Collegis, LLC

System and Organization Controls ("SOC") for
Service Organizations Report 3 (SOC 3®)

Report on the Collegis System
Relevant to Security

For the period March 1, 2019 to February 29, 2020

FGMK
ASSURANCE ▪ TAX ▪ ADVISORY

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

TABLE OF CONTENTS

Section 1

Independent Service Auditor’s Report

Identifying opportunities.
Delivering solutions.

Independent Service Auditor's Report

To the Executive Management of Collegis, LLC ("Collegis")

Oak Brook, Illinois

Scope

We have examined Collegis' accompanying assertion titled "Management's Assertion Provided by Collegis" (assertion) that the controls within the Collegis system were effective throughout the period March 1, 2019 to February 29, 2020, to provide reasonable assurance that Collegis' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Collegis is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. Collegis has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Collegis is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence

we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that controls were not effective to achieve Collegis' service commitments and system requirements based on the applicable trust services criteria; and
- performing procedures to obtain evidence about whether controls within the system were effective to achieve Collegis' service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Collegis system were effective throughout the period March 1, 2019 to February 29, 2020, to provide reasonable assurance that Collegis' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

FGMK, LLC

Chicago, Illinois
August 12, 2020

Section 2

Management's Assertion Provided by Collegis

Management's Assertion Provided by Collegis

We are responsible for designing, implementing, operating, and maintaining effective controls within the Collegis, LLC ("Collegis") system, throughout the period March 1, 2019 to February 29, 2020, to provide reasonable assurance that the commitments and system requirements relevant to security were achieved. Our description of the boundaries of the Collegis system is presented in Attachment A of this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2019 to February 29, 2020, to provide reasonable assurance that our commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Collegis' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the Collegis system were effective throughout the period March 1, 2019 to February 29, 2020, to provide reasonable assurance that our service commitments and system requirements were achieved based on the applicable trust services principle and criteria.

Collegis, LLC

Attachment A

Collegis' Description of the Boundaries of Its Collegis System

Collegis' Description of the Boundaries of Its Collegis System

Company Overview

Collegis, LLC ("Collegis," "Collegis Education," or the "Company") is an education industry services company that offers custom solutions for colleges and universities nationally. At Collegis, both our approach and our secure technology platform are rooted in the knowledge that can only come from our deep experience in higher education.

We understand the challenges institutions face to reach students, grow enrollments and, most importantly, improve student outcomes. We understand them because, for decades, we have assisted a diverse range of schools across the United States overcome those same challenges. What we learned along the way has shaped where we are today and has been instrumental in the design and delivery of our educational services and solutions.

The Collegis System

Cybersecurity continues to be a concern for higher education institutions. Security incidents within the higher education have seen year over year growth as the threats have also evolved to match the defense strategies of most technologies. The impact of a data breach includes reputation damage, productivity loss, forensic investigation, regulatory compliance, and technical support issues.

Collegis understands the importance of protecting information that is vital to the operations of higher education institutions. As such, Collegis designed the Collegis system to effectively detect and prevent security incidents. The Collegis system security follows the AICPA's "system" for SOC® reporting as:

1. Infrastructure: The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

2. Software: The application programs and IT system software that supports application

programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed inhouse, including details about whether the applications in use are mobile applications or desktop or laptop applications.

3. People: The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

4. Procedures: The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

5. Data: The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system.

The scope of this SOC 3® report includes Collegis' system components and does not include Collegis' customers' servers and endpoint devices at the campus locations.

Infrastructure

The Collegis system infrastructure includes a primary and a backup data center, both located in the U.S. The primary data center includes the server infrastructure, networking components (firewalls, routers, and switches), and data storage arrays. The backup data center contains a similar configuration. Collegis has implemented formal controls to manage this infrastructure. The Zayo data center location is restricted to authorized individuals through biometrics and key FOBs, and is further protected by video surveillance and man traps.

In addition, the Collegis system was developed with a layered security model that includes filtering technologies, internal and external next-generation firewalls, Cisco Adaptive Security Appliance ("ASA") firewalls, load balancing, and a demilitarized zone ("DMZ") at the external edge to allow traffic in and out of the public internet.

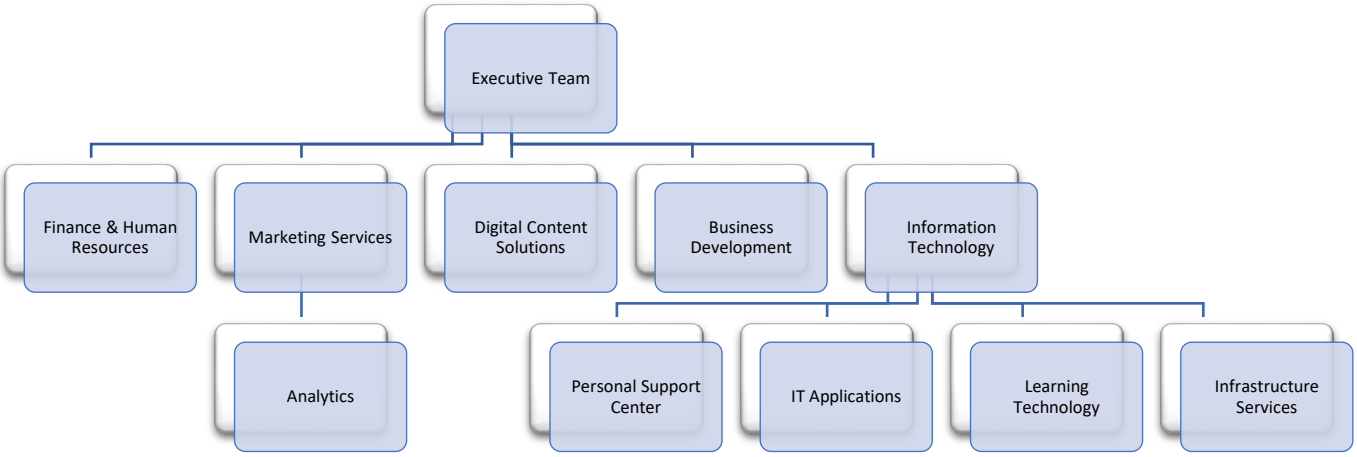
Software

Collegis uses and supports a variety of software applications to provide solutions to its customers. The Blackboard Learn and Moodle are learning management systems ("LMS") that provide educators, administrators, and learners with a single robust, secure, and integrated system to create personalized learning environments. Collegis manages and supports this application for its customers. However, Collegis is experienced with managing other LMS applications for its partners.

Collegis uses name-brand software products for networking, intrusion protection/detection, antimalware, user authentication, and monitoring of the Collegis system. Also, our system backup software is scalable and secure, and runs nightly backups using a disk-based system with backup data stored in our backup data center.

People

The Collegis system provides a framework for planning, executing, and maintaining educational business operations. Executive leadership has established an organizational structure that clearly defines each team's authorities, responsibilities and reporting lines. This structure is organized as follows:



Collegis Education follows a structured on and off boarding process to familiarize employees with the processes, systems, security practices, policies and procedures. Employees are provided with an on-boarding packet which contains the code of conduct and ethics of the organization and complete annual

security training to heighten awareness regarding current risks in IT.

Procedures

Collegis understands that an effective control environment begins at the top and permeates throughout the organization. Collegis consistently communicates the importance of internal controls during daily activities and company meetings. In addition, Collegis provides quarterly security awareness newsletters, and annual security policy training to its staff. Collegis also established processes, procedures, and controls to ensure that information relevant to the Collegis system is protected as expected by Collegis customers.

Specific examples of relevant policies and procedures include but are not limited to the following:

- Organization of Information Security
- Responsibility for Assets
- Data Classification
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- System Planning Acceptance
- Backup Policy
- Media Handling, Retention and Disposal Policy
- Exchange of Information
- User Access Management
- User Responsibilities
- Mobile Device Email Access Policy
- Incident Response and Support

Data

Collegis understands that in many cases we are stewards of our customers data. As such, the protection of our customers data is paramount. Collegis uses a distributed application architecture (“DAA”) as one of its most common development processes. Contingent on the contract arrangements, Collegis may collect, store and process all or part of an educational institution’s data.

The Moodle LMS application (otherwise referred to as “MyCourseLabs”) is an open-source application that Collegis has adopted and modified to contain very specific functions and features for its customers. The revisions (mostly theme related) made by Collegis to this application are kept within a code repository to maintain version control and is only available to a specific set of LMS engineers.

The Blackboard Learn LMS application is off-the-shelve in design. Collegis has modified and adopted this application to meet the specific needs of our customers. Revisions (mostly theme related) made by Collegis to this application are kept within a code repository to maintain version control and is only available to a specific set of LMS engineers.

Complementary User Entity Controls

Colleges' system control policies and procedures cover a majority of the overall control structure for each user. It is not feasible for the control objectives to be solely achieved by Collegis. Therefore, the use of complementary user entity controls are necessary, in combination with controls at Collegis, to provide reasonable assurance that Collegis' service commitments and system requirements are achieved based on the applicable trust services criteria.

Subservice Organization

Collegis utilizes a subservice organization to provide data center management and hosting services for the production environment of the Collegis system. This description of the boundaries of the Collegis system includes only the policies, procedures, and control activities at Collegis Education, and does not include the policies, procedures, and control activities at the subservice organization. Also, the examination by the Independent Service Auditor did not extend to the policies, procedures, and control activities at the subservice organization.

Attachment B

Principal Service Commitments and Collegis System Requirements

Principal Service Commitments and Collegis System Requirements

Collegis has designed and implemented the Collegis system components and related controls to meet our objectives and related partner requirements. These objectives are driven by our service commitments to our customers as documents and communicated through the IT service agreements, and within Collegis' policies, along with our privacy policy on our website at: https://www.collegiseducation.com/privacy.

Collegis includes formal documentation surrounding the system security commitments in individual partner agreements.

The Collegis system security commitments to our partners are standardized within our security policies, then reinforced annually with security policy training. These include, but are not limited to, the following:

- Personal and partner-provided information is secured to reduce the risk of unauthorized access, use, alteration, or disclosure and from accidental loss or corruption.
- Our websites and online services, as well as our servers, equipment, and Collegis-run networks used to store and process personal and partner-provided information, are secured.

Collegis maintains internal policies, practices, and controls designed to achieve our information security commitment to our partners, and to support the corresponding Collegis system requirements. Our Risk Management Committee meets periodically to identify risks, and to consider changes to our Collegis system and related controls as required to maintain our security over time.