Stile Education Pty Ltd - Stileapp.com Platform

As of 11/13/2024

A Type 1 Independent Service Auditor Report on Controls Relevant to Security

Stile

TABLE OF CONTENTS

Stile

SECTION I - Service Organization Management's Assertion

Strike Graph
999 Third Ave. 33rd Floor
Seattle, WA 98104

In connection with your engagement to report on Stile Education Pty Ltd's (service organization) description of its stileapp.com platform (system), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure. Our representations, as outlined in this letter, serve to enable you to form the following opinions on whether as of 11/13/2024:

- The System Description adheres to 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* (description criteria);
- The system was designed and implemented following the description criteria;
- The controls stated in the System Description (Description) were suitably designed;
- The controls stated in the Description provide reasonable assurance that Stile Education Pty Ltd's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security (applicable Trust Services Criteria) outlined in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

We confirm, to the best of our knowledge and belief, as of the date of this letter, the following representations were made to you during your examination:

1. We reaffirm our assertion, which is attached to the Description.
2. We have evaluated the presentation of the Description following the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria. All relevant matters have been considered and reflected in our evaluation and our assertion.
3. We have disclosed to you any of the following of which we are aware:
    a. Misstatements (including omissions) in the Description;
    b. Instances in which controls were not suitably designed and implemented;
    c. Instances in which controls did not operate effectively or as described;
    d. Any communications from regulatory agencies, user entities, or others affecting the presentation of the Description or the suitability of the design or operating effectiveness of the controls stated therein, including communications received between the end of the period addressed in our Description and the date of your report;
    e. All other known matters contradicting the presentation of the Description or the suitability of the design or operating effectiveness of the controls stated therein or contradicting our assertion.
4. We acknowledge responsibility for our assertion and for:

a. The presentation of the Description, following the description criteria and the suitability of the design and operating effectiveness of the controls, stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria;

b. Selecting the Trust Services category or categories to be included within the scope of the examination and determining that they are appropriate for our purposes;

c. The applicable Trust Services Criteria and related controls are stated in the Description.

5. We have disclosed to you any known events after the period covered by the Description up to the date of this letter that would have a material effect on the presentation of the Description or the suitability of the design or operating effectiveness of the controls stated therein or on our assertion. We have disclosed any changes in the controls that are likely to be relevant to report users, occurring through the date of this letter.

6. As agreed upon in the terms of the engagement, we have provided you with all information and access relevant to your examination and to our assertion.

7. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the presentation of the Description, following the Description criteria or to the suitability of the design and/or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria.

8. We have responded fully to all inquiries you made during the examination.

9. We have disclosed to you any of the following of which we are aware:

    a. Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the presentation of the Description or the suitability of the design or operating effectiveness of the controls stated therein;

    b. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization that may affect one or more user entities;

    c. All identified system incidents that significantly impaired the service organization's achievement of its service commitments and system requirements as of 11/13/2024.

We understand that your examination was conducted following attestation standards established by the AICPA. The examination was designed to express an opinion on whether, in all material respects, the Description is presented following the Description criteria; 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 also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

1. The Description presents the stileapp.com platform that was designed and implemented as of 11/13/2024, by the description criteria.

2. The controls stated in the Description were suitably designed as of 11/13/2024, to provide reasonable assurance that Stile Education Pty Ltd's service commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively as of 11/13/2024.

Stile

Alex Finkel

Alex Finkel, Head of Platform Engineering
Stile Education Pty Ltd

11.14.2024

Stile

SECTION II - Independent Service Auditor's Report

To: Stile Education Pty Ltd

Scope

Stile Education Pty Ltd has engaged Strike Graph to perform internal audit services. These services include a review of the System Description and test of the controls design related to the stileapp.com platform. The results of tests conducted by the Strike Graph internal audit team are used by the service auditor in a direct assistance capacity and adhere to the guidance outlined in AT-C Section 205.

We have examined Stile Education Pty Ltd's accompanying System Description based on the criteria for a description of a service system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (with Revised Implementation Guidance - 2022)*, and the suitability of the design of controls stated in the description as of 11/13/2024.

Our examination provides reasonable assurance that Stile Education Pty Ltd service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security (applicable Trust Services Criteria) outlined in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Service Organization's Responsibilities

Stile Education Pty Ltd is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to reasonably ensure that service commitments and system requirements are achieved. Stile Education Pty Ltd has provided the accompanying assertion titled "Service Organization Management's Assertion" (assertion) about the description and the suitability of the design of controls stated therein.

Stile Education Pty Ltd is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the service(s) 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 commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and the suitability of the design of controls stated in the description based on our examination. Attestation standards established by the AICPA conducted our examination. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented by the description criteria and whether 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 the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of the description of a service organization's system and the suitability of the design 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 criteria do not present the description and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description criteria present the description;
- 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;
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users. It may not include every aspect of the system that individual users may consider essential to meet their own informational needs.

Any system of internal control has inherent limitations, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not continuously operate effectively to reasonably ensure that the service organization's service commitments and system requirements are achieved based on the applicable Trust Services Criteria. Also, any projections to the future of any conclusions about the suitability of the design of controls are 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 over time.

Description of Tests of Controls

Section IV lists the specific controls we tested and the nature, timing, and results of those tests.

Opinion

In our opinion, in all material respects:

1. The description presents that Stile Education Pty Ltd – stileapp.com platform was designed and implemented as of 11/13/2024, following the description criteria.
2. The controls stated in the description were suitably designed as of 11/13/2024, to provide reasonable assurance that Stile Education Pty Ltd's service commitments and system requirements would be achieved based on the applicable Trust Services Criteria if its controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Stile Education Pty Ltd, user entities of Stile Education Pty Ltd – stileapp.com platform as of 11/13/2024, business partners of Stile Education Pty Ltd – stileapp.com platform, 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:

Stile

- The nature of the service provided by the service organization;
- How the service system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- User entity responsibilities and how they may affect the user entity's ability to use the service organization's services effectively;
- The applicable Trust Services Criteria;
- The risks 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.

Jajuan Williams

JaJuan Williams
Firm License: FP52300024
11.14.2024

Strike Graph

Stile

SECTION III - Description of Service Organization's System Overview of Operations

Company Background

Stile Education was founded in 2012 by Dr. Alan Finkel for a simple reason: to make science interesting, accessible, yet challenging for every student on the planet. Stile helps teachers bring their science classes to life with beautiful lessons based on real-world science and global issues.

Stile's resources are presented via our award-winning online teaching and learning platform, purpose-built to support both direct instruction and self-paced learning in modern science classrooms. Envisioned as a teacher's ultimate sidekick, Stile's technology is designed to put teachers in the driver's seat. It encourages collaboration and class debates, while making it simple to differentiate instruction and provide timely feedback. Stile's technology was co-created with teachers in Australian classrooms.

It's been battle tested by hundreds of thousands of students, and we're constantly refining it.

Overview of the System

Stile provides an online learning platform and science lessons for use by students in years 7-10 in the classroom, available at https://stileapp.com

Key Features

- Creation of lessons and quizzes
- Completion of quizzes and formative assessments on the stileapp.com platform
- Marking and feedback
- Live brainstorms and polls

Principle Service Commitments and System Requirements

Stile Education has designed its processes and procedures related to the stileapp.com (or the "System") to meet its objectives for reliability, privacy and security, to ensure that teachers and students are able to rely on being able to use stileapp.com in the classroom ("Services"). Those objectives are based on the service commitments that Stile Education makes to user entities and the operational and compliance requirements that it has established for the services. Stile Education's services are subject to the security requirements of security laws and regulations in the jurisdictions in which Stile Education services are offered. This report is limited in scope to the Security Trust Services Criteria based on guidance from the AICPA.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Use of modern encryption technologies to protect data both at rest and in transit.
- Network segmentation to ensure that customer data is not shared with other customers.
- A strong security culture during all phases of product development.

Stile

Stile Education establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Stile Education's system policies and procedures, system design documents, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the stileapp.com.

System Components

The stileapp.com platform is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of this system description is to delineate the boundaries of the system, which includes the services outlined above and the following components, described below: people, data, infrastructure, software, and processes.

The scope of this report includes the stileapp.com system. This report does not include the underlying hosting facilities provided by Amazon Web Services.

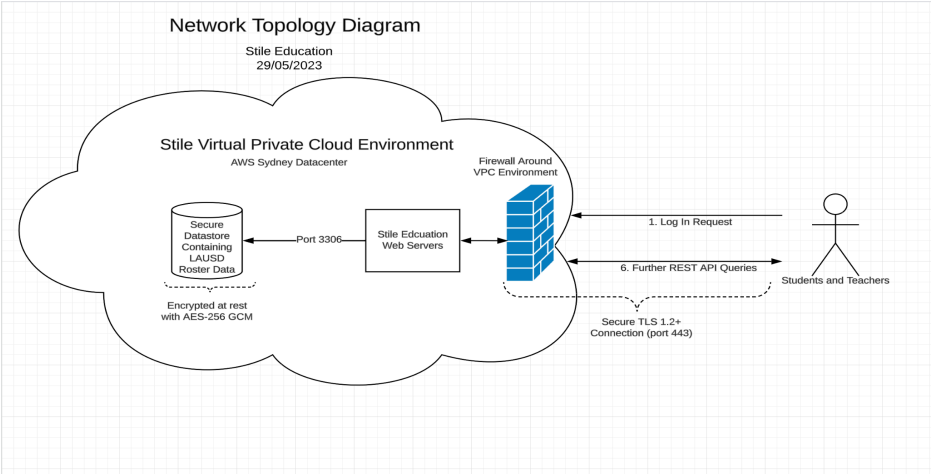
People

Stile Education is organized into functional areas. Within these functional areas, organizational and reporting hierarchies have been defined, and responsibilities have been assigned. Responsibilities for specific roles are clearly defined with job descriptions. The organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored.

- Product, comprising engineering, content and design
- Commercial, comprising sales, support, and success
- Operations, comprising finance, and HR

Data

Data Flow Diagram:



Stile

Data Collected by Stile:

Student Names	Optional	Stile displays student names (or optionally pseudonyms) to teachers when marking student assessments, arranging classes, and to enable moderation of class discussions, polls etc. If single sign on is not used, then students are presented with the option to enter a name when they first sign up to the platform. If single sign-on is used, then student names are set automatically based on data sent from the school's identity provider system.
Student Emails	Optional	Stile allows students to recover their passwords via email (if not using single sign-on) and notifies them when teachers invite them to new classes. Students can optionally use anonymous email addresses created by Stile.
Teacher Names	Optional	Teachers can enter a name (or pseudonym) to be shown to their students in the platform, and an alternate name (or pseudonym) that will be presented to their colleagues in the platform.
Teacher Emails	Required	Teacher email addresses are used for invitations, password recovery and transactional communications about their classes. Teachers are asked for their email when signing-up (if not using single sign-on)
Teacher media uploads	Optional	Teachers can upload files for their students including videos, photos documents and other media as part of building a lesson in the Stile platform
Student media uploads	Optional	Teachers can optionally request that students upload their work as a file, including photo/video files. If a teacher has enabled a moderated class discussion, then students can upload files to the discussion, including photos. Students can't upload files, photos, videos or other media unless a teacher has enabled one of the above features.
Attendance record data	Optional	Stile allows teachers to optionally select 'absent' as the reason for a student's assignment being incomplete, but Stile does not support maintaining a comprehensive attendance record.
Student work	Required	Students in Stile complete worksheets, including free text questions, multiple choice questions, interactive simulations and other kinds of student work
Student results	Required	Student work on assessments in the Stile platform is marked (automatically for some kinds of questions, or manually by the teacher for others) and those marks are tabulated and displayed to teachers in the platform.
Student chat comments	Optional	Stile allows optional in-class discussion, if the feature is enabled and moderated by a teacher. Stile also allows students to collaboratively brainstorm solutions to problems, and these submissions can optionally be shared within the class by a teacher.
Passwords	Optional	If using a single sign-on integration, Stile does not collect or allow the use of passwords. Otherwise, all users (teachers and students) are identified by a password stored by Stile using a modern, secure password-hashing algorithm (bcrypt).
Usage metadata	Required	Stile automatically records usage of the platform and actions taken in the platform. This data is used for multiple purposes: providing the core platform services (eg. showing authorship of a comment in the platform), for security and audit purposes (allowing our support team to track down unexpected changes), to enable effective operation of Stile's infrastructure (eg. predicting user counts so that servers can be provisioned), and to inform the development of improvements to the

		product (eg. monitoring anonymised usage of a new kind of question).
Browser IP addresses & User Agent strings	Required	Stile collects user agent strings and IP addresses from all requests automatically for security purposes, so that users can see where their account has been used from.

Data Classification

Level	Description	Examples	Restrictions
Secret	This data should only be handled automatically by machines, and either not stored at all, or only stored in hashed or encrypted formats to prevent accidental compromise of critical security systems.	User passwords, TLS keys, data encryption keys, TOTP codes etc.	• No human access allowed at all • Infrastructure operators may manage the code which modifies and manages these values • Information integrity is critical and must be verified by automated systems (MACs, checksums etc.)
Private	Any personally identifiable or sensitive information about students.	Student names, student emails, all content entered by students, content customisations by teachers, student marks, feedback etc. Production databases, database backups etc. HR records, resumes, interview notes.	• Stored securely in Stile's production cloud environment. Must never be copied to personal or company devices. • Always stored with strong encryption at-rest • Always transmitted with strong TLS encryption • Authorized Stile staff may access only with explicit consent from an authorized official (enforced with technical restrictions and audit processes) • May never be published or shared with a third party under any circumstances • Information integrity is important: only reliable, redundant, decay-resistant data storage systems may be used. Operationally critical information must be backed-up.
Confidential	Commercially sensitive information and all other personally identifiable or sensitive information (as described in Stile's data and privacy policy with the	Email and support correspondence, teacher names, teacher emails, teacher survey results, teacher PD attendance, school	• Authorized Stile staff may access only as needed • Always transmitted with strong TLS encryption • May be stored in production or corporate cloud

	Australian Privacy Principles) which isn't classified as 'Private'.	results etc. Anonymised usage information, anonymised log messages, anonymised interaction events, aggregated usage statistics, aggregated marks, aggregated student responses etc. Contract terms with schools, internal meeting minutes, strategy memos etc.	environments, in Stile's secure internal communication channels (GSuite Mail, Docs etc), or on individual managed devices as required. • May be published or shared with a third party only if completely anonymised, or with the explicit consent of all subjects • Information integrity is important: only reliable, redundant, decay-resistant data storage systems may be used. Operationally critical information must be backed-up.
Public		School names, school enrollment numbers etc.	• Stile staff may access freely • May be stored on any medium • May be published or shared with third parties as needed

Third Party Access

No third-party providers have access to our data.

Infrastructure

The primary infrastructure supporting the stileapp.com is comprised of:

AWS Computing Infrastructure		
Infrastructure	Type	Purpose
AWS Relational Database Services (RDS) - MySQL	Database	Primary production database
AWS S3	Database	Media files, long term storage
AWS EC2	Hosting	All web servers and compute
AWS IAM	Network	Identity management
AWS GuardDuty	Threat Detection Tool	Intelligent Threat Detection
AWS SecurityHub	Monitoring Tool	Monitors AWS Configuration for security issues
AWS Config	Monitoring Tool	Monitors changes to AWS Configuration

Software

Name	Purpose
AWS Sydney	Cloud hosting
AWS US-West	Language detection

Stile

Google G-suite	Email, calendar events, documents
Dead Man's Snitch	Meta-monitoring
Zamzar	Document transcoding
Zencoder	Video transcoding
Microsoft Azure	Backup storage
Github	Code storage, Issue tracking
Mailchimp	Mail automation
Mandril	Transactional email
Intercom	Live support chat
Pager Duty	Operational alerting
Google Analytics	Marketing site traffic analysis
Youtube	Video search
MixMax	Email tracking and automation?
Zendesk	Support articles
Salesforce	CRM
Slack	Messaging
Shopify	Selling merch
Stripe	Payment processing
Xero AU	Accounting and invoicing
Xero US	Accounting and invoicing
Buildkite	CI automation
Jamf	Staff device management
Asana	Project Management
Wistia	Online video hosting
Big Marker	Webinars
Zoom	Webinars
Google adwords	Advertising
Facebook	Community & advertising
Twitter	Community & advertising
Instagram	Community & advertising
Looker	Business intelligence visualization
Canva	Marketing
Lucid Charts	Process Mapping
Atlassian	Internal Wiki
Workable	HR Software
PandaDoc	Sales Contracts
Clockwise	Calendar Management
Twilio	SMS, notifications (staff only)

Apple business manager	
Ramp	Payments and Credit Cards in USA
Typeform	Two accounts, one with people ops and one with Sales
Prerender	Server-side rendering of dynamic content
Loom	Used by USA team (?)
1Password	Creating, storing, and sharing passwords
Microsoft Office	Powerpoint, Excel, Word (for those who need/prefer these)
PagerDuty	Oncall rotations

Processes

Both automated and manual processes have been established by the organization to support the operation of the stileapp.com system. These include procedures through which services activities are initiated, authorized, performed, and delivered. Management has developed policies that establish the organization's overall approach to internal controls related to security and operational processes. These policies comply with overall business objectives and are aimed to minimize risk through preventive measures, timely identification of irregularities, limitation of losses, and timely restoration.

The organization's policies include the definition of assignment responsibilities and address the following security life cycle processes which are further described in the Control Environment section of this document:

- Oversight, selection, documentation, implementation and monitoring of security controls
- Authorization, changes to, and termination of information system access
- Maintenance and support of the security system and necessary backup and offline storage
- Governance and processes for change management
- Incident response guidelines and processes
- Vendor oversight and processes to mitigate vendor risk
- IT and operational risk management

Subservice Organizations

The cloud hosting services provided by AWS are not included within the scope of this examination.

Stile

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communications, and Monitoring

Control Environment

Stile Education's control environment sets the tone of the organization and influences the control consciousness of its personnel. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. The control environment includes controls that may have a pervasive effect on the organization, an effect on specific processes, as well as security controls intended to effectively protect client data and provide a stable environment for the security of Stile Education's client-facing services. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

Integrity and Ethical Values

Integrity and ethical values are essential elements of Stile Education's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Stile Education's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Specific control activities that Stile Education has implemented in this area are:

- Working With Children checks for all staff
- Regular security training for all staff
- Strong leadership training program to embed values into the organization at all levels

Board/Owner/Management Oversight

Management Oversight - Stile Education's control consciousness is influenced significantly by the participation of its executive team. The executive team meets on a periodic basis to oversee operations management activities and to discuss and monitor related issues. Executive management meets and interacts with team members as a component of day-to-day operations to discuss business objectives and operational issues.

Stile's board of directors oversees the executive team and the proper function of the company as a whole, including taking direct responsibility for long term risk management.

Organizational Structure

Stile Education organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Stile Education management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Stile Education is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned.

Assignment of Authority and Responsibility

Stile Education's assignment of authority and responsibility 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 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 that 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.

Commitment to Competence

Stile Education is committed to providing the highest quality professional and technological resources. This includes management's consideration of the knowledge and skills necessary to accomplish tasks that define each employee's roles and responsibilities. To this end, management has implemented the following:

- Job scorecards for all roles
- Substantial employee training budget which managers are strongly encouraged to use
- Strong leadership training program

Accountability

Stile Education management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, management's attitudes and actions toward financial reporting, and management's attitudes toward information processing, accounting functions and personnel. Management meetings are held frequently to address issues as they are brought to management's attention. Stile Education' human resources policies and practices relate to employee hiring, orientation, training, evaluation, promotion, compensation, and disciplinary activities. Specific control activities that Stile Education has implemented in this area include:

- All hiring is overseen by the executive team and involves a rigorous standardized interview process
- Goals are set quarterly, tracked weekly, and progress is visible across the company

Controls

Security Management

Management has developed information security policies and related procedures to govern the security program at Stile Education. The Information Security Policy is maintained, reviewed and annually updated by the CEO. The development of an information security program, processes and procedures are the responsibility of the CTO. The Information Security Policies are reviewed and approved annually or as business needs change. Procedure documents related to access control and change management are updated as business needs change.

These policies and procedures cover the following key security life cycle areas:

- Data classification
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response

Logical and Physical Access

Stile's offices at 5/128 Exhibition St are protected by security card access and security cameras, but physical office access doesn't grant any privileged access to any of Stile IT systems, which all operate on a zero trust endpoint authentication basis.

All network access to sensitive systems is controlled by both a VPN, and individual SSO authentication to each system. All passwords are automatically generated and stored in a strong password manager. All logins require an MFA second factor.

Change Management

Stile Education has a Change Management Policy which governs deliberate changes to the IT environment, including infrastructure, data, and software development. The Change Management policy governs the request, documentation, testing and approval of changes. All technology acquisition, development and maintenance processes are governed by change management procedures. The Change Management Policy is communicated to relevant personnel and updated annually, or as business needs require. The CTO is the owner of the Change Management Policy and is responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on Company Operations.

Stile's industry leading ICT change-management process makes extensive use of automated testing, automated monitoring and manual review to ensure the highest quality standards are met consistently. Key steps in the change-release process are as follows:

- Significant ICT changes are initially planned in a Technical Requirements Description (TRD) document which is reviewed, improved and approved by senior engineering staff before work begins.
- All aspects of Stile's services and documentation (including TRDs) are managed through a central Version Control System (VCS), which allows all changes to be identified with a snapshot of the system code.
- All ICT changes — represented by a VCS snapshot — are manually tested in a development environment before being submitted for review.
- Before manual review and deployment, every submitted change must pass an extensive suite of automated tests. These tests cover every part of the system without exception, and include:
- Automatic enforcement of coding standards
- Unit testing of every system component in isolation
- Integration testing of whole server-side system
- Integration testing with real 3rd party service provider APIs
- Integration testing of the server and client systems together, including user-simulation via browser automation, and visual-difference testing
- Fault-injection testing in a simulated deployment environment
- All proposed changes are reviewed by engineers before being deployed. This process isn't just a formality: it regularly prompts a discussion which generates significant enhancements or design changes.
- Batches of changes are reviewed together by engineers before being deployed into the production environment
- All systems report extensive log, trace and metric data, describing the health of internal system processes, any unexpected events, and tracking the completion of expected workflows (request rates, response times, sign-in rates, usage of various features etc.). This data is used to ensure correctness in the development and testing phases, and to allow rapid, informed responses to incidents in production.

- Changes are all deployed with a blue-green process:
    1. The changed system is provisioned as a completely separate production environment
    2. All core functionality is tested in the new environment with built-in health monitoring systems and browser automation testing
    3. Then — only once the new system is confirmed to be working as expected — live traffic is transferred to the new system and key metrics are monitored for anomalous behaviour (which may indicate unexpected problems with the changes)
    4. If there is any unexpected behaviour from the new system, then traffic is redirected to the old system immediately to ensure uninterrupted service delivery while the anomaly is investigated.
    5. The old production environment will be de-provisioned only once the new system has been running reliably under significant load for at least 30 minutes.
- Deployed features are tested internally and with teachers in our beta tester program before being generally released (note: releasing new features is a separate step from deploying them, and can be instantly controlled by Stile's product team). This ensures that newly released features always work as expected in real classroom environments.
- A sample of deployed changes are re-reviewed internally by senior engineers and managers to audit for quality standards, and by groups of engineers as a learning exercise
- To allow rapid iteration and minimize deployment risk from large changesets, deployment of approved and tested changes happens at-least daily.
- Deployed systems are actively monitored for abnormalities and scanned/fuzz-tested for security vulnerabilities to rapidly detect any problems which have made it through to this point

Data Backup and Disaster Recovery

All key databases are backed up regularly, and our critical application databases — hosted on AWS RDS — have continual backup, enabling point-in-time recovery. These recovery processes are tested regularly.

Incident Response

Stile takes data confidentiality, integrity and availability very seriously and has strong data security measures in place. One of those measures is a sophisticated system of monitoring and alerting around all systems. These alerts allow rapid response to an incident in accordance with this plan. Stile maintains a 24/7 oncall rotation of expert engineers with escalation paths up to the CTO and CEO.

Vendor Management

The organization clearly defines vendor management roles, contract expectations and vendor risks in adherence to their Vendor Management Policy. Vendor management is overseen by the CFO. Formal contracts are utilized for vendor and business partner relationships; scope, responsibilities, compliance requirements and service levels (if required) are included in the contracts.

Stile Education performs due diligence activities over new vendors prior to contract execution and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk. Third party SOC 2 reports are reviewed for impact to the company environment.

System Monitoring

All critical systems export logs, metrics and traces which are analyzed via ChaosSearch, Grafana/Prometheus and Jaeger respectively. This data feeds into a sophisticated alerting system tied to playbooks, so that when system behavior deviates, a senior engineer steps in to investigate and remediate.

Various layers of continual automated testing and monitoring augment the above observability systems, including AWS GuardDuty, CrashTest fuzz testing, and our own in-house smoke testing suite.

Information and Communications

Information and communication is an integral component of the Stile Education internal control system. It is the process of identifying, capturing and exchanging information in the time frame necessary to conduct, manage and control the entity's operations. At Stile Education, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, service providers, and employees.

Daily standups are held to discuss the status of the current sprint activities which may include security tasks. Departmental meetings are utilized to align team objectives with company objectives. Engineering leaders meet fortnightly to look back on all on-call and security alerts triggered over the previous week. All staff are kept up to date through Stile's weekly newsletter and quarterly all hands meetings.
Stile success, support, and product teams manage frequent communication to our customers through a mix of status pages, newsletters, and in person meetings.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. Management has implemented monitoring controls to address timely and appropriate responses to issues that may impact information security. Automated systems (ex: IDS, firewall, vulnerability scans, patch alerts) are monitored for security events impacting Company systems and remediations are actioned as needed.

In addition, Management monitors the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to:

1. Determine if objectives are achieved
2. Identify any new risks that develop
3. Implement appropriate measures to address those risks

Risk Assessment

Management is responsible for identifying risks that threaten achievement of the control activities stated in the management's description of the services organizations systems. Management has implemented a process for identifying relevant risks that could affect the organization's ability to provide secure and reliable service to its users. The risk assessment occurs annually, or as business needs change, and covers identification of risks that could act against the company's objectives as well as specific risks related to a compromise to the security of data.

In addition, Stile Education considers fraud risks, vendor risks, and relevant laws and regulations when it conducts its annual risk assessment. The management team, with employee participation, identifies risks that could impede company objectives.

The level of each identified risk is determined by considering the impact of the risk itself and the likelihood of the risk materializing and high scoring risks are actioned upon. Risks are analyzed to determine whether the risk meets company risk acceptance criteria to be accepted or whether a mitigation plan will be applied. Mitigation plans include both the individual or department responsible for the plan and may include budget considerations.

Stile

Management considers the following in its risk assessment:

- Risks that could impact the security of the organization's IT environment
- Cross department risks that may impact security objectives
- Identification and assessment of changes, such as environmental, regulatory, and technological changes that could significantly affect the system of internal control for security
- Development and implementation of mitigation strategies for those risks
- Broader sectoral and industry-wide trends and threats which could affect our operations

Incidents in the Last 12 Months

There were no incidents related to a control failure or that impacted service commitments or system requirements, were required to be disclosed or had a material impact requiring disclosure.

Stile's services were designed with the assumption that certain controls would be implemented by user-entities. These controls should be in operation at user entities to complement Stile's controls. The user-entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user-entities:

- Ensure that appropriate user authentication controls are in place
- Effective maintenance and secure operation of school Identity Provider systems used in single sign on
- Strong endpoint security for student and teacher devices

Stile

SECTION IV - Description of Criteria, Controls, Tests, and Results of Tests

Testing Performed and Results of Entity-Level Controls

In planning the nature, timing, and extent of testing of the controls, Strike Graph considered the aspects of Stile Education Pty Ltd's control environment and tested those considered necessary.

In addition to the tests of the design of specific controls described below, procedures included tests of the following components of the internal control environment of Stile Education Pty Ltd:

- Management controls and organizational structure;
- Risk assessment process;
- Information and communication;
- Control activities;
- Monitoring.

Tests of the control environment included the following procedures, to the extent Strike Graph considered necessary: (a) a review of Stile Education Pty Ltd's organizational structure, including the segregation of functional responsibilities, policy statements, processing manuals, and personnel controls, (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls, and (c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing, and extent of the testing of controls relevant to achieving the service commitments and system requirements based on the applicable Trust Service Criteria.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), Strike Graph performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1. Inspect the source of the IPE,
2. Inspect the query, script, or parameters used to generate the IPE,
3. Tie data between the IPE and the source and/or
4. Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), Strike Graph inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Stile

Trust Services Criteria and Related Controls for Systems and Applications

On the following pages, the applicable Trust Services Criteria and the controls to achieve the service commitments and system requirements based on the criteria have been specified by and are the responsibility of Stile Education Pty Ltd. The “Tests Performed by Strike Graph” and the “Results of Tests" are the responsibility of the service auditor.

Information System Control Environment

The following controls apply to the services listed in Section III and their supporting technology environments.

Stile Education Pty Ltd Controls Mapped to Security Criteria

Criteria	Supporting Stile Education Pty Ltd Control Activity	Criteria Description
CC1.0	**Common Criteria Related to Control Environment**	
CC1.1	Employee Performance Vendor Due Diligence	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	Board Oversight	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	Organizational Chart Job Descriptions	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	Job Descriptions Tech Competence Employee Performance Vendor Due Diligence	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	Employee Performance Internal Controls	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives
CC2.0	**Common Criteria Related to Communication and Information**	
CC2.1	Risk Assessment Policy	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	Job Descriptions Employee Shared Drive Internal Controls Incidents External Incident Response: Responsibility IT Security Policy Data Flow Diagram Network Diagram Information Security Policy	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	Incidents External Penetration Test Internal Controls	The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0	**Common Criteria Related to Risk Assessment**	

CC3.1	Risk Assessment Policy Third Party SOC2 Risk Assessment Action Plans	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	Third Party SOC2 Business Continuity Risk Assessment Action Plans Data Flow Diagram Asset Inventory Network Diagram	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	Risk Assessment Policy	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	Third Party SOC2	The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0	**Common Criteria Related to Monitoring Activities**	
CC4.1	Vulnerability Scan Penetration Test Intrusion Detection Monitoring Infrastructure Internal Controls Tech Competence	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	Penetration Test	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management
CC5.0	**Common Criteria Related to Control Activities**	
CC5.1	Risk Assessment Action Plans Business Continuity Internal Controls Data Flow Diagram Network Diagram Separation of Duties: Developers Change Management: Segregation of Duties	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	Business Continuity User Access Review Logical Access Change Management Policy	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	Logical Access Internal Controls Vulnerability Scan Penetration Test Intrusion Detection Job Descriptions	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0	**Common Criteria Related to Logical and Physical Access Controls**	
CC6.1	Asset Inventory Provisioning Logical Access Vulnerability Scan Data Flow Diagram	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

	Disk Encryption Encryption at Rest	
CC6.2	Administrator Access User Access Review Termination of Access Review Privileged Access	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	Administrator Access Logical Access Termination of Access Review Privileged Access Separation of Duties: Developers Change Management: Segregation of Duties User Access Review	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4	Termination of Access	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	Data Retention/Deletion	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	Intrusion Detection	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	Disk Encryption	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	Vulnerability Scan Change Management Policy	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.0	**Common Criteria Related to System Operations**	
CC7.1	Vulnerability Scan Intrusion Detection	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	Intrusion Detection Vulnerability Scan Penetration Test	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	Incident Response: Process	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4	Incident Response: Responsibility Incident Response: Process	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	Incident Response: Process Restore	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0	**Common Criteria Related to Change Management**	
CC8.1	Change Management Policy Change Management: Application/Software Change Management: Ticketing System Change Management: Infrastructure Change Management: Emergency Process Separation of Environments	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0	**Risk Mitigation**	
CC9.1	Business Continuity	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	Vendor Due Diligence Vendor Management Policy Third Party SOC2 Vendor Review Vendor Risk Register Incidents External Termination of Access	The entity assesses and manages risks associated with vendors and business partners.

Stile

Security Criteria Mapped to Stile Education Pty Ltd Controls & Auditor Testing Performed and Results

Control Name	Control Specified by Stile Education Pty Ltd	Criteria	Test(s) Performed by Strike Graph	Result(s) of Test(s)
Administrator Access	Administrator access to the application, database, network, VPN, and operating system is restricted to authorized users.	CC.6.2 CC.6.3	Inspected the evidence provided for the Administrator Access control, noting that administrator access to the application, database, network, VPN, and operating system is restricted to authorized users.	No exceptions noted
Asset Inventory	An inventory of information assets, including hardware, software, processing facilities, and data, is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention.	CC.3.2 CC.6.1	Inspected the evidence provided for the Asset Inventory control, noting that an inventory of information assets, including hardware, software, processing facilities, and data, is maintained and updated at least annually. Assets have an assigned asset owner. Software assets are classified based on the data classification convention.	No exceptions noted
Board Oversight	The board of directors operates independently of management and meets quarterly to oversee the organization's internal control objectives	CC.1.2	Inspected the evidence provided for the Board Oversight control, noting that the board of directors operates independently of management and meets quarterly to oversee the organization's internal control objectives	No exceptions noted
Business Continuity	A Business Continuity Plan has been developed. The plan identifies a process, roles, and milestones for maintaining business continuity and restoring system functionality in the event of major disruption. The plan is reviewed and tested annually. Disaster recovery is included within the Business Continuity Plan.	CC.3.2 CC.5.1 CC.5.2 CC.9.1	Inspected the evidence provided for the Business Continuity control, noting that a Business Continuity Plan has been developed. The plan, in conjunction with the Incident Response Plan, identifies a process, roles, and milestones for maintaining business continuity and restoring system	No exceptions noted

			functionality in the event of major disruption. The plan is reviewed and tested annually. Disaster recovery is included within the Business Continuity Plan.	
Change Management Policy	A Change Management Policy and Procedures are in place to request, document, test, and approve changes. The CTO (Daniel Rodgers-Pryor) is responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on operations. All technology acquisition, development, and maintenance processes are governed by change management procedures. This policy is reviewed, updated, and approved annually.	CC.5.2 CC.6.8 CC.8.1	Inspected the evidence provided for the Change Management Policy control, noting that a Change Management Policy and Procedures are in place to request, document, test, and approve changes. The CTO is responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on operations. Technology acquisition, development, and maintenance processes are governed by change management procedures.	No exceptions noted
Change Management: Application/Software	All application changes for internally developed software are developed, tested, and approved prior to implementation.	CC.8.1	Inspected the evidence provided for the Change Management: Application/Software control, noting that application changes for internally developed software are developed, tested, and approved prior to implementation.	No exceptions noted
Change Management: Emergency Process	An emergency change process is followed for changes required in urgent situations.	CC.8.1	Inspected the evidence provided for the Change Management: Emergency Process control, noting that an emergency change process is followed for changes required in urgent situations.	No exceptions noted
Change Management: Infrastructure	Infrastructure changes are tested, reviewed, and approved by authorized personnel prior to implementation.	CC.8.1	Inspected the evidence provided for the Change Management: Infrastructure control, noting that infrastructure changes are tested, reviewed, and	No exceptions noted

			approved by authorized personnel prior to implementation.	
Change Management: Segregation of Duties	Segregation of duties exists during the infrastructure and application change process.	CC.5.1 CC.6.3	Inspected the evidence provided for the Change Management: Segregation of Duties control, noting that segregation of duties exists during the infrastructure and application change process.	No exceptions noted
Change Management: Ticketing System	A centralized ticketing and workflow tool tracks software change activity, including development, approvals and testing.	CC.8.1	Inspected the evidence provided for the Change Management: Ticketing System control, noting that a centralized ticketing and workflow tool tracks software change activity.	No exceptions noted
Data Flow Diagram	The data flow diagram is maintained and highlights the systems that require logical access controls per data classification level. The data flow diagram is updated annually or as business needs require.	CC.2.2 CC.3.2 CC.5.1 CC.6.1	Inspected the evidence provided for the Data Flow Diagram control, noting that the data flow diagram is maintained and highlights the systems that require logical access controls per data classification level.	No exceptions noted
Data Retention/ Deletion	Procedures are in place to remove data from production based on contractual and legal requirements. These procedures are reviewed, updated, and approved as needed.	CC.6.5	Inspected the evidence provided for the Data Retention/Deletion control, noting that procedures are in place to remove data from production based on contractual and legal requirements. These procedures are reviewed, updated, and approved as needed.	No exceptions noted
Disk Encryption	Disk encryption is enforced, by centrally managed data loss prevention rules, on all employee devices.	CC.6.1 CC.6.7	Inspected the evidence provided for the Disk Encryption control, noting that disk encryption is enforced, by centrally managed data loss prevention rules, on employee devices.	No exceptions noted
Employee Performance	A performance evaluation process is in place and employees are evaluated at least annually.	CC.1.1 CC.1.4 CC.1.5	Inspected the evidence provided for the Employee Performance control, noting that a performance evaluation process is in place and employees are	No exceptions noted

			evaluated.	
Employee Shared Drive	A centralized drive is in place for employees to access all corporate policies and procedures as well as job descriptions.	CC.2.2	Inspected the evidence provided for the Employee Shared Drive control, noting that a centralized drive is in place for employees to access corporate policies and procedures.	No exceptions noted
Encryption at Rest	All data at rest is encrypted using industry standard algorithms.	CC.6.1	Inspected the evidence provided for the Encryption at Rest control, noting that all data at rest is encrypted using industry standard algorithms.	No exceptions noted
Incident Response: Process	The incident response process includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security, confidentiality, or privacy. The root cause analysis is performed by the incident controller (a member of the oncall team) and reviewed along with all other heavily involved people.	CC.7.3 CC.7.4 CC.7.5	Inspected the evidence provided for the Incident Response: Process control, noting that the incident response process includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security, confidentiality, or privacy. The root cause analysis is performed by the incident controller (a member of the oncall team) and reviewed along with all other heavily involved people.	No exceptions noted
Incident Response: Responsibility	The design, implementation, maintenance, execution, and periodic testing of the security incident response program and data breach response procedures are the responsibility of the Security Officer. The	CC.2.2 CC.7.4	Inspected the evidence provided for the Incident Response: Responsibility control, noting that the design, implementation, maintenance, execution, and periodic testing of the	No exceptions noted

	Incident Response plan is reviewed, updated, and approved annually.		security incident response program and data breach response procedures are the responsibility of the Security Officer. The Incident Response plan is reviewed, updated, and approved annually.	
Incidents External	External parties may report system failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organization's support webpage. The incident is documented in accordance with the Incident Response Plan, if required.	CC.2.2 CC.2.3 CC.9.2	Inspected the evidence provided for the Incidents External control, noting that external parties may report system failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organization's support webpage.	No exceptions noted
Information Security Policy	The Information Security Policy is maintained, reviewed, and updated annually by the CTO and reviewed by the Deputy CEO.	CC.2.2	Inspected the evidence provided for the Information Security Policy control, noting that the Information Security Policy is maintained, reviewed, and updated annually by the CTO and reviewed by the Deputy CEO.	No exceptions noted
Internal Controls	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	CC.1.5 CC.2.2 CC.2.3 CC.4.1 CC.5.1 CC.5.3	Inspected the evidence provided for the Internal Controls control, noting that internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	No exceptions noted
Intrusion Detection	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.	CC.4.1 CC.5.3 CC.6.6 CC.7.1 CC.7.2	Inspected the evidence provided for the Intrusion Detection control, noting that threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting	No exceptions noted

Stile

			occurs on threats and results are actioned as appropriate.	
IT Security Policy	Internal users are required to read the IT Security Policy upon hire. The policy outlines rules for the acceptable use of information associated with information and information processing, as well as, appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services. The policy is updated by management as needed and available to all internal users.	CC.2.2	Inspected the evidence provided for the IT Security Policy control, noting that internal users are required to read and acknowledge the IT Security Policy upon hire. The policy outlines rules for the acceptable use of information associated with information and information processing, as well as, appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services. The policy is updated by management as needed and available to all internal users.	No exceptions noted
Job Descriptions	Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.	CC.1.3 CC.1.4 CC.2.2 CC.5.3	Inspected the evidence provided for the Job Descriptions control, noting that job descriptions are in place which define the skills and responsibilities for specific roles as they relate to information security.	No exceptions noted
Logical Access	Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, secure authentication requirements, role-based access, and the principle of least privilege. The policy is reviewed annually.	CC.5.2 CC.5.3 CC.6.1 CC.6.3	Inspected the evidence provided for the Logical Access control, noting that logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, secure authentication requirements, role-based access, and the principle of least privilege.	No exceptions noted
Monitoring Infrastructure	IT infrastructure monitoring tools are configured to monitor IT infrastructure availability and performance, generate	CC.4.1	Inspected the evidence provided for the Monitoring Infrastructure control, noting that IT infrastructure monitoring tools	No exceptions noted

	alerts when specific predefined thresholds are met or exceeded, and forecast capacity requirements to ensure system performance. Threat intelligence feeds are utilized.		are configured to monitor IT infrastructure availability and performance, generate alerts when specific predefined thresholds are met or exceeded, and forecast capacity requirements to ensure system performance. Threat intelligence feeds are utilized.	
Network Diagram	System boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.	CC.2.2 CC.3.2 CC.5.1	Inspected the evidence provided for the Network Diagram control, noting that system boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.	No exceptions noted
Organizational Chart	The business is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned. Organizational charts are updated as needed.	CC.1.3	Inspected the evidence provided for the Organizational Chart control, noting that the business is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned. Organizational charts are updated as needed.	No exceptions noted
Penetration Test	An independent, third party provider is contracted to perform penetration tests at least annually, or as business needs require. Test results are reviewed and tracked to resolution.	CC.2.3 CC.4.1 CC.4.2 CC.5.3 CC.7.2	Inspected the evidence provided for the Penetration Test control, noting that an independent, third party provider is contracted to perform penetration tests at least annually, or as business needs require. Test results are reviewed and tracked to resolution.	No exceptions noted
Provisioning	Logical/physical user access requests are documented and require approval prior to access being provisioned.	CC.6.1	Inspected the evidence provided for the Provisioning control, noting that logical/physical user access requests are documented and require approval	No exceptions noted

			prior to access being provisioned.	
Restore	Documented backup and restoration procedures for the network are maintained and reviewed annually. Backup restoration testing is performed at least annually.	CC.7.5	Inspected the evidence provided for the Restore control, noting that documented backup and restoration procedures for the network have been established. Backup restoration testing is performed at least annually.	No exceptions noted
Review Privileged Access	Administrative and privileged access, as defined by policy, is reviewed at least quarterly.	CC.6.2 CC.6.3	Inspected the evidence provided for the Review Privileged Access control, noting that administrative and privileged access, defined by policy, is reviewed at least quarterly.	No exceptions noted
Risk Assessment Action Plans	Risks identified through the risk assessment process are addressed by management and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion. Risk assessment results are shared with the IT leadership team annually.	CC.3.1 CC.3.2 CC.5.1	Inspected the evidence provided for the Risk Assessment Action Plans control, noting that risks identified through the risk assessment process are addressed by management and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion. Risk assessment results are shared with the IT leadership team annually.	No exceptions noted
Risk Assessment Policy	Risk assessment policy and procedures are in place and include how to identify risks, to evaluate risks, and how to address and mitigate those risks.	CC.2.1 CC.3.1 CC.3.3	Inspected the evidence provided for the Risk Assessment Policy control, noting that risk assessment policy and procedures are in place and include how to identify risks, to evaluate risks, and how to address and mitigate those risks.	No exceptions noted
Separation of Duties: Developers	Access to the source code repository is restricted to authorized employees.	CC.5.1 CC.6.3	Inspected the evidence provided for the Separation of Duties: Developers control, noting that access to the source code repository is restricted to authorized employees.	No exceptions noted

Stile

Separation of Environments	Production, testing, and development environments are logically and physically separated.	CC.8.1	Inspected the evidence provided for the Separation of Environments control, noting that production, testing, and development environments are logically and physically separated.	No exceptions noted
Tech Competence	The new hire screening process includes a consideration of the skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Background/reference checks are required prior to hire.	CC.1.4 CC.4.1	Inspected the evidence provided for the Tech Competence control, noting that the new hire screening process includes a consideration of the skills and competencies of the candidate. Background/reference checks are required prior to hire.	No exceptions noted
Termination of Access	A user's physical and logical access to IT systems is revoked within 24 hours of termination or transfer and all assets are returned to the organization when employment ends or their contract terminates. Exceptions are documented in an offboarding checklist and/or offboarding ticket.	CC.6.2 CC.6.3 CC.6.4 CC.9.2	Inspected the evidence provided for the Termination of Access control, noting that a user's physical and logical access to IT systems is revoked within 24 hours of termination or transfer and all assets are returned to the organization when employment ends or their contract terminates. Exceptions are documented in an offboarding checklist and/or offboarding ticket.	No exceptions noted
Third Party SOC2	Third party service providers' SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	CC.3.1 CC.3.2 CC.3.4 CC.9.2	Inspected the evidence provided for the Third Party SOC2 control, noting that third party service providers' SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	No exceptions noted
User Access Review	Management performs at least a quarterly review of user access to systems based on job duties. Inactive users are removed and	CC.5.2 CC.6.2 CC.6.3	Inspected the evidence provided for the User Access Review control, noting that management performs a review of	No exceptions noted

	removal is documented. The review is formally documented including system generated user listings and sign off by management.		user access to systems based on job duties. Inactive users are removed and removal is documented. The review is formally documented including system generated user listings and sign off by management.	
Vendor Due Diligence	Due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.	CC.1.1 CC.1.4 CC.9.2	Inspected the evidence provided for the Vendor Due Diligence control, noting that due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.	No exceptions noted
Vendor Management Policy	A policy and procedures are in place which govern the vendor management lifecycle. The policy is reviewed and re-approved by management annually. Procedures are defined for assessing vendor risk.	CC.9.2	Inspected the evidence provided for the Vendor Management Policy control, noting that a policy and procedures are in place which govern the vendor management lifecycle. The policy is reviewed and re-approved by management annually. Procedures are defined for assessing vendor risk.	No exceptions noted
Vendor Review	Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, and re-assess the vendors' security controls.	CC.9.2	Inspected the evidence provided for the Vendor Review control, noting that critical IT vendors and service providers are reviewed to update their risk profiles, assess performance against contracts, and re-assess the vendors' security controls.	No exceptions noted
Vendor Risk Register	A register of all vendors and service providers is maintained. The register includes vendor risk level which is assessed prior to engaging with the vendor	CC.9.2	Inspected the evidence provided for the Vendor Risk Register control, noting that a register of all vendors and service providers is maintained. The	No exceptions noted

	and re-assessed annually thereafter.		register includes vendor risk level.	
Vulnerability Scan	Vulnerability scans are performed quarterly to help identify security risks. Results are assessed and, where required, remediated.	CC.4.1 CC.5.3 CC.6.1 CC.6.8 CC.7.1 CC.7.2	Inspected the evidence provided for the Vulnerability Scan control, noting that vulnerability scans are performed to help identify security risks. Results are assessed and, where required, remediated.	No exceptions noted

Signature Certificate

Reference number: B87ZX-433BZ-MKXFJ-HBHME

Signer	Timestamp	Signature
Alex Finkel Email: alex.finkel@stileeducation.com		
Sent:	13 Nov 2024 13:39:04 UTC	
Viewed:	13 Nov 2024 22:59:52 UTC	
Signed:	13 Nov 2024 23:00:13 UTC	
Recipient Verification:		IP address: 203.129.146.182
✔Email verified	13 Nov 2024 22:59:52 UTC	Location: Melbourne, Australia
Jajuan Williams Email: jajuan@theladycfo.com		
Sent:	13 Nov 2024 13:39:04 UTC	
Viewed:	14 Nov 2024 14:00:35 UTC	
Signed:	14 Nov 2024 14:00:46 UTC	
Recipient Verification:		IP address: 184.90.154.208
✔Email verified	14 Nov 2024 14:00:35 UTC	
✔Passcode	14 Nov 2024 14:00:34 UTC	Location: Apopka, United States

Document completed by all parties on:
14 Nov 2024 14:00:46 UTC