UMU LLC

Independent Service Auditor's SOC3 Report

For

UMU Online Learning Platform

For The Period Of

September 01, 2024 – August 31, 2025

Attestation and Compliance Services

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To UMU LLC

Scope

We have examined UMU LLC accompanying assertion titled "Management's Assertion" that the controls within UMU Online Learning Platform were effective throughout the period September 01, 2024 to August 31, 2025 to provide reasonable assurance that UMU LLC's service commitments and system requirements were achieved based on the trust service criteria relevant to Security, Confidentiality, Availability, Processing Integrity and Privacy ("applicable trust services criteria") set forth in TSP Section 100, *Trust Services Criteria for Security, Confidentiality and Availability, Processing Integrity and Privacy (AICPA, Trust Services Criteria).*

UMU LLC uses various subservice organizations for data center hosting services. The description system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at UMU LLC, to achieve UMU LLC's service commitments and system requirements based on the applicable trust service criteria. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at UMU LLC, to achieve UMU LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents UMU LLC's controls, the applicable trust service criteria, and the complementary user entity controls assumed in the design of UMU LLC's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

UMU LLC 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 UMU LLC's service commitments and system requirements were achieved. UMU LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, UMU LLC is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve UMU LLC's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve UMU LLC's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within UMU LLC's UMU Online Learning Platform was effective throughout the period September 01, 2024 to August 31, 2025, to provide reasonable assurance that UMU LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CertPro CPA LLC

Certified Public Accountants
License Number: CF-0010928
State of Delaware
December 26, 2025

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within UMU LLC's UMU Online Learning Platform throughout the period September 01, 2024 to August 31, 2025 to provide reasonable assurance that UMU LLC's service commitments and system requirements relevant to Security, Confidentiality*,* Availability, Processing Integrity and Privacy were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 01, 2024 to August 31, 2025, to provide reasonable assurance that UMU LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality*,* Availability, Processing Integrity and Privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Confidentiality, Availability, Processing Integrity and Privacy (AICPA, Trust Services Criteria)*. UMU LLC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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

We assert that the controls within the system were effective throughout the period September 01, 2024 to August 31, 2025, to provide reasonable assurance that UMU LLC's service commitments and systems requirements were achieved based on the applicable trust services criteria.

For UMU LLC

Authorized Signatory

Shirley Wang

SECTION 3

DESCRIPTION OF THE SYSTEM

Types of Services Provided

UMU LLC is a performance learning platform founded in 2015 with staff and partners in the US, Japan, China, and Taiwan. The UMU platform allows for course builder, enterprise, Artificial Intelligence (AI) practice, and live stream features. Utilizing learning science and AI, the platform empowers training leaders and educators to drive performance and results.

UMU LLC's interactive platform is a training environment that fosters participation from trainees, allowing organizations to accurately gauge their audience and identify common interest topics. Organizations are able to curate their own training courses by using the course builder tool to upload content. The platform integrates gamification and social interaction into the content, improving training retention and enabling real-time feedback. Comprehensive dashboards are provided to help track the progress and engagement of trainees.

Any other services provided by UMU LLC are not in the scope of this report.

Principal Service Commitments and System Requirements

UMU LLC designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that UMU LLC makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that UMU LLC has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in Service-Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security principles include but are not limited to, the following:

- The fundamental design of UMU LLC's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- UMU LLC implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between UMU LLC and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

Processing Integrity commitments include, but are not limited to, the following:

- Procedures exist to prevent, or detect and correct, processing errors to meet the entity’s processing integrity commitments and system requirements.
- System output is complete, accurate, and distributed to meet the entity’s processing integrity commitments and system requirements.
- System inputs are measured and recorded completely, accurately, and timely to meet the entity’s processing integrity commitments and system requirements.

Privacy commitments include, but are not limited to, the following:

- Establishing privacy policies and procedures for specifying how personal information is handled.
- Establishing policies and procedures for collecting and retaining data.
- Implementing procedures for notifying data subjects in case of data breach.
- Obtaining user consent for data collection and for its usage.
- Implementing mechanisms for data subjects to access and control their data.

Such requirements are communicated in UMU LLC's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System used to Provide Services

Infrastructure & Network Architecture

UMU online learning platform is hosted in Tokyo (ap-northeast-1) and Oregon (us-west-2) regions in Amazon Web Services (AWS), and in europe-west4-a/b in Google Cloud Platform (GCP). UMU online learning platform uses a virtual and secure network environment on top of AWS and GCP infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a Virtual Private Cloud (VPC) and accompanying firewalls on the infrastructure provider.

UMU online learning platform ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer’s client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through an AWS or GCP Internet Gateway, over to a virtual private cloud that:

1. Houses the entire application runtime.
2. Protects the application runtime from any external networks.

The internal networks of AWS and GCP are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

Further, all VPC network flow logs are continuously monitored by Palo Alto Firewall for malicious activity and unauthorized behavior.

Software

UMU Online Learning Platform leverages various systems/applications like AWS, GCP including Outlook, Wazuh, Cortex, Workspace ONE, Prometheus, Asana, GitLab, Jenkins, Ansible as well as G Suite and Slack for client communication. These tools are deployed across a combination of cloud-based services and UMU Online Learning Platform's infrastructure components such as servers, databases, and storage systems.

UMU Online Learning Platform uses a subservice provider, Drata Platform, to provide continuous compliance monitoring of the company's system.

People

UMU LLC staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel has also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support UMU Online Learning Platform. These policies cover:

- Code Of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information Security
- Vendor Management
- Physical Security
- Risk Management
- Password
- Media Disposal
- Incident Management
- Endpoint Security
- Encryption
- Disaster Recovery
- Data Classification
- Confidentiality
- Business Continuity
- Access Control
- Acceptable Usage
- Vulnerability Management
- Human Resource Management

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

UMU LLC also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the UMU online learning platform software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Data

All data that is managed, processed and stored as a part of the UMU online learning platform software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts.

Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls of the in-scope system. UMU LLC reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the UMU online learning platform software application.

Logical Access

The UMU online learning platform software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application, and authenticates the database.

UMU LLC has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

The Information Security Officer is responsible for performing periodic reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the UMU LLC are reviewed, deployed, and managed. The policy covers all changes made to the UMU online learning platform software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information.
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Customer content and personal information are not used in non-production environments.

Incident Management

UMU LLC has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact UMU LLC via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of UMU LLC being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.

- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.

- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.

- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

Availability

UMU LLC has a documented Business Continuity Plan (BCP) and testing performed against the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Boundaries of the System

UMU Online Learning Platform depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

Complementary User Entity Controls

UMU Online Learning Platform’s controls related to UMU Online Learning Platform cover a subset of overall internal control for each user of their service. The control objectives related to UMU Online Learning Platform cannot be achieved solely by the controls put in place by UMU Online Learning Platform; each customer’s internal controls need to be considered along with UMU Online Learning Platform’s controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Complementary Subservice Organization Controls

UMU LLC uses subservice organizations in support of its system. UMU LLC's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the UMU LLC to be achieved solely by UMU online learning Platform. Therefore, user entity controls must be evaluated in conjunction with UMU LLC's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

UMU LLC periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports.
- Regular meetings to discuss performance.
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS, GCP	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	AWS, GCP	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS, GCP	CC6.4, A1.2
Business Continuity and Disaster Recovery Procedures are developed, reviewed, and tested periodically.	AWS, GCP	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	AWS, GCP	A1.2
A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	AWS, GCP	C1.1
A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	AWS, GCP	C1.2