Lessonly

Lessonly, Inc.

System and Organization Controls 2 Report

Report on Lessonly, Inc.'s Description of its Lessonly System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security placed in operation throughout the period of January 1, 2020 through June 30, 2020

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

themakogroup
CPAs | Advisors

Table of Contents

Section 1: Independent Service Auditor's Report

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design of Controls Relevant to Security

Lessonly, Inc.
1129 E. 16th Street
Indianapolis, IN 46202

Scope

We have examined Lessonly’s accompanying description of its Lessonly system found in Section 3 titled “Management’s Description of its Lessonly System” throughout the period of January 1, 2020 to June 30, 2020 (description) based on the criteria for a description of a service organization’s system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that Lessonly’s 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).

Lessonly uses subservice organizations to provide Cloud IaaS and PaaS for private cloud systems, managed detection and response, management of the facility network, and laptop setup and management services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lessonly, to achieve Lessonly’s service commitments and system requirements based on the applicable trust services criteria. The description presents Lessonly's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lessonly’s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization’s Responsibilities

Lessonly 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 Lessonly’s service commitments and system requirements were achieved. In Section 2, Lessonly has provided the accompanying assertion titled “Management’s Assertion Regarding its Lessonly System throughout the period January 1, 2020 to June 30, 2020” (assertion) about the description and the suitability of design of controls stated therein. Lessonly is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls 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 (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section 4, "Trust Services Principles, Criteria, Related Controls and Tests of Controls," of this report.

Opinion

In our opinion, in all material respects:

a. The description presents Lessonly's System that was designed and implemented throughout the period January 1, 2020 to June 30, 2020 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2020 to June 30, 2020 to provide reasonable assurance that Lessonly's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization applied the complementary controls assumed in the design of Lessonly's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period January 1, 2020 to June 30, 2020 to provide reasonable assurance that Lessonly's service commitments and system requirements

were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Lessonly's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4 "Trust Services Principles, Criteria, Related Controls and Tests of Controls," is intended solely for the information and use of Lessonly; user entities of Lessonly's system during some or all of the period January 1, 2020 to June 30, 2020; business partners of Lessonly subject to risks arising from interactions with the Lessonly system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

The Mako Group CPAs, PLLC

Detroit, MI
August 24, 2020

Section 2: Management's Assertion Regarding its Lessonly System throughout the period of January 1, 2020 to June 30, 2020

Lessonly

Assertion of the Management of Lessonly, Inc.

We have prepared the attached description, titled "Management's Description of its Lessonly System" (description), based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*. The description is intended to provide users with information about the Lessonly System, particularly system controls intended to meet the criteria for the security and availability principles set forth in *TSP 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria)*,* throughout the period January 1, 2020 to June 30, 2020.

Lessonly uses a subservice organization, Amazon Web Services (AWS), to perform Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and data center hosting services. The description includes only the applicable trust services criteria and related controls of Lessonly and excludes the applicable trust services criteria and related controls of AWS. The description does not extend to controls of the subservice organization.

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

a. The description fairly presents the Lessonly System throughout the period January 1, 2020 to June 30, 2020 as it relates to controls that are likely to be relevant to meeting the applicable trust services criteria. Our assertion is based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided.

(2) The components of the system used to provide the services, which are as follows:

- *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Processes.* The automated and manual procedures.
- *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

(3) The boundaries or aspects of the system covered by the description.

(4) For information provided to, or received from, the subservice organization, and other parties:

- How the information is provided or received and the role of the subservice organization and other parties.
- The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

- Complementary user entity controls contemplated in the design of the service organization's system.
- When the inclusive method is used to present a subservice organization and controls at the subservice organization.

(6) If the service organization presents the subservice organization using the carve-out method:

- The nature of the services provided by the subservice organization.
- Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organization to meet those criteria.

(7) Any applicable trust services criteria that are not addressed by a control and the reasons.

(8) In the case of a Type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description 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 report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

b. The controls stated in the description were suitably designed throughout the period January 1, 2020 to June 30, 2020 to meet the applicable trust services criteria.

c. The controls stated in the description operated effectively throughout the period January 1, 2020 to June 30, 2020 to meet the applicable trust services criteria.

Steven A Cornett

Steve Cornett
Director of Information Security
Lessonly, Inc.

Section 3: Management's Description of its Lessonly System

Overview of Lessonly Operations

Company Background

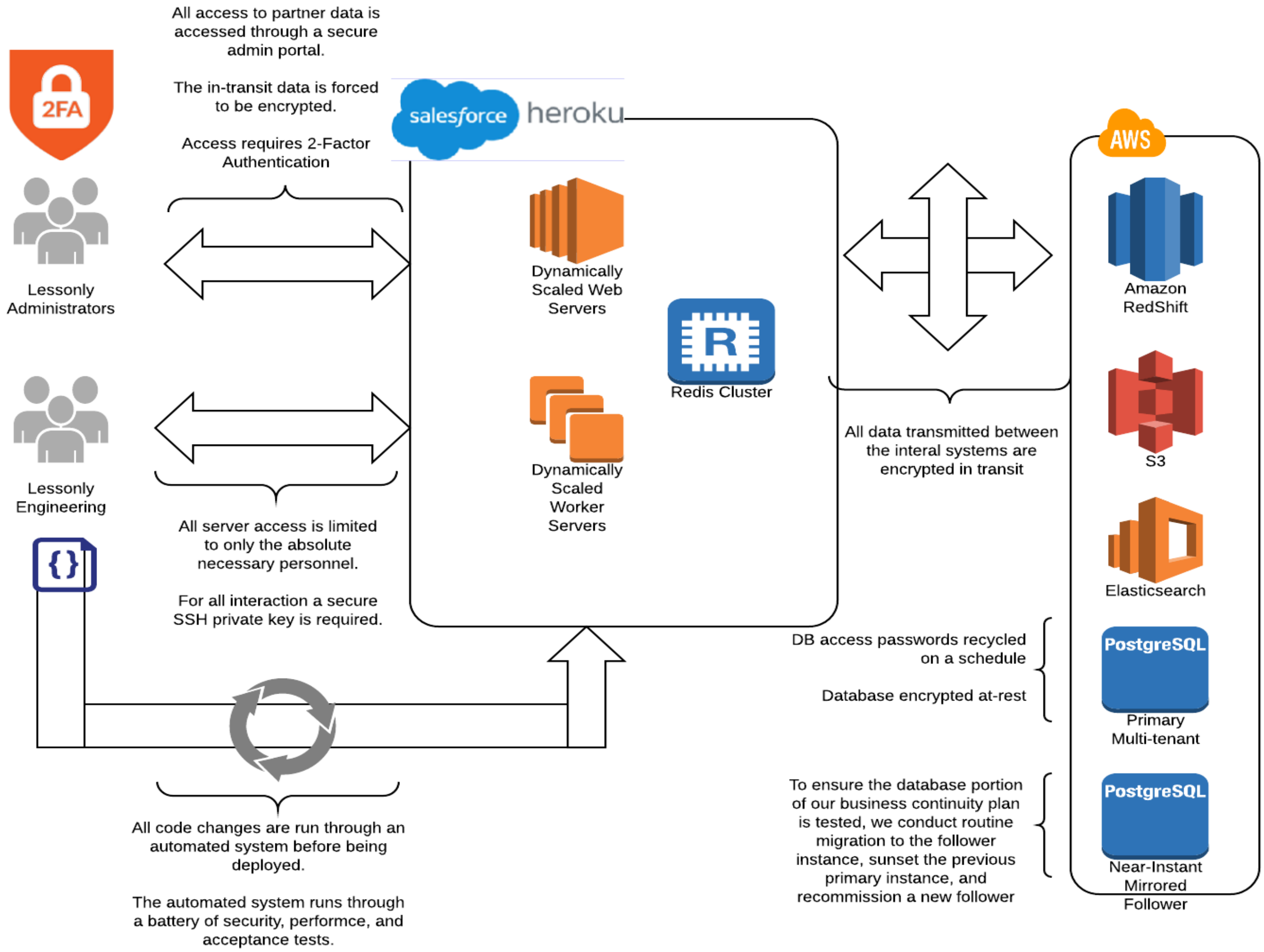
Lessonly was founded in 2012 to provide a cloud-based learning management system targeted at companies and teams that have to deal with rapid changes in how they do business. Although it can be used just like a traditional new hire onboarding system, it is built to support the rapid and easy creation and delivery of very timely training for customer-facing teams, such as Sales, Support, Customer Experience, and similar organizations. Lessonly is a privately-held company based in Indianapolis, Indiana, and employs approximately 150 individuals.

Description of Services Provided

Lessonly offers a single product, the Lessonly system. The primary version of the Lessonly system is a Software-as-a-Service (SaaS), multi-tenant system, but private cloud versions are available for customers that would prefer not to be part of a multi-tenant system. Other than that, the systems operate on the same code base. Lessonly is a web-based solution accessed via any of the major browsers (Chrome, Safari, IE, etc.). It was developed to run only on Amazon Web Services (AWS). Customers can deliver data to the system via direct entry, Application Program Interface (API), or Secure File Transfer Protocol (SFTP). Access is role-based, and with appropriate authorization, users can take lessons, record, and share practice sessions, create and update lessons, assign lessons, and monitor user progress on lessons.

The only data required by the Lessonly system is an employee name, an email address or username, and the lessons themselves. A work email address is usually captured so that alerts can be sent. Lessonly can be configured to capture some additional information, such as geographic location, that can aid in the assignment of lessons. No highly sensitive data, such as PCI, PHI, SSN, etc., is captured, stored, or used in the Lessonly system.

Following is a depiction of Lessonly's architecture:



All access to partner data is accessed through a secure admin portal.

The in-transit data is forced to be encrypted.

Access requires 2-Factor Authentication

All server access is limited to only the absolute necessary personnel.

For all interaction a secure SSH private key is required.

All code changes are run through an automated system before being deployed.

The automated system runs through a battery of security, performce, and acceptance tests.

All data transmitted between the interal systems are encrypted in transit

DB access passwords recycled on a schedule

Database encrypted at-rest

To ensure the database portion of our business continuity plan is tested, we conduct routine migration to the follower instance, sunset the previous primary instance, and recommission a new follower

Scope Definition

The scope of the review is limited to Lessonly System services performed in the Indianapolis, Indiana facility. The specific control activities may be found in Section 4 of this report.

Subservice Organization

Lessonly utilizes AWS for Cloud Infrastructure-as-a-Service (IaaS), AWS for Platform-as-a-System (PaaS) for private cloud systems, and Heroku in AWS for PaaS services for the multi-tenant system. Lessonly only uses AWS US-East for PaaS and IaaS. No Lessonly system data is stored outside of the United States. IaaS services include providing virtual machines (VMs) and virtual network infrastructure services. PaaS services include providing cloud-enabled applications, databases and tools, and data center hosting services include physical and environmental security safeguards. The services performed by AWS are not within the scope of this examination.

Functional Areas of Operations

- Executive management – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner

- Information Security – responsible for:
  - Quality assurance (QA) activities, including but not limited to operational QA, compliance, and certification against multiple government and third-party standards
  - Management of the vendor providing information technology, which protects information and systems from unauthorized access and use while maintaining integrity and availability
  - Management of the vendor providing Managed Detection and Response services for the Lessonly system
  - Management of the vendor providing lock and alarm systems for the Lessonly Indianapolis facility
- Product and Engineering – develops and improves the technology and software for the Lessonly system, and manages the IaaS and PaaS systems on which the Lessonly system runs
- Talent – provides human resources to Lessonly, including hiring, on-boarding, off-boarding, and new hire training

Infrastructure

The Lessonly system runs on AWS. We leverage Heroku for PaaS for our multi-tenant solution. Our private cloud systems use AWS directly for PaaS. All systems utilize Filestack for API services and a combination of services for the audio and video recording and editing functionality that is part of the Lessonly Practice service. These services are provided by Ziggeo, VidGrid, Wistia, and Hippo. All of these services operate in AWS, all data in transit between the systems is encrypted, and all data at rest is also encrypted. Lessonly uses ClamAV for antivirus protection. The Lessonly system uses a combination of AWS ACLs, Security Groups, and the AWS WAF to isolate system components.

Lessonly uses Meraki devices for its office network system. This consists of a firewall, a switch, and multiple access points. A limited number of Lessonly employees have virtual private network (VPN) access to the network, but the majority of users are only able to access the network when in the office. The network is used strictly to access the internet. Lessonly's Internet Service Provider (ISP) is CenturyLink. There are no servers on the network, and no customer data is stored on the network.

Data Management

The Lessonly system does not have a traditional "back-end." Customers have the ability to access and maintain their data (users, email addresses, lessons) directly in the system. Log files are captured for all changes to data in the system, but customers must request a report, which is generated by the engineering team, in order to review log data associated with their account.

CONTROL ENVIRONMENT

The control environment at Lessonly is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment include the integrity and ethical values, management's commitment to competence, its organizational structure, the assignment of authority and responsibility, and the oversight and direction provided by executive management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Lessonly's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Lessonly's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that Lessonly has implemented in this area are described below:

- Documented organizational policy statements are in place to communicate entity values and behavioral standards to personnel.
- Employees are required to sign an acknowledgment form indicating that they have been given access to the employee training system, which contains policies for employee conduct, and understand their responsibility for adhering to the associated policies and procedures.
- Background checks are performed for all employment candidates.

Executive Management Participation

Lessonly's control consciousness is overseen by its executive management team, who are also accountable for keeping Lessonly's advisory board informed about the company's security posture. The executive management team oversees management activities and meets on a regular basis to discuss matters pertinent to the organization's operations and to review financial results. Lessonly's executive management team may be found at:

https://www.lessonly.com/team/

Organizational Structure and Assignment of Authority and Responsibility

Lessonly's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Lessonly has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Lessonly's assignment of authority and responsibility includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes standard operating procedures relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. Lessonly has implemented organizational charts to communicate key areas of authority, responsibility, and lines of reporting to personnel. Employees are able to access these charts as needed via our payroll system. The charts are updated automatically as changes are made to staff, positions, and roles.

Commitment to Competence

Lessonly management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management seeks staff with significant experience, education, and understanding of working in a team environment. Lessonly supports ongoing training efforts to ensure its employees remain knowledgeable and competent in their respective fields. Specific control activities that Lessonly has implemented in this area are described below:

- Management considers the competence levels for particular jobs and translates required skills and knowledge levels into written position requirements.
- Job candidates are assessed to determine whether the candidate possesses the requisite level of competence to hold the position.

- Employees are encouraged to pursue external training and learning opportunities for improving skill sets and capabilities.

Accountability

Lessonly’s mission is to help people do better work so they can live better lives. Our core values of integrity, trust, diversity and teamwork, openness and honesty, and growth and development inform everything we do. Our way of delivering on our mission is to build powerfully simple, trackable training software that teams use to learn and practice what they do.

Our pursuit of these core values has resulted in a corporate culture based on shared values that guide how we lead, work, behave, and make decisions. They not only guide our internal conduct, but also our conduct with our customers, prospects, peers, and community. They also inform our policies and practices related to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Lessonly has implemented in this area are described below:

- Employee hiring procedures are in place to govern the hiring process.
- Employee termination procedures are in place to govern the termination process.

RISK ASSESSMENT

Management is responsible for identifying the risks that threaten achievement of the controls stated in management’s description of the system. Management has implemented a quality management process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding on actions to address them. New controls may also be discovered when designing, implementing, and documenting the system.

Lessonly faces a variety of risks from external and internal sources, and a precondition to effective risk assessment methodology is the establishment of strategic objectives, which are linked at different levels and internally consistent. The strategic objectives establish a basis for operations, reporting, and compliance objectives. Objectives are aligned with Lessonly’s risk appetite, which drives risk tolerance levels for our activities.

More specific objectives flow from the entity’s broad strategy. Entity-level objectives are linked and integrated with more specific objectives established for various “activities,” such as sales, marketing, and operations, making sure they are consistent. These sub-objectives, or activity-level objectives, include establishing goals and may deal with product line, marketing, financing, and profit objectives.

Lessonly has established certain broad categories, including:

- *Operations Objectives* — These pertain to effectiveness and efficiency of the entity’s operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management’s choices about structure and performance.
- *Security Objectives* — These objectives pertain to Lessonly’s compliance with our cybersecurity controls and adherence to laws and regulations to which we are subject. They are dependent on external factors and tend to be similar across entities or across an industry.

Risk Identification

Regardless of whether an objective is stated or implied, an entity’s risk assessment process should consider risks that may occur. It is important that risk identification be comprehensive. Lessonly has considered significant interactions with relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Our risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Lessonly executive management oversees risk management ownership and accountability. Senior management from different operational areas, as well as quality management personnel, are involved in the risk identification process. Management identifies elements of business risk, including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

Risk Factors

Management considers risks that may arise from both external and internal factors, including the following:

External Factors

- Changes in potential threat actors
- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Risk Analysis

Lessonly has two primary methods for analyzing risks:

- An annual company risk assessment based on NIST Special Publication 800-30 – This process involves the identification of threat actors and, based on the likelihood of attacks by these actors, the threat vectors likely to be used. It includes the evaluation of both external and internal threats.
- Real-time assessment of newly identified risks – Lessonly experiences a very low volume of actual new threats, such as discovered vulnerabilities, potential incidents, lost devices, etc.

Control Activities

Information Security, in conjunction with the product/engineering team, analyzes the likelihood of an identified risk being realized, and the impact of an event should the risk lead to an incident. If action is required as a result of the analysis, the work is prioritized and added to the appropriate queue to be addressed.

In some cases, changes to existing controls, or wholly new controls, will be required to address the risk. Information security, working in conjunction with the product/engineering team and Lessonly's security committee, will make recommendations about the required control changes, which will be reviewed by the committee and then implemented by the appropriate organization if approved.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Lessonly personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps that personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures, and control activities have been established, they are implemented, monitored, reviewed, and improved when necessary.

Lessonly's control activities are included in Section 4 of this report. The description of the service auditor's tests of the suitability of the design of controls and the results of those tests are also presented in Section 4, adjacent to the service organization's description of control activities. The results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Information Security

Control activities provide reasonable assurance that information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Lessonly maintains documented policies and procedures to help ensure that personnel follow standardized methodology related to items such as password policies, authentication and access control, auditing, and encryption. Conversely, when an employee is terminated, HR or the employee's manager notifies IT operations personnel who help ensure that access to the network domains, operating system, and database is revoked as required based on the employee's access. Annually, Lessonly reviews its sub-service organization's SOC 2 reports to confirm IT security and processes.

Access to the network domains is restricted through the use of an authentication protocol that requires a username and password. Lessonly has adopted the latest NIST password guidelines that recommend long but easy to remember phrases, which are only changed when there is reason to think the password may be compromised. Users may voluntarily change their password whenever they desire. In addition, if an end user enters an invalid password beyond the configured parameters, the end user will be locked out.

Administrative access to the AWS-based domains, containing the Lessonly system production application and database servers, is limited to selected system engineers and architects. At the operating system level, authentication to the application and database servers is restricted by protocols that point to the network domain password policies. Administrative access to production servers is limited to appropriate IT personnel. Access to the backend is restricted through an authentication protocol that requires a username and password. The password is required to meet password length and complexity requirements.

Data Communications

Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Lessonly has established policies and procedures related to data communications to help ensure that operations personnel follow standardized methodology, which includes remote access, application vulnerability and penetration testing, network and host-based intrusion detection, and encryption.

Production Network

Lessonly production hosts are located in the United States and reside in the AWS IaaS and PaaS environment. In addition, virtual IP (VIP) addresses enable Network Address Translation (NAT) functionality to manage IP addresses. The ability to modify Access Control Lists (ACLs) and VIP configurations is restricted to authorized personnel. In the event of a potential or actual security breach, product engineering personnel, in conjunction with

Information Security and our security operations center managed service provider, work to verify an actual breach has occurred. If that is confirmed, they identify the cause and remediate the breach immediately.

Firewall Configuration Changes

In the event that firewall and ACL configurations require modification, two-person approval is documented within the change management process. Changes that are made to AWS ACLs are considered firewall configuration changes and follow the firewall change management process.

Remote Access

Remote access to the Lessonly office network is secured through the use of an encrypted VPN. VPN users are required to use at least 128-bit encryption. The Lessonly office network is strictly used to access the internet. No servers run in this environment, and no customer data is stored here.

Application communications between clients and the Lessonly AWS-based system are protected using TLS v1.2, as are communications between layers in the Lessonly system.

Computer Operations

Control activities provide reasonable assurance that the systems are maintained in a manner that helps ensure system availability.

Lessonly has established policies and procedures to guide system operations personnel in the monitoring of production systems and response to system availability issues. One of the ways that Lessonly monitors system availability is through the use of an enterprise monitoring application, which provides system operations personnel with information related to central processing unit (CPU) utilization, available memory, free disk space, and system heartbeat. System operations personnel configure the enterprise monitoring system with levels above or below which an alert would automatically be triggered by the system and sent to system operations personnel. The alerts contain information pertaining to monitored network devices and are investigated and resolved by system operations personnel.

Throughout the investigation and resolution process, system operations personnel utilize a ticketing system to track infrastructure issues and details, such as the date, service affected, issue, and resolution. The Lessonly application is also monitored, and alerts are automatically generated and sent to system operations personnel when the application experiences performance issues above or below the configured thresholds.

Lessonly maintains policies and procedures related to patch management activities to help ensure that system operations personnel follow standardized methodology when applying operating system patches. A ticketing system is used to track patches through implementation.

Additionally, antivirus software is in place to help ensure system availability by monitoring the transmission of data or files and preventing certain viruses from entering the network. Virus signatures are updated automatically, many times per week. Results of the virus scan are investigated and resolved by system operations personnel. Lessonly performs periodic data restoration tests to help ensure data that is lost or unavailable, as a result of an error or an infrastructure issue, can be restored from the backup system.

Application Change Control

Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Lessonly maintains policies and procedures related to change development and deployment to help ensure that personnel follow the standardized methodology when performing application change control activities. Throughout the application change process, from design through implementation, a ticketing system is used to track requirements and approvals.

Administrative access privileges within the version control tool are limited to Engineering personnel. Development activities are performed in an environment that is physically and logically segregated from both the staging environment and production.

When development is completed, QA testing is performed by QA personnel to help ensure that the changes work as intended. When QA testing and code review are successfully completed, senior staff provides approval for the change release, which is captured within the change ticket.

In the event of an emergency change, a ticket that contains the details related to the change, including justification and approvals, is still required. The ability to implement changes, whether they are standard or emergency changes, is restricted to individuals that have administrative access within the production network domain or application server.

INFORMATION AND COMMUNICATION

Relevant Information

Information is necessary for Lessonly to carry out internal control responsibilities to support the achievement of its objectives related to the Lessonly system. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

Communication

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal control. Formal communication tools, such as organizational charts, training classes delivered in the Lessonly system, and job descriptions, are in place at Lessonly. Management's communications are made electronically, verbally, and through the actions of management.

Lessonly has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include periodic meetings with customer representatives, the use of email and chat, and a customer contact line to communicate time-sensitive information.

If incidents are discovered by or communicated to Lessonly, personnel follow a documented incident response plan. If a control change is needed to address the incident, it will follow the standard change process for controls. Incidents are documented within the ticketing system and tracked until resolved.

MONITORING

Monitoring Activities

Lessonly compliance leadership performs monitoring activities in order to continuously assess the quality of internal control over time, and updates management on status. Monitoring activities are used to initiate corrective action through Lessonly lessons, team or department meetings, and electronic communication. Monitoring activities are conducted periodically, and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Monitoring is completed through ongoing activities or separate evaluations. Management determines the need for separate evaluations through consideration of the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of ongoing monitoring. Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary, to ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of Lessonly's ongoing monitoring activities include the following:

- In carrying out its regular management activities, operations management obtains evidence that the system of internal control continues to function.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Operations personnel monitor AWS to ensure AWS is meeting its service level agreements (SLAs).
- External auditors provide recommendations on the way internal controls may be strengthened.
- Training seminars, planning sessions, and other meetings provide important feedback to management on whether controls are effective.
- Personnel are asked periodically to state explicitly whether they understand and comply with the entity's code of conduct.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk tend to be evaluated more often. Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by corporate management, along with any other internal control evaluations. Internal control evaluations may be performed upon special request of senior management. In addition, management utilizes the work of external auditors in considering the effectiveness of internal controls. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Quality Management

In order to support ongoing efforts to improve the quality of services and internal controls, the company has established a quality management organization.

Internal and External Auditing

Lessonly does not manage or have access to any highly sensitive data, such as PCI or PHI. Nevertheless, we are cognizant of the need to provide unbiased information about the ways we protect our customers' data and intellectual property. Lessonly has selected SSAE 18 SOC 2 as the basis for our quality and compliance program. Lessonly is also required to be General Data Protection Regulation (GDPR) compliant, is subject to the California Consumer Privacy Act (CCPA) and is a Privacy Shield participant. Lessonly conducts audits to examine company operations and service delivery based on the requirements of these programs.

Evaluating and Communicating Deficiencies

Deficiencies in an entity's internal control system may surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. This process enables an individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected.

Section 4: Trust Services Principles, Criteria, Related Controls and Tests of Controls

2017 Trust Services Criteria (TSC)				
TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
	CONTROL ENVIRONMENT			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Personnel, including contractors, are required to complete an onboarding path via Lessonly, which includes employee guidelines and policies, acceptable use requirements, and a Code of Conduct upon their hire and formally reaffirm them annually thereafter.	Select a sample of new and current employees during the examination period and obtain evidence that each completed a review of the Code of Conduct/employee guidelines upon hire or within the past year.	No exceptions noted.
		Personnel must pass a pre-employment screening, including background checks, before they may be hired by Lessonly.	Select a sample of new employees during the examination period and obtain evidence that background checks were performed prior to hire.	No exceptions noted.
		Management performs performance evaluations at least annually to communicate and hold individuals accountable for performance of internal controls.	Select a sample of current employees and obtain evidence that a performance evaluation was performed within the past year.	No exceptions noted.
		Lessonly has a documented Code of Ethics, acceptable use requirements, and employee guidelines, which are reviewed, updated if applicable, and approved by senior management annually.	Inspect the Code of Ethics to confirm that the conduct and standards outline Lessonly's commitments to integrity and ethical values. Confirm that the Code of Ethics, acceptable use requirements, and employee guidelines were approved by senior management within the examination period.	No exceptions noted.
		Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Select a sample of service providers and/or business partners and review the related agreement to ensure that it includes clearly defined terms, conditions, and responsibilities for the service provider/business partner.	No exceptions noted.
		Management monitors personnel compliance with the Code of Conduct through monitoring of workforce member complaints. A sanctions policy is in place for personnel who violate the Code of Conduct. Lessonly's website includes information describing how to report incidents and other ethical issues for employees and customers.	Inspect the Code of Ethics and employee guidelines to confirm that a sanctions policy for personnel who violate the Code of Conduct is included. In addition, inspect the Compliance Policy and Procedures and confirm that information for employees to report complaints is included. Inspect information provided to customers and confirm that it includes information describing how to report incidents and other ethical issues.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Executive Leadership Team understands and acknowledges the Lessonly Executive Team Security Responsibilities Policy to accept its oversight responsibilities in relation to established requirements and expectations.	Select a sample of Executive Leadership Team members and obtain evidence that each acknowledged the Executive Team Security Responsibility Policy during the examination period.	No exceptions noted.
		Members of Lessonly management with responsibilities relevant to security provide support to the Executive Leadership Team.	Inspect Executive Leadership Team meeting minutes and confirm that members of Lessonly management with responsibilities relevant to security provided support to the Board of Directors.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Lessonly maintains a current organization chart that is published and clearly defines the organization’s structure and reporting relationships.	Inspect the most recent organization chart and validate it was updated during the examination period and clearly defined the organization's structure and reporting relationships.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions upon hire and are communicated to managers and supervisors. Updates to job descriptions are maintained and communicated between managers and employees via routine performance evaluations.	Select a sample of new employees and obtain the job description for each role. Confirm that roles and responsibilities are clearly defined and communicated to managers and supervisors. In addition, select a sample of current employees and obtain the most recent performance evaluation. Confirm that updates to job descriptions are maintained.	No exceptions noted.
		Management performs performance evaluations at least annually to communicate and hold individuals accountable for performance of internal controls.	Select a sample of current employees and obtain evidence that a performance evaluation was performed within the past year.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Depending on job requirements and needs, employees complete continuous training pertaining to their specific job.	Select a sample of current employees and review the most recent performance evaluation to validate that any required continuous training was completed.	No exceptions noted.
		Personnel must pass a pre-employment screening, including background checks, before they may be hired by Lessonly.	Select a sample of new employees during the audit period and obtain evidence that background checks were performed prior to hire.	No exceptions noted.
		Lessonly has a documented Code of Ethics, acceptable use requirements, and employee guidelines, which are reviewed, updated if applicable, and approved by senior management annually.	Inspect the Code of Ethics to confirm that the conduct and standards outline Lessonly's commitments to integrity and ethical values. Confirm that the Code of Ethics, acceptable use requirements, and employee guidelines were approved by senior management within the examination period.	No exceptions noted.
		Management performs performance evaluations at least annually to communicate and hold individuals accountable for performance of internal controls.	Select a sample of current employees and obtain evidence that a performance evaluation was performed within the past year.	No exceptions noted.
		Policies and procedures, including the Lessonly employee guidelines, are maintained in Lessonly's system, to which all employees have access.	Inspect the company's intranet and determine that policies and procedures are maintained via the company's intranet, and validate that employees have access.	No exceptions noted.
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
		Documented data communication policies and procedures are in place to inform operations personnel of corporate data communication standards that include, but are not limited to, the following: * Remote Access * Patching * BYOD Policy * Security Vulnerability Tracking * Wireless Security Policy * Encryption	Inspect the IT Operational Policy, BYOD Policy, Wireless Security Policy, Encryption Policy, and Remote Access Policy documents and confirm they include data communication policies for remote access, vulnerability assessment, wireless communication, and encryption.	No exceptions noted.
		Lessonly has succession plans in place for key employees and management.	Inspect the Emergency Succession Plan and confirm that a formal succession plan for key employees and management is in place. In addition, inspect the Board of Directors meeting minutes and confirm that succession planning was discussed for key employees and management.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities are defined in written job descriptions upon hire and are communicated to managers and supervisors. Updates to job descriptions are maintained and communicated between managers and employees via routine performance evaluations.	Select a sample of new employees and obtain the job description for each role. Confirm that roles and responsibilities are clearly defined and communicated to managers and supervisors. In addition, select a sample of current employees and obtain the most recent performance evaluation. Confirm that updates to job descriptions are maintained.	No exceptions noted.
		Management performs performance evaluations at least annually to communicate and hold individuals accountable for performance of internal controls.	Select a sample of current employees and obtain evidence that a performance evaluation was performed within the past year.	No exceptions noted.
	COMMUNICATION AND INFORMATION			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
		Documented data communication policies and procedures are in place to inform operations personnel of corporate data communication standards that include, but are not limited to, the following: * Remote Access * Patching * BYOD Policy * Security Vulnerability Tracking * Wireless Security Policy * Encryption	Inspect the IT Operational Policy, BYOD Policy, Wireless Security Policy, Encryption Policy, and Remote Access Policy documents and confirm they include data communication policies for remote access, vulnerability assessment, wireless communication, and encryption.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Policies and procedures, including the Lessonly employee guidelines, are maintained in Lessonly's system, to which all employees have access.	Inspect the company's intranet and determine that policies and procedures are maintained via the company's intranet, and validate that employees have access.	No exceptions noted.
		Users receive information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns and complaints.	Select a sample of users/customers and inspect the information provided to each. Confirm that it included information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		Significant changes affecting customers, including changes as a result of incidents, are managed and communicated to the customer before implementation.	Select a sample of changes affecting customers and confirm that the changes were communicated to the affected customers.	No exceptions noted.
		Management provides security training at least annually and ensures that all employees attend the training.	Select a sample of employees and validate that security training was completed within the past year. In addition, inspect the Security Training Policy and confirm it contains security training requirements, including annual training attendance.	No exceptions noted.
		Documented data communication policies and procedures are in place to inform operations personnel of corporate data communication standards that include, but are not limited to, the following: * Remote Access * Patching * BYOD Policy * Security Vulnerability Tracking * Wireless Security Policy * Encryption	Inspect the IT Operational Policy, BYOD Policy, Wireless Security Policy, Encryption Policy, and Remote Access Policy documents and confirm they include data communication policies for remote access, vulnerability assessment, wireless communication, and encryption.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions upon hire and are communicated to managers and supervisors. Updates to job descriptions are maintained and communicated between managers and employees via routine performance evaluations.	Select a sample of new employees and obtain the job description for each role. Confirm that roles and responsibilities are clearly defined and communicated to managers and supervisors. In addition, select a sample of current employees and obtain the most recent performance evaluation. Confirm that updates to job descriptions are maintained.	No exceptions noted.
		Depending on job requirements and needs, employees complete continuous training pertaining to their specific job.	Select a sample of current employees and review the most recent performance evaluation to validate that any required continuous training was completed.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		Members of Lessonly management with responsibilities relevant to security provide support to the Executive Leadership Team.	Inspect Executive Leadership Team meeting minutes and confirm that members of Lessonly management with responsibilities relevant to security provided support to the Board of Directors.	No exceptions noted.
		Management monitors personnel compliance with the Code of Conduct through monitoring of workforce member complaints. A sanctions policy is in place for personnel who violate the Code of Conduct. Lessonly's website includes information describing how to report incidents and other ethical issues for employees and customers.	Inspect the Code of Ethics and employee guidelines to confirm that a sanctions policy for personnel who violate the Code of Conduct is included. In addition, inspect the Compliance Policy and Procedures and confirm that information for employees to report complaints is included. Inspect information provided to customers and confirm that it includes information describing how to report incidents and other ethical issues.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Policies and procedures, including the Lessonly employee guidelines, are maintained in Lessonly's system, to which all employees have access.	Inspect the company's intranet and determine that policies and procedures are maintained via the company's intranet, and validate that employees have access.	No exceptions noted.
		Users receive information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns and complaints.	Select a sample of users/customers and inspect the information provided to each. Confirm that it included information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		Lessonly maintains a current organization chart that is published and clearly defines the organization's structure and reporting relationships.	Inspect the most recent organization chart and validate it was updated during the examination period and clearly defined the organization's structure and reporting relationships.	No exceptions noted.
		Depending on job requirements and needs, employees complete continuous training pertaining to their specific job.	Select a sample of current employees and review the most recent performance evaluation to validate that any required continuous training was completed.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions upon hire and are communicated to managers and supervisors. Updates to job descriptions are maintained and communicated between managers and employees via routine performance evaluations.	Select a sample of new employees and obtain the job description for each role. Confirm that roles and responsibilities are clearly defined and communicated to managers and supervisors. In addition, select a sample of current employees and obtain the most recent performance evaluation. Confirm that updates to job descriptions are maintained.	No exceptions noted.
		Relevant information resulting from assessments conducted by external parties is communicated to the Executive Leadership Team.	Inspect Executive Leadership Team meeting minutes and confirm that results of external penetration testing and vulnerability scans were discussed with the Executive Leadership Team. In addition, inspect the Third Party Penetration Testing Policy and confirm it includes requirements to discuss assessment results with senior management.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		Significant changes affecting customers, including changes as a result of incidents, are managed and communicated to the customer before implementation.	Select a sample of changes affecting customers and confirm that the changes were communicated to the affected customers.	No exceptions noted.
		Management monitors personnel compliance with the Code of Conduct through monitoring of workforce member complaints. A sanctions policy is in place for personnel who violate the Code of Conduct. Lessonly's website includes information describing how to report incidents and other ethical issues for employees and customers.	Inspect the Code of Ethics and employee guidelines to confirm that a sanctions policy for personnel who violate the Code of Conduct is included. In addition, inspect the Compliance Policy and Procedures and confirm that information for employees to report complaints is included. Inspect information provided to customers and confirm that it includes information describing how to report incidents and other ethical issues.	No exceptions noted.
	RISK ASSESSMENT			
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Lessonly management tracks changes in compliance and regulatory requirements relating to Lessonly's products and services. When changes are noted, they are incorporated into Lessonly's risk assessment.	Inspect the Compliance Policy and Procedures and perform interviews to confirm that changes in compliance and regulatory requirements are tracked and incorporated into risk assessments. Review the completed risk assessment and confirm it includes compliance and regulatory requirements.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Significant changes affecting customers, including changes as a result of incidents, are managed and communicated to the customer before implementation.	Select a sample of changes affecting customers and confirm that the changes were communicated to the affected customers.	No exceptions noted.
		External vulnerability scans and external penetration tests are performed at least annually.	Inspect the most recent external vulnerability scan and external penetration test and validate they were performed within the past year. In addition, inspect the Third Party Penetration Testing Policy and confirm it requires annual penetration testing.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Significant changes affecting customers, including changes as a result of incidents, are managed and communicated to the customer before implementation.	Select a sample of changes affecting customers and confirm that the changes were communicated to the affected customers.	No exceptions noted.
		External vulnerability scans and external penetration tests are performed at least annually.	Inspect the most recent external vulnerability scan and external penetration test and validate they were performed within the past year. In addition, inspect the Third Party Penetration Testing Policy and confirm it requires annual penetration testing.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
	MONITORING ACTIVITIES			
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Subservice organizations are required to maintain their own security practices and procedures, including regular testing and updates of the business continuity and disaster recovery programs as well as patch management. Conformance is assessed annually through review of SOC 2 reports.	Obtain evidence that the subservice organization's most recent SOC 2 reports were reviewed in the past year. In addition, inspect the Sub-Service Security Review Policy and confirm it requires review of SOC 2 reports at least annually.	No exceptions noted.
		Lessonly has developed and maintains a documented baseline configuration of the internal control systems.	Obtain evidence that the baseline configuration of internal control systems are documented and maintained.	No exceptions noted.
		Management performs performance evaluations at least annually to communicate and hold individuals accountable for performance of internal controls.	Select a sample of current employees and obtain evidence that a performance evaluation was performed within the past year.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Subservice organizations are required to maintain their own security practices and procedures, including regular testing and updates of the business continuity and disaster recovery programs as well as patch management. Conformance is assessed annually through review of SOC 2 reports.	Obtain evidence that the subservice organization's most recent SOC 2 reports were reviewed in the past year. In addition, inspect the Sub-Service Security Review Policy and confirm it requires review of SOC 2 reports at least annually.	No exceptions noted.
	CONTROL ACTIVITIES			
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Lessonly has designed statically enforced segregation of duties to define what privileges are assigned to users within applications. In those instances that segregation of duties is not possible, management has implemented controls to monitor activity.	Inspect screenshots of application settings and confirm segregation of duties is enforced. Where segregation of duties is not possible, obtain evidence to confirm that management monitors the user activity.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Policies and procedures, including the Lessonly employee guidelines, are maintained in Lessonly's system, to which all employees have access.	Inspect the company's intranet and determine that policies and procedures are maintained via the company's intranet, and validate that employees have access.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
		Documented data communication policies and procedures are in place to inform operations personnel of corporate data communication standards that include, but are not limited to, the following: * Remote Access * Patching * BYOD Policy * Security Vulnerability Tracking * Wireless Security Policy * Encryption	Inspect the IT Operational Policy, BYOD Policy, Wireless Security Policy, Encryption Policy, and Remote Access Policy documents and confirm they include data communication policies for remote access, vulnerability assessment, wireless communication, and encryption.	No exceptions noted.
		Management performs performance evaluations at least annually to communicate and hold individuals accountable for performance of internal controls.	Select a sample of current employees and obtain evidence that a performance evaluation was performed within the past year.	No exceptions noted.
	LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
		At least annually, a security review of access rights to key systems, applications and physical locations is performed to validate employees have appropriate access and terminated employees have been removed.	Inspect the most recent access review and confirm that it was performed within the past year and included access rights to key systems, applications and physical locations. If any access changes were required due to the review, obtain evidence to confirm that the required change was made.	No exceptions noted.
		Customer database servers are configured to encrypt databases.	Inspect customer database server configurations and determine that databases are encrypted.	No exceptions noted.
		Privileged access to sensitive resources is restricted. Privileged access must be approved by management.	Inspect a list of user access to sensitive resources and validate that access is restricted based on job requirements and approved by management.	No exceptions noted.
		The ability to administer the server is restricted to users based on job position and need.	Inspect the server user access listing and confirm access is restricted based on job position and need.	No exceptions noted.
		Communications between clients and the Lessonly web application are secured using TLS 1.2 or greater encryption.	Inspect the most recent TLS scan and determine that communications between clients and the Lessonly web application are secured using TLS 1.2 or greater encryption.	No exceptions noted.
		Users are required to authenticate via a valid user account and password before being granted access to the Lessonly web application. Two factor authentication is in place for internal users, using an authenticator protocol. External users/customers can choose two factor authentication or password only.	Observe an external user logging onto the Lessonly web application and confirm that users are required to authenticate via a user account and password before being granted access to the application. Observe an internal user logging onto the Lessonly web application and confirm that internal users are required to authenticate via two factor authentication before being granted access to the application.	No exceptions noted.
		An automated monitoring tool is configured to monitor network domain logs. Alerts are sent to IT operations personnel upon detection of access and system events that include, but are not limited to, the following: * Account logons * Account management * System events * Abnormal activity	Inspect the automated monitoring tool and confirm that it is configured to monitor domain logs and send alerts to IT personnel upon detection of access and system events. Inspect a sample email alert and validate automated alerts are sent to IT personnel.	No exceptions noted.
		Lessonly identifies, inventories, classifies, and manages information assets.	Inspect the Device and Media Controls Policy and information asset inventory and confirm that management identifies, inventories, classifies, and manages the assets.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The ability to administer the server is restricted to users based on job position and need.	Inspect the server user access listing and confirm access is restricted based on job position and need.	No exceptions noted.
		At least annually, a security review of access rights to key systems, applications and physical locations is performed to validate employees have appropriate access and terminated employees have been removed.	Inspect the most recent access review and confirm that it was performed within the past year and included access rights to key systems, applications and physical locations. If any access changes were required due to the review, obtain evidence to confirm that the required change was made.	No exceptions noted.
		Privileged access to sensitive resources is restricted. Privileged access must be approved by management.	Inspect a list of user access to sensitive resources and validate that access is restricted based on job requirements and approved by management.	No exceptions noted.
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
		Management follows a termination procedure to verify that terminated employee accounts from the network domain and production server operating system are revoked upon termination.	Select a sample of terminated employees during the examination period and obtain evidence to confirm that appropriate personnel were notified of their termination.	No exceptions noted.
		IT operations personnel revoke terminated employees' access to all access control security groups upon notification of termination.	Select a sample of terminated employees during the examination period and obtain evidence to validate that their access was removed or disabled upon notification of termination.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	At least annually, a security review of access rights to key systems, applications and physical locations is performed to validate employees have appropriate access and terminated employees have been removed.	Inspect the most recent access review and confirm that it was performed within the past year and included access rights to key systems, applications and physical locations. If any access changes were required due to the review, obtain evidence to confirm that the required change was made.	No exceptions noted.
		Privileged access to sensitive resources is restricted. Privileged access must be approved by management.	Inspect a list of user access to sensitive resources and validate that access is restricted based on job requirements and approved by management.	No exceptions noted.
		The ability to administer the server is restricted to users based on job position and need.	Inspect the server user access listing and confirm access is restricted based on job position and need.	No exceptions noted.
		Management follows a termination procedure to verify that terminated employee accounts from the network domain and production server operating system are revoked upon termination.	Select a sample of terminated employees during the examination period and obtain evidence to confirm that appropriate personnel were notified of their termination.	No exceptions noted.
		IT operations personnel revoke terminated employees' access to all access control security groups upon notification of termination.	Select a sample of terminated employees during the examination period and obtain evidence to validate that their access was removed or disabled upon notification of termination.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Lessonly facilities are locked and badge access is required to enter the building.	Observe Lessonly facilities and validate that doors are locked and badge access is required to enter the building.	No exceptions noted.
		At least annually, a security review of access rights to key systems, applications and physical locations is performed to validate employees have appropriate access and terminated employees have been removed.	Inspect the most recent access review and confirm that it was performed within the past year and included access rights to key systems, applications and physical locations. If any access changes were required due to the review, obtain evidence to confirm that the required change was made.	No exceptions noted.
		Management follows a termination procedure to verify that terminated employee accounts from the network domain and production server operating system are revoked upon termination.	Select a sample of terminated employees during the examination period and obtain evidence to confirm that appropriate personnel were notified of their termination.	No exceptions noted.
		Subservice organizations are required to maintain their own security practices and procedures, including regular testing and updates of the business continuity and disaster recovery programs as well as patch management. Conformance is assessed annually through review of SOC 2 reports.	Obtain evidence that the subservice organization's most recent SOC 2 reports were reviewed in the past year. In addition, inspect the Sub-Service Security Review Policy and confirm it requires review of SOC 2 reports at least annually.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Lessonly facilities are locked and badge access is required to enter the building.	Observe Lessonly facilities and validate that doors are locked and badge access is required to enter the building.	No exceptions noted.
		At least annually, a security review of access rights to key systems, applications and physical locations is performed to validate employees have appropriate access and terminated employees have been removed.	Inspect the most recent access review and confirm that it was performed within the past year and included access rights to key systems, applications and physical locations. If any access changes were required due to the review, obtain evidence to confirm that the required change was made.	No exceptions noted.
		Management follows a termination procedure to verify that terminated employee accounts from the network domain and production server operating system are revoked upon termination.	Select a sample of terminated employees during the examination period and obtain evidence to confirm that appropriate personnel were notified of their termination.	No exceptions noted.
		For security purposes, all client data is logically partitioned by client in a database on a secure server.	Inspect the database server and confirm that client data is logically partitioned.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
		Customer database servers are configured to encrypt databases.	Inspect customer database server configurations and determine that databases are encrypted.	No exceptions noted.
		Access Control Lists (ACLs) are used to limit the source and type of traffic that can terminate on a device.	Inspect a screenshot from the firewall system and confirm ACLs are in place to limit the source and type of traffic that can terminate on a device.	No exceptions noted.
		The ability to administer the server is restricted to users based on job position and need.	Inspect the server user access listing and confirm access is restricted based on job position and need.	No exceptions noted.
		An automated monitoring tool is configured to monitor network domain logs. Alerts are sent to IT operations personnel upon detection of access and system events that include, but are not limited to, the following: * Account logons * Account management * System events * Abnormal activity	Inspect the automated monitoring tool and confirm that it is configured to monitor domain logs and send alerts to IT personnel upon detection of access and system events. Inspect a sample email alert and validate automated alerts are sent to IT personnel.	No exceptions noted.
		Communications between clients and the Lessonly web application are secured using TLS 1.2 or greater encryption.	Inspect the most recent TLS scan and determine that communications between clients and the Lessonly web application are secured using TLS 1.2 or greater encryption.	No exceptions noted.
		Documented data communication policies and procedures are in place to inform operations personnel of corporate data communication standards that include, but are not limited to, the following: * Remote Access * Patching * BYOD Policy * Security Vulnerability Tracking * Wireless Security Policy * Encryption	Inspect the IT Operational Policy, BYOD Policy, Wireless Security Policy, Encryption Policy, and Remote Access Policy documents and confirm they include data communication policies for remote access, vulnerability assessment, wireless communication, and encryption.	No exceptions noted.
		Users are required to authenticate via a valid user account and password before being granted access to the Lessonly web application. Two factor authentication is in place for internal users, using an authenticator protocol. External users/customers can choose two factor authentication or password only.	Observe an external user logging onto the Lessonly web application and confirm that users are required to authenticate via a user account and password before being granted access to the application. Observe an internal user logging onto the Lessonly web application and confirm that internal users are required to authenticate via two factor authentication before being granted access to the application.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Documented data communication policies and procedures are in place to inform operations personnel of corporate data communication standards that include, but are not limited to, the following: * Remote Access * Patching * BYOD Policy * Security Vulnerability Tracking * Wireless Security Policy * Encryption	Inspect the IT Operational Policy, BYOD Policy, Wireless Security Policy, Encryption Policy, and Remote Access Policy documents and confirm they include data communication policies for remote access, vulnerability assessment, wireless communication, and encryption.	No exceptions noted.
		For security purposes, all client data is logically partitioned by client in a database on a secure server.	Inspect the database server and confirm that client data is logically partitioned.	No exceptions noted.
		Communications between clients and the Lessonly web application are secured using TLS 1.2 or greater encryption.	Inspect the most recent TLS scan and determine that communications between clients and the Lessonly web application are secured using TLS 1.2 or greater encryption.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus software is utilized to detect and prevent transmission of data or files that contain certain virus signatures recognized by the antivirus software. The AV software is configured to update virus definitions and scan for virus signatures on a daily basis.	Inspect system screenshots and confirm that antivirus software is installed and the signatures are updated at least daily.	No exceptions noted.
		An automated monitoring tool is configured to monitor network domain logs. Alerts are sent to IT operations personnel upon detection of access and system events that include, but are not limited to, the following: * Account logons * Account management * System events * Abnormal activity	Inspect the automated monitoring tool and confirm that it is configured to monitor domain logs and send alerts to IT personnel upon detection of access and system events. Inspect a sample email alert and validate automated alerts are sent to IT personnel.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements. The procedures require that change requests are: * Authorized * Formally documented * Tested prior to migration to production * Reviewed and approved	Inspect the change management plan and confirm it requires that change requests are authorized, formally documented, tested prior to migration to production, and reviewed and approved. Select a sample of changes during the examination period and obtain evidence to confirm that each change was authorized, formally documented, tested prior to migration to production, and reviewed and approved.	No exceptions noted.
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.
	SYSTEM OPERATIONS			
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Lessonly has developed and maintains a documented baseline configuration of the internal control systems.	Obtain evidence that the baseline configuration of internal control systems are documented and maintained.	No exceptions noted.
		An automated monitoring tool is configured to monitor network domain logs. Alerts are sent to IT operations personnel upon detection of access and system events that include, but are not limited to, the following: * Account logons * Account management * System events * Abnormal activity	Inspect the automated monitoring tool and confirm that it is configured to monitor domain logs and send alerts to IT personnel upon detection of access and system events. Inspect a sample email alert and validate automated alerts are sent to IT personnel.	No exceptions noted.
		External vulnerability scans and external penetration tests are performed at least annually.	Inspect the most recent external vulnerability scan and external penetration test and validate they were performed within the past year. In addition, inspect the Third Party Penetration Testing Policy and confirm it requires annual penetration testing.	No exceptions noted.
		Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An automated monitoring tool is configured to monitor network domain logs. Alerts are sent to IT operations personnel upon detection of access and system events that include, but are not limited to, the following: * Account logons * Account management * System events * Abnormal activity	Inspect the automated monitoring tool and confirm that it is configured to monitor domain logs and send alerts to IT personnel upon detection of access and system events. Inspect a sample email alert and validate automated alerts are sent to IT personnel.	No exceptions noted.
		Website and application performance monitoring applications are utilized to monitor the availability of the Lessonly platform and are configured to send immediate notifications to IT operations personnel in the event of an availability issue.	Inspect system screenshots and a sample notification to confirm that the availability of websites and applications is monitored, and validate an immediate notification is sent to IT operations personnel when a website or application availability issue occurs.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
		A ticketing system is in place to manage system infrastructure issues, including incidents related to system security. Tickets are assigned to support personnel based on the nature of the ticket. All changes are documented in the ticketing system from initiation through deployment.	Observe the ticketing system and confirm that tickets are assigned to support personnel based on the nature of the ticket to manage system infrastructure issues, and validate changes are documented in the ticketing system from initiation through deployment. In addition, inspect the DevOps Ticketing System Policy and confirm a process is in place to properly assign tickets to support personnel.	No exceptions noted.
		A restore from backup media is performed at least annually.	Obtain evidence of the most recent restore from backup media and confirm it was completed in the past year.	No exceptions noted.
		System/database backups are performed on a near real-time basis. Management performs weekly reviews to confirm that the backups remain successful, and takes action to correct if they are not.	Obtain evidence to determine that system/database backups are performed on a daily basis and monitored by management.	No exceptions noted.
		Users receive information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns and complaints.	Select a sample of users/customers and inspect the information provided to each. Confirm that it included information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Users receive information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns and complaints.	Select a sample of users/customers and inspect the information provided to each. Confirm that it included information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		A ticketing system is in place to manage system infrastructure issues, including incidents related to system security. Tickets are assigned to support personnel based on the nature of the ticket. All changes are documented in the ticketing system from initiation through deployment.	Observe the ticketing system and confirm that tickets are assigned to support personnel based on the nature of the ticket to manage system infrastructure issues, and validate changes are documented in the ticketing system from initiation through deployment. In addition, inspect the DevOps Ticketing System Policy and confirm a process is in place to properly assign tickets to support personnel.	No exceptions noted.
		Significant changes affecting customers, including changes as a result of incidents, are managed and communicated to the customer before implementation.	Select a sample of changes affecting customers and confirm that the changes were communicated to the affected customers.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Users receive information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns and complaints.	Select a sample of users/customers and inspect the information provided to each. Confirm that it included information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		A ticketing system is in place to manage system infrastructure issues, including incidents related to system security. Tickets are assigned to support personnel based on the nature of the ticket. All changes are documented in the ticketing system from initiation through deployment.	Observe the ticketing system and confirm that tickets are assigned to support personnel based on the nature of the ticket to manage system infrastructure issues, and validate changes are documented in the ticketing system from initiation through deployment. In addition, inspect the DevOps Ticketing System Policy and confirm a process is in place to properly assign tickets to support personnel.	No exceptions noted.
		External vulnerability scans and external penetration tests are performed at least annually.	Inspect the most recent external vulnerability scan and external penetration test and validate they were performed within the past year. In addition, inspect the Third Party Penetration Testing Policy and confirm it requires annual penetration testing.	No exceptions noted.
		Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Significant changes affecting customers, including changes as a result of incidents, are managed and communicated to the customer before implementation.	Select a sample of changes affecting customers and confirm that the changes were communicated to the affected customers.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements. The procedures require that change requests are: * Authorized * Formally documented * Tested prior to migration to production * Reviewed and approved	Inspect the change management plan and confirm it requires that change requests are authorized, formally documented, tested prior to migration to production, and reviewed and approved. Select a sample of changes during the examination period and obtain evidence to confirm that each change was authorized, formally documented, tested prior to migration to production, and reviewed and approved.	No exceptions noted.
		An incident response plan has been documented to provide instruction to employees when security incidents or events occur. The plan establishes defined roles and responsibilities to oversee the implementation of incident response. In addition, annual testing of the incident response plan is performed.	Inspect the incident response plan and confirm that it includes instructions for employees when security incidents or events occur, establishes defined roles and responsibilities, and requires annual testing. Confirm that the incident response plan was tested within the past year.	No exceptions noted.
		Users receive information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns and complaints.	Select a sample of users/customers and inspect the information provided to each. Confirm that it included information describing how to use the system as well as support information, such as the process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		A ticketing system is in place to manage system infrastructure issues, including incidents related to system security. Tickets are assigned to support personnel based on the nature of the ticket. All changes are documented in the ticketing system from initiation through deployment.	Observe the ticketing system and confirm that tickets are assigned to support personnel based on the nature of the ticket to manage system infrastructure issues, and validate changes are documented in the ticketing system from initiation through deployment. In addition, inspect the DevOps Ticketing System Policy and confirm a process is in place to properly assign tickets to support personnel.	No exceptions noted.
	CHANGE MANAGEMENT			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Subservice organizations are required to maintain their own security practices and procedures, including regular testing and updates of the business continuity and disaster recovery programs as well as patch management. Conformance is assessed annually through review of SOC 2 reports.	Obtain evidence that the subservice organization's most recent SOC 2 reports were reviewed in the past year. In addition, inspect the Sub-Service Security Review Policy and confirm it requires review of SOC 2 reports at least annually.	No exceptions noted.
		Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements. The procedures require that change requests are: * Authorized * Formally documented * Tested prior to migration to production * Reviewed and approved	Inspect the change management plan and confirm it requires that change requests are authorized, formally documented, tested prior to migration to production, and reviewed and approved. Select a sample of changes during the examination period and obtain evidence to confirm that each change was authorized, formally documented, tested prior to migration to production, and reviewed and approved.	No exceptions noted.
		Lessonly has developed and maintains a documented baseline configuration of the internal control systems.	Obtain evidence that the baseline configuration of internal control systems are documented and maintained.	No exceptions noted.
		Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation.	Inspect system screenshots and verify that development environments are separate from test environments.	No exceptions noted.
		External vulnerability scans and external penetration tests are performed at least annually.	Inspect the most recent external vulnerability scan and external penetration test and validate they were performed within the past year. In addition, inspect the Third Party Penetration Testing Policy and confirm it requires annual penetration testing.	No exceptions noted.
		Developers do not have the ability to migrate changes into production environments without prior approval.	Inspect the change management plan and verify it addresses segregation of duties. Select a sample of changes during the examination period and verify that the same person did not develop and also migrate each change into production environments.	No exceptions noted.
		A ticketing system is in place to manage system infrastructure issues, including incidents related to system security. Tickets are assigned to support personnel based on the nature of the ticket. All changes are documented in the ticketing system from initiation through deployment.	Observe the ticketing system and confirm that tickets are assigned to support personnel based on the nature of the ticket to manage system infrastructure issues, and validate changes are documented in the ticketing system from initiation through deployment. In addition, inspect the DevOps Ticketing System Policy and confirm a process is in place to properly assign tickets to support personnel.	No exceptions noted.
	RISK MITIGATION			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.
		Lessonly maintains insurance to minimize the financial impact of any loss event.	Determine that the program includes cyber insurance for potential loss events.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Lessonly maintains insurance to minimize the financial impact of any loss event.	Determine that the program includes cyber insurance for potential loss events.	No exceptions noted.
		Subservice organizations are required to maintain their own security practices and procedures, including regular testing and updates of the business continuity and disaster recovery programs as well as patch management. Conformance is assessed annually through review of SOC 2 reports.	Obtain evidence that the subservice organization's most recent SOC 2 reports were reviewed in the past year. In addition, inspect the Sub-Service Security Review Policy and confirm it requires review of SOC 2 reports at least annually.	No exceptions noted.
		Documented information security policies and procedures are in place to guide personnel through information security standards that include, but are not limited to, the following: * Password Policy * Access Authorization Policy * IT Operational Policy * Audit Logging Policy * Encryption and Network Security Policy	Inspect the IT Operational Policy, Encryption Policy, Access Authorization Policy, and Password Policy documents and confirm they include information security standards, including policies for passwords, authentication and access control, auditing, and encryption.	No exceptions noted.

TSC Ref. #	Criteria	Control Description	Test Procedures Performed by The Mako Group CPAs, PLLC	Results of Tests
		Lessonly management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Executive Leadership Team. Assessments include evaluations of key controls and results of external assessments, such as vulnerability assessments. The assessment also identifies key information system processes that process relevant data into information to support internal controls. If changes to controls are determined to be necessary, action is taken and communicated.	Inspect the completed risk assessment and determine that it included evaluations of key controls and results of external assessments, such as vulnerability assessments, and identified key information system processes that process relevant data into information to support internal controls. Inspect Executive Leadership Team meeting minutes and confirm that the risk assessment was discussed with the Executive Leadership Team. If changes to controls were determined to be necessary, confirm that action was taken and communicated.	No exceptions noted.