SOC 3 Report for EdInvent Inc. d.b.a. Accredible.

An Independent Service Auditor's Report
on Controls Relevant to Security
January 1, 2025 to December 31, 2025

AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

Prescient Assurance LLC.
1900 Church Street, Suite 300
Nashville, TN, 37203

CPA

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

Table of Contents

SECTION 1

Management's Assertion

Accredible

Restricted Use & Distribution

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within EdInvent Inc. d.b.a. Accredible's Accredible Processing system (the system) throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that EdInvent Inc. d.b.a. Accredible's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period January 1, 2025 to December 31, 2025, 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 (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). EdInvent Inc. d.b.a. Accredible'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 in Attachment B.

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.

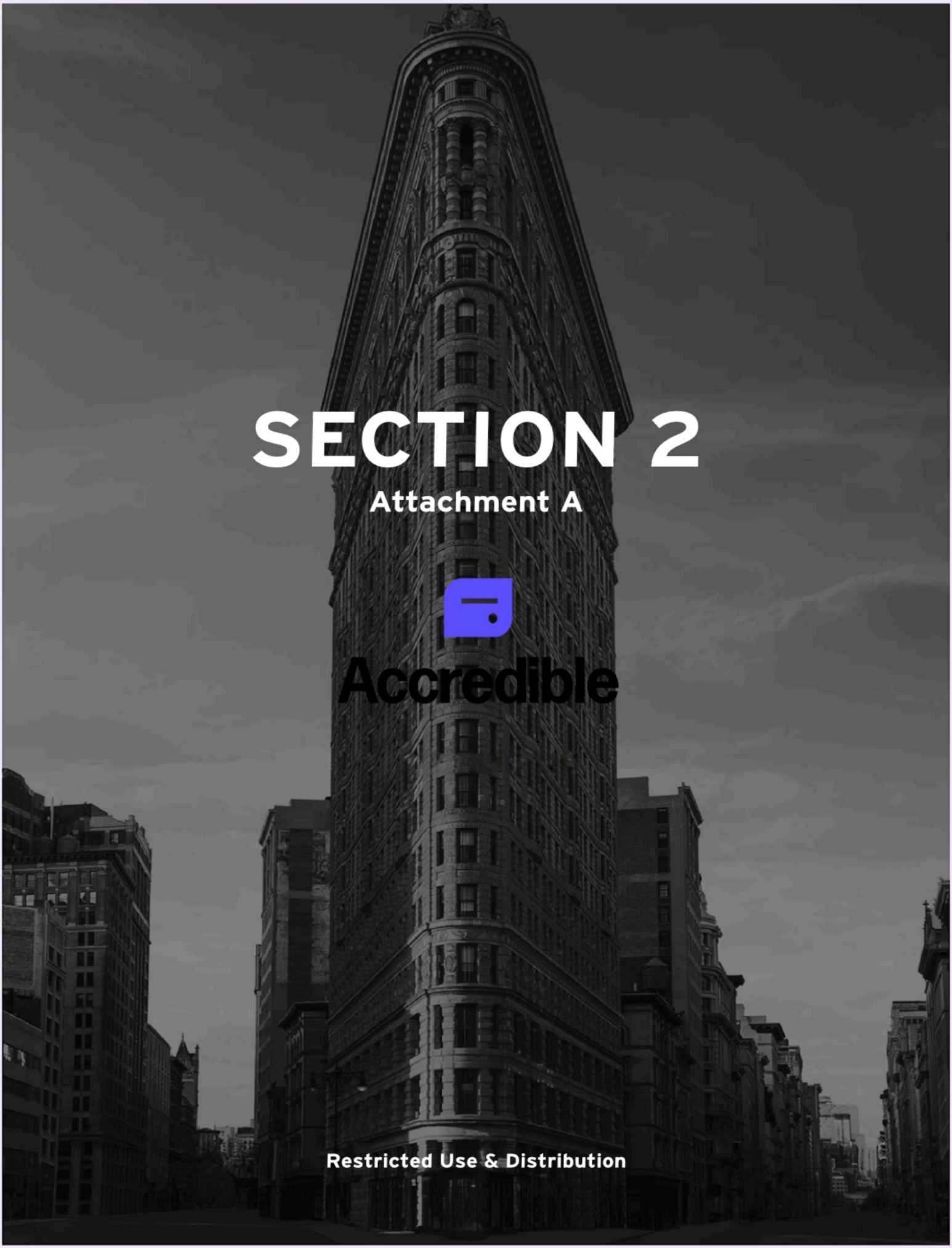
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EdInvent Inc. d.b.a. Accredible, to achieve EdInvent Inc. d.b.a. Accredible's service commitments and system requirements based on the applicable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

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 January 1, 2025 to December 31, 2025, 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.

DocuSigned by:
Alan Heppenstall
311D24E153CE4EF...

Alan Heppenstall
Chief Technology Officer
EdInvent Inc. d.b.a. Accredible


SECTION 2
Attachment A
Accredible
Restricted Use & Distribution

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 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.

The components that directly support the services provided to customers are described in the subsections below.

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:

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, supporting 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.

Logical Access

The System Access Control Policy establishes the access control requirements for requesting and provisioning user access for the System. The policy requires that access be denied by default, follow the principle of least privilege, and be granted only upon business need. Each user account is unique and is identifiable to an individual user. Segregation of duties is established on critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Domain-account management requests are routed to the designated asset owner or associated employee according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through the addition of individual user accounts to established domain security groups within the domain. Based on the configuration of a security group, any access requests require explicit approval from the assigned security group owner.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Account management processes prevent the creation of an account for individuals that do not have valid HR records. Select users can request removal of user accounts from the system. In addition, system owners can directly remove users from security groups.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Quarterly reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken as necessary based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password length and complexity. Accredible personnel are required to follow the Accredible password policy for all domains as well as local user accounts for all assets.

Access to the production environment is controlled through a designated set of access points and restricted to the Accredible teams. Users are authenticated to access points using domain credentials depending on where the production assets are located. Passwords, along with two-factor authentication used to access network devices, are restricted to authorized individuals and system processes based on job responsibilities.

Production servers are configured to authenticate through AWS Identity and Access Management (IAM). Production servers require users to perform two-factor authentication to gain access to the production servers using Elastic Compute Cloud (EC2) instance connect. EC2 instance connect enforces that connections made to the production server are encrypted.

Accredible maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within the Company and prioritized based on the asset's business value and criticality to the organization. The classification process is owned by the engineering team. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the asset management policy and vendor management policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets.

The inventory of virtual servers is monitored and maintained by the engineering team. The Company regularly checks for completeness and accuracy of the inventory to ensure that it represents the production environment appropriately. In addition, network architecture is maintained as part of the inventory process. Metadata of the assets is collected and maintained within the inventory that provides

Compute Operations

Accredible has established incident response procedures and centralized tracking tools, which consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via email. Users are made aware of their responsibilities of reporting incidents that will be investigated without any negative consequences against the reporting user. The Company incident response provides 24/7 event or incident monitoring and response services. The teams assess the health of various components, along with access to detailed information, when issues are discovered.

Accredible teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity and escalating accordingly to the appropriate groups for timely action. The engineering team documents, tracks, and coordinates responses to incidents. Where

required, security incidents are escalated to the privacy, legal, or executive management teams following established forensic procedures to support potential legal action after an information security incident.

Post-mortem activities are conducted for customer-impacting incidents or incidents with high severity. The post-mortems are reviewed by the engineering team during weekly review meetings with senior management. Incident and security post-mortem trends are reviewed and evaluated periodically and, where necessary, the platform or security program may be updated to incorporate improvements identified because of incidents.

Accredible utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

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.

System Boundaries

The boundaries of the Accredible 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.

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

Complementary Subservice Organization Controls (CSOCs)

The description does not extend to the services provided by AWS (the subservice organization). Section 4 of this report and the description of the system only cover the relevant trust services criteria and related controls in support of the achievement of Accredible's service commitments and system requirements and exclude the related controls of the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, Accredible's management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. Such controls are necessary, in combination with controls at Accredible, to provide reasonable assurance that Accredible's service commitments and system requirements were achieved. Because the related service commitments and system requirements can only be achieved if the CSOCs are suitably designed and operating effectively during the period January 1, 2025, to December 31, 2025, each user entity must evaluate Accredible's controls, related tests of controls, and results of tests described in section 4 of this report, considering the types of related CSOCs expected to be implemented at the subservice organization as shown below.

Subservice Organization	Services Provided	Criteria	Expected CSOCs
AWS	Infrastructure Hosting	CC6.4	Physical access to data centers is approved by an authorized individual.
		CC6.4	Physical access rights are revoked in a timely manner when no longer required.
		CC6.4	Physical access to data centers is reviewed periodically by appropriate personnel.
		CC6.4	Data center facilities are monitored using physical security monitoring controls, including video surveillance.
		CC6.4	Access to server location is managed by electronic access control devices.
		CC7.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

		CC7.5	Backup and recovery capabilities are maintained to support restoration of systems following security incidents or system failures.
		CC8.1	Changes are reviewed for business impact and approved by authorized personnel prior to migration to production.

Management of Accredible receives and reviews independent third-party assessment reports of its subservice organization annually. In addition, Accredible management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented at the subservice organization are suitably designed and operating effectively. Management monitors the subservice organization status page to stay informed of any changes in the services performed and has a customer support portal to relay any issues or concerns to subservice organization management.

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 that were not relevant to the Accredible's system as presented in this report.


SECTION 3
Attachment B
Accredible
Restricted Use & Distribution

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.

Security commitments

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- 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
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal

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

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 Accredible's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Accredible'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 the service organization has implemented in this area are described below:

- The company requires employees to acknowledge an employee handbook at the time of hire. Employees who violate the employee handbook are subject to disciplinary actions in accordance with a disciplinary policy.
- The company requires employees to sign a confidentiality agreement during onboarding.
- The company performs background checks on new employees.

Commitment to Competence

Accredible's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
- The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

Management's Philosophy and Operating Style

The Accredible management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Accredible can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Accredible, Inc. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- The company's board of directors meets at least quarterly and maintains formal meeting minutes. The board includes directors that are independent of the company.
- The company's board of directors or a relevant subcommittee is briefed by senior management at least quarterly on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.

Organizational Structure and Assignment of Authority and Responsibility

Accredible's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and

responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Accredible's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

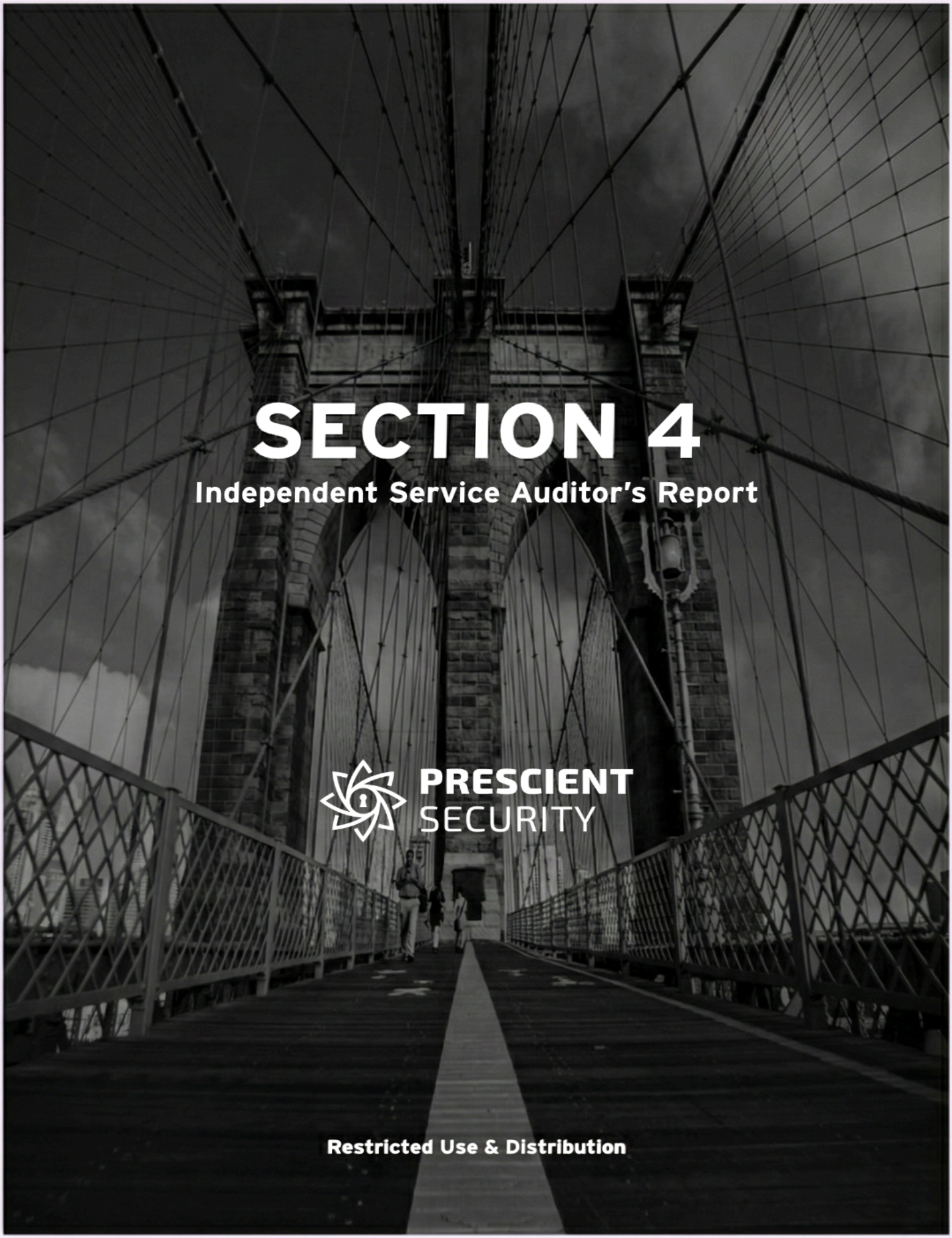
- The company maintains an organizational chart that describes the organizational structure and reporting lines.
- Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

Human Resource Policies and Practices

Accredible's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization is operating at maximum efficiency. Accredible's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counselling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- The company requires employees to acknowledge an employee handbook at the time of hire. Employees who violate the employee handbook are subject to disciplinary actions in accordance with a disciplinary policy.
- The company requires employees to sign a confidentiality agreement during onboarding.
- The company managers are required to complete performance evaluations for direct reports at least annually.
- The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.



SECTION 4

Independent Service Auditor's Report

PRESCIENT SECURITY

Restricted Use & Distribution

Independent Service Auditor's Report

To Management of EdInvent Inc. d.b.a. Accredible

Scope

We have examined EdInvent Inc. d.b.a. Accredible's (Accredible) accompanying assertion in Section I, titled "Management's Assertion" (the assertion) that the controls within EdInvent Inc. d.b.a. Accredible's Accredible Processing system (the system) were effective throughout the period January 1, 2025 to December 31, 2025, 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 (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*).

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 I, EdInvent Inc. d.b.a. Accredible has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, EdInvent Inc. d.b.a. Accredible 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 system requirements were achieved based on the applicable trust services criteria. 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 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve EdInvent Inc. d.b.a. Accredible'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 EdInvent Inc. d.b.a. Accredible'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.

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

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 risks 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 EdInvent Inc. d.b.a. Accredible's Accredible Processing system was effective throughout the period January 1, 2025 to December 31, 2025, 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 and is fairly stated, in all material respects.

Prescient Assurance LLC

Signed by:
Prescient Assurance
30A76903DD934BD...

Prescient Assurance
April 24, 2026