



**TRI-COUNTY COMPUTER SERVICE ASSOCIATION
STATE REGION - ISA, WAYNE COUNTY**

SAS 70

JUNE 12, 2004 THROUGH JULY 7, 2005



**Auditor of State
Betty Montgomery**

TABLE OF CONTENTS

I	INDEPENDENT ACCOUNTANT'S REPORT	1
II	ORGANIZATION'S DESCRIPTION OF CONTROLS	3
	CONTROL OBJECTIVES AND RELATED CONTROLS	3
	OVERVIEW OF OPERATIONS	3
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING	3
	Control Environment.....	3
	Risk Assessment.....	4
	Monitoring.....	5
	INFORMATION AND COMMUNICATION	5
	GENERAL EDP CONTROLS.....	6
	Development and Implementation of New Applications and Systems	6
	Changes to Existing Applications or Systems.....	6
	IT Security	7
	IT Operations.....	11
III	INFORMATION PROVIDED BY THE SERVICE AUDITOR	13
	GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS.....	14
	Changes to Existing Applications or Systems.....	14
	IT Security	15
	IT Operations.....	22
IV	OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION	24
	Data Acquisition Site Profile	24

This Page Intentionally Left Blank



Auditor of State Betty Montgomery

INDEPENDENT ACCOUNTANT'S REPORT

Executive Committee
Tri-County Computer Services Association (TCCSA)
2125-B Eagle Pass
Wooster, Ohio 44691

To Members of the Committee:

We have examined the accompanying description of controls of the Tri-County Computer Services Association (TCCSA) 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 TCCSA's controls that may be relevant to a member school district'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 member school districts applied the internal controls contemplated in the design of the TCCSA's controls; and (3) such controls had been placed in operation as of July 7, 2005. The control objectives were specified by the TCCSA 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 application presents fairly, in all material respects, the relevant aspects of the TCCSA's controls that had been placed in operation as of July 7, 2005. 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 TCCSA'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 12, 2004 to July 7, 2005. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to member school districts of the TCCSA and to their auditors to be taken into consideration along with information about the internal control at member school districts, when making assessments of control risk for member school districts. 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 12, 2004 to July 7, 2005.

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

The information in Section IV describing the data acquisition site is presented by the TCCSA to provide additional information and is not part of the TCCSA'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 member school districts and, accordingly, we express no opinion on it.

The description of controls at the TCCSA is as of July 7, 2005, and information about tests of the operating effectiveness of specified controls covers the period from June 12, 2004 to July 7, 2005. 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 TCCSA 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 TCCSA, its member school districts, and the independent auditors of its member school districts.

A handwritten signature in black ink that reads "Betty Montgomery". The signature is written in a cursive, flowing style.

Betty Montgomery
Auditor of State

July 7, 2005

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The TCCSA's 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 TCCSA's description of controls.

OVERVIEW OF OPERATIONS

The TCCSA is a subsidiary of the Midland Council of Governments (MCOG). The MCOG is a council of governments which exists to provide efficient and cost effective computer and data processing services to its member school districts. Currently, there are 20 member school districts in the Ohio counties of Wayne, Medina, Ashland, and Holmes. The TCCSA is located in Wooster.

The TCCSA is one of 23 not-for-profit computer service organizations serving more than 600 public school districts and county educational service centers in the state of Ohio. Throughout the remainder of this report, any reference to member school districts will also include the county educational service centers. These service organizations, known as Data Acquisition Sites (DA Sites) and their member school districts 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 school districts. Funding for this network and for the TCCSA is derived from the state of Ohio and from user fees.

Per section 3301.075 of the Revised Code, each DA Site must be organized in accordance with either section 3313.92 or Chapter 167 of the Revised Code. TCCSA is organized under section Chapter 167, and has established the MCOG as its fiscal agent to receive OECN funds from the ODE. The MCOG applies for and maintains the DA Site permit for the equipment purchased with state monies and holds legal title to this equipment.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the two oversight committees. One member from each member district is appointed to the legislative body of the council known as the assembly and is normally the district superintendent. The assembly meets at least twice per year to estimate program costs, approve annual appropriations, select officers and other members of the executive committee, and approve other matters as determined to require the approval of the assembly.

The executive committee is the governing body of the TCCSA and is composed of seven members and two ad hoc members. The composition of the executive committee must contain two superintendents; two treasurers; two at large members and the fiscal agent superintendent. The

executive director of TCCSA and the fiscal agent treasurer are the two ad hoc members. The executive committee is required to meet every two months.

The TCCSA employs a staff of 29 individuals and is supported by the following functional areas:

<i>Application Support:</i>	Facilitates the implementation and operation of fiscal and student services of the TCCSA which include USAS, USPS, SAAS/EIS, EMIS, and GAAP application systems, and provides user training and support.
<i>Educational Technology Support:</i>	Facilitates the implementation and operation of educational technology services to TCCSA member school districts and provides user training and support.
<i>Network/Systems Support:</i>	Designs and supports the TCCSA computer systems, its networked communications systems and provides user training and support as needed.
<i>Help Desk Support:</i>	Implements and supports the Computer Associates™ help desk software, named Unicenter Service Desk (USD).

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

The TCCSA follows the same personnel policies and procedures as the Midland Council of Governments. When necessary, additional TCCSA policies have been developed and approved by the MCOG board to address concerns of TCCSA. Detailed job descriptions exist for most positions. Job descriptions have not been created for two new positions related to the support of the helpdesk software. The TCCSA 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 TCCSA's 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 in a computer-related field, and all the TCCSA 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. In addition, management encourages staff members to obtain additional training and pays 100% of incurred costs of attending professional development seminars. Employee evaluations are conducted annually. The board performs an annual evaluation of the executive director.

Risk Assessment

The TCCSA does not have a formal risk management process; however, the TCCSA executive committee is made up of representatives from the member school districts who actively participate in the oversight of the TCCSA.

As a regular part of its activity, the TCCSA executive committee addresses:

- New technology.
- Realignment of the TCCSA organization to provide better service.
- Personnel issues, including hiring, termination, and evaluations.
- Additional services provided to member school districts 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 TCCSA has identified operational risks resulting from the nature of the services provided to the member school districts. 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 structure of the TCCSA data center has been organized to provide a quick response to service problems. Employee positions are broken down between application support and technical support. Software and technical support managers report directly to the executive director. Key management employees have worked for TCCSA for many years and are experienced with the systems and controls at the TCCSA. The TCCSA 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, TCCSA 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, and computer security reports are monitored on an ongoing basis by management. Some of these reports are automatically run through a scheduler program and are sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily.

INFORMATION AND COMMUNICATION

The aspects of the information and communication component of internal control as they affect the services provided to member school districts are discussed within the General EDP control section.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The TCCSA staff members do not perform system development activities. Instead, the TCCSA utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the Northwest Ohio Computer Association (NWOCA), another DA Site of the OECN. The 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, the Ohio Department of Education (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 DA Site forum which is monitored by the SSDT system analysts. All OECN DA Sites and a majority of member school districts have access to forum conferences, providing end-user participation in the program development/change process.

The TCCSA personnel do not perform program maintenance activities. Instead, they utilize the applications supplied to them by the SSDT. The OECN requires the DA Site 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 DA Sites' 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. The SSDT informs the DA Sites that they will support only the latest release of the state software beginning 30 days following the software release date.

The TCCSA 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 the 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 DA Sites, has entered into a license under the Campuswide Software License Grant Program (CSLG) through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of Hewlett Packard (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 DA Sites for a limited series of HP software packages as approved by the board of trustees of the MCOECN.

- Provide telephone technical support to the participants 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 DA Sites' 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 DA Sites 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 sites 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 TCCSA, 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.

The NBEC provides documentation and support for new releases of the operating system. New releases include documented changes to the operating system and implementation procedures. The NBEC provides OpenVMS documentation on the OECN web site, for the current version of the operating system, accessible by all DA Sites. In addition, the TCCSA has purchased its copy of the operating system disks from the NBEC via the MCOECN Value-Added Reseller (VAR) program, which offers the operating system software at a reduced rate. Current release documentation is maintained by the executive director at the TCCSA.

IT Security

The TCCSA has a security policy that outlines the responsibilities of member school district personnel, the TCCSA personnel, and any individual or group not belonging to the member school district or the TCCSA.

The TCCSA staff are 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 for TCCSA employees is established, granted and reviewed by the executive director and no authorization form is used.

Member school districts users are granted access upon the receipt of a written authorization form from the district's superintendent. All access requests forms are maintained at TCCSA.

Student authorization forms for Internet and e-mail accounts are maintained at the district. These accounts are not on the Alpha server.

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 OpenVMS to monitor any security violations on TCCSA systems:

ACL:	Gives file owners the option to selectively alarm certain files and events. READ, WRITE, EXECUTE, DELETE, or CONTROL modes can be audited.
AUDIT:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
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.
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.

The districts have the ability to run reports that show all of the users on the system for a specific district. This allows the districts to confirm user access. Annually, TCCSA will send an e-mail to the district reminding them to verify accounts on the system. The districts are not required to respond unless they have changes that need to be made.

The TCCSA uses Sophos Anti-Virus software which interactively scans all inbound and outbound e-mail.

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

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 any 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 any interactive operations. The TCCSA utilizes proxy logins.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the TCCSA. To promote user accountability, UICs are individually assigned to the member school district users of the TCCSA system. UIC based protection controls access to objects such as files, directories, and volumes.

The CAPTIVE and RESTRICTED flags are used for various application and system utility accounts. The CAPTIVE and RESTRICTED flags are typically not used for system administrative accounts (TCCSA staff members) because access to the DCL prompt is necessary for them to perform their job duties. Additionally, user accounts are not typically set with CAPTIVE or RESTRICTED flags, as their logins are captured within a menu system preventing access to the DCL command line. User accounts are also set with the NORMAL parameter giving them the minimum level of access privileges. UIC based protection to production programs and data prevents WORLD WRITE or DELETE access.

The system forces users to periodically change their passwords. All general user accounts as well as all TCCSA staff member user accounts, have a standard password lifetime. System or application maintenance accounts on the system have significantly longer password lifetimes. These accounts do not affect financially significant functions and are not able to access financial applications. Passwords are set to expire when a new user identification code is issued or when a user has forgotten his password. This parameter requires the user to change his password during the first logon procedure. A minimum password length for user and administrative accounts has been established. Identifiers have been assigned to district personnel to aid in the resetting of passwords.

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.

System parameter standards have been established through the use of established defaults. Any changes are logged and reviewed by the executive director or by the manager of software applications and support in the executive director's absence.

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 OpenVMS 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. 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 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. OpenVMS 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 member school district users have NORMAL privileges.

The WRITE and DELETE access capabilities are not activated for WORLD access to the files in the SYSSYSROOT directories. The UIC associated with each of these files is within the MAXSYSGROUP number.

To limit access to security files, the TCCSA 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.

Access to the OECN software packages is controlled at the DAS level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate OpenVMS 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.

Member school districts have been set up with sub-networks which have addresses not recognizable to the Internet. Firewall equipment and routing devices deny all outbound traffic requests originating from the sub-network. Instead, the requests are routed to the firewall where an address translation is performed. The firewall and routing devices also deny access to all inbound traffic unless it is bound for the firewall. TCCSA also makes available an Internet content filter. The filter is an optional service which screens Internet site requests for unsuitable content.

The data processing department is located in an office building which is secured by both key lock and a security system. All doors are locked during off hours. During daytime hours the main door is unlocked, however, data processing personnel are present at all times. An individual must enter the printer room to access the computer room. The door to the printer room is always locked and is protected by a key pad lock. The combination is known by the data processing staff and the maintenance personnel. Motion detectors are in place throughout the building.

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

- Hand-held fire extinguishers.
- Air condition/humidity control devices.
- The computer room contains a UPS (Un-interruptible Power Supply), to provide power to key computer components for a short period of time during power interruptions.
- The computer room has a raised floor to reduce the risk of damage from flooding.

IT Operations

Traditional computer operations procedures are minimal since users at the member school districts initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. In addition, every employee has access to SiteScape Forum which is a billboard system that addresses a variety of problems common to Alpha users.

TCCSA staff have maintained a listing of individuals to contact in the event of complications with the hardware environment. A service agreement with HP has been entered into by TCCSA to provide continued maintenance on all critical and sensitive peripheral equipment. The operating

system monitors the hardware environment and reports all hardware malfunctions automatically through the console maintained by the system. A hardware error log which documents errors identified by the OpenVMS operating system is reviewed by the executive director and the manager of software applications. TCCSA also has service agreements which cover the communication and firewall equipment.

“What’s up Gold” is used to monitor network communication problems and equipment outages in a real time setting. “Down” equipment is displayed on the terminal of one of the network technicians. Users also play a key role in identifying problems by contacting TCCSA when hardware or software problems are encountered.

Member school districts are responsible for handling abnormal terminations. If the users cannot solve the problem they will contact TCCSA staff. TCCSA security practices prohibit the alteration of district data by TCCSA staff members. Data entry or processing errors must be corrected by district users within the context of the application. Member school districts have the option of printing an AUDIT report that shows all activity changes to their data files.

Certain routine jobs are initiated for system maintenance. TCCSA is responsible for operational maintenance tasks, such as system backups, log reports, and other maintenance directed at the whole system. These processes are automatically initiated with the use of DECScheduler. DECScheduler is a program that continually submits jobs on the Alpha system.

Individual member school districts are responsible for running their own regular reports which are batch processes. Batch processes are initiated and completed by the individual member school districts. However, TCCSA runs some batch processes for the processing of EMIS data.

TCCSA helps prevent database failure or corruption through the use of a program called Perfect Disk, which is run through DECScheduler. Perfect Disk will scan all files once a week to verify all files are readable (e.g., no bad blocks, sectors or chains). Data integrity is maintained by the software through validity checks of all input. If a problem is found by Perfect Disk, an e-mail is sent to the executive director, and the manager of software applications.

The TCCSA follows the guidelines of the OECN for backing up system programs, data and related documentation. Incremental backups are performed Monday through Thursday on the production server. Full system backups are performed on Friday on the production server. The tapes are stored in the computer room and are rotated off-site to a safety deposit box at least twice a week. The backup tapes are documented in a backup log.

Daily backups are maintained for approximately 5 weeks. All data required by law to be maintained for a specific duration is maintained by the TCCSA. Calendar year and fiscal year end information is stored indefinitely for all the TCCSA member school districts.

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 TCCSA'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 TCCSA and procedures performed at member school districts that utilize the TCCSA.

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 or Systems

Changes to Existing Applications or 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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
In order to maintain continued support of their application software, the TCCSA is required to install new releases within 30 days of the software release date.	To ensure the USAS, USPS, SAAS, and EMIS software tested at the SSDT is the same version used at TCCSA, a cyclical redundancy check (CRC) of the object program files for each application was compared to the CRC of the latest ODE version tested at the SSDT.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements, and problems corrected. Updated user and system manuals are also made available.	Inspected the documentation and observed that updated manuals are available online.	No exceptions noted.
The TCCSA participates in the CSLG/ESL program, which provides operating system support, upgrades, and related documentation.	Inspected the TCCSA's CSLG licensing agreement with the NBEC for the current fiscal year.	No exceptions noted.
Technical manuals are available for the Alpha server.	Observed and inspected the current Alpha manuals on site at the TCCSA. Observed the online manuals at the OECN 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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The TCCSA has established a data system security policy and a network privacy and acceptable use policy to outline user responsibilities regarding computer security and access. The policies are maintained on TCCSA's web site and are accessible by the member school districts.	Inspected the data system security policy and network privacy and acceptable use policy to confirm user responsibilities are documented. Inspected TCCSA's web site to confirm the policies are maintained online.	No exceptions noted.
Authorization from the appropriate district management is required before setting up a user account on the system as documented on the user access authorization form. Users must sign to acknowledge their review and consent of the network privacy and acceptable use policy.	Using a security analysis tool, selected 60 user accounts from a population of 4,117 and inspected the user access authorization form and the network privacy and acceptable use form to confirm the required forms and signatures were present.	No exceptions noted.
Security related events, such as break-in attempts and excessive log failures, are enabled through OpenVMS. The events are logged to audit journals to monitor potential security violations.	Inspected the enabled security alarms and audits on the system to confirm security related events are reported.	No exceptions noted.
Security violations are extracted and compiled into a detailed security report.	Inspected the security report. Inquired with the executive director and the manager of software applications and support regarding the report review process.	The security violation log is generated, but is not reviewed on a daily basis.
A banner screen indicating users consent to TCCSA's user policies is displayed when a user logs on to the system. The banner screen text is included in the startup process for the system.	Inspected the banner to confirm it is displayed upon logon and inspected the content of the message. Inspected the file to confirm the banner screen is part of the startup process.	Controls operating as described.

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 access is confirmed annually with district management through a negative confirmation process. The TCCSA has developed a program which enables member schools to create a report listing all users from their district.	Observed the executive director utilize the program to view the users on the system. Inspected a sample e-mail sent to district personnel related to the most recent confirmation.	Controls operating as described.
Anti-virus software is installed on the MailMarshal server and user terminals. Definitions are updated daily, and infected items are quarantined to help prevent and detect computer viruses.	Inspected the following information, relating to the Sophos anti-virus software, to confirm anti-virus software is actively scanning for viruses: <ul style="list-style-type: none"> • NetIQ MailMarshal Configurator for virus scanners. • NetIQ MailMarshal Configurator for inbound anti-virus rulesets. • NetIQ MailMarshal Configurator for bothways anti-virus rulesets. • Listing of virus detections for one week in June 2005. Inspected the anti-virus update information from the Sophos event log and anti-virus settings from the Sophos scheduling screens.	No exceptions noted.
Member School District User Control Considerations: Confirm district management makes users aware of the confidential nature of passwords and that users should take precautions to ensure passwords are not compromised. Confirm district management immediately requests the TCCSA to revoke the access privileges of district personnel when they leave or are otherwise terminated. Confirm district management is responding to account confirmation requests from the TCCSA.		

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
<p>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 TCCSA. The number of profiles with pre-expired passwords is limited.</p>	<p>Using a security analysis tool, extracted information from the user authorization file to identify:</p> <ul style="list-style-type: none"> • User accounts with a password minimum length less than TCCSA's standard. • User accounts with a password lifetime greater than TCCSA's standard. • User accounts with pre-expired passwords. <p>Inspected the above exception reports to identify relevant exceptions.</p>	<p>There were 992 (24%) accounts out of 4117 that were pre-expired.</p>
<p>Individual user profiles are used to grant access rights and privileges. The user profiles on the system do not consist of an excessive number of inactive or disabled users.</p>	<p>Using security analysis tools, extracted the following information from the user authorization file:</p> <ul style="list-style-type: none"> • Inactive user accounts. • Accounts never logged into. • DISUSERED user accounts. <p>Inspected the listed accounts.</p>	<p>There were 215 (5%) accounts out of 4117 that have not been logged into in over 180 days. There were 246 (6%) accounts that have never been logged into. The number of DISUSERED accounts was less than 1% (14).</p>
<p>A password change identifier is used to enable district personnel to reset passwords in the event someone at the district forgets their password. The identifiers are restricted by district and normally granted to treasurers, technical coordinators and EMIS coordinators.</p>	<p>Inspected the user accounts having the password change identifier and inquired with the executive director regarding ownership of the listed accounts.</p>	<p>No relevant exceptions noted.</p>
<p>Log-in parameters have been set to control and monitor sign-on attempts.</p>	<p>Inspected the log-in parameter settings.</p>	<p>No exceptions noted.</p>

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Log-in scripts are used to restrict user access to the command prompt.	A security analysis tool was used to extract information from the user authorization file to confirm the use of "login scripts". Inspected the login scripts of the member districts to confirm the login scripts were captive in nature restricting the users only to the OECN menu system.	No exceptions noted.
A program, HITMAN, constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at startup.	Inspected the HITMAN parameters to confirm they were set to automatically logoff inactive users. Inspected the startup file to confirm the HITMAN utility is part of the startup procedures.	No exceptions noted.
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts do not allow blanket access.	Inspected the network proxy listing for wild card characters.	No exceptions noted.
Access to production data files and programs is restricted to authorized users.	From a directory list of executable files, extracted and inspected files with WORLD access. Inspected a listing of data files for WORLD WRITE and/or DELETE access for all member school districts.	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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between member school districts.	Inspected the network diagrams to confirm components of the network which control Internet access. Inspected the firewall configuration for evidence that Internet traffic is restricted through the firewall. Inspected e-mails and help desk tickets requesting adjustments to the firewall configuration.	External traffic to the production server is not restricted.
The TCCSA internal network uses a private internal addressing scheme, which is unable to be used over the Internet.	Displayed the connection type of all users logged into the system to confirm the existence of a private internal 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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user management.	Using security analysis tools, extracted accounts containing USAS, USPS, SAAS/EIS, and/or EMIS OECN identifiers from the user authorization file. Selected 60 user accounts from a population of 562 and compared the access granted to the access requested on the user authorization forms.	For seven of the 60 accounts reviewed, the access granted was not in agreement with the access requested on the user authorization form.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized DA-Site users.	Using security analysis tools, extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inspected the list of accounts.	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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Member School District User Control Consideration: Confirm the User Identification Codes (UICs), passwords and associated access privileges are issued only 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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
WORLD access to “key” system files is restricted.	Inspected the system file directory listing for WORLD Write or Delete access. Inspected the file protection masks on the security files.	No exceptions noted.
System level UICs and elevated privileges are restricted to authorized personnel.	Inspected the MAXSYSGROUP value. Using a security analysis tool, extracted accounts from the user authorization file to identify: <ul style="list-style-type: none"> • Accounts with a UIC less than the MAXSYSGROUP value. • Accounts with elevated privileges. Inspected the listed accounts.	No exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the user authorization alternate parameter. Inspected the system directory listings for an alternate user authorization file.	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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Remote access to the firewall configuration used to control Internet access is restricted through password protection.	Inspected the firewall configuration to confirm passwords were enabled.	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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Physical access to the computer room and its contents is restricted to authorized personnel.	Inspected the key pad entry devices and existence of motion detection devices throughout the period of fieldwork.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, humidity or changes in temperature.	Inspected the computer room and observed the existence of temperature and humidity controls and elevated flooring. Inspected the TCCSA building and observed the existence of smoke detectors and fire extinguishers.	No exceptions noted.

Member School District User Control Considerations: Confirm PCs and terminals are protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals. Confirm communication lines, junctions and modems are 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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The TCCSA performs certain routine jobs for reporting EMIS data automatically through various programs and a scheduling program, DECScheduler.	<p>Inspected the EMIS batch processing scripts and DECScheduler jobs responsible for the automation of EMIS reporting.</p> <p>Inspected the OpenVMS system startup printout to confirm that DECScheduler was initialized during the startup of the system.</p>	No exceptions noted.
A disk maintenance utility, Perfect Disk, is scheduled with the use of the DECScheduler program to perform maintenance on a predetermined schedule. Redundant text files are purged via a scheduled procedure.	Inspected the DECScheduler program for the disk maintenance utility and the purge text files procedure.	No exceptions noted.
TCCSA has a hardware maintenance agreement with HP, DataServ, and Cisco Systems for maintenance or repair of both the main processing and network routing equipment.	Inspected the hardware maintenance agreements for services covered and period of coverage.	No exceptions noted.
All data center equipment is covered by insurance.	Inspected the insurance policy and payment documentation for evidence of coverage.	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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Backups of programs and data are performed regularly.	Inspected the backup command procedures for the TCCSA production servers. Inspected the daily summary backup logs for the audit period. Inspected the DECScheduler procedures to confirm backups are automatically scheduled daily.	No exceptions noted.
Backup tapes are stored in secure on and off-site locations and are rotated regularly.	Inspected an inventory listing of backups maintained on and off-site. Inspected the off-site storage facility with the field services technician and confirmed the off-site backups agreed to the inventory listing.	No exceptions noted.
Member School District User Control Considerations: Confirm the district retains source documents for an adequate period to ensure data can be re-entered in the event the data files are destroyed prior to being backed up and rotated off-site. Confirm the district establishes and enforces a formal data retention schedule with the TCCSA for the various application data files.		

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

DATA ACQUISITION SITE PROFILE OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name: Tri-County Computer Services Association (TCCSA)
Number: 19
Node Name: TCCSA

Chairperson: Edward Swartz
Superintendent
Tri-County Educational Services Center

Fiscal Agent District: Midland Council of Governments (MCOG)

Administrator: Stuart Workman
Executive director
TCCSA

Address: 2125-B Eagle Pass
Wooster, OH 44691

Telephone: 330-264-6047
FAX: 330-264-5703

Web site: www.tccsa.net

OTHER SITE STAFF

Doug Ackerman	Field services technician
Mary Barber	Educational technologist
John Beno	Workstation repair
Ben Burge	Field services technician
Deb Carroll	Software support specialist
Glenn Caudill	District network supervisor
Roger Doty	Field services technician
Daniel Erickson	Educational technologist
Jim Franks	Manager of software applications and support
Thomas Grandy	Educational technologist
Shelley Hughett	Software support specialist
Jonathan Johnson	Field services technician
Sean Linder	Field services technician
Philip McNaull	Field services technician
Kennard Meng	Technology coordinator
Dan Morton	District repair specialist
Terry Noel	CA-USD project manager
Michael Osborn	CA-USD project manager
Dan Ortiz	Field services technician
Joseph Picking	Educational technology coordinator
Joanne Porr	Educational technologist
Alice Rehm	Secretary
Rebecca Rosecrans	Educational technologist
Keith Studer	Field services technician
Roy Templeman	Field services technician
John R. VanLanen	Manager of network operations
Kyle Whitford	Field services technician
Sherry Williams	Assistant manager of software applications and support

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

<u>Model Number</u>		<u>Installed</u>		<u>Capacity/Density/Speed</u>	
CPU:	Compaq Alpha GS60	Lines/Ports:	N/A	Memory Installed:	5.0 GB
Disk:	RZ1EF	Units:	2	Total Capacity:	80.0 GB
Disk:	RZZ229	Units:	11	Total Capacity:	49.5 GB
Disk:	RZ29	Units:	25	Total Capacity:	450.0 GB
Tape Unit:	TZ89	Units:	1	Max Density:	N/A
Tape Unit:	TZ88	Units:	1	Max Density:	N/A
Tape Unit:	TZ207	Units:	1	Max Density:	9 track 6250
Tape Unit:	MSL5000 SDLT Tape Library	Units:	1	Total Capacity:	320GB
Printer:	HP 2566	Units:	1	Print Speed:	200 LPM
Printer:	HP 2562	Units:	1	Print Speed:	400 LPM

MEMBER SCHOOL DISTRICT SITE DATA

<u>IRN</u>	<u>MEMBER SCHOOL DISTRICT</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
062042	Ashland County - West Holmes Career Center	Ashland	X	X	X	X
043505	Ashland City SD	Ashland	X	X	X	X
045823	Hillsdale Local SD	Ashland	X	X	X	X
045468	Loudonville-Perrysville Ex Village SD	Ashland	X	X	X	X
045831	Mapleton Local SD	Ashland	X	X	X	X
047688	East Holmes Local SD	Holmes	X	X	X	X
047696	West Holmes Local SD	Holmes	X	X	X	X
044974	Wadsworth City SD	Medina	X	X	X	X
050534	Chippewa Local SD	Wayne	X	X	X	X
050542	Dalton Local SD	Wayne	X	X	X	X
050559	Green Local SD	Wayne	X	X	X	X
050567	North Central Local SD	Wayne	X	X	X	X
050575	Northwestern Local SD	Wayne	X	X	X	X
044610	Orrville City SD	Wayne	X	X	X	X
045591	Rittman Ex Village SD	Wayne	X	X	X	X
050583	Southeast Local SD	Wayne	X	X	X	X
050526	Tri-County Educational Service Center	Wayne	X	X	X	X
050591	Triway Local SD	Wayne	X	X	X	X
051714	Wayne County Career Center	Wayne	X	X	X	X
045120	Wooster City SD	Wayne	X	X	X	X
TOTALS:			20	20	20	20



**Auditor of State
Betty Montgomery**

88 East Broad Street
P.O. Box 1140
Columbus, Ohio 43216-1140
Telephone 614-466-4514
800-282-0370
Facsimile 614-466-4490

TRI-COUNTY COMPUTER SERVICES ASSOCIATION

WAYNE 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
DECEMBER 6, 2005**