	Software development coordinator	Henderson Thompson	Field service technician
Melissa Higgs-Horwell	Curriculum integration coordinator	Joshua Jones	Field service technician
Josh Leeth	Network engineer	Matt Schuman	Field service technician
Robert Morgensen	Technical assistant	Justin Brewster	Field service technician
Dave Smith	Technical assistant	Shain Kelley	Field service technician
Debbie Lisath	INFOhio liaison	Cynda Jessee	Office manager
Barbara Clemmons	Media specialist/grants coordinator	Melissa Kiebler	Executive secretary

*No longer a SCOCA employee as of 8/5/08. The SCOCA contracts his service through the MC OECN.

HARDWARE DATA

Central Processors and Peripheral Equipment

Model Number		Installed		Capacity/Density/Speed	
CPU:	HP AlphaServer ES45	Units:	3 CPUs	Memory Installed:	16 GB
Disk:	EVA 4000 SAN	Units:	1	Total Capacity:	4420.90 GB
Tape Unit:	Spectralogic T120	Units:	3	Max Density:	320 GB

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
061903	Adams County/Ohio Valley Local SD	Adams	X	X	X	X
000442	Manchester Local SD	Adams	X	X	X	X
046029	Brown County ESC	Brown	X	X	X	X
046037	Eastern Local SD	Brown	X	X	X	X
046045	Fayetteville-Perry Local SD	Brown	X	X	X	X
045377	Georgetown Exempted Village SD	Brown	X	X	X	X
046078	Ripley Local SD	Brown	X	X	X	X
050799	Southern Hills JVSD	Brown	X	X	X	X
046060	Western Brown Local SD	Brown	X	X	X	X
047613	Bright Local SD	Highland	X	X	X	X
047621	Fairfield Local SD	Highland	X	X	X	X
045401	Greenfield Exempted Village SD	Highland	X	X	X	X
047639	Lynchburg-Clay Local SD	Highland	X	X	X	X
047761	Oak Hill Union Local SD	Jackson	X	X	X	X
045294	Chesapeake Union Ex Village SD	Lawrence	X	X	X	X
047928	Dawson-Bryant Local SD	Lawrence	X	X	X	X
047936	Fairland Local SD	Lawrence	X	X	X	X
044149	Ironton City SD	Lawrence	X	X	X	X
047910	Lawrence County ESC	Lawrence	X	X	X	X
051185	Lawrence County JVSD	Lawrence	X	X	X	X
047944	Rock Hill Local SD	Lawrence	X	X	X	X
047951	South Point Local SD	Lawrence	X	X	X	X
047969	Symmes Valley Local SD	Lawrence	X	X	X	X

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
043760	Circleville City SD	Pickaway	X	X	X	X
049072	Pickaway County ESC	Pickaway	X	X	X	X
049080	Logan Elm Local SD	Pickaway	X	X	X	X
049106	Westfall Local SD	Pickaway	X	X	X	X
049122	Eastern Local SD	Pike	X	X	X	X
051375	Pike County JVSD	Pike	X	X	X	X
049130	Scioto Valley Local SD	Pike	X	X	X	X
049158	Waverly City SD	Pike	X	X	X	X
049155	Western Local SD	Pike	X	X	X	X
049494	Adena Local SD	Ross	X	X	X	X
043745	Chillicothe City SD	Ross	X	X	X	X
049502	Huntington Local SD	Ross	X	X	X	X
049510	Paint Valley Local SD	Ross	X	X	X	X
051433	Pickaway-Ross JVSD	Ross	X	X	X	X
138222	Ross-Pike County ESC	Ross	X	X	X	X
049528	Southeastern Local SD	Ross	X	X	X	X
049536	Union Scioto Local SD	Ross	X	X	X	X
049544	Zane Trace Local SD	Ross	X	X	X	X
049593	Bloom-Vernon Local SD	Scioto	X	X	X	X
049619	Green Local SD	Scioto	X	X		X
049601	Clay Local SD	Scioto	X	X		X
049627	Minford Local SD	Scioto	X	X	X	X

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
044461	New Boston Local SD	Scioto	X	X		X
049635	Northwest Local SD	Scioto	X	X		X
044669	Portsmouth City SD	Scioto	X	X	X	X
051490	Scioto County JVSD	Scioto	X	X	X	X
143644	Sciotoville Community SD	Scioto	X	X		X
009964	Sciotoville Elementary Academy	Scioto	X	X		X
125658	South Central Ohio ESC	Scioto	X	X	X	X
049643	Valley Local SD	Scioto	X	X		X
049650	Washington Nile Local SD	Scioto	X	X	X	X
049668	Wheelersburg Local SD	Scioto	X	X	X	X
050393	Vinton County Local SD	Vinton	X	X	X	X
044032	Gallipolis City SD	Gallia				X
TOTALS:			**56**	**56**	**49**	**57**

Mary Taylor, CPA
Auditor of State

SOUTH CENTRAL OHIO COMPUTER ASSOCIATION
(SCOCA)

PIKE COUNTY

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

Susan Babbitt

CLERK OF THE BUREAU

CERTIFIED
OCTOBER 16, 2008

88 E. Broad St. / Fourth Floor / Columbus, OH 43215-3506
Telephone: (614) 466-4514 (800) 282-0370 Fax: (614) 466-4490
www.auditor.state.oh.us