LAKE GEAUGA COMPUTER ASSOCIATION
STATE REGION - ISA, LAKE COUNTY

SAS 70

JULY 24, 2004 THROUGH JULY 29, 2005

Auditor of State
Betty Montgomery

TABLE OF CONTENTS

This Page Intentionally Left Blank

Auditor of State
Betty Montgomery

INDEPENDENT ACCOUNTANT'S REPORT

Committee Members
Lake Geauga Computer Association (LGCA)
8221 Auburn Road
Concord Township, OH 44077

To Members of the Committee:

We have examined the accompanying description of controls of the Lake Geauga Computer Association (LGCA) 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 LGCA'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 LGCA's controls; and (3) such controls had been placed in operation as of July 29, 2005. The control objectives were specified by the LGCA management for the processing of USAS, USPS, SAAS/EIS, and EMIS with the assistance of the Ohio Department of Education. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the LGCA's controls that had been placed in operation as of July 29, 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 member school districts applied the controls contemplated in the design of the LGCA'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 July 24, 2004 to July 29, 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 LGCA 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 July 24, 2004 to July 29, 2005.

The relative effectiveness and significance of specific controls at the LGCA 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 LGCA to provide additional information and is not part of the LGCA'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 LGCA is as of July 29, 2005, and information about tests of the operating effectiveness of specified controls covers the period from July 24, 2004 to July 29, 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 LGCA 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 LGCA, its member school districts, and the independent auditors of its member school districts.

Betty Montgomery

Betty Montgomery
Auditor of State

July 29, 2005

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The LGCA'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 LGCA's description of controls.

OVERVIEW OF OPERATIONS

The LGCA is a not-for-profit computer service organization that services 18 member school districts in the Ohio counties of Cuyahoga, Geauga and Lake. The primary function is to provide information technology services to its member school districts with some emphasis being placed on accounting, payroll, and inventory control services. LGCA also provides limited services, such as Internet access, to parochial and other school districts; however, these districts are not voting members of the assembly. The LGCA is located in Concord Township.

The LGCA 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 LGCA 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. LGCA is organized under section 3313.92 and is thus required to have a board of education serve as its fiscal agent to receive OECN funds from the ODE. For this reason, the Geauga County Educational Service Center serves as the fiscal agent for LGCA and performs certain functions that might otherwise be performed by the LGCA. Essentially, these functions are to apply for and maintain the DA Site permit for the central data processing equipment purchased with state monies and to hold legal title to this equipment.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the director and the executive committee. The superintendent and treasurer of each member district are members of the legislative body of the LGCA, known as the assembly. Each district has one vote, cast by the superintendent or his designee. 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 LGCA and consists of six district superintendents, five district treasurers and two "at large" members selected from the user groups. The executive committee is required to meet at least quarterly. The executive committee has also established several advisory committees to assist in the operation of the LGCA and its programs. Standing committees include a planning/policy committee, a finance committee and a personnel committee.

The LGCA has prepared a continuous improvement plan as required by the Ohio Department of Education.

The LGCA employs a staff of 16 individuals and is supported by the following functional areas:

- *Operational Support:* Facilitates the implementation and operation of all supported software, and provides user training and support.
- *Systems Support:* Designs and supports the LGCA computer systems and its networked communications systems and provides user training and support.

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

The LGCA is generally limited to recording user organization transactions and processing the related data. Users are responsible for authorization and initiation of all transactions. Management reinforces this segregation of duties as a part of its orientation process for new employees, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced LGCA employees may alter user data and only at the request of the member school district. Documentation supporting the change is kept on file at LGCA.

The LGCA follows the same personnel policies and procedures as their fiscal agent, the Geauga County Educational Service Center. Detailed job descriptions exist for all positions. The LGCA 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 LGCA'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.

The Management Council of the Ohio Education Network (MCOECN) has established the format for the staff development program including the requirements for continuing education units and the procedures for the regional staff development committees in each of the five regions of the MCOECN. Thus, LCGA 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. Employee evaluations are conducted annually.

Risk Assessment

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

- New technology.
- Realignment of the LGCA 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 LGCA 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 LGCA organization is structured so that department managers report directly to the director. Key management employees have worked here for many years and are experienced with the systems and controls at the LGCA. The LGCA director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

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 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 LGCA staff does not perform system development activities. Instead, the LGCA 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 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 LGCA 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 LGCA uses a software utility called OECN_INSTALL to unpack these zipped files and install each individual package into its proper OECN directory. The OECN_INSTALL utility has two options which will either install the new release on the system or install a patch for a current release. This utility ensures that all required components are installed properly and consistently.

Only vendor supplied changes are made to the operating system or system software documentation. The Northern Buckeye Education Council (NBEC), which 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 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 for 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 participating DA Sites' 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 LGCA, 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 LGCA 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 LGCA.

IT Security

The LGCA has a security policy that outlines the responsibilities of member school district personnel, the LGCA personnel, and any individual or group not belonging to the member school district or the LGCA. In addition to the security policy, the LGCA uses a banner screen that is displayed before a user logs in to the system. The screen informs the user that unauthorized access of the system is prohibited and individuals using this computer system are subject to having their activities monitored by the LGCA personnel.

The LGCA 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 director.

Users from the member school districts are granted access upon the completion of an account request form. Access authorization is required from the superintendent or treasurer. A listing, which indicates user access and privileges within the district, is sent out annually to the respective superintendents to verify the users on their system are properly authorized.

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/or security audits have been enabled through OpenVMS to monitor any security violations on the LGCA system:

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 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.

A batch processed command procedure executes each night to extract security violations from the audit log and creates detail and summary reports of security events. These security monitor reports are e-mailed to the director and the director of technology and are reviewed daily. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed.

The LGCA utilizes Sophos Anti-Virus software on the Alpha server to scan all inbound and outbound e-mail. If a virus is found, the e-mail is quarantined and the LGCA user is sent an e-mail message informing them of the virus.

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.

The LGCA uses proxy logins. A proxy login enables a user logged in at a remote node to be logged in automatically to a specific account at the local node, without having to supply 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.

User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the LGCA and to all personnel at the member school districts which use the LGCA system. UICs are assigned at the member school district's request. UIC based protection controls access to objects such as files, directories, and volumes.

Certain limited-access accounts require a less restrictive environment than captive accounts. Accounts under which network objects run, for example, require temporary access to DCL. Such accounts must be set up as restricted accounts, not captive accounts. User accounts should be set with the RESTRICTED flag instead of the CAPTIVE flag if they need to use network applications like MAIL or network proxy accounts. The RESTRICTED and CAPTIVE flags are typically not used for LGCA staff accounts because access to the DCL prompt is necessary for them to perform their job functions. However all other users, such as treasurers, district staff, teachers and students, are assigned the RESTRICTED and CAPTIVE flags respectively. The RESTRICTED flag allows access to MAIL, but because the CAPTIVE flag is also assigned, the use of the SPAWN command to gain access to the DCL prompt is prohibited.

The system forces users, who use the various software packages, to periodically change their passwords. The DEFAULT account password lifetime and password length fields have been set according to the standards established by LGCA. Passwords are set to expire (masking the account with the pre-expired parameter PWDEXPIRE) 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.

The operating system has system parameters called SYSGEN 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 HP established defaults. Any changes are logged and reviewed by the director.

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 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 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 system directories. The UIC associated with each of these files is within the MAXSYSGROUP number. To limit access to security files, the LGCA has limited the WORLD access for the 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 DA Site 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.

The LGCA utilizes a Cisco PIX (Private Internet Exchange) box to control traffic to and from the Internet. Member school districts have been set up with sub-networks which have addresses not recognizable to the Internet. This is called a private internal network. Some of the school districts and LGCA mail and web servers are set up with public addresses. These addresses are specifically identified in the PIX box configuration. In addition, access to the production server is restricted to specific IP addresses.

The computer room is located within an enclosed area of the LGCA offices. Both the LGCA offices and the computer room are secured at all times with an electronic key system. The only individuals with electronic keys to the computer room are the LGCA staff. There is a motion sensor that is activated outside the computer room after the close of business for the day.

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

- Fire extinguishers.
- HFC 277ea extinguishing system.
- Temperature control device.
- Motion sensors.

IT Operations

Traditional computer operations procedures are minimal because users at the member school districts initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All LGCA employees have access to a procedure manual, which provides directions and guidelines for most of the operational functions performed. They also have access to operations procedure manuals for the Alpha system. In addition, all users, except students, have access to SiteScape forum, which is a bulletin board that allows the LGCA employees to communicate with users across the state. Users can post questions and/or comments to the LGCA staff.

Occasionally, software problems may occur which require intervention by the DA Site staff. Support staff members are instructed not to make data changes unless requested in writing. The member school districts may print out an AUDIT report which shows all activity changes to the data file. Certain routine jobs are initiated for system maintenance. LGCA is responsible for operational maintenance tasks, such as system backups, log reports, and other maintenance directed at the whole system. They use an automated program called DECScheduler which schedules and performs these tasks. DECScheduler is a program which continually submits jobs on the Alpha system.

The director of technology monitors for disk drive failures daily. For technical and software support, all time spent with the districts is logged into a database. Periodically, the director of technology creates a summary report of the time spent by LGCA employees on software and hardware issues for the districts.

LGCA has a maintenance agreement with HP for the computer equipment used at the data center.

Network and Internet traffic is monitored on a regular basis. The tools used to monitor traffic on the router and firewalls are typically used for trouble shooting purposes only. CiscoWORKS Manager is used to monitor physical connections to the network. This tool provides information regarding problems with physical network connections. In addition, the director of technology uses Multi Router Traffic Router software (MRTG) and a Fluke Enterprise LANMeter to monitor network traffic. This tool is used periodically and reports information regarding network traffic, link speed and port errors.

The LGCA performs backups of both system data and programs. A full backup for the Alpha server is completed daily Monday through Friday on digital linear tapes (DLT). These tapes are stored in a fire-resistant safe off-site at the Auburn Career Center, located across the street from the LGCA.

Daily backup tapes are kept in a one month rotation and year-end tapes dating back to 1981 are kept at LGCA in the computer room. A backup tape log is maintained by the user liaison. A short version of a printout of the backup completion status is reviewed by the user liaison. If a problem with the backup has occurred, a full backup log is reviewed to determine the exact point of failure. In addition, the director of technology is e-mailed the status of the prior night's backup process.

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

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

<table>
<tr><td colspan="2"><b>Changes to Existing Applications or Systems -</b> <i>Control Objective:</i>
<b>Change Requests</b> - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>In order to maintain continued support of the application software provided by the SSDT, DA Sites are required to install new releases within 30 days of the software release date.</td><td>To ensure the USAS, USPS, SAAS/EIS, and EMIS software tested at the SSDT is the same version used at LGCA, 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</td><td>No relevant exceptions noted.</td></tr>
<tr><td>The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals are also made available.</td><td>Inspected the release notes and updated manuals for the most recent release.</td><td>No exceptions noted.</td></tr>
<tr><td>The LGCA participates in the CSLG/ESL program which provides operating system support, software upgrades and software related documentation.</td><td>Inspected the LGCA’s CSLG licensing agreement with the NBEC for the current fiscal year.</td><td>No exceptions noted.</td></tr>
<tr><td>Technical manuals are available for the OpenVMS operating system.</td><td>Observed and inspected the current Alpha manuals on site at the LGCA.</td><td>No exceptions noted.</td></tr>
</table>

IT Security

<table>
<tr><td colspan="2"><b>IT Security -</b> <i>Control Objective:</i>
<b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The LGCA has established a data system security policy that outlines user responsibilities regarding computer security and access.</td><td>Inspected the data system security policy to confirm user responsibilities are documented.</td><td>No exceptions noted.</td></tr>
</table>

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:*
Authorization from the appropriate district management is required before user accounts are created.	Inquired about authorization procedures with the director of technology. Sampled 60 user accounts from a population of 524. Inspected the forms for authorization signatures.	One of the 60 accounts selected for review did not have an authorization form on file.
Member school districts are asked to confirm user accounts annually when they are asked to sign and return their service agreement with LGCA.	Inspected the signed service agreements between LGCA and the member school districts to confirm responses were received from all member school districts.	Signed service agreements and confirmation of user accounts were not received for the following districts: • Warrensville Heights City SD • Ledgemont Local SD • Fairport Harbor Exempted Village SD • Perry Local SD
Banner screens indicating users' consent to LGCA'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 screen displayed during login to the production system. Inspected the startup process for the production system.	No exceptions noted.
Security related events, such as break-in attempts and excessive login failures, are enabled through OpenVMS. The events are logged to audit journals for monitoring of potential security violations.	Inspected the enabled security alarms and audits.	No exceptions noted.
Security violations are extracted, compiled into summary and detailed security reports, and emailed to the director and director of technology daily through OpenVMS command procedures on the system. Daily, the reports are reviewed for login failures, breakins, and changes to the user authorization file. The command procedures are automatically resubmitted to the system daily.	Inspected a security monitor report and the command procedures which e-mails the report to both the director and directory of technology.	No exceptions noted.

<table>
<tr><td colspan="2"><b>IT Security -</b> <i>Control Objective:</i>
<b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Anti-virus software is installed and definitions are automatically updated to help prevent and detect computer viruses.
A file within the PMDF mail application searches for the words virus and alert in e-mail messages from the virus software vendor, Sophos. Upon receipt of the alerts, a command procedure is automatically initiated to download the latest virus identity (IDE) files from Sophos.</td><td>Inspected the following to confirm the anti-virus software is maintained to adequately prevent and detect computer viruses:
• PMDF file used to initiate the anti-virus update command procedure.
• Command procedure used to download anti-virus updates.
• An example e-mail from Sophos indicating a virus alert.
• Printout of the current Sophos product version and latest virus identity (IDE) files.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>Member School District User Control Considerations:</b>
Confirm district management makes users aware of the confidential nature of passwords and that the users should take precautions to ensure passwords are not compromised.
Confirm district management immediately requests the DA Site to revoke the access privileges of district personnel when they leave or are otherwise terminated.
Confirm the district has a documented acceptable use policy defining what activities are deemed appropriate for use of the Internet access provided to the district. Internet users should be required to accept the terms of the policy before access is provided.
Confirm district management is responding to account confirmation requests from the DA Site.</td></tr>
</table>

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Individual user profiles are used to grant access rights and privileges for the system. The user profiles on the system do not consist of an excessive number of inactive, disabled, or high-privileged profiles.	Using a security analysis tool, extracted the following information from the user authorization file: • Inactive user accounts. • User accounts that are DISUSERED. • User accounts with ELEVATED privileges, defined as those accounts having more than the minimum privileges to use the system. Inspected the results of the extracted information and discussed with the director of technology for appropriateness.	No relevant exceptions noted.
Password parameters are in place to aid in the authentication of user access to the production system. Passwords used by individual profiles are in accordance with the password policies established by the LGCA. The number of profiles with pre-expired passwords is limited.	Using a security analysis tool, extracted information from the user authorization file to identify: • User accounts with a password minimum length less than the established value; • User accounts with a password lifetime greater than the established values; • User accounts with pre-expired passwords. Inspected the above exception reports and inquired with the director of technology to identify relevant exceptions.	No relevant exceptions noted.
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts do not permit blanket access.	Inspected the network proxy listing for wild card characters.	No exceptions noted.
Access to the OpenVMS command line (DCL) is restricted.	Created a batch file utilizing security analysis tools, and inspected user accounts that do not have the AUDIT, CAPTIVE, DISCTYLY, DISUSER or RESTRICTED flags set.	No relevant exceptions noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings.	No exceptions noted.

<table>
<tr><td colspan="3"><b>IT Security -</b> <i>Control Objective:</i>
<b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>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.</td><td>Inspected the HITMAN parameters to determine if they were set to automatically logoff inactive users.
Inspected the startup file to determine whether the HITMAN utility is part of the startup procedures.</td><td colspan="2">No relevant exceptions noted.</td></tr>
<tr><td>Access to production data files and programs restricted to authorized users.</td><td>A command procedure was run to search all district data files and application executable files for the USAS, USPS, SAAS/EIS and EMIS applications for the presence of any WORLD access.
Inspected the listings of data and executable files having WORLD access.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between member school districts.</td><td>Inspected the network diagram to confirm components of the network which control Internet access.
Inspected the router and firewall configurations for evidence that Internet traffic is restricted through the firewall. In addition, confirmed the existence of a private internal network.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

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 on requests from user management.	Using a security analysis tool, extracted accounts with the OECN identifiers for the USAS, USPS, SAAS/EIS, and EMIS application system. Selected 60 accounts from a population of 524 to confirm the identifiers granted per the user authorization file were in agreement with the identifiers authorized per the access request form.	One of the 60 accounts selected for review did not have an authorization form on file. Three of the 60 accounts had identifiers which were not authorized per the access request form.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized DA Site users.	Using a security analysis tool, extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inspected the list of accounts.	No exceptions noted.
Member School District User Control Consideration: Confirm 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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
System level UICs and high-privileged profiles are restricted to authorized personnel.	Inspected the MAXSYSGROUP value. Using a security analysis tool, extracted accounts from the user authorization file to identify: • Accounts with a UIC less than the MAXSYSGROUP value. • Accounts with elevated privileges. Inspected the listed accounts.	No relevant 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:*
Use of an alternate user authorization file is not permitted.	Inspected the value of the user authorization alternate parameter. Inspected the system directory listings to determine if an alternate user authorization file existed.	No exceptions noted.
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.
Remote access to the firewall used to control Internet access is restricted through password protection.	Inspected the firewall configuration to confirm passwords were enabled and to confirm that remote access was restricted. Independently inquired with the director of technology and the communications/Apple specialist to confirm they are the only individuals with knowledge of the passwords for the firewall.	No exceptions noted.
Firewall configuration changes are authorized via electronic mail requests or verbally from district technical coordinators to the director of technology or communications/Apple specialist. Implications of firewall configuration changes are communicated to the district technical coordinators.	Inspected five e-mail requests for changes to the firewall configuration. Independently inquired with the director of technology, the communications/Apple specialist, and the technology coordinator of Chardon schools to confirm that firewall configuration changes are requested by district technical coordinators via e-mail and that implications are discussed.	No exceptions noted.

<table>
<tr><td colspan="2"><b>IT Security -</b> <i>Control Objective:</i>
<b>Physical Security</b> - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Physical access to the computer room and its contents is restricted to authorized personnel.</td><td>Observed the existence of motion sensors and an electronic key entry system.
Inquired with the director of technology about the physical access controls.</td><td>No exceptions noted.</td></tr>
<tr><td>Environmental controls are in place to protect against and/or detect fire or changes in temperature.</td><td>Inspected the computer room and observed the following environmental controls:
• Fire extinguishers.
• HFC 277ea extinguishing system.
• Temperature control device.
• Uninterruptible power supply.
• Backup generator.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>Member School District User Control Considerations:</b>
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 the communication lines, junctions and modems are secured in an area restricted to only authorized individuals.</td></tr>
</table>

IT Operations

<table>
<tr><td colspan="2"><b>IT Operations -</b> <i>Control Objective:</i>
<b>System Administration and Maintenance</b> - Appropriate procedures should be established to ensure the system is properly maintained and monitored.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The LGCA has an overall operating procedure manual that is available at all times to the LGCA personnel. In addition, current Alpha manuals are maintained on-site and online.</td><td>Inspected the content of the LGCA procedure manual.
Confirmed the availability of the Alpha manuals both on-site at LGCA and on-line.</td><td>No exceptions noted.</td></tr>
</table>

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The LGCA performs certain routine jobs for system maintenance through a scheduling program, DECScheduler.	Inspected the DECScheduler listing of jobs. Inspected the OpenVMS system startup file printout to confirm that DECScheduler was initialized during the startup of the system.	No exceptions noted.
Technical support incidents are logged into a time tracking system and are reviewed periodically by the director of technology.	Inspected a technical services time retrieval form for the month of July 2005 for a single LGCA staff technical support staff member. Inquired with the director of technology regarding the process for documenting technical and software support requests from the member school districts.	No exceptions noted.
Upon login of the director of technology, device errors are automatically displayed. The director of technology monitors these device errors daily.	Inspected a printout of the device error listing displayed upon login of the director of technology. Inquired of the director of technology regarding the procedures for monitoring device errors.	No exceptions noted.
A service agreement with HP covers maintenance and failures of the computer hardware.	Inspected the HP Hardware Service Agreement for services covered and period of coverage.	No exceptions noted.
CiscoWORKS Manager is used to monitor the network for hardware failures. The software displays the physical network connections in a graphical network diagram and highlights problem areas.	Physically observed online the use of CiscoWORKS by the director of technology.	No exceptions noted.

<table>
<tr><td colspan="3"><b>IT Operations -</b> <i>Control Objective:</i>
<b>System Administration and Maintenance</b> - Appropriate procedures should be established to ensure the system is properly maintained and monitored.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Multi Router Traffic software (MRTG) and a Fluke Enterprise LANMeter are used periodically to monitor network traffic and errors.</td><td>Physically observed online the use of MRTG software for traffic analysis of Kirtland Middle School by the director of technology.
Physically observed the Fluke Enterprise LANMeter tool. Inquired of the director of technology regarding the use of the Fluke Enterprise LANMeter tool.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Data center equipment is covered by insurance.</td><td>Inspected the insurance policy and payment documentation for evidence of coverage.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>IT Operations -</b> <i>Control Objective:</i>
<b>Backup</b> - Up-to-date backups of programs and data should be available in emergencies.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Backups of programs and data are performed daily.</td><td>Inspected the DECScheduler listing of jobs and ABS application command file to confirm the backup job was scheduled to run daily.
Physically observed online a directory listing of zipped backup log files to confirm backups were performed throughout the audit period.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Backup tapes are stored in a secure off-site location.</td><td>Inspected the off-site storage facility with the InfOhio application technician/tech support.
Confirmed tapes listed on the backup tape inventory listing were stored off-site.</td><td colspan="2">The LGCA’s off-site storage facility for backup tapes is located directly across the street. No other relevant exceptions noted.</td></tr>
<tr><td colspan="4"><b>Member School District User Control Considerations:</b>
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 LGCA for the various application data files.</td></tr>
</table>

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

DATA ACQUISITION SITE PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name:	Lake Geauga Computer Association (LGCA)
Number:	6
Node Name:	LGCA
Chairperson:	Matthew Galemmo Superintendent Geauga County Educational Service Center
Fiscal Agent District:	Geauga County Educational Service Center
Administrator:	James C. Turk Director LGCA
Address:	8221 Auburn Road Concord Township, OH 44077
Telephone:	440-357-9383
FAX:	440-457-8713
Web site:	www.lgca.org

OTHER SITE STAFF

Brian Ruffner	Director of technology
Daniel Salaciak	Technical support
Joe Slepko	Technical support
Bob Wurm	Technical support
Fred Pohto	Technical support
John Renwick	Technical support
Crystal Pagano	Technical support
Sue Vinborg	Programmer / analyst
John Klein	Programmer / analyst
Barb Borris	User liaison
Shirley Erjavec	User liaison
Linda Pohto	User liaison
Bonnie Pisching	InfOhio specialist
Donna Waldorf	InfOhio specialist (Left April 2005)

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number:		Installed:		Capacity/Density/Speed:	
CPU:	Compaq Alpha Server 41000 (QUAD 600MHZ CPU)	Lines/Ports:	N/A	Memory Installed:	7 GB
Disk:	RZ28-BA	Units:	4	Total Capacity:	8 GB
Disk:	RZ1DB-VW	Units:	6	Total Capacity:	54 GB (45 due to RAID)
Storage Enclosure:	RA7000	Units:	1		
Controller:	HSZ70	Units:	1	Total Capacity:	128 MB WB Cache
Tape Unit:	TSZ07-CA	Units:	1	Max Density:	1600/6250 TBLTOP SCSI
Tape Unit:	TZ89N	Units:	1	Max Density:	35-70GB 5.25” SE DLT
Printer	LG06	Units:	1	Print Speed:	600 LPM

MEMBER SCHOOL DISTRICT SITE DATA

IRN	MEMBER SCHOOL DISTRICT	COUNTY	USAS	USPS	SAAS	EMIS
043554	Beachwood City SD	Cuyahoga	X	X	X	X
045286	Chagrin Falls Exempted Village SD	Cuyahoga	X	X	X	X
045005	Warrensville Heights City SD	Cuyahoga	X	X	X	X
041767	Berkshire Local SD	Geauga	X	X	X	X
047175	Cardinal Local SD	Geauga	X	X	X	X
047183	Chardon Local SD	Geauga	X	X	X	X
047159	Geauga County Educational Service Center	Geauga	X	X	X	X
047191	Kenston Local SD	Geauga	X	X	X	X
047209	Ledgemont Local SD	Geauga	X	X	X	X
047217	Newbury Local SD	Geauga	X	X	X	X
047225	West Geauga Local SD	Geauga	X	X	X	X
045369	Fairport Harbor Exempted Village SD	Lake	X	X	X	X
047878	Kirtland Local School District	Lake	X	X	X	X
047860	Lake County Educational Service Center	Lake	X	X	X	X
044628	Painesville City Local SD	Lake	X	X	X	X
047894	Painesville Township Local SD	Lake	X	X	X	X
047902	Perry Local SD	Lake	X	X	X	X
051169	Auburn Career Center	Lake	X	X	X	X
TOTALS:			**18**	**18**	**18**	**18**

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

LAKE GEAUGA COMPUTER ASSOCIATION

LAKE 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