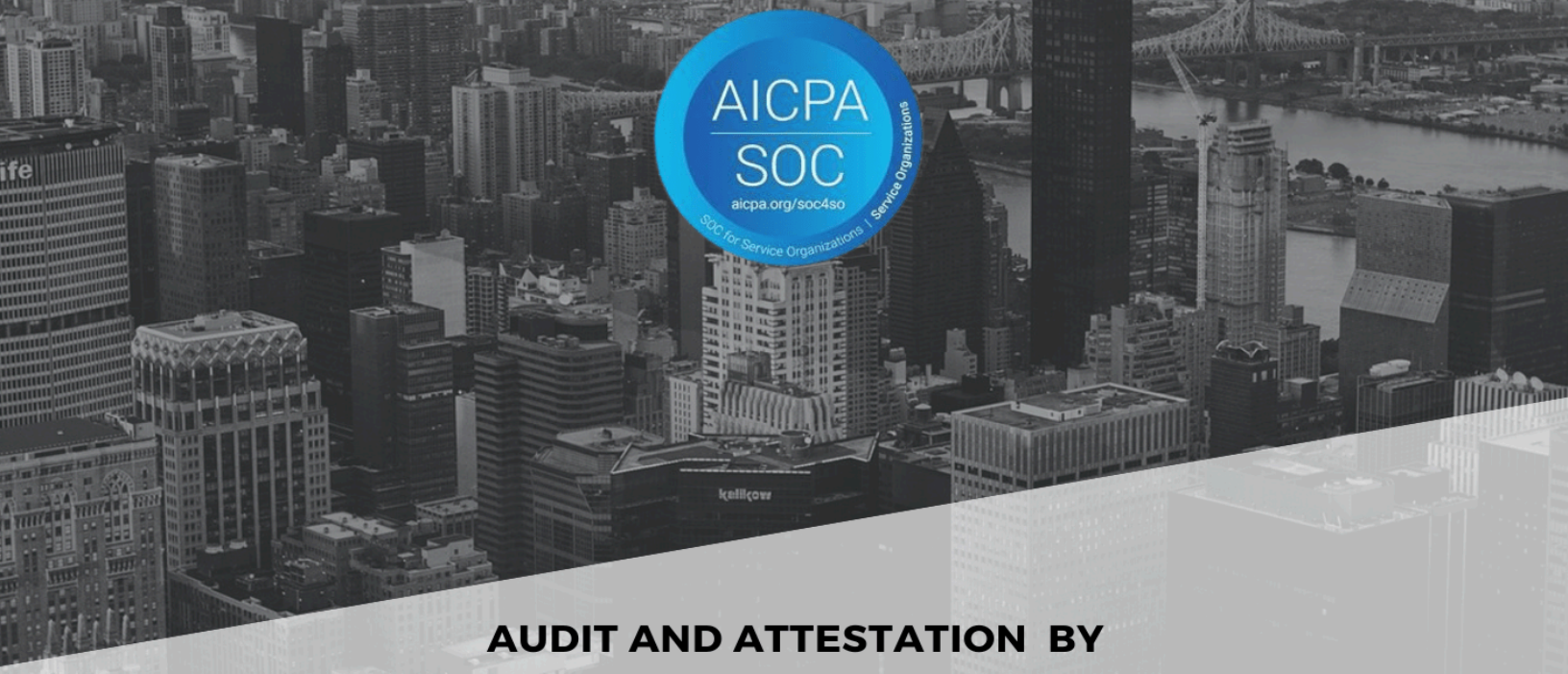
Accredible

SOC 3 Report

EdInvent Inc. d.b.a. Accredible.

January 1, 2024 to December 31, 2024

An Independent Service Auditor's Report on Controls Relevant to Security



AUDIT AND ATTESTATION BY

PRESCIENT
ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

Management's Assertion **4**
Independent Service Auditor's Report 7
Scope 7
Service Organization's Responsibilities 7
Service Auditors' Responsibilities 8
Inherent Limitations 8
Opinion 9
Attachment A **10**
Company Overview and Types of Products and Services Provided 11
The Principal Service Commitments and System Requirements 12
The Components of the System Used to Provide the Services 13
People 13
Processes and Procedures 13
Boundaries of the System 14
The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved 15
Integrity And Ethical Values 16
Management's Philosophy and Operating Style 16
Human Resources 17
Change Management 17
Reporting deficiencies 17
Complementary User Entity Controls (CUECs) 18
Complementary Subservice Organization Controls (CSOCs) 19
Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant 20
Disclosures of Significant Changes In Last 1 Year 20

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of EdInvent Inc. d.b.a. Accredible.'s system throughout the period January 1, 2024 to December 31, 2024, 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 3® Report. The description is intended to provide report users with information about EdInvent Inc. d.b.a. Accredible.'s system that may be useful when assessing the risks arising from interactions with EdInvent Inc. d.b.a. Accredible.'s system, particularly information about system controls that EdInvent Inc. d.b.a. Accredible. has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

EdInvent Inc. d.b.a. Accredible. uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EdInvent Inc. d.b.a. Accredible., to achieve EdInvent Inc. d.b.a. Accredible.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EdInvent Inc. d.b.a. Accredible.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EdInvent Inc. d.b.a. Accredible., to achieve EdInvent Inc. d.b.a. Accredible.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EdInvent Inc. d.b.a. Accredible.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'s controls.

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

a. The description presents EdInvent Inc. d.b.a. Accredible.'s system that was designed and implemented throughout the period January 1, 2024 to December 31, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that EdInvent Inc. d.b.a. Accredible.'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 and user entities applied the complementary controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'s controls during that period.
c. The controls stated in the description operated effectively throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that EdInvent Inc. d.b.a. Accredible.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'s controls operated effectively throughout the period.

DocuSigned by:
Alan Heppenstall
311D24E153CE4EE...

Alan Heppenstall
CTO
EdInvent Inc. d.b.a. Accredible.

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: EdInvent Inc. d.b.a. Accredible.

Scope

We have examined EdInvent Inc. d.b.a. Accredible.'s ("EdInvent Inc. d.b.a. Accredible.") accompanying description of its Accredible Processing System system found in Section 3, titled EdInvent Inc. d.b.a. Accredible. System Description throughout the period January 1, 2024, to December 31, 2024, 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 3® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that EdInvent Inc. d.b.a. Accredible.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

EdInvent Inc. d.b.a. Accredible. uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EdInvent Inc. d.b.a. Accredible., to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents EdInvent Inc. d.b.a. Accredible.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'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.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EdInvent Inc. d.b.a. Accredible., to achieve EdInvent Inc. d.b.a. Accredible.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EdInvent Inc. d.b.a. Accredible.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'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 complementary user entity controls.

Service Organization's Responsibilities

EdInvent Inc. d.b.a. Accredible. 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 EdInvent Inc. d.b.a. Accredible.'s service commitments and system requirements were achieved. In Section 1, EdInvent Inc. d.b.a. Accredible. has provided the accompanying assertion titled "Management's Assertion of EdInvent Inc. d.b.a. Accredible." (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. EdInvent Inc. d.b.a. Accredible. 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 Auditors' 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 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 operating 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 the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. 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.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. 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.
5. 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.
6. Evaluating the overall presentation of the description.

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of 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.

Opinion

In our opinion, in all material respects:

a. The description presents EdInvent Inc. d.b.a. Accredible.'s system that was designed and implemented throughout the period January 1, 2024, to December 31, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that EdInvent Inc. d.b.a. Accredible.'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 and user entities applied the complementary controls assumed in the design of EdInvent Inc. d.b.a. Accredible.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that EdInvent Inc. d.b.a. Accredible.'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 EdInvent Inc. d.b.a. Accredible.'s controls operated effectively throughout the period.

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

Signed by:
Prescient Assurance
BDAFCCDC4A4A409...

Prescient Assurance LLC
March 21, 2025

SECTION 3

Attachment A

Company Overview and Types of Products and Services Provided

EdInvent Inc. doing business as (dba) Accredible ("Accredible" or "the Company") provides a software-as-a-service (SaaS) platform that enables educational and training providers to design, create, deliver, and manage digital credentials. Digital credentials include open badges, digital certificates, and blockchain records that represent achievements such as a degree, qualification, designation, course completion, or event attendance. Additional services are provided to facilitate the viewing, verification, and use of credential data by third parties.

Accredible is headquartered in Mountain View, CA, USA, with a subsidiary based in Ely, Cambridgeshire, UK.

The system description in this section of the report details the Accredible Processing System ("the System"). Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization)

The Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Accredible Processing System. Commitments are communicated via written certificate cloud services terms and conditions.

System requirements are specifications regarding how the System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	Accredible will maintain administrative, physical, and technical safeguards for the protection of customer data. Those safeguards will include measures for preventing unauthorized access, use, modification or disclosure of customer data by Accredible personnel, with the following exceptions: • To provide the services of the Accredible Processing System and prevent or address service or technical problems. • To comply with applicable law. • As expressly permitted in writing by the customer. • Accredible will host, maintain, and operate the Accredible Processing System for use by the customer and authorized users.	• Logical access standards • Physical access standards • Employee provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management • Incident handling standards • Change management standards • Vendor management • System monitoring • Firewall standards

The Components of the System Used to Provide the Services

The boundaries of the Accredible Processing System are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Accredible Processing System.

People

The Company develops, manages, and secures the Accredible Processing System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing Company-wide activities, establishing and accomplishing goals, and managing objectives.
Operations	Responsible for performing Company-wide activities related to finance, legal, human resources and operations.
Product & Engineering	Responsible for the development, testing, deployment, and maintaining new code for the Accredible Processing System. Responsible for access controls and security of the production environment.
Customer Success	Responsible for the onboarding of new customers, support existing customers, and ensuring that customers use the Accredible Processing System effectively.
Design	Responsible for branch design as well as user interface/user experience (UI/UX) design features and enhancements.
Sales	Responsible for helping prospective customers understand if Company products are appropriate for their business needs.

Processes and Procedures

Procedures include the automated and manual procedures involved in the operation of the Accredible Processing System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and human resources (HR). These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the Accredible Processing System:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Change Management

The change management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Software, system, and configuration changes, including major releases, minor releases, and hotfixes, are managed through a formal change and release management procedure and tracked using a centralized ticketing system. Changes are requested, approved, tracked, and implemented throughout the release life cycle, which includes the product and engineering planning, release management, deployment, and post-deployment support phases. Change requests are documented, assessed for their risks, and approved for acceptance or otherwise evaluated by the designated personnel.

Quality assurance testing is performed prior to the software release through each pre-production environment (i.e., local development and staging) based on defined acceptance criteria. Changes are reviewed for their adherence to established change and release management procedures prior to closure. Once deployed, changes are monitored for success; failed implementations are immediately rolled back, and the change is not considered complete until it is implemented and validated to operate as intended.

Boundaries of the System

The boundaries of the EdInvent system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly

support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the EdInvent system.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

Applicable Trust Services Criteria

The Trust Services Category that is in scope for the purposes of this report is security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the information or systems and affect the entity's ability to meet its objectives.

Many of the criteria used to evaluate a system are shared amongst all categories; for example, the criteria related to risk assessment apply to the security category. As a result, the criteria for the security category are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category.

The common criteria are organized as follows:

- Control environment: The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
- Communication and information: The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
- Risk assessment: The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
- Monitoring activities: The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
- Control activities: The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
- Logical and physical access controls: The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
- System operations: The criteria relevant to how the entity manages the operation of system(s)

and detects and mitigates processing deviations, including logical and physical security deviations.

- Risk mitigation: The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security category. The Company has elected to exclude the availability, processing integrity, confidentiality, and privacy categories.

Control Environment

Integrity And Ethical Values

Accredible has an Acceptable Use Policy and Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. Accredible has also developed employee confidentiality agreements that prohibit the inappropriate use and disclosure of customer or Company information. All employees are required to sign an acknowledgment form that they have received and agree to follow the Acceptable Use Policy, Code of Conduct, and Confidentiality Agreement prior to their start dates.

Company management conducts semi-annual performance reviews with personnel to maintain compliance with organization policies and codes of conduct. Employees and contractors who violate the code of conduct are subject to disciplinary actions.

Board Of Directors

Accredible has a board of directors that meets quarterly. The board of directors is responsible for Company oversight of management and internal control.

Management's Philosophy and Operating Style

Accredible's senior management takes a proactive approach to running the business. Executive management is heavily involved in all phases of the business operations and committed to providing customer support. Management uses a top-down approach to establish or improve specific business objectives for business units and functions, including IT, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives.

Authority and Responsibility

Management and employees are assigned levels of authority and responsibility to facilitate effective internal control. The Chief Technology Officer (CTO) is responsible for overseeing the control environment and executing Accredible's strategy and other decisions as agreed upon by executive management and advisors. The engineering team reports to the CTO.

As part of the development of specific business objectives, the Chief Executive Officer (CEO) updates the Company's overall objectives with the objectives of the business units and other functional areas.

HR Policies and Practices

Accredible maintains formal hiring and termination policies and procedures. Applicants with a role in the delivery of services are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and employee expectations. They are evaluated on their level of

education, the merits of their past experience, a positive performance history, and knowledge of relevant security controls and processes. Through the onboarding process, all new hires must pass a background check and complete security awareness training.

If an employee violates any statute of the employee handbook or Accredible's policies, or otherwise acts in a manner deemed contrary to Accredible's mission and objectives, whether purposefully or not, the employee is subject to sanctions up to and including termination.

All employees go through a documented -annual performance review cycle. At least once per year, employees and their managers establish goals and expectations for their job performance and assess their performance during the previous twelve months. Employees whose performance is not in alignment with established goals and expectations for job performance or who are not fulfilling their job responsibilities may be put on a remediation plan by their managers to improve performance.

Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Complementary User Entity Controls (CUECs)

The Company's controls related to the Accredible Processing System cover only a portion of overall internal control for each user entity of the Accredible Processing System. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. Controls to provide reasonable assurance that the Company is notified of changes in: • User entity vendor security requirements.

	• The authorized users list.
CC2.3	It is the responsibility of the user entity to have policies and procedures to: • Inform their employees and users that their information or data is being used and stored by the Company. • Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4 CC6.5 CC7.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at- home agents for which the user entity allows connectivity.

Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to the Accredible Processing System cover only a portion of the overall internal control for each user entity of the Accredible Processing System. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection. AWS' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, the Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Accredible Processing System to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	AWS is responsible for encrypting data at rest on physical servers in its possession.
CC6.4	AWS is responsible for restricting data center access to authorized personnel. AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5	AWS is responsible for securely decommissioning and physically destroying production assets in its control.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC7.2	AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

There were no specific security Trust Services Criteria as set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria), that were not relevant to the system as presented in this report.

Disclosures of Significant Changes In Last 1 Year

There were no changes that are likely to affect report users' understanding of how Accredible Processing System is used to provide the service from January 1, 2024, to December 31, 2024.