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

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2012 THROUGH MARCH 31, 2013

Dave Yost • Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

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

To Members of the Board:

Scope
We have examined SCOCA's accompanying Description of its Alpha ES45 system used for processing transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), and School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS) throughout the period April 1, 2012 to March 31, 2013 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of SCOCA's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The SCOCA uses the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, and SAAS/EIS application systems. The Description in section 3 includes only the controls and related control objectives of the SCOCA and excludes the control objectives and related controls of the NWOCA. Our examination did not extend to controls of the NWOCA.

Service organization's responsibilities
In section 2, SCOCA has provided an Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. SCOCA is responsible for preparing the Description and for the Assertion, including the completeness, accuracy, and method of presentation of the Description and the Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period April 1, 2012 to March 31, 2013.

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the Description. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in section 3. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The information in section 5 describing the information technology center is presented by the management of SCOCA to provide additional information and is not part of the SCOCA's Description of controls that may be relevant to a user entity'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 entities and, accordingly, we express no opinion on it.

Inherent limitations
Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion
In our opinion, in all material respects, based on the criteria described in SCOCA's Assertion in section 2,

a. the Description fairly presents the system that was designed and implemented throughout the period April 1, 2012 to March 31, 2013.

b. the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2012 to March 31, 2013 and user entities applied the complementary user entity controls contemplated in the design of the SCOCA's controls throughout the period April 1, 2012 to March 31, 2013.

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period April 1, 2012 to March 31, 2013.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Restricted use
This report, including the Description of tests of controls and results thereof in section 4, is intended solely for the information and use of SCOCA, user entities of SCOCA's system during some or all of the period April 1, 2012 to March 31, 2013, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Dave Yost
Auditor of State
Columbus, Ohio

June 18, 2013

This Page Intentionally Left Blank

South Central Ohio Computer Association
175 Beaver Creek Road
P.O. Box 577
Piketon, Ohio 45661

We have prepared the description of South Central Ohio Computer Association (SCOCA) *Alpha ES45* system for user entities of the system during some or all of the period April 1, 2012 to March 31, 2013, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a) the Description fairly presents the Alpha ES45 System made available to user entities of the System during some or all of the period April 1, 2012 to March 31, 2013 for processing their transactions. The SCOCA service organization uses the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, and SAAS/EIS. The Description includes only the controls and related control objectives of the SCOCA service organization and excludes the control objectives and related controls of the NWOCA service organization. The criteria we used in making this assertion were that the Description

   i) presents how the System made available to user entities was designed and implemented to process relevant transactions, including

      1) the classes of transactions processed.

      2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the System.

      3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the System.

      4) how the System captures and addresses significant events and conditions, other than transactions.

      5) the process used to prepare reports or other information provided to user entities' of the System.

      6) specified control objectives and controls designed to achieve those objectives.

      7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the System.

   ii) does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and the independent auditors of those user entities, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b) the Description includes relevant details of changes to the service organization's System during the period from April 1, 2012 to March 31, 2013.

c) the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period April 1, 2012 to March 31, 2013 to achieve those control objectives and subservice

organizations applied the controls contemplated in the design of SCOCA service organization's controls. The criteria we used in making this assertion were that

i) the risks that threaten the achievement of the control objectives stated in the Description have been identified by the service organization;

ii) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

iii) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

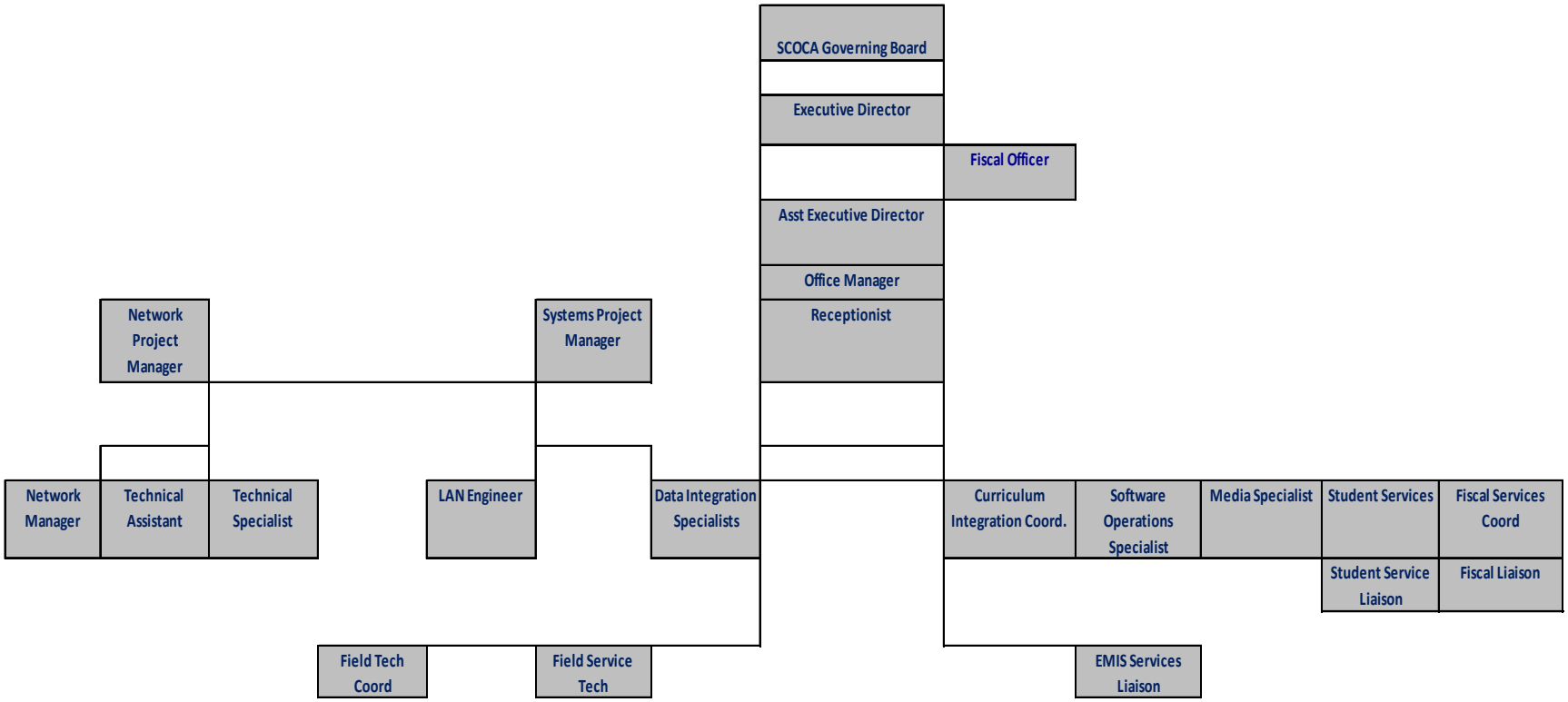
Shawn Clemmons
Executive Director
June 18, 2013

SECTION 3 - DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

The South Central Ohio Computer Association's (SCOCA) control objectives and related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results", to eliminate the redundancy that would result from listing them here in section 3 and repeating them in section 4. Although the control objectives and related controls are included in section 4, they are, nevertheless, an integral part of the SCOCA's description of controls.

OVERVIEW OF OPERATIONS



The SCOCA is one of 22 governmental computer service organizations serving more than 900 educational entities and 1.4 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 entity" 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).

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 (fiscal officer), make its own purchases, hire staff, and have debt obligations. Prior to July 1, 2012, the SCOCA was organized under ORC 3313.92 and the Pike County JVSD served as their fiscal agent. Beginning with July 1, 2012, they re-organized into a COG, and replaced their fiscal agent with an employee who is serving as their fiscal officer.

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. The governing board is composed of 21 members, which includes 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 five-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, 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 55 individuals. The SCOCA provides support in 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 user entity 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 provides input 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. Providing 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:	User entities may contract with SCOCA to act as their EMIS Coordinator to submit EMIS data to ODE.
Field Technical Services:	User entities may contract with SCOCA for a technician to work in their user entity or they may contract with SCOCA to act as their tech coordinator.

The managers of each of the functional areas report to the assistant executive director, who then reports to the executive director.

The SCOCA is generally limited to recording user entity transactions and processing the related data. User entities 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 entity.

The SCOCA adopted their own personnel policies and procedures. All policies are 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 full-time staff member must attend at least 20 hours of approved professional development training annually, and part-time staff member training hours are prorated. All the SCOCA staff members are permitted and encouraged to attend professional training as deemed necessary. Staff evaluations are conducted annually by the assistant executive director and the executive director evaluates the assistant executive director. The governing board is in charge of the annual evaluation for the executive director.

The SCOCA is also subject to ITC Site Reviews by the Management Council – Ohio Education Computer Network MCOECN. These site reviews are conducted by a team consisting of an employee of the Ohio Department of Education (ODE), two current and/or former user entity administrators, two current and/or former ITC Directors, and one additional team member to provide training to subsequent teams. Approximately three to five ITC site reviews are conducted annually. The sites chosen for review are designated by the OECN Oversight Advisory Committee as approved by ODE. The guidelines and recommended procedures for these reviews are based on the Ohio Administrative Code, which cover the

following areas: governance, administration, finance, personnel and staff development, physical facilities, hardware, software, user in-service, and operations. The SCOCA's last site review was performed in September 2008. No additional site review has been scheduled.

Beginning with July 1, 2012, the SCOCA put in place COG Agreements with their user entities for certain computer, data processing, and applications services. The user entities agree to pay a fee based upon a fee schedule set forth by the governing board and they agree to abide by the policies and procedures implemented by the SCOCA. These agreements are in effect until terminated in writing by either the user entity or the SCOCA.

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 entities 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 entities. 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 Computer Control" section of this report.

Monitoring

The SCOCA organization is structured so that department managers report directly to the assistant executive director. Key management has been employed with SCOCA for over ten years. 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 entities.

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 entities are discussed within the "General Computer Control" section.

GENERAL COMPUTER CONTROLS

Development and Implementation of New Applications or 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 (MCOECN), 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/or 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, and SAAS) has its own public and ITC forum which is monitored by the SSDT system analysts. All OECN ITC's and a majority of user entities 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. Upon notification of their availability from SSDT, ITCs obtain quarterly updates by downloading zipped files from the SSDT's download site. The source code is not distributed with these files. Release notes, which explain the changes, enhancements and problems corrected, are provided via the SSDT website. User and system manager manuals are also made available via the SSDT website with these releases. The SSDT informs the ITCs that they will support only the latest release of the state software beginning thirty days following the software release date.

The software operations specialist at SCOCA uses a procedure created in-house to install the new releases. This procedure calls up the INSTALL_PACKAGE (procedure created by SSDT and supplied to all ITC's) which installs the new releases on their system. This procedure unpacks the zip file and INSTALL_PACKAGE and installs each individual package into the proper OECN directories ensuring that all required components are installed properly and consistently.

Only vendor-supplied changes are made to the operating system or system software documentation. As a participating member of the MCOECN, an ITC can enter into a cooperative agreement, "Campuswide Software License Grant (CSLG) and Education Software Library (ESL) Program", through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of Hewlett Packard (HP), and other supplier's, software packages as approved by the MCOECN board of trustees.

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

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

- Provide telephone technical support to the participant'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 and maintain support on one (1) license of Process Software's Multinet TCP/IP stack for each system registered under this program.

As a participating member of the MCOECN program, the participating ITCs agree to the following:

- Maintain its status as a member in good standing of the MCOECN as a qualification for participating in (or continuing to participate in) this program.

- Read, sign, and comply with the rules and regulations of the CSLG Program as operated by the MCOECN.

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

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

- Make payments to MCOECN 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 and on the operating system media. New releases include documented changes to the operating system and implementation procedures. The SCOCA has their own copy of the operating system disks and documentation. If an upgrade is required, they would purchase this from INS, a third-party vendor in partnership with the MCOECN. This is part of the Technology Solutions Group (TSG) program under the MCOECN (mc•tsg). This program allows the SCOCA to purchase their operating system media at a reduced cost. The current release documentation is maintained by the software operations specialist at SCOCA. No new releases were installed during the audit period.

IT Security

The SCOCA has a security policy that outlines the responsibilities of user entity personnel, the SCOCA personnel, and any individual or group not belonging to the user entity 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. This screen is not visible to the users if they connect to the system via the SSH protocol. SSH is more secure than standard Telnet connection including less vulnerability to packet sniffing and other security issues. Telnet access is not permitted from "outside" of the SCOCA network and its associated connected entities.

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. User entity personnel are granted access upon written authorization from the treasurer at the user entity. User account setup can be handled one of two ways.

1.) The treasurer, if appropriate access is assigned, can use an automated account request process to submit a request to have a new account created. When prompted, the required information for the new account is entered. A procedure runs every hour to create accounts, based upon the information provided by the user entities, and sends an e-mail to the user entity regarding the newly established or updated account. This procedure creates an account with limited privileges, but no identifiers. This procedure is not available when using USASWeb or when logging in via the Internet. If application access is required, the user entity must send a written request via email, fax, or helpdesk ticket to the SCOCA.

2.) The treasurer can send a written request via email, fax or helpdesk ticket to the SCOCA. The SCOCA uses a similar process to create accounts. When prompted, the required information for the account is entered and the account is created immediately with limited privileges, but no identifiers. Once the account is created, any application access that was requested is then assigned.

Both automated procedures log the creation of the new accounts in a log file. The log records the request type, the account name, who requested it and the date/time the account was created. All requests for application (USAS, USPS, and SAAS/EIS) access are logged in the helpdesk by SCOCA personnel. Account requests for a new treasurer will be requested by the user entity's superintendent or by the out-going treasurer upon appointment of the new treasurer.

Account deletions are processed by SCOCA staff based on requests from authorized personnel at the user entities or from the user confirmation process. SCOCA staff process the deletion through an automated procedure (DELACCOUNT) and the deletion is recorded in the log file. For security reasons, deletions may be processed as determined by the systems manager in the event an account is no longer being utilized without authorization from the user entities.

Annually, the SCOCA initiates a positive confirmation of users and their associated access rights with user entity management. The user entity's treasurer is requested to confirm users' system access was properly authorized. Additional follow-up is completed with user entities failing to respond by the request deadline.

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

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 are reported as both alarms and audits; less critical events are 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 procedure executes each night to extract any security violations from the audit journal and creates a summary report and a detail report. These security monitoring reports are e-mailed to the assistant executive director and executive director and reviewed daily. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and necessary corrective action.

The SCOCA utilizes a pair of network appliances to scan all inbound and outbound e-mail for viruses. If a virus is found, the e-mail is rejected outright. Hourly updates to the antivirus definition are provided automatically by the vendor and firmware upgrades are performed to enhance performance.

Access to web based applications including USAS, USPS, and SAAS/EIS is authenticated through a secure interface with a valid system username and password. Once authenticated, users are automatically given only those privileges assigned in each user's default login security profile.

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 which enable 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.

User Identification Codes (UIC) are individually assigned to all users. All user entity personnel are assigned unique UICs and are assigned at the request of the user entity. 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.

Users must provide a valid operating system username and password to authenticate to the USAS and USPS web applications. Once

authenticated, users are automatically given only those privileges assigned in each user's default login security profile. The SSDT developed a program called OECN_RPC (Remote Procedure Call) service which, in conjunction with VXS created by the SSDT, allows users to authenticate through a XML interface using standard operating system authentication policies. If authentication is successful, the RPC service "impersonates" the user by acquiring an operating system security profile of the authenticated user (i.e. default privileges and security identifiers). Once the RPC has acquired the corresponding security profile the operating system process has the same security rights as the authenticated user. The network client then provides a code indicating the user entity data to be used. The RPC service uses the user entity code to define logical definitions to associate the server process with the desired user entity data.

Only default privileges from the user's authorization file record are enabled during a session. The session does not enable any authorized privileges. Therefore, when the service process accesses data files, their default login security profile is used. A user can select predefined OECN software functions that are available to the OECN_RPC service. (For example, USAS functions for posting a requisition). When the user has finished using the respective web application the logout button is clicked to disconnect. Alternatively, the session may disconnect automatically after the configured inactivity timeout.

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. When a user logs in to the USAS and/or USPS web applications, the user authorization file is updated to reflect that a non-interactive login has occurred. When a user logs in to the FISCWEB application, the user authorization file is not updated to reflect that a login has occurred.

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 to correctly enter a password on a terminal on which the system password is in effect.
- The user is limited in login attempts over a phone line or network connection. Once the specified number of attempts has been made without success, the connection is terminated.
- The length of time is restricted between login retry attempts after each login failure.
- The length of time a user terminal, or node, is permitted to attempt a logon is considered 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 users after a predetermined period of inactivity. 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. In addition, the USAS and USPS web applications will monitor service inactivity and disconnect users after a predetermined period of non-use.

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 authorization file 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 entity personnel 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 following:

- Authorization file - contains account information to identify which users are allowed access to accounts on the system.
- Proxy file - Contains proxy account information to identify which remote users are allowed access to proxy accounts on the system.
- Rights file - Contains names of the reserved system identifiers and identifiers for each user.

User entities 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 system.

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.

User entities connect to the system through E-Term or Reflections emulation software, which is based on a Telnet or SSH session. Users are permitted several logon attempts before their account is locked, requiring appropriate SCOCA staff to unlock the account. The account will automatically unlock if enough time passes before another failed attempt occurs. This amount of time is variable depending on the number of additional failed login attempts. Access inside the network would require a physical connection to a switch, wireless bridge, or router. The SCOCA does not permit Telnet sessions from outside of their network. Users are able to connect remotely using Persona emulation software.

All users at SCOCA boot up to a Windows-based operating system and are automatically authenticated to the Windows 2000 network. Each user has a unique user-ID and authenticating password that permits them access to network resources. Once on the network, users can access the system server either by using E-Term emulation software or other terminal emulation software, or entering the server's IP address. The SCOCA maintains license agreements for all users of E-term emulation software.

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 rights. 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 and SAAS/EIS application data files.

The OECN_SYSMAN identifier is a special identifier that grants access to all other identifiers and packages automatically. In other words, the OECN_SYSMAN identifier grants the user the same access as OECN_USAS, OECN_USPS, etc., for all packages without having to grant each individual identifier. This identifier may be granted to ITC personnel without granting any special operating system level privileges. It is not necessary to grant OECN_SYSMAN if the user already has the BYPASS privilege. Users that have the BYPASS privilege will automatically be granted the OECN_SYSMAN identifier.

The OECN_SYSMAN identifier is defined by state software and the BYPASS privilege is controlled by the operating system so they work the same for all ITC's. The OECN_SYSMAN grants access to software functions inside the software. It does not grant access to data. The BYPASS privilege allows the user full access to all protected objects, totally bypassing UIC-based protection, access control list (ACL) protection, and mandatory access controls. With the BYPASS privilege, a user has unlimited access to the system. Only SCOCA staff has this identifier and/or privilege.

The firewall has been configured for remote operation. Such remote access is restricted through a series of authenticating passwords and knowledge of the IP address is necessary for alteration of the firewall configuration files. Only designated SCOCA staff 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 a security card to gain access to the building. All entries via the security cards are logged including time, date and cardholder. In addition, the computer room doors are equipped with the same security card system.

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 temperature control systems.
- CO_2 fire extinguishers.
- FM 200 room fire suppression system with dual chemical discharging containers.
- Uninterruptible power supplies (UPS).
- Power kill switch.
- Power distribution device used to prevent power surges to any of the equipment in the computer room.
- Generac 54kW and Kohler 30 backup generators.

The smoke detectors, humidity and heat alarms are connected to the alarm system to alert the executive director. The heat and smoke detectors are connected to the fire suppression system and alert local emergency services when activated.

IT Operations

Traditional computer operations procedures are minimal because users at the user entities 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 entities in performing data entry transactions. This is necessary so staff can respond to participating user entities' requests and assist in resolving data entry errors. User entities are responsible for changes to their own data. Occasionally the SCOCA staff will assist the user entities with data changes upon receipt of an e-mail. SCOCA will assist the user entity using Datatrieve or other SSDT-supplied software. Information is transferred from the e-mail account fiscal_help into the CA Unicenter Help Desk and documentation is maintained by the SCOCA staff. All data changes are done in a test environment, called Fiscal_Scratch. Once the user entity is satisfied with the changes, it is moved into the live environment by the SCOCA staff. In addition, user entities 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. Manual processes for evaluating system performance are conducted on an “as needed” basis. This includes running a vendor-provided routine, called AUTOGEN, to assure the system is configured properly based on the current work load. On occasion, manual defragmentation is done by creating a new data storage unit, LUN, and performing a file by file copy to this new LUN. In addition, they conduct operational maintenance tasks, such as: system backups, file rebuilds, data 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 the program, 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 identify affected files and reason for error. Any problems found are corrected by SCOCA staff, if possible. Data problems seldom occur; therefore, the systems manager has not needed to run this utility during the past year. 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 logged via the statewide helpdesk, CA Unicenter. This is a protected web-based on-line utility that is accessible to all SCOCA employees via their website. Each helpdesk call is assigned a ticket number and a SCOCA representative, responsible for troubleshooting and documenting the resolution in the ticket. Standard reports are available for review by the SCOCA staff.

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 to determine the reason equipment is not responding and decide appropriate action.

The SCOCA follows the guidelines of the OECN for backing up system programs, data, and related documentation. The SCOCA performs incremental system backups daily Monday through Sunday through a network connection to a STORServer backup appliance provided by the MCOECN in a secure data-center geographically distant from the SCOCA main offices. The STORServer contains 2 types of online file storage: tape and disk. All primary backups are stored for 90 days on disk with a secondary copy kept on tape in the event of disk failure. Backup restores are controlled by the STORServer. The system maintains a database of what data are needed in order to restore data in a timely and efficient manner. Restores are generally very quick and seamless, depending on what data is needed to be restored. Data retention is controlled by policies set within the STORStorserver. The backup job resubmits itself to the backup queue upon completion.

A backup job notification email is sent to a distribution list that includes the assistant executive director, system's project manager, operation Specialist, LAN engineer, and data integration specialist each day to confirm a successful backup occurred. If the backup is not successful, errors are investigated and a new backup is run, if necessary. The backup log is retained and filed. The STORServer is periodically used to restore files for users and this can be frequently depending on the time of the year. Procedures to do test restores with the MCOECN TSG DR Site are in development.

All system and program documentation related to essential services such as USPS, USAS and SAAS is stored electronically and is subject to the same backup procedures as the other data files. All data is required by law to be maintained for a specific duration by the SCOCA. This information is also available on the SSDT web site, so if a backup goes bad, they can still get the information from the Internet.

The SCOCA has hardware maintenance agreements with Service Express and MCPc. The SCOCA maintains Protect-All and MCOECN agreements for business recovery purposes. In addition, all data processing equipment is covered under an insurance policy.

COMPLEMENTARY USER ENTITY CONTROLS

The applications were designed with the assumption that certain controls would be implemented by user entities. This section describes additional controls that should be in operation at the user entities to complement the controls at the SCOCA. User auditors should consider whether the following controls have been placed in operation at the user entity:

1. User entities should have controls over their own web applications which access their data stored at the SCOCA.

2. User entity management should have practices to ensure users are aware of the SCOCA security policies and the confidential nature of passwords and the precautions necessary to maintain their confidentiality.

3. User entity management should immediately request the SCOCA to revoke the access privileges of user entity personnel when they leave or are otherwise terminated.

4. User entities should have documented acceptable use policies to define the activities deemed appropriate for use of the Internet. Internet users should be required to accept the terms of the policy before access is provided.

5. Access privileges should only be issued to authorized users who need access to computer resources to perform their job function.

6. 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.

7. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.

8. User entities 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.

9. User entities should establish and enforce a formal data retention schedule with SCOCA for the various application data files.

The complementary user entity controls presented above do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at the user entity.

SECTION 4 – INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

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 entity'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 entities 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 COMPUTER CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications and/or Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
In order to maintain continued support of the application software provided by the SSDT, ITCs are required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) checksum of the object files for USAS, USPS and SAAS at SCOCA was compared to the CRC checksum of the object files at SSDT.	No 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 available on the SSDT website for the most recent release to confirm that all current documentation is provided to the SCOCA.	No exceptions noted.
Documentation for the current version of the operating system and new releases are provided on the HP web site.	Inspected the online manuals for the operating system at the HP web-site.	No 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 a COG agreement which addresses computer security and access for SCOCA staff and user entities.	Inspected the COG agreements and by laws that were in place during the audit period and inquired about its distribution to the staff and user entities.	No exceptions noted.
Authorization from the user entity's management is required prior to creating a user account on the system.	Identified all new accounts with an OECN identifier for a total population of 147 accounts. Selected 22 new user accounts to confirm the request was in the account request log and was requested by either an authorized personnel from the user entity or SCOCA staff. Inspected the following to confirm the process for requesting and creating accounts. • The command procedures used to request new accounts. • The process request command procedure that creates the accounts. • The default account. • The DEScheduler to identify the job that runs the process request program.	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:*
User entities 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 entities.	Confirmed the process used for positive confirmation of users with the fiscal services coordinator. Inspected confirmation documentation for evidence the confirmation process included verification forms and user listing sent to the user entities. Inspected returned listings from the user entities to confirm the reports were signed and dated.	No exceptions noted.
The SCOCA staff implements requested changes to user entity access based on returned confirmations.	Inspected SCOCA staff members' initials on the returned documentation indicating the necessary changes were completed.	No exceptions noted.
A pair of network appliances is used to scan all inbound and outbound e-mail for viruses. Definitions are updated hourly.	Confirmed with the system support specialist the measures used for protecting the servers from viruses, including anti-virus software. Inspected system documentation from the server to confirm: • The existence of anti-virus software. • The configuration/frequency of the scans. • The use of the update schedule.	No exceptions noted.
Tracking of security related events, such as break-in attempts and excessive log failures, is enabled through the operating system. The events are logged to audit journals for monitoring of potential security violations.	Inspected the security audits in place 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 SCOCA staff daily through command procedures on the system.	Confirmed security monitoring procedures in place, 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.

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:*
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 in place to confirm wild card characters are not used.	No exceptions noted.
Access to the operating system command line is restricted to authorized users.	Indentified and inspected user accounts that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER or RESTRICTED flags set. Inquired with the executive director 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 account access to the system and agree to password policies established by the SCOCA.	Inspected information from the system user authorization file to identify: • Accounts with password minimum lengths less than SCOCA's established value. • Accounts with a password lifetime greater than SCOCA's established value. Inquired with the executive director regarding the appropriateness of the listed accounts.	There were 105 of 1,888 accounts with a password lifetime greater than SCOCA's standard. All had password lifetimes set to "none". • 4 of 105 were SCOCA accounts. Even though they had lifetime equal to "none", 3 accounts had recent password changes and 1 was pre-expired. All parameters were corrected by the end of field work. • 2 of 105 were user accounts. Parameters for these accounts were corrected by the end of fieldwork. The remaining 99 accounts cannot have forced password changes due to the nature of the accounts and the way they are used to access the system. They include: • 20 HR KIOSK accounts • 2 OECN accounts • 13 system or utility accounts • 54 DASL accounts • 1 FTP account • 9 FORMSHARE accounts No other exceptions were 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 expiration for the web applications is defined at the system or process level.	Inspected the system logical that controls remote access to confirm password expiration is enforced for the web applications. Inspected print screens showing the message received when the user's password is expired and needs to be changed.	No exceptions noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the login parameter settings in place to confirm sign-on attempts are controlled.	No exceptions noted.
System and web application activity is monitored and inactive users are automatically disconnected after a predetermined amount of idle time.	Inspected the HITMAN parameters in place 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. Inspected the configuration for the timeout values on the USAS and USPS Web system.	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 and SAAS/EIS application programs to identify production files with WORLD access and executable files with WORLD Write and/or Delete access. Inspected a listing of user entity data files and identified files with WORLD access.	There is one USAS executable file (CERTIFICATE.EXE) that has WORLD Write access. This is a customizable form used by the user entities. There are no other executable files with WORLD Write or Delete access. No user entities had WORLD access on their data files.

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 entities 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 confirm • 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.
Access to the Internet is restricted through the wireless access points.	Inquired about the configuration of the wireless network to confirm how the wireless network was set up. Confirmed available access points using network tools. Inspected the access control list, configuration of the network and restrictions.	No exceptions noted.
Connection to the system from the user entities is restricted through emulation software installed on each authorized user's computer. Telnet sessions are not allowed from outside the SCOCA network.	Confirmed user entity access restrictions to the system with the software operations specialist. Confirmed that Telnet sessions are not allowed from outside the SCOCA network.	No 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.	Inspected a listing of all identifiers from the user authorization file for evidence of the use of identifiers to segregate access to the applications. Identified all new accounts with an OECN identifier for a total population of 147 accounts. Selected 22 new user accounts and compared the requested identifiers to those identifiers granted on the system.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized users.	Identified accounts in the user authorization file with an OECN_SYSMAN identifier and inspected the listing with the executive director to confirm only appropriate users were assigned the identifier.	No exceptions noted.

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 file protection masks on the system and security files to confirm WORLD Write and/or Delete access is absent.	No exceptions noted.
System level user identification codes are restricted to authorized personnel.	Identified the maximum system group number. Inspected a listing of all accounts with a UIC less than the maximum system group number from the user authorization file. Confirmed the appropriateness of identified accounts.	No exceptions noted.

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:*
An alternate user authorization file is not permitted to be used and does not exist.	Inspected the value of the alternate user authorization parameter to confirm the use of an alternate user authorization file is not permitted. Inspected the system directory listings to confirm that an alternate user authorization file does not exist.	No exceptions noted.
Remote access to the firewall and router configurations used to control Internet access is restricted through password protection.	Inspected the firewall and router configurations in place during the audit period to confirm passwords are required to access the equipment used to control Internet access. Confirmed with the network manager that passwords are changed periodically.	No exceptions noted.
Individual user profiles are used to grant access rights and privileges in accordance with SCOCA policy. The system does not consist of an excessive number of high-privileged profiles.	Inspected a listing of user accounts with elevated privileges and inquired with the executive director to confirm that elevated privileges are limited to authorized users.	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 and access cards and observed use of the devices during audit field work to confirm that these devices restrict access to the building and computer room. Inspected the TYCO and ADT agreements and payment to confirm monitoring services were in place.	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:*
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 the existence of environmental controls over the computer room with the LAN engineer. Inspected the agreement for the backup generators to confirm maintenance is kept current.	No exceptions noted.

IT Operations

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure that 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 to confirm that 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.	Inquired with the network manager and inspected documentation from SolarWinds showing the status of the user entity's equipment and indicating monitoring of the network.	No exceptions noted.
Service agreements with Service Express and MCPc covers maintenance and failures on the computer hardware.	Inspected the service agreements and payment documentation for the audit period. Inquired with the executive director regarding their level of service support satisfaction.	No exceptions noted.
Requests for changes to user entity data files are submitted via phone call or e-mail and are documented in the help desk application by SCOCA staff.	Confirmed the process for making changes to user entity data with the fiscal services coordinator. Inspected four help desk tickets for completed changes to data.	No exceptions noted.
All data center equipment is covered by insurance in case of loss or damage.	Inspected the insurance policy and invoice from the executive director to confirm the computer equipment is covered by insurance and the policy was in effect during the audit period.	No exceptions noted.
The SCOCA maintains a Protect All service agreement for their hardware systems in the event of a disaster, accident or environmental hazard.	Inspected the agreement to confirm coverage. Inspected the payment for Protect All to confirm it existed during the audit period.	No exceptions noted.

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The SCOCA has two generators and Un-Interruptible Power Supplies (UPS) to maintain power in the event of a power outage.	Inquired about use of the generators and 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 generators outside the SCOCA facility and inquired about procedures for testing the generators. Inspected the maintenance agreement and payment documentation.	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:*
Incremental system backups of programs, data and network are performed nightly to the disaster recovery site in Columbus. The status of the backups is reviewed daily by the SCOCA staff.	Confirmed backup procedures with the LAN engineer and inspected the STORserver policy, backup queue, and status log to confirm that data is sent to the off-site facility on a nightly basis.	No exceptions noted.
Full system backups of programs and data are performed nightly and sent to the disaster recovery site in Columbus.	Confirmed backup procedures with the LAN engineer and inspected the STORserver policy and status log to confirm that data is sent to the off-site facility.	No exceptions noted.
Backup data is restored annually as part of the DR Services Recovery Agreement with the MCOECN.	Inspected the DR Services Recovery Agreement and evidence of restore. Confirmed the existence of the agreement with the executive director.	No exceptions noted.

SECTION 5 - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION *(Unaudited)*

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

CENTER DATA

Name:	South Central Ohio Computer Association (SCOCA)
Number:	15
Node Name:	SCOCA
Chairperson:	Shane Shope Superintendent Lynchburg-Clay LSD
Fiscal Officer:	Sandee Benson
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

Brian Birkhimer	Assistant executive director	Ryan Hawk	Field technical coordinator
Ryan Satterfield	Software operations specialist	Luke Stevenson	Field technical coordinator
Debbie Davis	Fiscal services coordinator	Ron Johnson	Field technical coordinator
Andrea Leeth	Fiscal liaison	William Deacon	Field technical coordinator
Alyssa Pflaumer	Fiscal liaison II	Heckie Thompson	Field technical coordinator
Gary Marion	Student service liaison	Mike Drake	Field technical coordinator
Terry Claxton	Student service liaison II	Evan Mercer	Field technical coordinator
Missy Merrit	Student service liaison II (Part-time)	Jonathon Bowman	Field technical coordinator
Jamie Tuggle	Student service liaison II	Darrell Jividen	Field technical coordinator
Karen Lawhun	Student service liaison II	Josh Jones	Field technical coordinator
Patricia Cluxton	EMIS services liaison	Tyler Cantrell	Field technical coordinator
Rhonda Palmer	EMIS services liaison	Dustin Dixon	Field technical coordinator
Rhonda Birkhimer	EMIS services liaison	Michael Layman	Field technical coordinator
Kim Davis	EMIS services liaison	Kenneth Wigginton	Field service technician
Steve McCann	EMIS services liaison	Matt Schuman	Field service technician
Peggy Whyte	Curriculum integration coordinator	Darin Rader	Field service technician
Norm Brabson	Network manager	Matt Downs	Field service technician
Josh Leeth	Network project manager	Derek Boyer	Field service technician
Robert Morgensen	LAN Engineer	Kevin Colley	Field service technician
Justin MacCrae	Data integration specialist	Charles Davis Jr.	Field service technician
Les Burkholder	Systems project manager	Alex Lawhorn	Field service technician
Justin Brewster	Technical specialist	Brian Ross	Field service technician
Lonnie Mercer	Technical specialist	Adam Dailey	Field service technician
Dave Smith	Technical assistant	Nathan Garman	Field service technician
Timothy Tackett	Technical assistant	Travis Miller	Field service technician
Barbara Clemmons	Media specialist/grants coordinator	Cynda Jessee	Receptionist (Part-time)
Sandee Benson	Fiscal Officer	Melissa Kiebler	Office manager

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 4400 SAN	Units:	48 Spindles	Total Capacity:	12572 GB
Backup Unit:	STORServer S3000	Units:	1	Max Density:	1.6 TB per tape compressed

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS	OTHER*
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
043760	Circleville City SD	Pickaway	X	X	X	X

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS	OTHER*
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
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

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS	OTHER*
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
013233	Southern Ohio Academy	Scioto	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:			**57**	**57**	**49**	**58**

OTHER* - Applications other than USAS, USPS, and SAAS/EIS, used by the user entities.

This page intentionally left blank.

Dave Yost • 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
AUGUST 1, 2013

88 East Broad Street, Fourth Floor, Columbus, Ohio 43215-3506
Phone: 614-466-4514 or 800-282-0370 Fax: 614-466-4490
www.ohioauditor.gov