A-LIGN

Elevate K-12

Type 2 SOC 3

2025

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2025 to March 31, 2025

Table of Contents

SECTION 1

ASSERTION OF ELEVATE K-12 MANAGEMENT

ASSERTION OF ELEVATE K-12 MANAGEMENT

April 11, 2025

We have prepared the accompanying description of Elevate K-12's ('Elevate' or 'the Company') Remote Teaching Platform services titled "Elevate K-12's Description of Its Remote Teaching Platform services throughout the period January 1, 2025 to March 31, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Remote Teaching Platform services that may be useful when assessing the risks arising from interactions with Elevate's system, particularly information about system controls that Elevate 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 (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*).

Elevate uses Amazon Web Services, Inc. (AWS) and Microsoft Azure (Azure) to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Elevate, to achieve Elevate's service commitments and system requirements based on the applicable trust services criteria. The description presents Elevate's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Elevate's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents Elevate's Remote Teaching Platform services that was designed and implemented throughout the period January 1, 2025 to March 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2025 to March 31, 2025, to provide reasonable assurance that Elevate's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Elevate's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2025 to March 31, 2025, to provide reasonable assurance that Elevate's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Elevate's controls operated effectively throughout that period.

Jake Galey

Jake Galey
VP of Finance
Elevate K-12

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Elevate K-12

Scope

We have examined Elevate's accompanying description of its Remote Teaching Platform services titled "Elevate K-12's Description of Its Remote Teaching Platform services throughout the period January 1, 2025 to March 31, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2025 to March 31, 2025, to provide reasonable assurance that Elevate'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*).

Elevate uses AWS and Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Elevate, to achieve Elevate's service commitments and system requirements based on the applicable trust services criteria. The description presents Elevate's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Elevate's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Elevate 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 Elevate's service commitments and system requirements were achieved. Elevate has provided the accompanying assertion titled "Assertion of Elevate K-12 Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Elevate is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

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

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

Independence and Ethical Responsibilities

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 users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects,

a. the description presents Elevate's Remote Teaching Platform services that was designed and implemented throughout the period January 1, 2025 to March 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2025 to March 31, 2025, to provide reasonable assurance that Elevate's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Elevate's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2025 to March 31, 2025, to provide reasonable assurance that Elevate's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Elevate's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4*,* is intended solely for the information and use of Elevate, user entities of Elevate's Remote Teaching Platform services during some or all of the period January 1, 2025 to March 31, 2025, business partners of Elevate subject to risks arising from interactions with the Remote Teaching Platform services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
April 11, 2025

SECTION 3

ELEVATE K-12'S DESCRIPTION OF ITS REMOTE TEACHING PLATFORM SERVICES THROUGHOUT THE PERIOD JANUARY 1, 2025 TO MARCH 31, 2025

OVERVIEW OF OPERATIONS

Company Background

EDBLOX, Inc., d.b.a. Elevate K-12, established in 2015, is an education technology company that develops and provides live online group instruction classes with a focus on general kindergarten to 12th-grade education (K-12). The Company's headquarters are located in Chicago, Illinois, and it serves customers throughout the United States of America. Its customers consist of public-school districts and private schools that do not have enough qualified teachers to teach live classes for their student base. The Company offers certified teachers, state-compliant curriculum, and online class delivery technology to deliver live online classes in school and during school hours.

Description of Services Provided

At Elevate, we enable high-quality live teaching for every learner in the United States:

- Remarkable Live Teaching: We empower schools nationwide with expert virtual teachers who specialize in engagement strategies and dynamic online instruction. With an average of 13 years of experience, certified educators build meaningful connections while delivering flexible, high-quality learning. Supported by ongoing coaching and development, they drive student success and foster equitable learning for all.
- High-Quality Academic Products and Services: We offer a diverse portfolio of courses, including core subjects, enrichment, ELL (English Language Learner), Special Education, and remedial support, tailored to meet the unique needs of students and schools. Additional services like teacher collaboration and office hours create impactful learning experiences that inspire growth and achievement.
- Seamless District Integration and Support: We create a unified experience for schools and teachers by integrating solutions with district systems, including SSO (Single Sign-On), Curriculum, LMS (Learning Management System), SIS (School Information System), and Gradebooks. Through strong customer success activities, collaborative partnerships, and joint success planning, we ensure smooth onboarding and ongoing support to drive sustainable, long-term outcomes for districts and students alike.
- Impactful Tech Products: Technology powers the Elevate ecosystem, equipping schools and teachers with tools like the SandD Portal, Live Digital Classroom Portal, and Teacher Homeroom. Advanced matching ensures the best teacher fit based on key parameters, while program data analytics provide schools with insights into student activity and learning. Through partnerships with Edlink, Salesforce, Planhat, and Nearpod, we deliver seamless, integrated solutions that enhance the experience.

Principal Service Commitments and System Requirements

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

Elevate's commitments to users are communicated through Master Service Agreements (MSAs), the online Privacy Policy, and detailed service descriptions.

Components of the System

Infrastructure

Elevate's services are deployed in a multi-tenant architecture. The systems application infrastructure is hosted by both AWS and Azure, which provide scalable cloud hosting services as subservice organizations.

Elevate's Security Policy ensures that workstations are equipped with appropriate security software and regularly updated with the latest patches. In the event of security threats, automated systems respond with quarantine or removal actions as necessary. The Information Technology (IT) and Security and Infrastructure Teams maintain defenses and monitor vulnerabilities across the network and application infrastructure.

Security monitoring includes multiple layers of traffic detection for malicious content. Third-party penetration tests are conducted annually to identify vulnerabilities and assess the security of production systems. Additionally, employee workstations meet minimum security standards, and backup workstations are maintained to minimize operational disruptions.

Primary infrastructure used to provide Elevate's Remote Teaching Platform services includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Servers	Cloud hosting
Azure	Servers	Cloud hosting
Firewalls	Cisco MX95 and Fortigate 80F	Filters traffic into and out of the private network supporting the corporate offices
Switches	Cisco MS355 and Fortigate 80F	Connects devices on the corporate network by sending message to the specific device(s) that need to receive it
WAP	Cisco MR46 and Ruijie Reyee RG-RAP226 and TP-Link EAP660 HD	Access points for devices to connect to secure wireless network in the corporate offices

Software

Primary software used to provide Elevate's Remote Teaching Platform services includes the following:

Primary Software	
Software	**Purpose**
Microsoft 365	E-mail/Data/Collaboration Vendor
Cisco Meraki	Network Security and Virtual Private Network (VPN)
Zscaler	Server Access Control
Microsoft Defender	EDR/EDP System
Microsoft Entra ID	Identity and Access Control
Datto - Backupify	Backup for Microsoft 365
Snowflake	Data Warehousing Solution
Dynamics 365	Teacher and Class Rostering and Tracking
Microsoft Sentinel	Incident Response and Alerting
1Password	Password management and security
Microsoft Purview	Audit Logging and Incident Review
Dynatrace	Used for monitoring AWS cloud

Primary Software	
Software	**Purpose**
CoreStack	Monitor cloud cost and security
8x8	Audio and video streaming in live classes
Otus	Learning Management System
WatchRTC	Monitor and capture audio video packets
Secureworks	User for vulnerabilities scanning
BrowserStack	Testing in various browser and OS combinations
Azure DevOps	Code repository and deployments

People

Elevate employs dedicated team members to handle major product functions, including operations, and support. The Engineering/IT Team monitors the environment, as well as manages data backups and recovery.

Elevate strives to hire the right people for the right job as well as training them in their specific tasks and ways to keep the company and its data secure.

Elevate has a staff of approximately 200 organized in the following functional areas:

Teacher Community and Marketing: Responsible for recruiting, hiring, training, and allocating teachers. This team also promotes brand awareness through multiple media channels.

Customer Success, Sales, and Operations: Customer Succes is responsible for proactively assisting customers in achieving their desired outcomes with the service. Sales is responsible for selling products and services to customers, including prospecting, engaging with customers, and closing deals. The sales function is responsible for generating revenue and growing the business. Operations is responsible for the activities, processes, and functions needed to provide services to customers, including customer service and IT and technical support.

Product Management: Responsible for guiding a product through its lifecycle. This includes prioritizing the features, enhancements, and user experience. Product Management works with cross-functional teams to ensure the right products get built in the right way to drive business success and user satisfaction.

People: The People Team oversees payroll, benefits administration, and compliance, ensuring seamless execution of employee lifecycle processes such as onboarding and offboarding. Additionally, the People Team owns the end-to-end recruitment process, attracting, hiring, and retaining top talent, manages leadership coaching, employee growth initiatives, and performance development program, and implements policies and programs that enhance workplace culture, engagement, internal progression/mobility and organizational effectiveness.

Finance: Responsible for the accuracy of financial reporting, tax compliance, corporate treasury matters, client invoicing, payment and procurement processing. Also responsible for budgeting and partnering with leadership to set strategic direction of the business.

Engineering: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. IT and Security team within Engineering is responsible for managing laptops, software, and other technology involved in employee productivity and business operations, including information security and data privacy while complying with regulations, standards, and industry best practices.

Data

Data, as defined by Elevate, constitutes any information collected from employees, candidates, users, customers, vendors, or other parties that provide information to Elevate.

Elevate utilizes multiple databases, file stores, and object stores to store and process the data. To assist with the data handling procedures, Elevate has a documented Data Management Plan that defines system and operational requirements for retention, encryption, and storage. The Plan is updated on at least an annual basis.

Elevates' systems, procedures, use of data, and services are in accordance with the Family Education Rights and Privacy Act (FERPA) governing the use of student data.

Student data is stored on servers within the United States.

Elevate receives Student Data from Schools and Users in order to provide Services under its Agreement with the School. Elevate receives personally identifiable information such as a student's first and last name, through information provided by the User.

Elevate collects Student Data and User personally identifiable information from the school.

Student Data we collect and store from the School includes, but is not limited to the student's and/or User's:

- First and last name
- Grade level (for example: sixth grade, seventh grade, etc.)
- User-generated content
- Student generated content, school records, such as attendance, grades, assessments, and Individual Education Plan status, teacher comment and feedback

<u>How Student Data is Used</u>

Elevate uses Student Data for educational purposes, to provide Services pursuant to an Agreement, to improve education Services, for purposes requested by the School, as permitted by applicable law, for customer support, to enforce access and security controls, to conduct system audits.

Elevate teachers access Student Data via livestream education instruction platform. Elevate's teachers are able to access a Student's personally identifiable information such as Student e-mail addresses, Student generated content, IEP status, and first and last names in conducting assessments and in delivering instruction. Teachers are able to see a Student's likeness via online streaming in School classrooms in order to provide instruction, and Elevate teachers are able to engage in livestream conversations with Students in School classrooms with a member of the School's staff present. Elevate's employees only access such Student Data to the extent necessary for such teachers to provide Services under an Agreement with the School.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Elevate policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Elevate team member.

Physical Security

Elevate's production servers are maintained by AWS and Azure. Physical and environmental security protections are the responsibility of AWS and Microsoft. Elevate reviews the attestation reports and performs a risk analysis of AWS and Microsoft on at least an annual basis.

This report does not include the cloud hosting services provided by AWS and Azure.

Logical Access

Elevate provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes.

IT is responsible for provision access to the system based on the employee's role. The employee is responsible for reviewing Elevate's policies and completing security training. When an employee is terminated, IT is responsible for deprovisioning access to in scope systems immediately upon employee's termination. Access reviews of logical systems are required to occur at least annually.

Computer Operations - Backups

Customer data is backed up and monitored by the Engineering Infrastructure Team for completion and exceptions. If there is an exception, the Infrastructure Team will perform troubleshooting to identify the root cause and either rerun the backup immediately or as part of the next scheduled backup job. Backup infrastructure is maintained in the AWS and Microsoft clouds. Backups occur daily and are encrypted, with access restricted to key personnel. Testing is conducted quarterly to ensure backups can be successfully restored to a sandbox environment.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Elevate has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Elevate staff validate that patches have been installed and if applicable that reboots have been completed.

Elevate uses AWS and Microsoft cloud services to host the platform with multiple availability zones configured to allow the resumption of services in the event of an outage at a single location.

Elevate monitors the capacity utilization of computing to support service uptime.

The Engineering Team is responsible for performing daily backups of data necessary to resume the in-scope services. The Engineering Team monitors backups for any errors.

Change Control

Elevate has a documented Systems Development Life Cycle (SDLC) to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing, and approval procedures. A ticketing system is utilized to document changes in the application. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment. Version control software is utilized to maintain source code and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the cloud infrastructure supporting the services to help ensure that there is no single point of failure. In the event that a primary system fails, the redundant system is configured to take its place.

Penetration testing is conducted on an annual basis to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology.

Vulnerability scans are performed monthly on the environment. The third-party vendor uses industry standard scanning technologies. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis.

Boundaries of the System

The scope of this report includes the Remote Teaching Platform services performed in the Chicago, Illinois facilities.

This report does not include the cloud hosting services provided by AWS and Azure.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the three months preceding the end of the review period.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the three months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security criteria were applicable to the Elevate Remote Teaching Platform Services System.

Subservice Organizations

The scope of this report includes the Remote Teaching Platform services performed in the Chicago, Illinois facilities.

This report does not include the cloud hosting services provided by AWS and Azure.

Subservice Description of Services

AWS and Azure provide cloud hosting services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of physical access to the facilities.

Complementary Subservice Organization Controls

Elevate's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Elevate's services to be solely achieved by Elevate control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Elevate.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Responsible for restricting data center access to authorized personnel.
		Responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
		Responsible for securely decommissioning and physically destroying production assets in its control.
		Responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers.
		Responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply.
		Responsible for overseeing the regular maintenance of environmental protection at data centers.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

Elevate management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Elevate performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Elevate's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Elevate's services to be solely achieved by Elevate's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Elevate.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Service Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entity's locations, user entities auditors should exercise judgement in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Elevate.
2. User entities are responsible for notifying Elevate of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Elevate services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Elevate services.
6. User entities are responsible for immediately notifying Elevate of any actual or suspected information security breaches, including compromised user accounts, those used for integrations, and secure file transfers.