EVERFI

Service Auditors' Report on Controls at a Service Organization (SOC 3®) Relevant to Security

For the Period August 15, 2020 to February 14, 2021

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of EVERFI, Inc.:

Scope

We have examined EVERFI, Inc.'s ("EVERFI") accompanying assertion titled "Assertion by Management of EVERFI, Inc." ("assertion") that the controls within EVERFI's digital learning platforms, Foundry and Homeroom (system) were effective throughout the period August 15, 2020 to February 14, 2021, to provide reasonable assurance that EVERFI'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, *Trust Services Criteria*).

EVERFI used subservice organizations during the period under audit to provide a private cloud hosting environment and other cloud based services. 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 EVERFI, to achieve EVERFI's service commitments and system requirements based on the applicable trust services criteria. 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

EVERFI 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 EVERFI's service commitments and system requirements were achieved. EVERFI has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, EVERFI 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 Auditors' 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 August 15, 2020 to February 14, 2021 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve EVERFI'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 EVERFI'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 the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within EVERFI's system were effective throughout the period August 15, 2020 to February 14, 2021, to provide reasonable assurance that EVERFI's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SC+H Attest Services, P.C.

SC&H Attest Services, P.C.
Sparks, Maryland
April 16, 2021

EVERFI

Assertion by Management of EVERFI, Inc.

We, as management of EVERFI, Inc. ("EVERFI" or the "Company"), are responsible for designing, implementing, operating, and maintaining effective controls within EVERFI's digital learning platforms, Foundry and Homeroom (system) throughout the period August 15, 2020 to February 14, 2021, to provide reasonable assurance that EVERFI's service commitments and system requirements relevant to security were achieved. Our attached description of the boundaries of the system identifies the aspects of the system covered by our assertion.

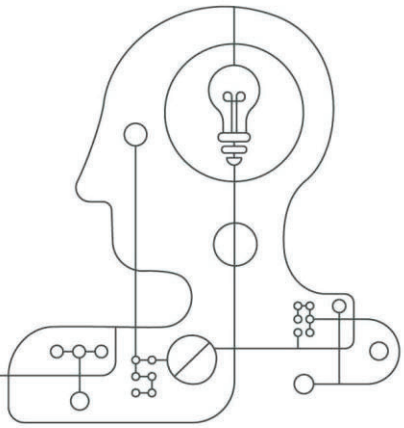
We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 15, 2020 to February 14, 2021, to provide reasonable assurance that EVERFI's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, *Trust Services Criteria)*. EVERFI's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented within the attached description.

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 August 15, 2020 to February 14, 2021, to provide reasonable assurance that EVERFI's service commitments and system requirements were achieved based on the applicable trust services criteria.

EVERFI, Inc.

EVERFI, Inc.



Introduction

Company Overview

EVERFI, Inc. ("EVERFI" or the "Company") is an international technology company driving social change through education, to address the most challenging issues affecting society, ranging from financial wellness to prescription drug safety to workplace conduct and other critical topics. Founded in 2008, EVERFI is fueled by its Software-as-a-Service (SaaS) community engagement platform.

Description of Services Provided

EVERFI provides a full suite of socially aware digital learning services to over 3,100 customers, serving a variety of markets. EVERFI provides cloud-based learning tools designed to provide critical skills curriculums, while bringing together the public and private sectors to change the way that education is delivered. EVERFI has reached more than 41 million learners across the K-12, higher education, and adult markets with more than 250 digital education courses on social issues.

EVERFI's applications provide the ability for customers and their authorized users to manage their user accounts, while EVERFI personnel support the functionality of EVERFI's digital course platforms. EVERFI's two main digital learning platforms are Foundry and Homeroom.

Principal Service Commitments and System Requirements

EVERFI designs its processes and procedures related to its course platforms to meet its objectives to deliver digital learning services. Those objectives are based on the service commitments that EVERFI has made to user entities, the laws and regulations that govern the provision of software services, and the financial, operational, and compliance requirements that EVERFI has established for the services.

Security commitments to user entities are documented and communicated in the Company's Privacy Policy, Master Services Agreements and other customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of its course platforms that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

EVERFI establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in EVERFI's system policies and procedures, system design documentation, and contracts with domestic 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 have been documented on how to carry out specific manual and automated processes required in the operation and development of the digital learning platform.

Organizational Structure

The Company's organizational structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job function. The structure provides for clearly defined roles, responsibilities, and lines of authority for reporting and communication.

Each department is managed by employees with significant experience and education in their respective field. Duties are segregated to ensure adequate financial and operational controls.

Oversight of the organization is facilitated via the existence of an independent Board of Directors. The Board of Directors meet quarterly to discuss the business, including reviews of financial performance of the organization, strategic deliberations of the Company's strategy and focus, and approval of plans of action to provide ongoing support to the organization through its various stages of growth.

The Company's Security Council, comprised of senior members of the Engineering, Legal & Finance teams, meets quarterly to discuss the business, including oversight of the development and performance of internal control.

Leadership Team

The leadership team provides overall direction to the Company. All members of the leadership team are actively engaged in the review, approval, and administration of the policies and procedures associated with business operations and the platforms supported by the Company.

EVERFI's leadership team consists of the Chief Executive Officer; President and CoFounder, Enterprise; President and CoFounder Enterprise & International; Chief Operating Officer; Chief Financial Officer; Chief Product Officer; Chief Technology Officer; and General Counsel.

The leadership team has the ultimate responsibility for all activities, including the internal control system, the assignment of authority and responsibility for operational activities, and the establishment of reporting relationships and authorization protocols. The leadership team in conjunction with the Board of Directors are responsible for establishing the strategic plan and all aspects of operational and financial management.

Relevant Aspects of the Control Environment, Risk Management, Information and Communication, Monitoring, and Control Activities

We believe internal control consists of five interrelated components;

Control Environment: This sets the tone of a company, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Risk Management: This is a company's identification and analysis of risks relevant to the achievement of its objectives and forming a basis for determining how the risks should be managed.

Information and Communication: Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control a company's operations.

Monitoring: The entire internal control process must be monitored, and modifications are made as necessary. To support the modification, the systems react dynamically and change as conditions warrant.

Control Activities: Control policies and procedures must be established and executed to help ensure that the actions identified by management are completed as necessary to address risks for achievement of a company's control objectives.

Set out below is a description of the components of internal control related to the services that may be relevant to users of the system(s).

Control Environment

The objectives of internal control as it relates to the Company are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant trust services criteria, that assets are protected from unauthorized acquisition, use or disposition, and that processes and procedures are executed in accordance with management's authorization and instruction.

The control environment reflects the overall attitude and awareness of management and personnel considering the importance of controls and the emphasis given to controls in policies, procedures, and actions. Management has established and maintains controls designed to monitor compliance

with established policies and procedures. The remainder of this subsection discusses the risk management process, information and communication, and monitoring. The internal control structure is refreshed based on the Security Council and management's assessment of risks facing the Company.

Risk Management

The process of identifying, assessing, and managing risks is a critical component of the Company's internal control system. The purpose of the risk assessment process is to identify, assess, and manage risks that affect the Company's ability to achieve objectives. Management also monitors controls to consider whether they are operating as intended, and whether they need to be modified for changes in conditions or risks.

In conjunction with the strategic planning, management evaluates the organizational structure, including reporting lines, and participates in ongoing risk assessment procedures to evaluate threats to business objectives and operations, including but not limited to relationships with vendors, business partners and other parties; environmental, regulatory, technological, and fraud threats to the system(s) security; and the development and performance of internal control. Changes to identified threats are also considered. Discussions, including determination of risk mitigation strategies to reduce risk to acceptable levels, are facilitated via completion of an annual, formal risk assessment. When the need for a new control is identified, management develops the requirements for the new control, including consideration of both manual and automated, and preventative and detective controls. Meeting minutes are maintained.

The risk management program includes the use of insurance to minimize the financial impact of any potential loss events.

Information and Communication

Information and communication are an integral component of the Company's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control operations. This process encompasses the primary classes of transactions of the Company, including the dependence on, and complexity of, information technology. At the Company, information is identified, captured, processed, and reported by various information systems.

The Company has various information security policies to help ensure that employees understand their individual roles and responsibilities within the control environment and to ensure significant events are communicated and handled timely.

The IT team is in constant communication in order to monitor and manage their department's progress as it relates to the achievement of responsibilities, including internal control. Information necessary to achieve the Company's service commitments and system requirements is disseminated.

Contractual agreements provide a mechanism for communicating the terms of service within the Company and between the Company, customers and vendors with access to sensitive data (i.e. high-

risk vendors). Contractual terms outline terms and payment for services, use of services, and enforcement. Management reviews and approves each contractual agreement with customers. Any changes are reviewed by management and sent to the necessary team(s) for execution of the changes. The terms and conditions, security commitments, and obligations and responsibilities of high-risk vendors, including subservice organizations, are clearly defined and agreed upon.

Management has made contact information available to external users, consumers, auditors, regulators, vendors and others on the applicable website(s).

Monitoring

Monitoring is an integral part of the Company's internal control framework. Monitoring activities consist of assessments and the quality control process, which monitors changes in the industry as well as internal controls.

Ongoing monitoring procedures are built into the normal recurring activities and include regular management and supervisory activities. Managers of the various organizational units are in regular communication with personnel and may question the accuracy of information that differs significantly from their knowledge of operations.

The IT and Engineering Cloud Architecture teams capture security events in audit logs and conduct periodic reviews of activities within all related departments. Related department reviews include tests and review of policies and procedures including logical access, physical access, software network monitoring, change management, incident response, and backups.

Management reviews and approves all Company policies prior to release to verify they don't breach any security concerns and to confirm that they do not conflict with any of the existing security policies. The team monitors security best practices and trains staff on their use.

Furthermore, the Company is responsible for ensuring that the environment is equipped with the latest security products, as necessary, and is responsible for keeping up to date with the latest exploits and vulnerabilities. The Company completes continuous automated internal and external vulnerability scans in order to facilitate the security of the system. Additionally, detailed vulnerability assessments are performed annually. Any high-risk vulnerabilities identified are tracked through resolution.

Subservice Organizations

The Company uses subservice organizations to provide various services. The scope of this report does not include the controls at the applicable subservice organizations.

The following is a description of the services each subservice organization provides:

Subservice Organization	Service Provided
Amazon Web Services (AWS)	Secure, cloud-based content management and collaboration. Private cloud hosting environment providing environmental protections, and physical security.
Google	Secure, cloud-based suite of services providing productivity applications, email hosting, and online communications.
Salesforce	Salesforce provides a customer relationship management (CRM) tool to store and manage customer information in one central location.

The Company has identified the following control to help monitor the subservice organizations:

- Annually, the Company's management obtains and inspects the latest applicable subservice organization's SOC report(s) to ensure an unqualified opinion, appropriate coverage over the audit period, implementation of relevant complementary subservice organization controls, and that noted exceptions are appropriately reviewed by a member of management for potential impact.

Complementary User Entity Control Considerations

The Company has determined that certain complementary controls should be implemented by external users to achieve certain criteria included in this report. The complementary user entity controls are listed below.

The list of complementary user entity control considerations presented below should not be regarded as a comprehensive list of all controls that should be employed by users. There may be additional controls that would be deemed appropriate that are not identified in this report.

Complementary User Entity Control
External users are responsible for periodically reviewing those with access to the portal, including terminations, to ensure only authorized users maintain active access privileges.
External users are responsible for establishing physical and logical security protection over all workstations, servers, and communication hardware that interface with their environment and that are housed in their facilities or other locations under their control or supervision.
External users are responsible for reporting any application problems, including unauthorized use of any password or account or any other known or suspected breach of security encountered and to provide such assistance as is necessary to permit problem resolution.
External customer administrators are responsible for establishing procedures to provide an initial password to learners, when EVERFI password authentication is used.

Complementary User Entity Control
User organizations utilizing single sign-on (SSO) integrations are responsible for managing their password configurations, including change frequency.
Where applicable with SSO integrations, customers are responsible for providing valid security assertion markup language (SAML) certificates for their systems and properly importing EVERFI's SAML certificates.
Customers are responsible for establishing documented policies and procedures for the transfer and sharing of information within their organization and with third-party entities.
Customers are responsible for provisioning, maintaining, and disabling admin and learner access in accordance with their internal access management policies.
Customers are responsible for adhering to the Terms of Service defined on company website: https://everfi.com/terms-of-service.
Where applicable, customers are responsible for the configuration of the user organization application programming interface (API) system level calls to access EVERFI's API. Customers should reference https://resources.everfi.com/help/technical-integrations/api/ for more information.