LICKING AREA COMPUTER ASSOCIATION (LACA)
STATE REGION - ISA, LICKING COUNTY

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2017 THROUGH MARCH 31, 2018

Dave Yost · Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

SECTION 3 – DESCRIPTION OF LACA'S ITGC SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

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

OVERVIEW OF OPERATIONS

The LACA is one of 18 governmental cooperative shared technology service organizations serving more than 973 educational entities and 1.475 million students in the state of Ohio. These service entities, known as Information Technology Centers (ITCs), and their users make up the Ohio Education Computer Network (OECN) authorized pursuant to Section 3301.075 of the Revised Code. Such sites, in conjunction with the Ohio Department of Education (ODE), comprise a statewide delivery system to provide comprehensive, cost-efficient accounting and other administrative and instructional computer services for participating Ohio entities. Funding for this network and for the LACA is derived from the state of Ohio and from user fees.

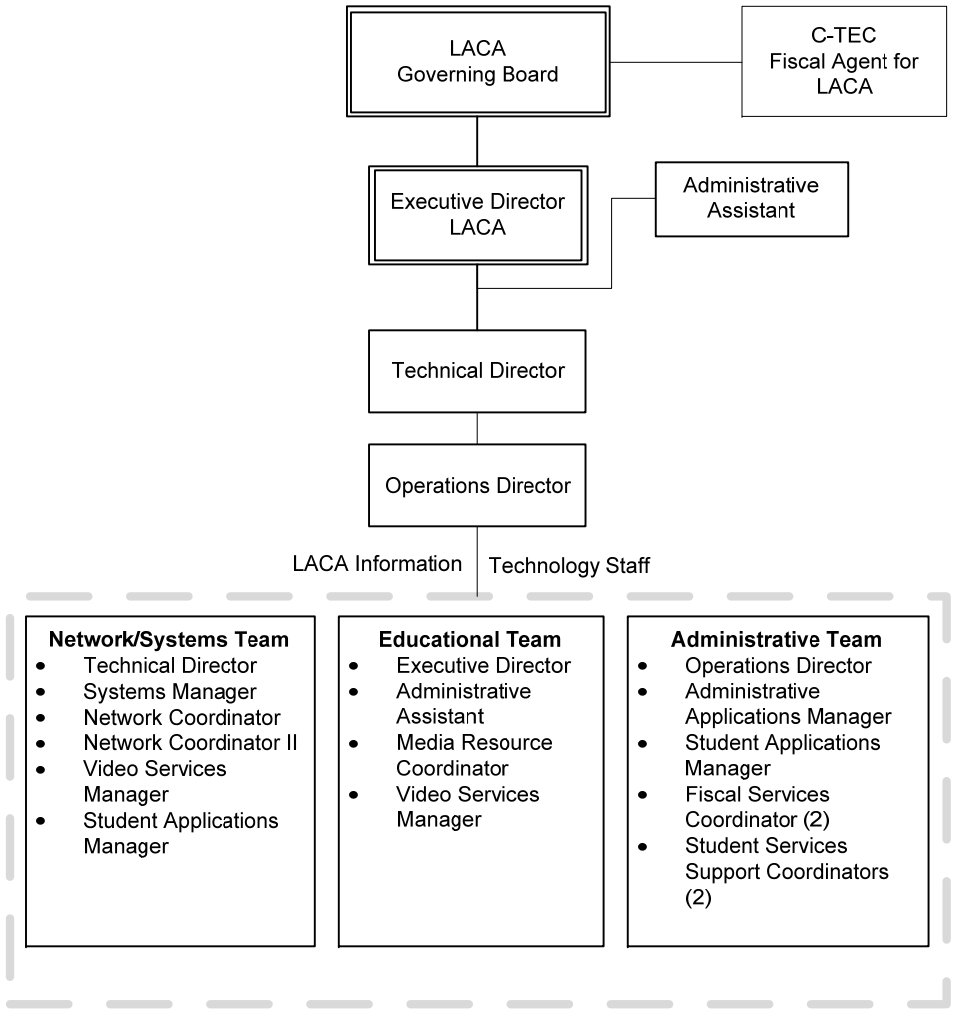
ITCs provide information technology services to user entities, public school districts, community (charter) schools, JVS/career & technical centers, educational service centers (ESCs) and parochial schools; however, not all entities subscribe to the same services. Throughout the remainder of the report,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

- Uniform School Accounting System (USAS).
- Uniform Staff Payroll System (USPS).
- School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS).

ITCs are organized as either consortia under ORC 3313.92 or Councils of Government (COG) under ORC 167. ORC 3313.92 allows for user entities to create a partnership (a consortia) to resolve mutual needs. One of the members of the consortia is designated as fiscal agent. The fiscal agent provides all accounting, purchasing, and personnel services for the consortia. A "COG" under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. The LACA is organized under section 3313.92. The Career and Technology Center of Licking County (C-Tec) serves as the fiscal agent for the LACA.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment



Operations are under the control of the executive director and the governing board. The governing board is the governing body of the LACA and is composed of twenty members, one Superintendent from each member user entity served by the LACA. The board meets four times a year, with additional meetings as necessary. The board has also established several sub-committees to assist in the operation of the LACA.

The LACA employs a staff of 17 individuals, including the executive director, and is supported by the following functional areas:

Fiscal Administration Services:	Provides end user support and training for all fiscal service applications, including USAS, USPS, and SAAS/EIS.
Technical WAN Services:	Supports the LACA computer systems and its networked communications systems. In addition, provides users a variety of educational technology services, including software and Internet access, e-mail, training, technology planning, and technical assistance.
Student Administration:	Supports end users in all aspects of the student service applications.
Library Services Support:	Supports end users with library services programs.

The LACA is generally limited to recording user entity transactions and processing the related data. User entities are responsible for authorization and initiation of all transactions. The LACA's management reinforces this segregation of duties as a part of its new employees' orientation process, through on the job training, and by restricting employee access to user data. User entities rarely request the LACA to make changes to their data once entered; however, when they do request it, only experienced LACA staff members are allowed to make these changes. The LACA maintains a file of all approved changes for each user entity.

The LACA's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the entity require some type of college degree in a computer-related field, and require professional development and other training as a condition of continued employment. Each staff member must attend at least twenty hours of approved professional development training annually, and part-time staff member training hours are prorated. Management permits and encourages staff members to obtain additional professional training as deemed necessary.

The LACA has documented their own personnel policies and procedures, separate from their fiscal agent. When necessary, these policies have been updated and approved by the LACA governing board to address new concerns. Detailed job descriptions exist for all positions. The reporting structure and job descriptions are periodically updated to create a more effective entity. Staff evaluations are conducted annually by the executive director. In addition, the board performs an annual evaluation of the executive director.

The LACA is also subject to ITC Site Reviews by the Ohio Department of Education (ODE) and the Management Council – Ohio Education Computer Network (MC). These site reviews are conducted by a team consisting of an employee of the Ohio Department of Education (ODE), two current and/or former user entity administrators, two current and/or former ITC Directors, and one additional team member to provide training to subsequent teams. Approximately three to five ITC site reviews are conducted annually. The sites chosen for review are designated by the OECN Oversight Advisory Committee as approved by ODE. The guidelines and recommended procedures for these reviews are based on the Ohio Administrative Code, which cover the following areas: governance, administration, finance, personnel and staff development, physical facilities, hardware, software, user in-service, and operations. The LACA's site review was completed in December 2013.

The LACA has Service Level Agreements (SLA) with their user entities for certain computer, data processing, and applications services. The user entities agree to pay a fee based upon a fee schedule set forth by the governing board and they agree to abide by the security policies implemented by the LACA. These SLAs are re-signed every fiscal year.

Risk Assessment

The LACA does not have a formal risk management process; however, the governing board is comprised of representatives from the user entities who actively participate in the oversight of the LACA. As a regular part of its activity, the board addresses:

- New technology.
- Realignment of the LACA entity to provide better service.
- Personnel issues, including hiring, termination, and evaluations.
- Additional services provided to user entities and other entities.
- Changes in the operating environment as a result of ODE requirements, Auditor of State and other accounting pronouncements, and legislative issues.

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

Monitoring

The LACA entity is structured so that staff of the network/systems team reports to the executive director, the administrative team reports to the executive director, and the educational team reports to the executive director. The director of technology operations director reports to the executive director. The key management employees have worked for the LACA for many years and are experienced with the systems and controls at the LACA. The 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, the LACA uses a variety of "key indicator" reports to monitor the processes involved in processing transactions for user entities.

Hardware, software, network performance, database integrity, Internet usage, computer security and user help desk 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. In addition, the executive director, the director of technology, and the administrative applications manager receive the same reports and monitor them for interrelated and recurring problems.

INFORMATION AND COMMUNICATION

The aspects of the information and communication component of internal control as it affects the services provided to user entities are discussed within the IT General Control section.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

Development and Implementation of New Applications and/or Systems

The LACA staff does not perform system development activities. Instead, the LACA utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the Northwest Ohio Computer Association (NWOCA), another Information Technology Center (ITC) of the OECN. The ODE determines the scope of software development for state-supported systems. The Fiscal State Software Oversight Committee (SOC), which consists of members from the MC, the Ohio Association of School Business Officials (OASBO), the ODE and the SSDT, assists in prioritizing specific goals and objectives. The SOC meets as needed to monitor SSDT projects and provide feedback on project priorities.

Changes to Existing Applications or Systems

End-users have access to the SSDT website that contains user and technical documentation for the applications. Specific support issues or questions can be communicated to the SSDT via helpdesk software. Solutions are communicated directly to LACA staff. Global issues are posted to the SSDT support website.

The LACA personnel do not perform program maintenance activities. Instead, they utilize the applications supplied to them by the SSDT. The OECN requires the ITC to keep the version of each application current based on the provider's standard for continued support. Procedures are in place to ensure the SSDT developed applications are used as distributed. Upon notification of their availability from SSDT, ITCs obtain quarterly updates by downloading zipped files from the SSDT's download site. The source code is not distributed with these files. Release notes, which explain the changes, enhancements and problems corrected, are provided via the SSDT website. User and system manager manuals are also made available via the SSDT website with these releases. The SSDT informs the ITCs that they will support only the latest release of the state software and encourage installation within 30 days following the software release date.

The LACA 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. As a participating member of the MC, an ITC can enter into a cooperative agreement, "Campuswide Software License Grant (CSLG) and Education Software Library (ESL) Program", through the MC, for acquiring and/or providing software maintenance services for a limited series of Hewlett Packard (HP), and other supplier's, software packages as approved by the MC board of trustees.

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

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

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

- Track and maintain an accurate listing of all HP hardware and software covered under the agreement.
- Provide and maintain support on one (1) license of Process Software's Multinet TCP/IP stack for each system registered under this program.

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

- Maintain its status as a member in good standing of the MC as a qualification for participating in (or continuing to participate in) this program.
- Read, sign, and comply with the rules and regulations of the CSLG Program as operated by the MC.
- Provide unrestricted privileged access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems, distributing software, or assuring licensing compliance.
- Provide HP or MC 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 MC for services under the agreement within 30 days of the receipt of an invoice for said services.

Before new releases are installed at the LACA, a backup of the application or operating system affected by the change is prepared to ensure retention of the existing application or operating system in case of an error stemming from the upgrade process. Documentation and support for new releases of applications are provided by the SSDT. Application release notes are distributed with each quarterly release and are also available through the web site.

Documentation for the current version of the operating system and new releases are provided on the HP web site and on the operating system media. New releases include documented changes to the operating system and implementation procedures. The LACA has their own copy of the operating system disks and documentation. If an upgrade is required, they would purchase this from a third-party vendor in partnership with the MC. The LACA is able to purchase the operating system software at a reduced cost under MC. The current release documentation is maintained by the director of technology. No new releases were installed during the audit period.

IT Security

The LACA has a security policy in place that outlines the responsibilities of user entity personnel, the LACA personnel, and any individual or group belonging to neither. Additionally, the LACA uses a banner screen that is displayed before a user logs onto the system. The screen informs the user that "unauthorized use may result in denial of future privileges, revocation of access to the system and/or prosecution under the law."

The LACA grants its staff 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. Data center access is established, granted and reviewed by the executive director and no authorization form is used.

User entities are granted access through LAMA (LACA Account Management Application), a web-based workflow system for maintaining user

access. Designated administrators in the user entities enter requests for new accounts, access changes, or deletion of accounts. Each request is individually approved by the superintendent (or designee) through the LAMA web interface. If fiscal (USAS, USPS, etc) access is requested, the treasurer (or designee) will need to approve the request in LAMA as well. After a request has the required user entity-level approvals, the request is then routed into the work queue of a LACA staff member to be completed. Different members of the LACA's staff build accounts, remove accounts, or grant the access, depending on the service area (fiscal support grants fiscal access, Progress Book support grants Progress Book access, etc). After the LACA marks the request completed, the original submitter of the request receives an automated e-mail letting them know it is complete. Each quarter, a representative of each user entity is e-mailed and asked to log into LAMA to audit and confirm the listing of user accounts and assigned access rights for their user entity. The LACA requires all users with LACA accounts to agree to the LACA's Internet Acceptable Use Policy, which is also completed and tracked in LAMA.

The LACA policies and procedures are partly enforced through the use of system alarms and audits. Security alarm messages are sent to an operator terminal that has been enabled to receive security event messages. Security audit messages are sent to the audit log file; alarms are sent to the operator log file. Access to the operator log and audit log is limited to data processing personnel. Critical events should be reported as both alarms and audits; less critical events can be written to a log file for later examination. The following security alarms and security audits have been enabled through the operating system to monitor any security violations on the LACA 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:	Produces a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables auditing of changes made to the system user authorization file (UAF) or network proxy authorization file in addition to auditing changes to the rights database.
BREAK-IN:	Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS and DETACHED break-in types can be monitored.
LOGFAILURE:	Provides a record of logon failures. The BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS, and DETACHED logon failure types can be monitored.

A batch processed command procedure executes each night to extract any security violations from the operator log and places them in a file for subsequent review by the executive director. The report contains information on unsuccessful logon attempts and any use of the AUTHORIZE command, which is used to modify the user authorization file. The SYSTEM account owns the command procedure and only users with system privileges can access the command procedure or file.

The LACA is currently using Trend Micro antivirus software. They use anti-virus software in conjunction with Mail Marshall (spam e-mail filtering software) on two network servers to scan all inbound and outbound e-mail. Anti-Virus definitions are automatically updated on network servers and individual PC's. If a virus is found, the e-mail is discarded and logged.

The LACA conducted phishing exercises internally and among districts they support.

Primary logical access control to the HP computers is provided by security provisions of the operating system. This includes access to data,

programs and system utilities. When a user logs in to use the system interactively, or when a batch or network job starts, the operating system creates a process that includes the identity of the user. The operating system manages access to the process information using its authorization data and internal security mechanisms.

The LACA utilizes proxy logins for local administration of the Web Server only. The LACA does not allow proxy logins to remote systems. 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. Proxy records are located in the proxy file.

A User Identification Code (UIC) is individually assigned to all data processing personnel employed at the LACA. All user entities are assigned a group UIC and each user within that user entity is assigned unique UIC. The UIC is assigned at the request of the user entity. UIC based protection controls access to objects such as files, directories, and volumes.

Certain limited-access accounts require a less restrictive environment than captive accounts. Accounts, under which network objects run, for example, require temporary access to the command line. 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 CAPTIVE flag is used for all user accounts not belonging to the LACA staff or the system.

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

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

The system forces users to change their passwords periodically. All interactive UIC accounts have a specified password lifetime. The student applications manager sets passwords to expire when a new user identification code is issued or when a user has forgotten his password. This parameter requires the user to create a unique password when they first logon. Supervisors are notified via e-mail of the user account and the status of the password field. The minimum password length for each user has been established.

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 connection is terminated.
- 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 executive director and director of technology.

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

An Access Control List (ACL) may be associated with each object recognized by the operating system. When an access request is made to an object, ACLs are always checked first, which either grants or denies 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 the MAXSYSGROUP number. (2) Users with system privileges. (3) Users with group privileges whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

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

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

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

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

Certain privileges can override all UIC-based and ACL protection. The operating system analyzes privileges included in the user's authorization file record and places the user in one of seven categories depending on which privileges have been granted to the user. Default privileges are those authorized privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login, and must be enabled or disabled by the user. All user entity users have NORMAL privileges.

Access to the OECN software packages is controlled at the ITC level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate 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 and SAAS/EIS application data files.

OECN_SYSMAN is an identifier which grants access to all packages. The OECN_SYSMAN identifier grants the user the same access as OECN_USPS, OECN_USAS, etc., for all packages without having to grant each individual identifier. The identifier is defined by state software so it works the same for all ITCs. The identifier grants access to software functions inside the software. It does not grant access to data. Only the LACA staff has this identifier.

The write and delete access capabilities are not activated for WORLD access to the files in the system directory. The UIC associated with each of these files is within the MAXSYSGROUP number. To limit access to security files, the LACA 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.

A firewall and additional routing devices have been placed between the Internet access provided by the OECN network and the two segments of the internal 10-dot network used by the LACA and its user entities. To allow for LACA IP traffic to flow to the Internet, a firewall has been installed at the gateway to the Internet. The firewall has been configured to assign the 10-dot internal network addresses to a true IP Internet address.

The LACA is located on the third floor of an office building. The doors to LACA's office areas are locked and data center personnel are present at all times. Access to LACA's office area requires a key fob. Visitors must push a button to call a staff member to gain access. The computer room is located on another floor of the building. A keyed lock secures the computer room itself; only the LACA staff and the maintenance personnel have access. The building is always locked, with the exception of the main entrance doors. A building receptionist is located at the main doors to direct visitors to the proper location. In addition, motion detectors and an alarm system are armed to detect unauthorized access to the building.

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

- Smoke detectors.
- Halon fire extinguishers.
- Sapphire fire suppression system.
- Liebert environmental system.
- Humidity and temperature sensors.
- Un-interruptible power supply (UPS).

- Sprinkler system.
- Transfer switch and natural gas generator.

IT Operations

Traditional computer operations procedures are minimal because users at the user entities initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All the LACA employees have a procedures manual, which provides directions and guidelines for most of the operational functions performed. They also have access to operations procedure manuals for the Alpha systems.

Certain routine batch jobs can be initiated at the LACA for system maintenance and security monitoring. All daily processes that are run by the LACA are scheduled through a scheduler. This utility runs a list of periodic batch jobs scheduled by the executive director.

The LACA prevents file or data corruption with several programs that are run automatically through the scheduler procedure. This procedure is programmed to be re-submitted automatically each day. The purpose of these programs is to ensure the integrity of user entity files.

Hardware maintenance agreements exist with Service Express, Presidio, and MC; all are paid annually. The agreement with Presidio provides for hardware maintenance of the LACA routers and switches. The agreement with the MC is for the STORServer. In addition, all data processing equipment is covered under an insurance policy.

The LACA documents personnel authorized to make changes to user entity data through the completion of individual Fiscal Authority Change Forms. The form states authorized users have the authority to authorize the LACA staff to make specific changes to user entity fiscal data under the contracting service applications of the respective user entity. Requests for changes are to be made via fax or email prior to changes being made. The written requests are then maintained in the user entity's file.

The LACA performs full system backups daily, Sunday through Saturday. Daily backups for the system are maintained for at least four weeks. Backups are performed nightly to an off-site StorServer housed by the MC. All data required by law to be maintained for a specific duration is maintained by the LACA. Calendar year and fiscal year end information is stored indefinitely for all the LACA user entities. Periodic restores of data are performed at the request of the user entities. These restores are generally requested via the helpdesk when data has been accidentally deleted or due to user error. Annual restores of data are performed by the executive director using the MC Disaster Recovery site hardware, and are documented by the MC DR Restore Validation document.

User entities are responsible for handling abnormal terminations. If the users cannot solve the problem, they will contact the LACA. The executive director, the director of technology and the network coordinator handle the majority of service calls from the user entities for problems with the network. The executive director, student applications manager, and the administrative applications manager handle the majority of service calls from user entities for problems with the system.

COMPLEMENTARY USER ENTITY CONTROLS

LACA's controls related to its Information Technology General Controls (ITGC) System only cover a portion of overall internal control for each user entity of LACA. It is not feasible for the control objectives related to the ITGC System to be achieved solely by LACA. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with LACA's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified under each control objective below, where applicable. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.
1. User entities should maintain current service level agreements with LACA for USAS, USPS, SAAS, and technical support.

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.
1. User entities should have controls over their own web applications which access their data stored at the LACA. 2. User entity management should have practices to ensure users are aware of the confidential nature of passwords and the precautions necessary to maintain their confidentiality. 3. User entity management should immediately request the LACA to revoke the access privileges of user entity personnel when they leave or are otherwise terminated. 4. User entity management should complete requested user confirmations. 5. User entities should have documented acceptable use policies to define the activities deemed appropriate for use of the Internet. Internet users should be required to accept the terms of the policy before access is provided. 6. User entity management should participate in cyber awareness training offered by the LACA.

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

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.
1. PCs and terminals should be protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals. 2. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.

IT Operations - *Control Objective:* **Backup -** Up-to-date backups of programs and data should be available in emergencies.
1. User entities should retain source documents for an adequate period to ensure data can be re-entered in the event that data files are destroyed prior to being backed up and rotated off-site. 2. User entities should establish and enforce a formal data retention schedule with the LACA for the various application data files.

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

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

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

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.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

Changes to Existing Applications and Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
In order to maintain continued support of the application software provided by the SSDT, ITCs are encouraged to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) checksum of the USAS, USPS, OECN, and SAAS object files at LACA was compared to the CRC checksum of the object files released by the SSDT.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals for the applications are also provided on the SSDT web site.	Inspected the release notes and updated manuals available on the SSDT website for the most recent release to confirm that all current documentation is provided to the LACA. Confirmed that installation procedures, explanation of changes, enhancements, and/or corrections are documented and communicated to the LACA.	No exceptions noted.
Documentation for the current version of the operating system and new releases are provided on the HP web site.	Inspected online documentation to confirm the LACA is provided with the most current documentation for the operating system.	No exceptions noted.

IT Security

IT Security - *Control Objective:* **Security Management -** Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The LACA has established policies and procedures regarding computer security and access for its staff and user entities. Acceptance of the policies is enforced in the Service Level Agreements (SLA).	Inspected the LACA security policies and inquired with the executive director about methods of its communication to users and sign-off requirements.	No exceptions noted.
LAMA is used to request new user account access and must be completed by an authorized user entity representative before a user account can be added on the system.	Selected 8 of 66 new user accounts with identifiers for the USAS, USPS, or SAAS/EIS applications. Inspected the online account application forms for new users to confirm the online forms were authorized by the appropriate user entity management. Inspected a user entity account authorization form that is completed by the user entity stating who is authorized to request new accounts.	No exceptions noted.

IT Security - *Control Objective:* **Security Management -** Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
User accounts and access rights are confirmed quarterly with user entity management through a positive confirmation process via the LAMA application.	Confirmed the review process with the executive director. Inspected an example of the follow-up e-mail sent to the user entities requesting the account review be performed. Inspected the acknowledgement screen within the LAMA application used to confirm the account reviews were completed. Inspected the status screen to identify the user entities that had completed the quarterly account review.	No exceptions noted.
Tracking of security related events, such as break-in attempts and excessive log failures, is enabled through the operating system. The events are logged to audit journals for monitoring of potential security violations.	Inspected the security audits to confirm security related alarms were appropriately enabled.	No exceptions noted.
A procedure runs nightly to create reports that list security violations from the audit journal and e-mails the reports to the executive director for review.	Inquired with the executive director about security monitoring procedures including the process for monitoring reports and the frequency of review. Inspected the following information relating to the security monitor reports to confirm reports are produced and available for review daily: • Example of a security monitor report. • Security Monitor command procedure utilized to generate the report • Scheduler command procedure and listing.	No exceptions noted.

IT Security - *Control Objective:* **Security Management -** Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Anti-virus software runs on the servers to help protect against computer viruses. Definitions are updated daily and all viruses found are reviewed by the director of technology. Malware training was conducted to help educate employees regarding computer threats.	Inquired about anti-virus and monitoring procedures with the director of technology. Inspected the following with the director of technology to confirm an anti-virus program is utilized and updated periodically. Inspected phishing print screens to confirm malware training was performed during the audit period.	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls -** Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to not allow blanket access.	Inspected the proxy listing to confirm wild card characters are not used.	No exceptions noted.
Password parameters are in place to aid in the authentication of access to the system and agree to password policies established by the LACA.	Inspected the results of extracted information from the user authorization file to identify: • Accounts with password minimum lengths less than the established guidelines of LACA. • Accounts with password lifetimes not equal to the established guidelines of LACA.	No exceptions noted.
Password expiration for the web applications is defined at the system or process level.	Inspected the command procedure that controls password changes to confirm the use of password expiration for web applications.	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls -** Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the system login parameters to confirm parameters were set to control and monitor sign-on attempts.	No exceptions noted.
System and web application activity is monitored and inactive users are automatically disconnected after a predetermined amount of idle time.	Inspected the HITMAN parameters to confirm parameters were set for idle time and the action to be taken against inactive users. Inspected the system startup file to confirm that the HITMAN program was part of the startup procedures. Inspected the configuration for the timeout values on the USAS and USPS web system.	No exceptions noted.
Access to production data files and programs is restricted to authorized users.	Identified and inspected production data files with WORLD access and executable files with WORLD write and/or delete access.	No exceptions noted.
Firewalls and a routing system are used to control Internet traffic and maintain a logical segregation between user entities.	Inspected the network diagram from the director of technology to confirm components of the network which control internet access. Inspected the firewall and router configurations to confirm the existence of a private internal network.	No exceptions noted.
Telnet sessions are not allowed from outside the LACA network.	Confirmed the process of connecting to the system from outside of the LACA network with the executive director.	No exceptions noted.
Access to off-site backup data files and programs is restricted to authorized users.	Inspected a user listing and confirmed with the executive director that off-site backup data files and programs are restricted to authorized users.	No exceptions noted.

IT Security - *Control Objective:* **Application Level Access Controls -** Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user entity management.	Inspected a listing of all OECN identifiers for the USAS, USPS and SAAS/EIS applications to confirm the use of identifiers to segregate access to the applications. Selected 8 of 66 new user accounts with an OECN identifier to confirm the identifiers requested matched the identifiers granted.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized users.	Extracted information from the user authorization file to identify user accounts having the OECN_SYSMAN identifier to confirm only appropriate users were assigned the identifier.	No exceptions noted.

IT Security - *Control Objective:* **System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
WORLD access to “key” system and security files is restricted.	Inspected the file protection masks on the system files to confirm WORLD write and/or delete access was absent. Inspected the file protection masks on the security files to confirm WORLD access was absent.	No exceptions noted.
System level user identification codes are restricted to authorized personnel.	Identified the maximum system group number, which defines system level privileged accounts, and inspected a listing of all accounts with a UIC less than the maximum system group number. Confirmed the appropriateness of the accounts with the executive director.	No exceptions noted.

IT Security - *Control Objective:* **System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
An alternate user authorization file is not permitted to be used and does not exist.	Inspected the value of the alternate user authorization file parameter to confirm the parameter's setting does not allow for the use of an alternate user authorization file. Inspected the system directory listings to confirm an alternate user authorization file does not exist.	No exceptions noted.
Remote access to firewall and router configurations used to control Internet access is restricted through password protection.	Inspected the firewall and router configurations to confirm passwords were required to access the configuration menus and to confirm remote administration was permitted. Inquired with the executive director to confirm firewall password policies were in place.	No exceptions noted.
Individual user profiles are used to grant access rights and privileges in accordance with LACA policy.	Extracted information from the user authorization file to identify user accounts with elevated privileges and confirmed the appropriateness of the listed accounts with the executive director.	No exceptions noted.

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Physical access to the computer room, building, and office area is restricted to authorized personnel.	Inspected the computer room key locked door to confirm access is restricted to authorized personnel. Inspected the office area key fob locked door to confirm access is restricted to authorized personnel. Observed that all visitors are required to enter through the main entrance of the building and check in with the front desk staff.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, humidity, changes in temperature, or power failures.	Observed with the executive director, the existence of environmental controls over the computer system. Inspected the Liebert system (power, temperature and humidity monitoring), natural gas generator, and observed the existence of smoke detectors and fire extinguishers.	No exceptions noted.
The LACA has a generator and Un-Interruptible Power Supplies (UPS) to maintain power in the event of a power outage.	Inquired about use of the generator and UPS with the executive director to confirm power could be supplied to keep the system running in the event of a power outage. Observed the UPS in the computer room and the generator outside the LACA facility and inquired about procedures for testing the generator.	No exceptions noted.

IT Operations

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The LACA maintains hardware service support agreements with Service Express and Predisio to cover hardware maintenance and failures.	Inspected the Service Express and Predisio hardware service agreements, purchase orders, invoices, and payment histories for the audit period for evidence of coverage.	No exceptions noted.
Routine system maintenance programs, such as purging of email, reorganizing of application files, and analyzing files are scheduled and run to help prevent file failure and data corruption.	Confirmed routine system maintenance procedures with the executive director. Inspected the scheduled programs to confirm that routine system maintenance programs are automatically scheduled to execute.	No exceptions noted.
The LACA monitors network performance and hardware failures through use of IP Check. Logs of failures are reviewed and problems are fixed by appropriate personnel.	Confirmed the use of IP Check software with the executive director. Confirmed procedures for monitoring and observed real time monitoring and error resolution. Inspected e-mails that were sent to the network team when errors occurred.	No exceptions noted.
Requests for changes to user entity data files must be written and requested by personnel who are listed on the user entity's Fiscal Authority Change form. Changes to user entity files are documented and retained in the corresponding user entity's file at the LACA.	Inspected the Fiscal Authorization List maintained by LACA and an example Fiscal Authority Change form from the fiscal services coordinator. Confirmed the process authorized users follow for changing user entity data with the fiscal services coordinator.	No exceptions noted.
Data center hardware and software equipment is covered by an insurance policy.	Inspected the insurance policy and payment to confirm LACA equipment is insured in the event of a disaster.	No exceptions noted.

IT Operations - *Control Objective:* **Backup -** Up-to-date backups of programs and data should be available in emergencies.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Backups of systems and data are scheduled nightly to an off-site server in central Ohio. The backup procedure and status are monitored daily.	Inspected the following documents to confirm backups are automated, verified and monitored. • DECScheduler job listing. • Backup command procedures. • Backup log files. • Status completion reports/ • Barracuda backup schedule and logs.	No exceptions noted.
The LACA maintains a “backup as a service” agreement with the MC for the backup program license and disk space usage.	Inspected the payment documentation for the backup software license and backup storage space fee to confirm it was paid during the audit period.	No exceptions noted.
The retention and rotation of tapes is managed by the STORServer based on policies.	Inspected the STORServer retention settings to confirm they adhere to the LACA data retention policy.	No exceptions noted.
Backups are tested on an annual basis as part of the disaster recovery services agreement.	Inspected the confirmation from the MC stating the LACA was able to restore data from the MC DR facility.	No exceptions noted.

SECTION 5 - OTHER INFORMATION PROVIDED BY LACA *(Unaudited)*

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name:	Licking Area Computer Association (LACA)
Number:	8
Node Name:	LACA
Chairperson:	Trevor Thomas Superintendent Heath City School District
Fiscal Agent:	Career and Technology Education Centers of Licking County (C-TEC)
Administrator:	Chad Carson Executive Director LACA
Address:	150 S. Quentin Road Newark, OH 43055
Telephone:	740-345-3400
FAX:	740-345-3427
Website:	www.LACA.org

OTHER SITE STAFF

Mary Myers	Administrative applications manager
Patricia Zelei	Fiscal service coordinator
Kari Snyder	Fiscal service coordinator
Joey Alexander	Director of technology
Dean Reineke	Director of operations
Charles Gillogly	Technical services coordinator
David Stein	Video services manager
Robert Rittenhouse	Network coordinator
Jonathan Stoehr	Network coordinator
Jerry Eby	Student applications manager
Annie Epperson	Student services support coordinator
Trish Baker	Media resource coordinator
Meghan Stoker	Student services support coordinator
Elizabeth Petty	Student services support coordinator
Leanne Phillips	Administrative assistant
Melissa Elliott	Instructional resource coordinator

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

	Model Number	Installed	Capacity/Density/Speed
CPU:	HP Alphaserver ES45 68/1250 (4CPU)	Lines/Ports : N/A	Memory Installed: 16GB (production unit)
	HP Alphaserver ES45 68/1250 (2CPU)	Lines/Ports: N/A	Memory Installed: 8GB (failover unit)
Disk:	EVA4400 SAN	Units: 1	Total Capacity: 24 TB

USER ENTITY SITE DATA								
			STATE SOFTWARE				eFinancePLUS[(a)]	
IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS	OTHER*	Financial	Payroll
019752	Lancaster CSD	Fairfield	X	X	X	X		
011439	Renaissance Academy	Franklin	X	X				
044420	Mount Vernon CSD	Knox	X	X	X	X		
045393	Granville EVSD	Licking	X	X	X	X		
044115	Heath CSD	Licking	X	X	X	X		
047985	Johnstown Monroe LSD	Licking	X	X	X	X		
047993	Lakewood LSD	Licking	X	X	X	X		
047977	Licking County ESC	Licking	X	X	X	X		
043927	Career and Technical Center of Licking County	Licking	X	X	X	X		
048009	Licking Heights LSD	Licking				X	X	X
044453	Newark CSD	Licking	X	X	X	X		
048025	North Fork LSD	Licking	X	X	X	X		
058033	Northridge LSD	Licking	X	X	X	X		
045278	Southwest Licking LSD	Licking	X	X		X		
000162	Newark Digital Academy	Licking	X		X	X		
000941	Par Excellence Academy	Licking	X	X		X		
044388	Medina CSD	Medina	X	X	X	X		
048835	East Muskingum LSD	Muskingum	X	X	X	X		

USER ENTITY SITE DATA								
			STATE SOFTWARE				eFinancePLUS[(a)]	
IRN	**USER ENTITY**	**COUNTY**	**USAS**	**USPS**	**SAAS**	**OTHER***	**Financial**	**Payroll**
149328	Foxfire High School	Muskingum	X		X	X		
012033	Foxfire Intermediate School	Muskingum	X		X	X		
045450	Maysville LSD	Muskingum	X	X	X	X		
048876	Tri-Valley LSD	Muskingum	X	X	X	X		
048884	West Muskingum LSD	Muskingum	X	X	X	X		
045351	Crooksville EVSD	Perry	X	X	X	X		
TOTALS			**23**	**20**	**20**	**23**	**1**	**1**

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

“eFinancePlus” – User Entity uses financial services other than State Software, from WOCO which provides Tier 1 support, and the controls are not tested as part of the LACA SOC 1 Report. Use WOCO’s SOC 1 report for eFinancePLUS application software.