OHIO AUDITOR OF STATE
KEITH FABER

TABLE OF CONTENTS

This Page Intentionally Left Blank

OHIO AUDITOR OF STATE
KEITH FABER

65 East State Street
Columbus, Ohio 43215
(614) 466-3402 or (800) 443-9275
StateRegion@ohioauditor.gov

Independent Service Auditor's Report

Board of Directors
Western Ohio Computer Organization (WOCO)
129 East Court St.
Sidney, Ohio 45365

To Members of the Board:

Scope
We have examined management of WOCO's description of its Information Technology General Controls (ITGC) System for processing user entities' transactions for the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), Inventory, and eFinancePLUS applications throughout the period April 1, 2023 to March 31, 2024, included in section 3, "Management of WOCO Service Organization's Description of Its ITGC System" (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Management of WOCO's Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of WOCO believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the ITGC System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in section 5, "Other Information Provided by Management of WOCO" is presented by management of WOCO to provide additional information and is not a part of management of WOCO's description of its system made available to user entities during the period April 1, 2023 to March 31, 2024. Information about WOCO's ITC Profile including site data, other site staff, and user entity site data, has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

WOCO uses the Management Council (MC), a subservice organization, to provide hosting and managed support for the user entity transactions of the eFinancePLUS vendor application system provided by PowerSchool. The MC has an eFinancePLUS Update Subscription Service ("USS") that updates the instance(s) to the latest monthly, compliance, year-end, and annual releases of eFinancePLUS. The USS includes unlimited monthly updates to existing eFinancePLUS server(s) and includes upgrades to new annual releases. The description includes only the control objectives and related controls of WOCO and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by WOCO can be achieved only if complementary subservice organization controls assumed in the design of WOCO's controls are suitably designed and operating effectively, along with the related controls at WOCO. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of WOCO's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities
In section 2, WOCO has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. WOCO is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period April 1, 2023 to March 31, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations
The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or

operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

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

Opinion
In our opinion, in all material respects, based on the criteria described in management of WOCO's assertion

a. the description fairly presents the ITGC System that was designed and implemented throughout the period April 1, 2023 to March 31, 2024.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2023 to March 31, 2024 and subservice organization and user entities applied the complementary controls assumed in the design of WOCO's controls throughout the period April 1, 2023 to March 31, 2024.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2023 to March 31, 2024 if complementary subservice organization and user entity controls assumed in the design of WOCO's controls operated effectively throughout the period April 1, 2023 to March 31, 2024.

Restricted Use
This report, including the description of tests of controls and results thereof in section 4 , is intended solely for the information and use of management of WOCO, user entities of WOCO's system during some or all of the period April 1, 2023 to March 31, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Keith Faber

Keith Faber
Auditor of State
Columbus, Ohio

August 5, 2024

This Page Intentionally Left Blank

WOCO
Western Ohio Computer Organization

Management of WOCO's Assertion

We have prepared the description of the Western Ohio Computer Organization's (WOCO) Information Technology General Controls (ITGC) System entitled "Management of WOCO Service Organization's Description of Its ITGC System" (description) for processing user entities' transactions for the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), Inventory, and eFinancePLUS applications throughout the period April 1, 2023 to March 31, 2024 for user entities of the system during some or all of the period April 1, 2023 to March 31, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

WOCO uses the MC, a subservice organization, to provide hosting and managed support for the user entity transactions of the eFinancePLUS vendor application system provided by PowerSchool. The MC has an eFinancePLUS Update Subscription Service ("USS") that updates the instance(s) to the latest monthly, compliance, year-end, and annual releases of eFinancePLUS. The USS includes unlimited monthly updates to existing eFinancePLUS server(s) and includes upgrades to new annual releases. The description includes only the control objectives and related controls of WOCO and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by WOCO can be achieved only if complementary subservice organization controls assumed in the design of WOCO'S controls are suitably designed and operating effectively, along with the related controls at WOCO. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of WOCO's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

a) the description fairly presents the ITGC System made available to user entities of the system during some or all of the period April 1, 2023 to March 31, 2024, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The WOCO service organization has a vendor relationship with the State Software Development Team (SSDT) who are employed through the MC and uses the USAS, USPS, and Inventory application software as provided by the SSDT. The criteria we used in making this assertion were that the description:

   i) presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

      1) the types of services provided, including, as appropriate, the classes of transactions processed.

      2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

      3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the

correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

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

5) the process used to prepare reports and other information for user entities.

6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii) includes relevant details of changes to the service organization's system during the period covered by the description.

iii) does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the ITGC System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b) the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period April 1, 2023 to March 31, 2024, to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of WOCO's controls throughout the period April 1, 2023 to March 31, 2024. The criteria we used in making this assertion were that

i) the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii) the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

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

D. D. Wall

Donn Walls, Executive Director
Western Ohio Computer Organization (WOCO)

SECTION 3 – MANAGEMENT OF WOCO SERVICE ORGANIZATION'S DESCRIPTION OF ITS ITGC SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

WOCO's control objectives and related controls are included in section 4 of this report, "Management of the WOCO service organization's description of its control objectives and related controls, and the 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 WOCO's description of controls.

OVERVIEW OF OPERATIONS

WOCO is one of 17 governmental service organizations serving approximately 1,100 educational entities and 1.8 million students in the state of Ohio. These service organizations, known as Information Technology Centers (ITCs), and their users make up the Ohio Education Computer Network (OECN) authorized pursuant to Section 3301.075 of the Revised Code. Such sites, in conjunction with the Ohio Department of Education and Workforce (ODEW), 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 WOCO is derived from the state of Ohio and from user fees.

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

State Software Development Team (SSDT):

- Uniform School Accounting System (USAS).
- Uniform Staff Payroll System (USPS).
- Inventory

PowerSchool:

- eFinancePLUS (eFP)

Subservice Organization

WOCO offers PowerSchool's eFinancePLUS application as an alternative to the state software provided by the State Software Development Team (SSDT). WOCO uses the Management Council (MC), a subservice organization, to provide hosting and managed support for the user entity transactions of the eFinancePLUS vendor application provided by PowerSchool. The MC has an eFinancePLUS Update Subscription Service ("USS") that updates instance(s) to the latest monthly, compliance, year-end, and annual releases. The USS includes unlimited monthly updates to existing server(s) and includes upgrades to new annual releases. WOCO is responsible for providing Tier 1 support to users of the application system. Tier 1 support involves establishing user accounts on Active Directory (AD) and assigning roles and permissions within the application to appropriate user entity personnel. WOCO fiscal support provides assistance with the application to their user entities and escalates issues to PowerSchool for anything they are unable to resolve.

The description in section 3 and the control objectives in section 4 include only the control objectives and related controls of WOCO and exclude the control objectives and related controls of the MC and PowerSchool's USS.

ITCs are organized as either consortia under ORC 3313.92 or Council of Governments (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. WOCO is organized under ORC 167 and is not required to have a board of education serve as its fiscal agent.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and WOCO board of directors. One member from each member user entity is appointed to the legislative body known as the organization assembly and is normally the user entity superintendent. The assembly meets once a year and is responsible for electing the board of directors, approving new cooperative ventures, the annual budget, the basic fee schedule, and amendments to WOCO's constitution.

The board of directors is the governing body of WOCO and is composed of the superintendent of the fiscal agent, two superintendents from each of the counties within WOCO's service area, one representative each from the treasurer and student service users, one non-voting independent user entity representative and a chartered school member representative. The board meets bimonthly beginning in August of each fiscal year and at other times as deemed necessary. The board has also established several advisory committees to assist in the operation of WOCO and its programs.

WOCO employs a staff of 16 individuals including the executive director and is supported by the following functional areas:

School Accounting System: Facilitates the implementation and operation of fiscal services and provides user training and support for the USAS, USAS and eFinancePLUS applications.

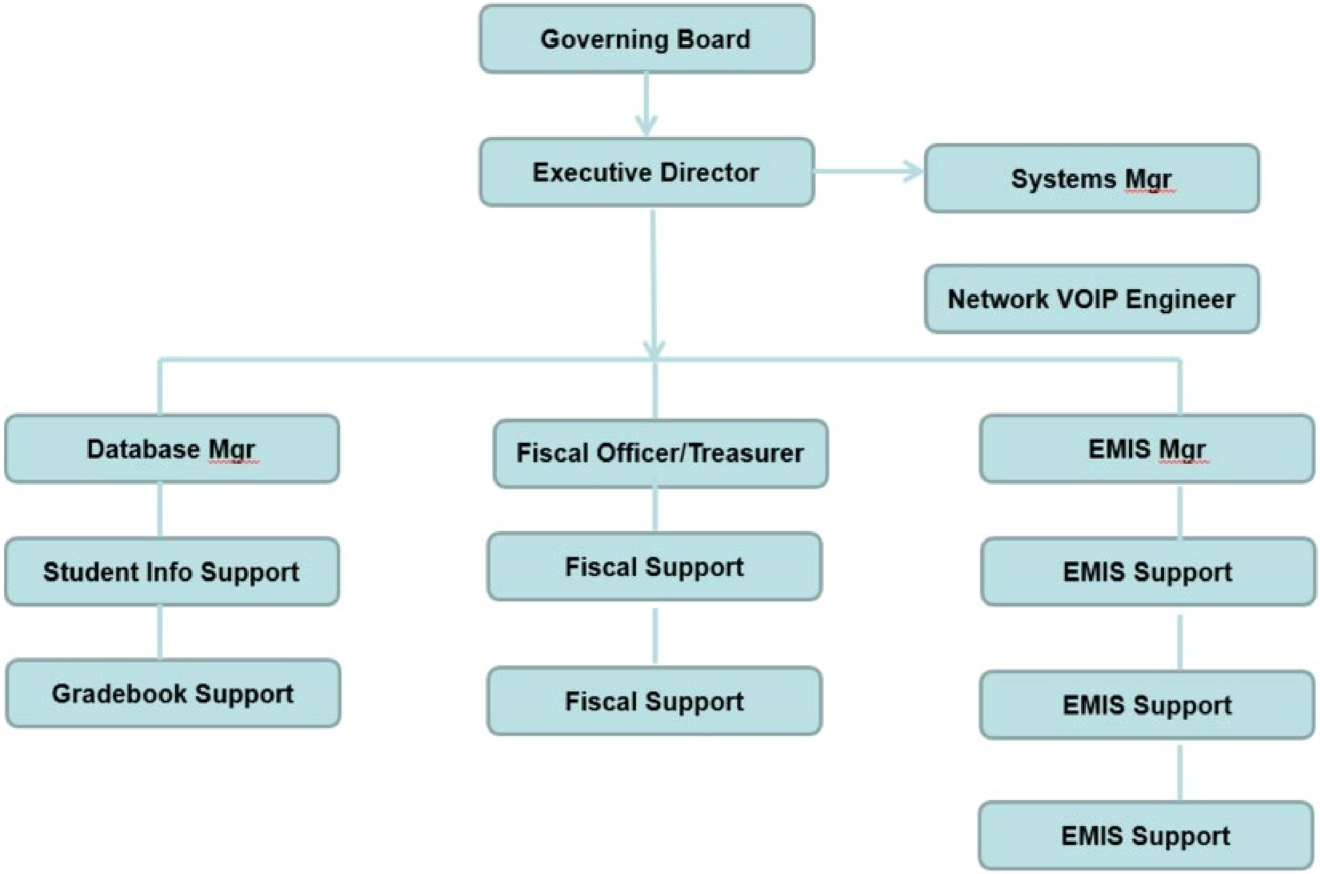
Staff Payroll Systems: Facilitates the implementation and operation of fiscal services and provides user training and support for the USPS, USPS and eFinancePLUS applications.

EMIS Services Support: Provides support for the SAAS/EIS application including archival and retrieval of data, data-entry, data processing, data import/export, equipment inventory, vehicle inventory, GAAP reporting, fixed asset accounting, and year-end processing.

Technology: Provides a variety of educational technology services to subscribing WOCO user entities including software and Internet access, training, technology planning, content filtering, firewall configuration, DNS services and technical assistance.

Student Services Support: Provides end user support and training for WOCO user entities for student software application.

WOCO Organization Chart



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

WOCO is generally limited to recording user entity 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 new employee orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced employees may alter user data and only at the request of the user entity.

WOCO follows the same personnel policies and procedures adopted by their Governing Board. Detailed job descriptions exist for all positions. WOCO 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.

WOCO's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree in a computer-related field, and all WOCO staff members are required to attend professional development and other training as a condition of continued employment. In addition, management encourages staff members to obtain additional training by providing a tuition reimbursement program for approved college work, and by paying 100% of incurred costs in attending professional development seminars. Employee evaluations are conducted annually.

WOCO is also subject to ITC Site Reviews by the MC on behalf of the ODEW. These site reviews are conducted by a team consisting of three current employees of the MC and three current ITC Directors or other ITC administrative personnel. Four ITC site reviews are typically conducted annually, following a pre-determined schedule to review each ITC at least once every five years. The overall five-year schedule and any yearly adjustments are directed and approved by ODEW. WOCO's last site review was completed in 2018.

Risk Assessment

WOCO does not have a formal risk management process; however, the board of directors comprises representatives from the user entities who actively participate in the oversight of WOCO.

As a regular part of its activity, the board addresses:

- New technology.
- Realignment of WOCO organization 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 ODEW requirements, Auditor of State and other accounting pronouncements, and legislative issues.

In addition, WOCO 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 Controls" section of this report.

Monitoring

WOCO organization is structured so that department managers report directly to the executive director. Key management employees have worked here for many years and are experienced with the systems and controls at WOCO. WOCO 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, WOCO uses a variety of "key indicator" reports to monitor the processes involved in processing transactions for user entities.

Hardware, software, network, database integrity, internet usage, computer security and user help desk reports are monitored on an ongoing basis by departmental management. Some of these reports are automatically run through a scheduler program and sent to management via e-mail.

Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the technology manager receives the same reports and monitors for interrelated and recurring problems.

Monitoring of the Subservice Organization

WOCO uses the MC, a subservice organization, to provide hosting and managed support for the user entity transactions of the eFinancePLUS vendor application provided by PowerSchool. The MC receives services and support from PowerSchool's USS to maintain the eFP application.

WOCO management and its fiscal staff monitor the work performed by the MC on a regular basis. WOCO executive director, along with other ITC directors, participate in approximately nine meetings and retreats per year sponsored by the MC to discuss current MC operations. WOCO fiscal staff monitors the MC community portal for the eFinancePLUS application to monitor customer complaints and other updates related to eFinancePLUS. The MC provides reports to WOCO fiscal staff showing inactive AD accounts; disabled accounts and roles assigned to each user.

INFORMATION AND COMMUNICATION

The aspects of the information and communication component of internal control as they affect the services provided to user entities are discussed within the IT General Controls section.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

WOCO Environmental Overview

WOCO offers two financial application systems to their user entities: State Software (USAS, USPS and Inventory) and eFinancePLUS by PowerSchool. The eFinancePLUS application is hosted on servers provided by the MC. The MC receives services and support from PowerSchool's USS to maintain the eFP application.

WOCO user entities choose whether to use either of the two state software systems or the eFinancePLUS software.

Acquisition and Implementation of New Applications or Systems (State Software)

WOCO staff do not perform system development activities. Instead, WOCO utilizes the software developed and supplied by the SSDT. .

The ODEW determines the scope of software development for state-supported systems. The State Software Steering Committee (SSSC)—which consists of members from the MC, the Ohio Association of School Business Officials (OASBO), user entity treasurers, ITC directors and fiscal staff, the ODEW and the SSDT—assists in prioritizing specific goals and objectives. The SSSC meets quarterly and has working groups focused on prioritization, report creation, support, training and documentation that meet monthly.

Changes to Existing Applications and Systems (State Software)

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 WOCO staff. Global issues are posted to the SSDT support website.

WOCO 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. Nightly procedures run on the host to update the State Software. 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.

Before software updates are installed at WOCO, 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.

IT Security (State Software)

WOCO has a computer network and Internet acceptable use policy that outlines the responsibilities of user entity personnel, WOCO personnel, and any individual or group not belonging to the user entity or WOCO.

Authorization from appropriate user entity management is required before setting up an account for the State Software applications. New user access will be granted upon an email or helpdesk ticket from the user entity treasurer, until a proper account request program or form can be developed.

WOCO staff and user entities authenticate through Lightweight Directory Access Protocol (LDAP) to access the State Software applications via a secure site login. Only WOCO staff have access within the application for user entity support. LDAP account policies have been set and Admin access to LDAP policies is limited to WOCO staff. There is one administrative account and a few service accounts that authenticate locally in the application. For these accounts password parameters governing minimum password length and complexity have been established as well as authentication break-in and detection rules. The administrative access is limited to WOCO staff at the application, virtual host, network, and operating system levels.

Detection control alerts are enabled through Microsoft AD audit policies to automatically track security related events such as excessive login failures and unauthorized change attempts at the network level.

Kerberos has been turned on and used to authenticate user access in the WOCO Active Directory. All settings have been defined and are in line with the "best practices" available from Microsoft.

The SIEM tool, Vijilan, is utilized by monitoring logs for the State Software servers, endpoint security, Vcenter, and AD, and various network elements. Vijilan analyzes the various logs to identify trends and escalate items for WOCO to investigate. The tool is configured to send notifications to the systems manager for investigation.

WOCO utilized and enforced the State software two-factor authentication setting for user accounts. WOCO required all accounts to have two-factor authentication, except for those accounts with a role of: "Read Only" or "Requisition Only". For required accounts, the user is forced to utilize Cisco DUO to log in and authenticate to LDAP.

Access to the Internet has been provided to the user entities of WOCO. Access is provided through the Ohio K-12 network via the Ohio Academic Resources Network (OARnet) and is routed to WOCO. WOCO utilizes Sophos Anti-Virus software on the servers to scan all inbound and outbound e-mail.

InfosecIQ by TechGuard cybersecurity training was made available to WOCO and its user entities via the MC.

Through a firewall and router, user entities have been set up with sub-networks that have addresses not recognizable to the Internet, known as a private internal network. The firewall and router also prevent all outside connections from accessing inside hosts or servers, unless the IP address originated from inside the network or the user entity requests certain access to their network from outside (i.e. HTTP, and e-mail, etc.). Remote access to the firewall and network equipment is restricted through password protection. Additionally, passwords are encrypted in the devices' configurations. WOCO has a threat detection engine running on the firewall that covers all downstream servers.

WOCO staff use an internal wireless access point to provide a convenient means of access to the network. Wireless traffic is encrypted from point to point within the building. Access to the wireless device configuration is controlled through password protection.

WOCO's computer room is located in the Shelby County Annex in Sidney. The door to the computer room always remains locked. The main doors to the building are locked during non-business hours. WOCO's offices are located on the first floor and basement of the same building. There are two entrances into WOCO's offices. Both doors are locked and use a keypad for entry as does the computer room.

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

- A Cummins diesel generator supplies power in the event of an outage
- Halon fire extinguishers.
- Leibert system to monitor temperature and humidity.
- Raised flooring.
- Power distribution device to prevent power surges to any of the equipment in the computer room.
- Un-Interruptible Power Supplies ensure the system will continue to operate in the event the power fails.
- Smoke detectors.

IT Operations (State Software)

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.

Certain routine jobs are initiated for system maintenance. WOCO is responsible for operational maintenance tasks, such as system backups, cleanup of files, security, and other maintenance directed at the whole system. These tasks are performed by Cron – the Linux task scheduler.

WOCO utilizes software to monitor network performance and hardware failures. The application pings the network hardware continuously to see each if each device responds. If a device fails to respond, the software indicates a failure and an alert is sent to the systems manager for resolution.

Common problems that arise daily, are usually handled by WOCO service representatives over the phone. Critical problem aspects from the console log, such as system failures, are reviewed periodically by the systems manager.

WOCO has a network maintenance contract with Logicalis for the communication connections to the user entities.

Full system backups are performed daily for the computer system. Backups are stored on-site via local disk, off-site on the 2nd floor of US Bank in a locked cabinet, and off-site at the MC's Datacenter located at the State of Ohio Computer Center All data required by law to be maintained for a specific duration is maintained by WOCO. Calendar year and fiscal year-end information is stored indefinitely for all WOCO user entities. WOCO's data processing equipment is covered under an insurance policy.

Acquisition and Implementation of New Applications or Systems (eFinancePLUS)

WOCO contracts with the MC for hosting of the eFinancePLUS application system. Frequent planning, conversion, and training meetings are held over the phone, via webinar, and on-site between PowerSchool, WOCO personnel, and applicable user entity staff during implementation of the eFinancePLUS application system.

Project management of the eFinancePLUS application implementation process is guided by PowerSchool. A calendar/implementation tracking spreadsheet is used to communicate progress and milestones required to complete the conversion.

WOCO personnel and applicable user entity staff members review the accuracy of the eFinancePLUS data conversion before live implementation. User entity staff members are required to approve the accuracy of the eFinancePLUS data conversion with PowerSchool and WOCO staff.

Training meetings are conducted on-site and via webinar by PowerSchool to acquaint WOCO personnel and applicable user entity staff with the eFinancePLUS application. End users also have access to the website that contains user and technical documentation for the application. Specific support issues or questions can be communicated via helpdesk software. WOCO provides Tier 1 support for users and are responsible for escalation of issues and or questions they are unable to answer to the MC for possible solution. Solutions are communicated directly to WOCO staff. eFinancePLUS is hosted by the MC and WOCO provides Tier 1 support for the eFinancePLUS application to its user entities.

Changes to Existing Applications and Systems (eFinancePLUS)

WOCO personnel do not perform program maintenance activities for the eFinancePLUS application system. Instead, they utilize the applications supplied to them by the eFinancePLUS vendor (PowerSchool), which are hosted and maintained at the MC. Procedures are in place at the MC to ensure the PowerSchool developed applications are used as distributed. The source code is not distributed with these files.

PowerSchool personnel notify the MC personnel via email when an upgrade or a patch to the eFinancePLUS application is available. An upgrade/patch notification email is typically sent to communicate the setup information, detail of issues being corrected and the expected date and time for implementation. WOCO personnel review the timeline, and if found to be acceptable, notify user entity treasurers via email of the impending upgrade or patch. Release notes, which explain the changes, enhancements and problems corrected, are available via the PowerSchool support website and the MC community portal. The eFinancePLUS application upgrades/patches are installed by PowerSchool and the MC. Prior to any upgrade or patch, the application database is backed up in case any errors occur during the upgrade/patch process.

IT Security (eFinancePLUS)

Some user entity end users of the eFP application, as identified in section 5 below, are using their own identity provider (e.g. Google Identity, AD, Microsoft, etc) policies to gain access to the application. These user entities are responsible for setting up their own authentication method.

For all other user entities that do not use their own identity provider, WOCO uses AD Manager to create user entity network access accounts for eFinancePLUS. User entities send WOCO a help desk ticket or an email requesting the AD account be created. Users are assigned a user-id and password. Access to the MC network is restricted via this user-id and authenticating password. Password and account parameters are enforced at the network level to aid in the authentication of user access to the system. AD accounts are disabled after 180 days of inactivity through an MC defined rule in ADManager. Monthly WOCO distributes the disabled user report to user entities. Firewall and anti-virus protection is the responsibility of the MC.

All end user entities are responsible for creating the user profile within the application and assigning application access rights.

InfosecIQ by TechGuard cybersecurity training was made available to WOCO and its user entities via the MC.

IT Operations (eFinancePLUS)

Incremental and full backups of the eFinancePLUS application and database are performed by the MC. At fiscal year-end and calendar year-end an archive of each eFinancePLUS database is made by WOCO after each user entity has processed all transactions and balanced, but before accruals have been cleared. WOCO has incorporated an archival step into the user entity year end checklist that requires user entities to request an archive of the eFinancePLUS database. The archive is stored for six months by the MC.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

WOCO's controls related to its Information Technology General Controls (ITGC) System only cover a portion of overall internal control for each user entity of WOCO. It is not feasible for the control objectives related to the ITGC System to be achieved solely by WOCO. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with WOCO'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.

IT General Control Procedures (State Software)

Changes to Existing Applications and Systems - *Control Objective:*
Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.

1. User entities should have controls over their own web applications to ensure only thoroughly tested and authorized web applications are implemented.

2. User entities should maintain current service level agreements with their ITC for USAS, USPS, and Inventory 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 entity management should have practices to ensure users are aware of the confidential nature of passwords and the precautions necessary to maintain their confidentiality.

2. User entity management should immediately request the ITC to revoke the State Software access privileges of user entity personnel when they leave or are otherwise terminated.

3. 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.

4. User entity management should provide training to ensure users have the knowledge to detect cyber threats and the procedures of how to report these threats to management.

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 their ITC for the various application data files.

IT General Control Procedures (eFinancePLUS)

Changes to Existing Applications and Systems - *Control Objective:*
Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.

1. User entities should have controls over their own web applications, to ensure only thoroughly tested and authorized web applications are implemented.
2. User entities should maintain current service level agreements with their ITC for eFinancePLUS support.

IT Security - *Control Objective:*
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 entity management should have practices to ensure users are aware of the security policies of their ITC and that users take precautions to ensure passwords are not compromised.
2. User entity management should immediately notify the ITC to revoke the MC Active Directory and eFinancePLUS group access privileges of user entity personnel when they leave or are otherwise terminated.
3. 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.
4. User entity management should review eFinancePLUS application user access on a regular basis to ensure access is commensurate with current job responsibilities.
5. User entity management should respond to the monthly AD disabled report provided by the ITC.
6. User entity management should establish procedures to add/change/delete user access to the eFinancePLUS application.
7. For user entities authenticating into the eFinancePLUS application using their own identity provider policies, user entity management should establish and review authentication security event logs, such as invalid logon attempts, to detect unauthorized access attempts.
8. For user entities authenticating into the eFinancePLUS application using their own identity provider policies, password controls addressing minimum length, complexity, reuse and expiration should be enforced.
9. For user entities authenticating to eFinancePLUS application using their own identity provider policies, password lockout policies should be enforced to limit invalid logon attempts.
10. For user entities authenticating into the eFinancePLUS application using their own identity provider policies, multifactor authentication (MFA) policies should be enforced.
11. For user entities authenticating into the eFinancePLUS application using their own identity provider policies, administrative access to the identity provider software should be restricted to authorized staff.

IT Security - *Control Objective:*
Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.

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

13. User entity management should provide training to ensure users have the knowledge to detect cyber threats and the procedures of how to report these threats to management.

14. 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.

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

IT Operations - *Control Objective:*
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 help 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 ITC for the various application data files.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

The MC controls related to the hosting of the eFinancePLUS application cover only a portion of overall internal control for each user entity of WOCO. It is not possible for the control objectives related to eFinancePLUS to be achieved solely by WOCO. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with WOCO's controls and the related tests and results described in section 4 of this report, taking into account the related complementary subservice organization control expected to be implemented at the subservice organization as described below.

Management Council (MC) of the OECN
Changes to Existing Applications and Systems - *Control Objective:* Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.
1. MC is responsible for having procedures in place to notify ITC staff of impending upgrades or patches to both the Active Directory (AD) system and the eFinancePLUS application. 2. MC is responsible for having procedures in place to request changes to PowerSchool for the eFinancePLUS application.
IT Security - *Control Objective:* 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. MC is responsible for having established access control policies at the Active Directory level to ensure appropriate password policies over minimum and maximum length, password history, password complexity and password expiration have been established. 2. MC is responsible for having procedures in place to notify ITC staff of failed logon and/or account lockouts for Active Directory. 3. MC is responsible for having procedures in place to monitor access and/or changes to the application databases. 4. MC is responsible for ensuring that "delegated admin access" for ITC staff to manage ERP accounts is supported by appropriate authorization from their ITC management. 5. MC administrators are responsible for ensuring the ITC delegated admin accounts are locked down to their specific ITC organization unit (OU) consisting of only that ITC's user entities. 6. MC administrators are responsible for ensuring the application databases have been appropriately locked down within each ITC OU to ensure the appropriate segregation between each user entity. 7. MC is responsible for ensuring firewall and system logging is enabled and sufficient for their purposes. 8. MC is responsible for appropriate physical access restrictions and environmental dangers to the off-site location have been addressed.

Management Council (MC) of the OECN
IT Operations - *Control Objective:* Up-to-date backups of programs and data should be available in emergencies.
1. MC/PowerSchool is responsible for having procedures in place to backup user entity data and stores that data in a secure off-site location. 2. MC/PowerSchool is responsible for having procedures in place to monitor backups for successful completion. 3. MC/PowerSchool is responsible for having procedures in place to test backup data periodically.

SECTION 4 – MANAGEMENT OF WOCO SERVICE ORGANIZATION'S DESCRIPTION OF ITS CONTROL OBJECTIVES AND RELATED CONTROLS, AND THE INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Information Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at WOCO.

Our examination was limited to the control objectives and related controls specified by WOCO in Sections 3 and 4 of the report and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, WOCO's controls may not compensate for such weaknesses.

WOCO's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by WOCO. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by WOCO, we considered aspects of WOCO's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Test	*Description*
Inquiry	Inquiry of appropriate personnel and corroboration with management.
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control.
Reperformance	Reperformance of the control.

In addition, as required by paragraph .35 of AT-C section 205, Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

WOCO offers the following two financial application systems to their user entities: State Software (USAS, USPS, and Inventory) and eFinancePLUS by PowerSchool. The State Software applications are hosted at WOCO. The eFinancePLUS application is hosted on servers provided by the MC. MC receives services and support from PowerSchool's Updated Subscription Service (USS) to maintain the eFP application.

Testing below is designated as either State Software and/or eFinancePLUS. Testing related to eFinancePLUS (eFP) is restricted to only the controls in place at WOCO.

Changes to Existing Applications and Systems *(State Software)*

Changes to Existing Applications and Systems - *Control Objective*: **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
WOCO uses the SSDT provided cron job script to schedule a nightly run to search for updates from the SSDT's Delivery Pipeline.	Inspected the SSDT WIKI to confirm that updates are automatically implemented. Inspected the cron jobs to confirm that updates are set to automatically check for and pull updates nightly.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals are also made available.	Inspected the release notes and updated manuals for the audit period to confirm that all current documentation is provided to WOCO.	No exceptions noted.

IT Security (*State Software)*

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 appropriate user entity management was required before setting up an account for USAS, USPS, and Inventory applications.	Inspected access requests for the 22 of 153 new or modified user accounts to confirm proper authorization by the treasurer and/or superintendent.	No exceptions noted.

<table>
<tr><td colspan="3"><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 colspan="2"><i>Test Results:</i></td></tr>
<tr><td>User entities are required to confirm user accounts with a positive confirmation. Then WOCO tracks the status of the confirmation and performs any necessary follow-up communication to facilitate a response from the user entity.</td><td>Inspected the confirmations returned to WOCO for evidence that each user entity signed and returned the confirmation.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Anti-virus software runs on the servers to help protect against computer viruses.
Definitions are updated automatically and infected items are quarantined.</td><td>Inspected the anti-virus update schedule to confirm software and virus protection is being provided.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>InfosecIQ by TechGuard security awareness training was made available to WOCO and its user entities.</td><td>Inspected InfosecIQ security training report to confirm they are involved in providing training to their staff and user entities.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>System log activity is reviewed and monitored through the use of a SIEM tool.</td><td>Obtained SIEM tool screen prints to confirm that log data is being pushed to the SIEM tool for review and monitoring.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

<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>Password parameters are set for AD users and cannot be modified by the user entity.</td><td>Inspected the external password policies to confirm password policies exist for users logging on externally to AD.
Inspected the password policies to confirm password policies exist for users logging onto AD.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

<table>
<tr><th colspan="2">**IT Security -** *Control Objective:*
System Level Access Controls - Access to the computer system, programs, and data should be appropriately restricted.</th><th>***Control Objective Has Been Met***</th></tr>
<tr><td>*Control Procedures:*</td><td>*Test Descriptions:*</td><td>*Test Results:*</td></tr>
<tr><td>A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user entities.</td><td>Inspected the firewall configuration for inbound and outbound control lists with the systems manager for existence of a private internal network and to confirm well known ports are controlled.
Inspected the threat license and rule to confirm a threat detection engine was running on the firewall that covers all downstream servers.</td><td>No exceptions noted.</td></tr>
<tr><td>The wireless access point located at WOCO and used by WOCO staff is encrypted to prevent unauthorized access to the system.</td><td>Inspected the control utility screen with the systems manager to confirm the extent of the wireless component of the network and the use of encryption.</td><td>No exceptions noted.</td></tr>
<tr><td>For accounts setup to authenticate through external security settings, detection control alerts are enabled through Microsoft Windows Active Directory Audit Policies to track security related events such as break-in attempts and excessive login failures. The events are logged for monitoring of potential security violations.</td><td>Inspected the audit policies in place over the WOCO AD to confirm security related events are audited.</td><td>No exceptions noted.</td></tr>
<tr><td>Active Directory Kerberos policies have been defined to authenticate user access.</td><td>Inspected the Active Directory Kerberos policies to confirm the policies have been defined to authenticate user access.</td><td>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:*
State Software authentication default break-in detection and evasion has been enabled.	Inspected State Software rules to confirm break-in detection and evasion has been enabled and monitoring procedures are in place.	Monitoring procedures are not in place. No other exceptions noted.
Admin account and service accounts authenticate internally via the application password settings.	Inspected the user listings with the systems manager to confirm external authentication was set to false for the Admin account and service accounts. Inspected the internal password policies for each user entity to confirm password policies exist for users logging on internally.	A hard lockout is not in place for the State Software applications. No other exceptions noted.
Only WOCO staff have "user entity admin" accounts for the State Software applications.	Inspected the user lists showing admin accounts, with the systems manager, to confirm only WOCO staff have user entity admin accounts.	No exceptions noted.
WOCO utilized and enforced the State Software two-factor authentication setting for user accounts.	Inspected 22 of 806 user accounts to confirm MFA settings were in place.	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:*
Only WOCO staff has access to the Linux Docker host that houses the State Software (USAS,USPS, and Inventory).	Inspected the etc/passwd file with the systems manager to confirm only authorized users have been given access to the root account.	No exceptions noted.
Access to the VMWare Management Console is restricted to WOCO personnel.	Inspected access to the VMWare Management Console with the systems manager to confirm only WOCO staff have access.	No exceptions noted.

<table>
<tr><td colspan="3"><b>IT Security -</b> <i>Control Objective:</i>
<b>System Software and Utilities Access Controls -</b> Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.</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>Only WOCO staff have domain admin accounts.</td><td>Inspected domain admin accounts with the systems manager to confirm only WOCO staff have domain admin accounts.</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 user entities.</td><td>Inspected the firewall configuration, for inbound and outbound control lists, with the systems manager for existence of a private internal network and to confirm well known ports are controlled.
Inspected the threat license and rule to confirm a threat detection engine was running on the firewall that covers all downstream servers.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Remote access to firewall and router configurations used to control Internet access is restricted to authorized personnel and is password protected.</td><td>Inspected the firewall configurations to confirm passwords are required to access the configuration menus and to confirm remote administration is allowed.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>WOCO utilized MFA Cisco Duo to enforce two-factor authentication for remote access to the WOCO network.</td><td>Inspected the MFA Cisco Duo settings to confirm parameters were in place and set to industry standards.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>WOCO utilized MFA CISCO DUO and administrative rights are limited to WOCO staff and approved users.</td><td>Inspected the DUO admin users to confirm they are appropriate.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

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 and its contents is restricted to authorized personnel.	Toured the computer room and made inquiry regarding personnel access with the systems manager to confirm the computer room is restricted to authorized personnel.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, humidity, or changes in temperature.	Toured the computer room with the systems manager to confirm environmental controls are in place to protect against and/or detect fire, humidity, or changes in temperature.	No exceptions noted.

IT Operations *(State Software)*

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:*
Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.	Inspected the vSphere HA configuration with the system manager to confirm virtual machines on a failed host are restarted	No exceptions noted.
Data center equipment is covered by an insurance policy.	Inspected the insurance policy and payment documentation for evidence of coverage.	No exceptions noted.
The application software, SolarWinds, monitors network performance and alerts staff of hardware failures.	Inquired with the systems manager regarding detection and resolution of failed hardware problems and use of the network monitoring software. Inspected text message alerts received by the systems manager to confirm notification of hardware failures.	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:*
WOCO uses the SSDT provided cron job script to schedule and run State Software backups.	Inspected the cron job script with the system manager to confirm backups are set to run each night and have been successful. Inspected the backup log with the system manager to confirm State Software backups are stored in a secure off-site location.	No exceptions noted.
WOCO is notified upon completion whether or not a backup ran successfully.	Inspected the backup notification with the system manager to confirm WOCO is being notified whether backups ran successfully or failed.	No exceptions noted.

Changes to Existing Applications and Systems (eFinancePLUS)

Changes to Existing Applications and Systems – *(Control Objective)* Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Power School distributes release notes when application updates are released.	Inspected the release notes available for the most recent release to confirm current documentation is available.	No exceptions noted.

IT Security (eFinancePLUS)

IT Security – *(Control Objective)* Management should ensure the implementation of access control policies and procedures, 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:*
Access to create users within the AD is limited to delegated administrators.	Inspected the AD listing by ITC to confirm only authorized users can add accounts for WOCO user entities.	No exceptions noted.

<table>
<tr><td colspan="3"><b>IT Security –</b> <i>(Control Objective)</i>
Management should ensure the implementation of access control policies and procedures, 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 colspan="2"><i>Test Results:</i></td></tr>
<tr><td>InfosecIQ by TechGuard security awareness training was made available to WOCO and its user entities.</td><td>Inspected InfosecIQ security training report to confirm they are involved in providing training to their staff and user entities.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Authorization from appropriate user entity management is required before setting up an AD user account.</td><td>Inspected the help desk ticket for 22 new user accounts with the fiscal officer/fiscal support to confirm proper authorization of AD users.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>AD administrator access was restricted to authorized users.</td><td>Inspected the AD listing by ITC to confirm AD administrator accounts were appropriate.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>AD accounts are disabled after 180 days of inactivity. Monthly AD disabled reports are distributed to user entities.</td><td>Sampled 3 out of 12 monthly AD disabled reports with fiscal officer/fiscal support to confirm that disabled reports were distributed to user entities.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>eFinancePLUS application users are restricted to predefined logical access roles and resources that grant varying access.</td><td>Inspected user roles and resources to confirm users can be restricted to their defined segregation of duties.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

IT Operations *(eFinancePLUS)*

<table>
<tr><td colspan="3"><b>IT Operations</b> - Control Objective:
System Administration and Maintenance - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>WOCO requires a database archive to be completed at fiscal year-end and calendar year-end.</td><td>Inspected the help desk request and successful DB archive message with fiscal support to confirm the process for requesting and processing database archives.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

SECTION 5 - OTHER INFORMATION PROVIDED BY MANAGEMENT OF WOCO - Unaudited

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

CENTER DATA

Name:	Western Ohio Computer Organization (WOCO)
Number:	7
Node Name:	WOCOA
Chairperson:	Scott Howell Superintendent Midwest Regional ESC
Fiscal Officer/Treasurer:	Deb Meyer, Fiscal Officer / Fiscal Support
Administrator:	Donn Walls Executive Director WOCO
Address:	129 East Court Street, 1st Floor Sidney, OH 45365
Telephone:	937-498-2161
FAX:	937-497-7233
Web Site:	www.woco-k12.org

OTHER SITE STAFF

Deb Meyer	Fiscal officer/ fiscal support
Mandy Alexander	EMIS manager
Dave Bollheimer	Fiscal support
Andrew Sanford	Fiscal Lead support
Jessica Kitchen	Fiscal support
Nick Howell	Fiscal support
Julie Ellis	Database manager / Student Information Support
Mike Wagner	Systems manager
Jay Wentz	Student Information Support
Beth Shreve	Student Information Support/EMIS support
Kristen Copas	EMIS support
Pam Mohler	EMIS support
Andy Kemmer	Student Information Support
Michael Moeller	Network and voice engineer
Jon Axe	Tech support

			eFinancePLUS[a]			State Software[b]		
IRN	USER ENTITY	COUNTY	Financial	Payroll	Other[c]	USAS	USPS	Inventory
000288	Auglaize County Education Academy	Auglaize				X		
045930	Auglaize County ESC	Auglaize				X	X	X
045674	Yellow Springs EVSD (MVECA user entity)	Green	X	X				
045948	Minster Local SD	Auglaize	X	X				
045955	New Bremen Local SD	Auglaize	X	X				
045963	New Knoxville Local SD	Auglaize	X	X				
045971	Waynesfield-Goshen Local SD	Auglaize	X	X				
046193	Graham Local SD	Champaign	X	X				
046185	Madison-Champaign ESC	Champaign	X	X				
045484	Mechanicsburg Exempted Village SD	Champaign				X	X	
046201	Triad Local SD	Champaign				X	X	X
044941	Urbana City SD	Champaign	X	X				
046219	West Liberty-Salem Local SD	Champaign				X	X	X
045633	Versailles Exempted Village SD	Darke				X	X	
011324	Hardin Community School	Hardin				X		
047498	Hardin Northern Local SD	Hardin				X	X	
044172	Kenton City Schools	Hardin	X	X				
047506	Ridgemont Local SD	Hardin				X	X	
047514	Riverdale Local SD	Hardin				X	X	X
047522	Upper Scioto Valley Local SD	Hardin	X	X				

			eFinancePLUS[a]			State Software[b]		
IRN	USER ENTITY	COUNTY	Financial	Payroll	Other[c]	USAS	USPS	Inventory
043588	Bellefontaine City Schools	Logan	X	X				
048074	Benjamin Logan Local SD	Logan				X	X	X
048082	Indian Lake Local SD	Logan	X	X				
014777	Midwest Regional ESC	Logan				X	X	
051334	Ohio Hi-Point Career Center [d]	Logan	X	X				
048090	Riverside Local SD [d]	Logan	X	X				
062125	Upper Valley Career Center [d]	Miami	X	X				
049759	Anna Local SD	Shelby	X	X				
049767	Botkins Local SD	Shelby				X	X	X
049775	Fairlawn Local SD	Shelby				X	X	X
049783	Fort Loramie Local SD	Shelby				X	X	X
049791	Hardin-Houston Local SD	Shelby				X	X	X
049809	Jackson Center Local SD	Shelby	X	X				
049817	Russia Local SD	Shelby				X	X	X
044784	Sidney City Schools [d]	Shelby	X	X				
085654	West Ohio Computer Association (WOCO)	Shelby				X	X	
048611	Bethel Local Schools	Miami				X	X	X
046359	West Clermont LSD (HCC user entity)	Clermont	X	X				
044107	Hamilton City (SWOCA User Entity)	Hamilton	X	X				
047365	Northwest Local (SWOCA user entity)	Hamilton	X	X				
047381	Southwest Local (SWOCA user entity)	Hamilton	X	X				

			eFinancePLUS[a]			State Software[b]		
IRN	**USER ENTITY**	**COUNTY**	**Financial**	**Payroll**	**Other[c]**	**USAS**	**USPS**	**Inventory**
139303	Monroe Local (SWOCA user entity)	Butler	X	X				
045500	Milford Exempted Village (SWOCA user entity)	Clermont	X	X				
TOTALS:			**24**	**24**	**0**	**19**	**17**	**11**

[a] eFinancePLUS – If applicable, dates in the Financial and Payroll columns indicate the fiscal year the user entity went live on the applications

[b] State Software – If applicable, dates in the USAS, USPS and Inventory columns indicate the date the user entity went live on the applications

[c] Other – Applications used by the user entities other than State Software and eFinancePLUS

[d] User entity is authenticating into the eFinancePLUS application using their own identity provider policies as described in section 3. Applicable CUECs in section 3 apply.

OHIO AUDITOR OF STATE
KEITH FABER

WESTERN OHIO COMPUTER ORGANIZATION
WOCO SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

SHELBY COUNTY

AUDITOR OF STATE OF OHIO CERTIFICATION

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

Certified for Release 9/3/2024