SIMPLIFI HOLDINGS, LLC

Simpli.fi Demand Side Platform and Bidtellect Platform

SOC 2, Type II

System and Organization Controls (SOC) for Service Organizations Report throughout the period September 1, 2025 to August 31, 2026

Report of Independent Service Auditor issued by Aprio LLP

This report is intended solely for the information and use of the Company, user entities of the Company's System throughout the Specified Period, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators.

Table of Contents

I. Report of Independent Service Auditor 1

II. Simplifi Holdings, LLC's Assertion 6

III. Simplifi Holdings, LLC's Description of its System and Controls 8

A. Scope and Purpose of the Report 8

B. Company Overview and Background 8

C. Principal Service Commitments and System Requirements 9

D. Components of the System Used to Provide the Services 10

E. System Incidents 14

F. Relevant Aspects of the Overall Control Environment 14

G. Description of Controls 16

H. User Entity Responsibilities 18

I. Subservice Organizations 19

J. Non-Applicable Trust Services Criteria 22

K. Changes to the System During the Specified Period 22

L. Additional Information about Management's Description 22

IV. Description of the Trust Services Category, Criteria, and Simplifi Holdings, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results 23

A. Types and Descriptions of the Tests of Operating Effectiveness 23

B. Trust Services Category, Criteria, Control Activities, and Testing Provided by the Service Auditor 25

V. Other Information Provided by Simplifi Holdings, LLC 156

A. Management's Responses to the Testing Exceptions 156

I. Report of Independent Service Auditor

Board of Directors and Management of Simplifi Holdings, LLC

Scope

We have examined Simplifi Holdings, LLC's (the "Company" or "Simplifi") accompanying description of its Simpli.fi Demand Side Platform and Bidtellect Platform (the "System") titled *Simplifi Holdings, LLC's Description of its System and Controls* ("description") throughout the period September 1, 2025 to August 31, 2026 (the "Specified Period") 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* (With Revised Implementation Guidance – 2022) (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of the controls stated in the description throughout the Specified Period to provide reasonable assurance that the Company'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* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*).

The information included in Section V of this report, *Other Information Provided by Simplifi Holdings, LLC,* is presented by management of the Company to provide additional information and is not a part of the Company's description. Information about *Management's Responses to Testing the Exceptions* has not been subjected to the procedures applied in the examination of the description and of the suitability of the design of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

The Company uses various subservice organizations to support the Simpli.fi Demand Side Platform and Bidtellect Platform as described in the *Subservice Organizations* section in Section III of this report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company'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.

Service Organization's responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Simplifi Holdings, LLC's Assertion* ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Company 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 (AICPA).

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

An examination of a 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, and
- evaluating the overall presentation of the description.

Service Auditor's independence and quality control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We have applied the Statements on Quality Control Standards established by the AICPA and, accordingly, have designed, implemented, and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in 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 policies or procedures may deteriorate.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Basis for Qualified Opinion

The Company states in the description of the System in Section III of this report that a peer review, including a review of the Simpli.fi Demand Side Platform code for vulnerabilities, is performed on source code changes prior to migration into the production environment and that all changes to the Simpli.fi Demand Side Platform must be approved by a member of management prior to promotion into production. However, as noted in Section IV, *Description of the Trust Services Category, Criteria, and Simplifi Holdings, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results*, Control Activities CC 8.1-02 and CC 8.1-03 were not operating effectively throughout the period September 1, 2025 through August 31, 2026, as peer reviews and management approvals were not consistently performed for changes to the Simpli.fi Demand Side Platform prior to promotion into production. As a result, controls were not operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved for the Simpli.fi Demand Side Platform based on the following trust services criterion, Common Criteria CC8.1: *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives*.

Qualified Opinion

In our opinion, except for the matters described in the preceding paragraph, in all material respects,

a. The description presents Simplifi Holdings, LLC's Simpli.fi Demand Side Platform and Bidtellect Platform that was designed and implemented throughout the period September 1, 2025 to August 31, 2026, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period September 1, 2025 to August 31, 2026, to provide reasonable assurance that Simplifi Holdings, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the Specified Period and if the subservice organizations (Refer to the Subservice Organizations section in Section III) applied the complementary controls assumed in the design of Simplifi Holdings, LLC's controls throughout the period September 1, 2025 to August 31, 2026.

c. The controls stated in the description operated effectively throughout the period September 1, 2025 to August 31, 2026, to provide reasonable assurance that Simplifi Holdings, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Simplifi Holdings, LLC's controls operated effectively throughout the period September 1, 2025 to August 31, 2026.

Restricted use

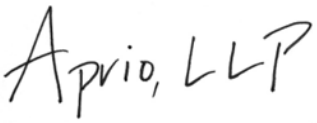
This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Company, user entities of the Company's Simpli.fi Demand Side Platform and Bidtellect Platform during some or all of the period September 1, 2025 to August 31, 2026, business partners of the Company subject to risks arising from interactions with the Simpli.fi Demand Side Platform and Bidtellect 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:

- 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 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; and
- 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.

Aprio, LLP



Atlanta, Georgia
November 5, 2026

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

II. Simplifi Holdings, LLC's Assertion

We have prepared the accompanying description of Simplifi Holdings, LLC's (the "Company" or "Simplifi") Simpli.fi Demand Side Platform and Bidtellect Platform (the "System") titled *Simplifi Holdings, LLC's Description of its System and Controls* ("description") throughout the period September 1, 2025 to August 31, 2026 (the "Specified Period"), 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* (With Revised Implementation Guidance – 2022) (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with Simplifi's system, particularly information about system controls that Simplifi 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* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*).

The Company uses various subservice organizations to support the Simpli.fi Demand Side Platform and Bidtellect Platform as described in the *Subservice Organizations* section in Section III of this report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Simpli.fi, to achieve Simpli.fi's service commitments and system requirements based on the applicable trust services criteria. The description presents Simpli.fi's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Simpli.fi's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. The description presents the System that was designed and implemented throughout the Specified Period, in accordance with the description criteria.

b. Except for the matters described in the last paragraph of this assertion, the controls stated in the description were suitably designed throughout the Specified Period to provide reasonable assurance that Simpli.fi's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the Specified Period, and if the subservice organizations (Refer to the *Subservice Organizations* section in Section III) applied the complementary controls assumed in the design of the Company's controls throughout the Specified Period.

c. Except for the matters described in the last paragraph of this assertion, the controls stated in the description operated effectively throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria and if the complementary subservice organization controls assumed in the design of the Company's controls operated effectively throughout the Specified Period.

The Company states in the description of the System in Section III of this report that a peer review, including a review of the Simpli.fi Demand Side Platform code for vulnerabilities, is performed on source code changes prior to migration into the production environment, and that all changes to the Simpli.fi Demand Side Platform must be approved by a member of management prior to promotion into production. However, as noted in Section IV, *Description of the Trust Services Category, Criteria, and Simplifi Holdings, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results*, Control Activities CC 8.1-02 and CC 8.1-03 were not operating effectively throughout the period September 1, 2025 through August 31, 2026, as peer reviews and management approvals were not consistently performed for changes to the Simpli.fi Demand Side Platform prior to promotion into production. As a result, controls were not operating effectively to provide reasonable assurance that the Company's service commitments and system requirements were achieved for the Simpli.fi Demand Side Platform based on the following trust services criterion:

- Common Criteria CC 8.1: *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives*.

III. Simplifi Holdings, LLC's Description of its System and Controls

A. Scope and Purpose of the Report

This report describes the control structure of Simplifi Holdings, LLC (the "Company" or "Simplifi") as it relates to its Simpli.fi Demand Side Platform and Bidtellect Platform (the "System") throughout the period September 1, 2025 to August 31, 2026 (the "Specified Period") for the Security Trust Services Category. This report, including the description of controls in Section IV of this report, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the Specified Period, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding, as defined in the *Restricted Use* portion of Section I. This report is not intended to be, and should not be, used by anyone other than these specified parties.

The 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* (With Revised Implementation Guidance – 2022) (AICPA, *Description Criteria*), is intended to provide user entities, business partners, practitioners, and regulators with information about the System, particularly system controls intended to provide reasonable assurance that Simplifi'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* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*). It was prepared taking into consideration the attestation standards established by the American Institute of Certified Public Accountants (the "AICPA"). As this description is intended to focus on features that may be relevant to the internal control of Simplifi's customers and other specified parties, it does not encompass all aspects of the services provided or procedures followed by Simplifi.

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Company Overview

Simplifi Holdings, LLC (the "Company" or "Simplifi") is a privately held LLC, founded in 2010, that is headquartered in Fort Worth, TX. Simplifi is engineered to unify digital behaviors and real-world movement into actionable performance signals, so brands can target, optimize, and measure campaigns where consumer decisions actually happen. Simplifi offers an integrated workflow software and programmatic advertising platform, providing solutions to over 2,000 media teams, agencies, and brands, and enabling campaign execution, audience targeting, and performance optimization across multiple digital advertising channels. Simplifi's investors include private equity firms such as Blackstone and GTCR.

Simpli.fi Demand Side Platform and Bidtellect Platform Overview

Simplifi provides an integrated workflow software and programmatic advertising platform, serving agencies, advertisers, and media buying organizations. The System unifies broad multi-channel programmatic execution — across Connected TV (CTV), mobile, video, audio, display, and social — with specialized native and native video capabilities powered by integrated Bidtellect technology, including proprietary "cookie less" engagement and optimization capabilities. The System is offered via self-service, managed-service, and API integration models, and includes workflow software and tools for campaign management, audience building, and reporting. The scope of this report includes the supporting solutions and controls relevant to the Simpli.fi Demand Side Platform and the Bidtellect Platform as they are delivered to customers.

Key capabilities of the System include advanced audience targeting tactics, such as geo-fencing, location-based audience targeting, keyword search and contextual targeting, site retargeting, and addressable audience solutions; native display and native video ad serving that provides access to in-feed video and recommendation unit inventory across publisher networks; and "cookie less" measurement and contextual intelligence capabilities that score and optimize campaign performance based on post-click site engagement metrics (for example, time on site, scroll depth, and conversion behavior) without relying on traditional cookie-based tracking. These capabilities are designed to help customers maximize return on ad spend (ROAS) across digital channels and media types.

C. Principal Service Commitments and System Requirements

Simplifi designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments that Simplifi makes to user entities, the laws and regulations that govern the provision of the services, and the operational and compliance requirements that Simplifi has established for the services. Security commitments to user entities are documented and communicated in Master Service Agreements (MSAs) 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:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Performing regular vulnerability scans over the system and network, and penetration tests over the production environment;
- Maintaining operational procedures for managing security incidents and breaches, including notification procedures;
- Use of encryption technologies to protect customer data both at rest and in transit; and
- Maintaining data retention and disposal procedures.

Simplifi establishes operational requirements that support the achievement of its security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Simplifi's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

D. Components of the System Used to Provide the Services

Supporting Systems Overview

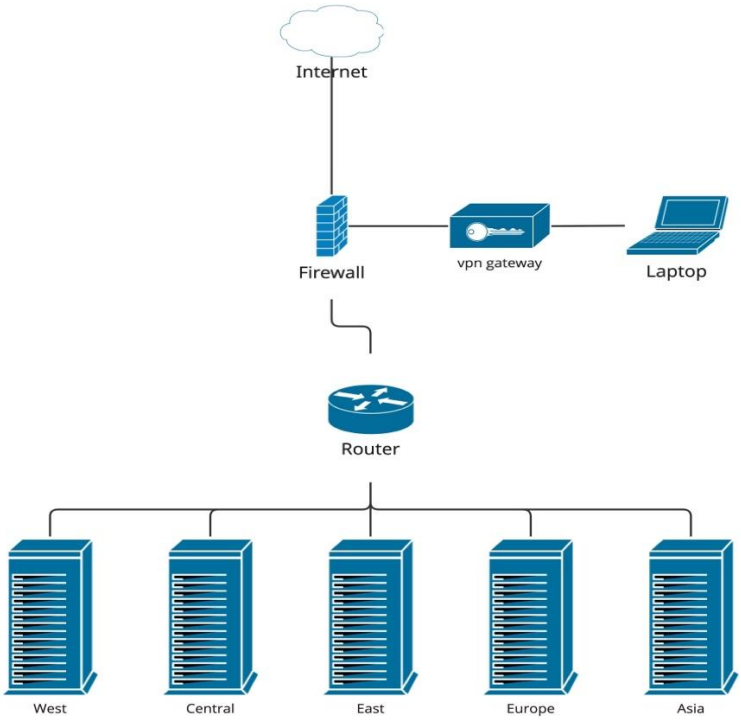
1. Infrastructure and Databases

Simplifi maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description, and owner. To outline the topology of its network, the Company maintains network diagrams for the Simpli.fi Demand Side Platform and the Bidtellect Platform.

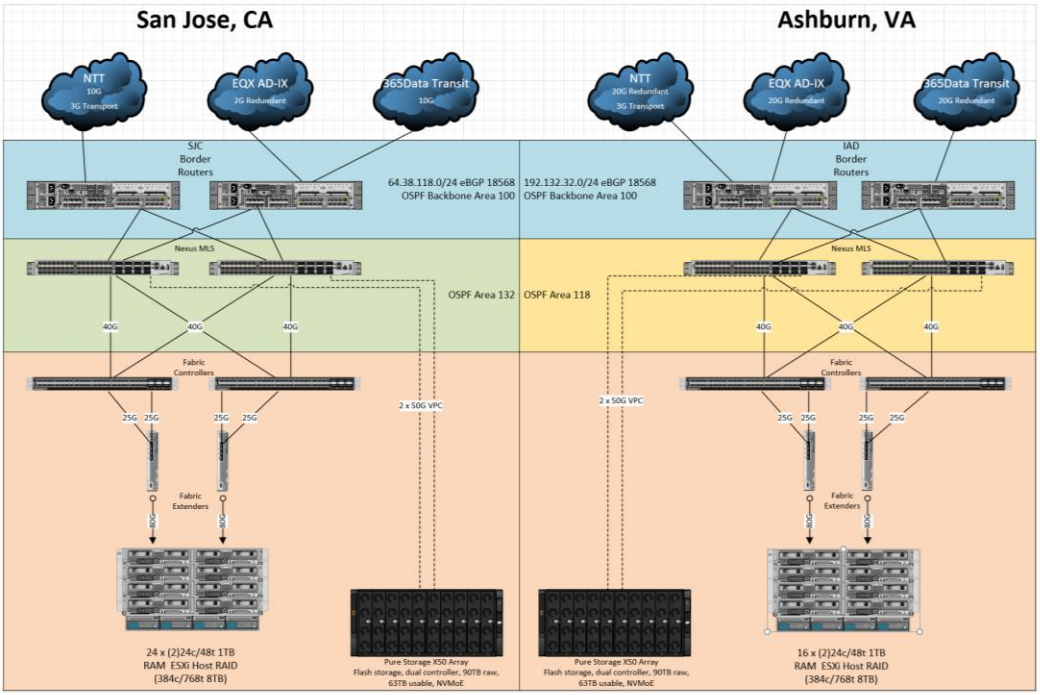
The Simpli.fi Demand Side Platform is hosted in a cloud environment on Google Cloud Platform (GCP), a third-party Infrastructure-as-a-Service provider.

The Bidtellect Platform operates in an on-premise production environment, including dedicated servers and SQL and Vertica databases, physically hosted at a third-party co-location data center (International Business Exchange (IBX)) operated by Equinix.

Simpli.fi Demand Side Platform



Bidtellect Platform



Systems Overview	Purpose
Cisco Duo	Multi-factor authentication (MFA) for Bidtellect on-premise production environment.
Equinix	Third-party co-location data center (International Business Exchange (IBX) facility) providing physical hosting for the on-premise Bidtellect production environment
GCP Identity and Access Management (IAM)	Access control and permissions management within GCP infrastructure
Google BigQuery	Relational database and data warehousing
Google Cloud Platform (GCP)	Cloud-hosted system infrastructure
Google Cloud SQL	Relational database and data warehousing
Google Cloud Storage	Cloud object storage
Okta	Cloud identity management and single sign-on (SSO)
On-premise production servers (Bidtellect)	Physical servers hosting the Bidtellect production environment
SQL Database	Relational database supporting the Bidtellect production environment
Vertica Database	Analytical database supporting the Bidtellect production environment
Company-owned endpoint devices	Workstations running Windows and macOS operating systems

2. Supporting Software Tools

The following third-party software, services, and tools support the wider System's processes and controls, and are in scope only to the degree that they form part of the System's control processes:

Supporting Software Tools	Purpose
Confluence	Knowledge management and collaboration
Datadog	System monitoring and log management
GitHub	Source code control
Google Cloud Key Management Service	Encryption key management and storage
Google Drive	Cloud-based file storage, part of Google Workspace
Google Workspace	Cloud-based file storage and general office productivity applications
Jamf	Endpoint management for macOS devices
JIRA	Development task definition and tracking; ticket and project management
Microsoft Endpoint Manager	Endpoint/mobile device management for Windows devices
PagerDuty	Incident management and on-call alerting
Patch Manager Plus	Automated patch management software that applies patches for routine maintenance and in response to identified vulnerabilities.
Salesforce	Customer relationship management
Slack	Internal communication tool
Vanta	Security and compliance monitoring

3. People

The Company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. Simpli.fi has a staff of approximately 600 employees organized in the following functional areas:

- *Leadership*- Executive Leadership directs activities such as legal, compliance, training, contracting, accounting, finance, human resources, and other business-related tasks. These individuals help to ensure business objectives are met through management of staff or direct contribution. These individuals are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. The members of the Executive Leadership Team include:
    - Cali Tran, Chief Executive Officer
    - Evan Kolter, Chief Financial Officer & Interim CEO
    - Michael Schoen, Chief Product and Technology Officer
    - Susan Rothwell, Chief Revenue Officer
    - Luke Baldrica, Legal Counsel

- *Operations* - Staff that maintain production infrastructure and manage access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.
- *Information Technology* - Staff that manage laptops, software, and other technology involved in employee productivity and business operations.
- *Product Development* - Staff that are responsible for the development, testing, deployment, and maintenance of the source code for the system, as well as the product life cycle, including adding additional product functionality.

4. Data

Data, as defined by Simplifi, constitutes user and account data. This includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function. Data is categorized into the following major types:

- Public data – information that is not confidential and can be made public without any implications for Simplifi (for example, press releases and public website content).
- Internal data – information that is approved by management and protected from external access (for example, internal memos, design documents, product specifications, and correspondence).
- Customer data – information received from customers for processing or storage by Simplifi, including customer PII, customers' customers' PII, and any information subject to a confidentiality agreement with a customer.
- Company data – information collected and used by Simplifi to operate the business, including legal documents, contractual agreements, and employee PII.

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured and utilized by the Company in delivering its services. All personnel and contractors of the Company are obligated to respect and, in all cases, to protect customer data. Simplifi has policies and procedures in place to properly secure and handle customer data, and these policies and procedures are reviewed on at least an annual basis.

5. Policies and Procedures

The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users. The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.

Management has developed and communicated policies and procedures to manage the information security of the System. Changes to these procedures are performed annually and authorized by management, the Executive Leadership Team, and control owners. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess 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
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

E. System Incidents

There were no system incidents during the Specified Period that were the result of controls that were not suitably designed or operating effectively that management is aware of. There were also no incidents during the Specified Period that resulted in a significant failure in the achievement of one or more of the Company's service commitments and/or system requirements of which management is aware.

F. Relevant Aspects of the Overall Control Environment

A company's internal control environment reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning controls and the emphasis given to controls, as expressed by the Company's policies, procedures, methods, and organizational structure. The following is a description of the components of internal control pertaining to the Company's systems.

1. Control Environment and Control Activities

a. Management

The Company's Board of Directors meets at least annually and maintains formal meeting minutes.

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy. The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

Integrity and ethical values are essential elements of the Company's control environment and include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Management balances continued growth in a rapidly changing technology space with responsible stewardship of the sensitive data and workflows that customers entrust to the Company. The management team meets frequently to be briefed on technology changes that affect the services, new security technologies that can help protect customer workflows, and regulatory changes that may require changes to the System. Major planned changes to the business are reviewed by the management team to ensure they are compatible with the Company's core product offerings and its obligations to new and existing customers.

b. Organizational Structure

Management maintains the Company's organizational structure dynamically within the Company's HR Portal. The organizational chart is available to internal users via the Company's HR Portal.

The Company's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored, and is based in part on the Company's size and the nature of its activities. The assignment of authority and responsibility addresses how reporting relationships and authorization hierarchies are established and is supported by policies and communications intended to ensure that personnel understand the Company's objectives, how their individual actions contribute to those objectives, and how and for what they will be held accountable.

c. Personnel

The Company performs background checks and/or reference checks on new employees and contractors with access to the in-scope systems at the time of hire.
Performance reviews are performed for employees of the Engineering Department on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities.
The Company requires employees to complete security awareness training within thirty business days of hire and at least annually thereafter. The Company requires employees to acknowledge the Code of Conduct and information security policies at the time of hire. Employees who violate the Code of Conduct or information security policies are subject to disciplinary actions in accordance with the Code of Conduct. The Company requires contractors with access to customer data to comply with confidentiality and data protection requirements, including the Code of Conduct. The Company requires contractors with access to customer data to sign a confidentiality agreement at the time of engagement. The Company requires employees to sign a confidentiality agreement during onboarding.

The Company's human resources policies and practices address employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Management has considered the competence levels required for particular jobs and translated the required skills and knowledge into written position requirements, and training is provided to maintain the skill level of personnel in certain positions. Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

2. Risk Assessment

The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

As part of the risk assessment process, the Company maintains a risk register to track systems and procedures that could present risks to meeting the Company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. These tasks are incorporated into the Company's regular product development process so they can be addressed predictably and iteratively, and the risk register is reevaluated annually.

3. Monitoring

Monitoring is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring results are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. Upper management evaluates the facts and circumstances related to any suspected control breakdown and determines whether the issue was isolated or requires a change in the Company's procedures or personnel.

The results of ongoing monitoring procedures are documented and tracked in an internal risk management tracking tool. Escalation procedures for notifying management of identified risks are documented in Company policies, and risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the tracking tool, and management reviews reported deficiencies and corrective actions during annual risk meetings.

4. Information and Communication

The Company uses several information and communication channels to share information with management, employees, contractors, and customers. Chat systems and email are the primary internal and external communication channels, and structured data is communicated internally through SaaS applications and project management tools. In-person and video all-hands meetings are used to communicate company priorities and goals from management to all employees.

G. Description of Controls

1. Logical Access

The Company provisions employee and contractor access to infrastructure through a role-based access control model designed to support least-privilege access and consistent, repeatable provisioning and deprovisioning processes. Access to in-scope systems is organized into administrator, user, and no-access roles. The Company's Digital Workplace team is responsible for provisioning access based on each employee's role and for deprovisioning access to in-scope systems upon termination.

Requests to add and/or modify access to the system components for the Simpli.fi System are approved by each user's manager or other appropriate personnel prior to access being granted. Access to the system components for the in-scope production environments is removed or disabled according to Service Level Agreements (SLAs). The Company has a Data Protection Policy in place to help ensure that confidential data is properly secured and restricted to appropriate personnel.

Authentication

Administrative access to GCP, including super administrator access, is restricted to appropriate personnel based on job function. Access to GCP requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device. Super administrator access to GCP requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device. Access to Okta requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device. Administrative access to Okta is restricted to appropriate personnel based on job function.

Virtual Private Network (VPN) access, including administrative access, is restricted to appropriate personnel based on job function. Access to the unique Secure Shell (SSH) Keys is restricted to appropriate personnel based on job function. Direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid Secure Shell (SSH) key. Administrative access to the Simpli.fi Demand Side Platform's databases is restricted to appropriate personnel based on job function.

Administrative access to the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function. Administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function. Direct access to the on-premise Bidtellect production environment, including servers, databases, and the Bidder application, requires VPN access and multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.

Password Parameters

Password parameters for Okta are configured as follows: minimum password length: fifteen characters, password history: 24 passwords, and password complexity: enabled. Password parameters for GCP are configured as follows: minimum password length: fifteen characters and password complexity: enabled.

2. Change Management

The Company has a formal Secure Development Policy (SDP) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. Version control software is in place to manage current versions of source code for the in-scope production environments. The ability to modify the source code of the production environments is restricted to appropriate personnel based on job function. The Company restricts access to migrate changes to the production environment to appropriate personnel based on job function.

Prior to implementation, all changes to the Simpli.fi Demand Side Platform are tested in a development environment separate from the production environment. All changes to the Simpli.fi Demand Side Platform must be approved by a member of management prior to promotion into production. A peer review, including a review of the Simpli.fi Demand Side Platform code for vulnerabilities, is performed on the source code change prior to migration into the production environment. Any issues identified as a result of the review must be resolved before the change is moved into the production environment.

All changes to the Bidders application in the on-premise production environment must be approved by a member of management prior to promotion into production. Prior to implementation, all changes to the Bidders application in the on-premise production environment are tested in a staging environment separate from the production environment. All infrastructure changes to the on-premise production environment (server, operating system, and databases) must be approved by a member of management prior to promotion into production.

The Company maintains a formal inventory of production system assets. The production environment's infrastructure is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers are hardened against security threats. Server builds leverage a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform. Server builds leverage a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment.

3. Incident Response and Vulnerability Management

The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs). An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated. The Company utilizes a log management tool to identify events that may have a potential impact on the Company's ability to achieve its security objectives. The logs are maintained and protected from alteration, and access is restricted to appropriate personnel based on job function. The Company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

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

The Company has established an internal communication channel for users to report potential security issues or fraud concerns. Each report is reviewed by the appropriate management personnel, based on the nature of the potential security issue or fraud concern. The Company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. Each report is reviewed by the appropriate management personnel, based on the nature of the reported system information on failures, incidents, concerns, and other complaints. The Company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's Incident Response Plan.

The Company's network is segmented to prevent unauthorized access to customer data. The Company's network diagram are available to IT Security personnel via GitHub. The Company uses firewalls and configures them to prevent unauthorized access. The Company reviews its firewall rulesets at least annually. Required changes are tracked to completion. The Company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. The Company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. To protect mobile devices supporting the service, the Company has implemented protections such as remote wipe, remote lock, encryption, and patch management. Antivirus software is in place on all Company-owned endpoint devices. Virus definitions are automatically downloaded and deployed to Company-owned endpoint devices each business day. Company-owned endpoint devices are configured to enforce hard drive encryption to access the Company's network.

4. **Third-Party and Vendor Management**

   The Company provides a description of its products and services to internal and external users. The Company has a vendor management program in place which includes the following: critical third-party vendor inventory, vendor's security requirements, and review of critical third-party vendors at least annually. The Company has written agreements in place with critical vendors and third parties. These agreements include security commitments applicable to that entity.

5. **Business Continuity and Disaster Recovery**

   A Business Continuity and Disaster Recovery Plan has been developed and is documented.

6. **Backup Management**

   Backups of the production environment and related databases of the Simpli.fi Demand Side Platform are configured to be performed at least daily. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved. Backups of the production environment and related databases of the on-premise Bidtellect production environment are configured to be performed at least daily. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved. Access to the backup tool is restricted to appropriate personnel based on job function. The backup tool is configured to automatically protect backups of the production environment utilizing Advanced Encryption Standards (AES) or a Secure Hash Algorithm (SHA). The Company's legacy on-premise databases housing sensitive customer data utilize application-layer encryption to protect data at rest. Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time.

H. User Entity Responsibilities

Each user entity must evaluate its own system of internal controls for effective risk management and compliance. The internal controls described in this report occur at and are managed by the Company and only cover a portion of a comprehensive internal control structure relevant to a user entity. Each user entity must address the various aspects of internal control that may be unique to its particular organization. This section highlights those portions of the internal control structure that user entities have responsibility to develop and maintain but should not affect the ability of the Company to achieve its service commitments and system requirements.

Related Control Area	User Entity Responsibilities
Monitoring & Communication	• Customers are responsible for notifying Simpli.fi of changes made to technical or administrative contact information. • Customers are responsible for ensuring the supervision, management, and control of the use of Simpli.fi services by their personnel. • Customers are responsible for immediately notifying Simpli.fi of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
Policies & Procedures	• Customers are responsible for understanding and complying with their contractual obligations to Simpli.fi. • Customers are responsible for maintaining their own system(s) of record. • Customers are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Simpli.fi services.
Data Transmission	• Customers are responsible for providing Simpli.fi with a list of approvers for security and system configuration changes for data transmission.

I. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations. The most significant subservice organizations used by the Company are noted below.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Equinix	The Company uses Equinix for its third-party colocation data center services for the hosting of servers and equipment for the Bidtellect Platform, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the Bidtellect Platform including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure such as physical servers and physical access to the Data Centers hosting the Bidtellect Platform; • Controls around the change management processes for the underlying infrastructure supporting the Bidtellect Platform; and • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. In addition, the Company has identified the following control activity to help monitor the subservice organization: • The Company has a vendor management program in place which includes the following: critical third-party vendor inventory, vendor's security requirements, and review of critical third-party vendors at least annually.	CC 2.1* CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.8* CC 7.5* CC 8.1* CC 9.1*
Google Cloud Platform (GCP)	The Company uses GCP's Google Compute Engine (GCE) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment for the Simpli.fi Demand Side Platform, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses Google BigQuery, Google Cloud SQL, Google Cloud Key Management Service (KMS), and Google Cloud Storage as a Platform-as-a-Service. Google Cloud Storage provides object storage through a web service interface. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the Simpli.fi Demand Side Platform including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform;	CC 2.1* CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the configuration settings within the GCE instance to ensure that data is encrypted and stored as per the configuration settings selected with GCP; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components for Google BigQuery, Google Cloud SQL, Google Cloud KMS, and Google Cloud Storage such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over Google BigQuery, Google Cloud SQL, Google Cloud KMS, and Google Cloud Storage including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls over Google Cloud Storage redundancy, including controls over data replication; and • Controls over the change management processes for the GCP Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform Google BigQuery, Google Cloud SQL, Google Cloud KMS, and Google Cloud Storage components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: • The Company has a vendor management program in place which includes the following: critical third-party vendor inventory, vendor's security requirements, and review of critical third-party vendors at least annually.	
Okta	The Company uses Okta for its Software-as-a-Service platform for identity management services. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the Simpli.fi Demand Side Platform including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure and such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the software and infrastructure supporting the in-scope production environment; • Controls over incident monitoring, response, and follow up; • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls over storage redundancy, including controls over data replication; • Controls over the encryption of transmitted and stored data within the platform; and	CC 2.1* CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over managing patching for the software and infrastructure supporting the platform. In addition, the Company has identified the following control activity to help monitor the subservice organization: • The Company has a vendor management program in place which includes the following: critical third-party vendor inventory, vendor's security requirements, and review of critical third-party vendors at least annually.	

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at these subservice organizations that support the service organization's service commitments and system requirements are in place and are operating effectively.*

J. Non-Applicable Trust Services Criteria

Security Trust Services Category		
Non-Applicable Trust Services Criteria		**Simplifi Holdings, LLC's Rationale**
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A – The Company's colocation provider, Equinix, hosting provider, Google Cloud Platform (GCP), and Software-as-a-Service provider, Okta, are responsible for physical security controls. The Company does not maintain any hard copy data or store any customer information physically.

K. Changes to the System During the Specified Period

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service during the Specified Period.

L. Additional Information about Management's Description

The controls supporting the service organization's service commitments and system requirements based on the applicable trust services criteria are included within Section IV of this report, *Description of the Trust Services Category, Criteria, and Simplifi Holdings, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results*. Although the applicable trust services criteria and related control activities are presented within Section IV, they are an integral part of the Company's description of its system.

IV. Description of the Trust Services Category, Criteria, and Simplifi Holdings, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results

A. Types and Descriptions of the Tests of Operating Effectiveness

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to provide user entities of the Company's System, those prospective user entities, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System. The description is intended to provide users with information about the System. Our examination was limited to the applicable trust services criteria and related control activities specified by the Company in sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations. It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the control activities specified by the Company. In planning the nature, timing, and extent of our testing of the control activities to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

Description of Test Procedures Performed

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel regarding the control activity and/or corroborated responses with management
Observation	Observed the application, performance, or existence of the control activity
Inspection	Inspected documents, records, electronic files, or other evidence indicating performance of the control activity
Reperformance	Reperformed the operation of the control activity, through normal procedures or through the use of automated techniques, where appropriate

Testing of Key Reports

As required by paragraph .36 of AT-C section 205, Examination Engagements (AICPA, Professional Standards) when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

For tests of control activities requiring management's use of information produced by the entity (IPE), including electronic audit evidence (e.g., control activities requiring system-generated populations for sample-based testing), Aprio 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:

- Inspected the source of the IPE;
- Inspected the query, script, or parameters used to generate the IPE;
- Reconciled data between the IPE and the source; and
- Inspected the IPE for anomalous gaps in sequence or timing to determine that the data was complete, accurate, and maintained its integrity.

For tests of controls requiring management's use of IPE in the execution of the control activities (e.g., a list of changes to the ticketing system which tracks the different steps in the change management process), we inspected management's procedures as applicable to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Test of Operating Effectiveness

The tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those control activities, and the extent of compliance with them, were sufficient to provide reasonable assurance, but not absolute, assurance the applicable trust services criteria were achieved throughout the Specified Period. Our tests of operating effectiveness of control activities were designed to cover a representative number of transactions throughout the Specified Period, for each of the control activities listed in Section IV. In selecting particular tests of operating effectiveness of the control activities, Aprio considered (1) the nature of the control activities being tested; (2) the types and competence of available evidential matter; (3) the nature of the trust services categories and criteria to be achieved; and (4) the expected efficiency and effectiveness of the test. Such tests were used to evaluate the fairness of the presentation of the description of the System and to evaluate the operating effectiveness of specified control activities.

Any deviations are disclosed in Section IV of the report no matter the level of materiality.

Table 1: Sampling Table Based on Population Size				
Number of Deviations	**<100**	**100-200**	**201 – 1,000**	**>1,000**
0	20% [a]	22	25	40
1	30% [a]	35	40	70
2	N/A [b]	N/A [b]	60	100

a - This would be applied against the total population (i.e., a population of 50 assuming no deviations would be a sample of ten).

b - Sampling would not be used in this situation.

Table 2: Sampling Table Based on Infrequently Operating Controls			
Control Frequency & Population Size	**12 Months Sample Size**	**6 Months Sample Size**	**3 Months Sample Size**
Annually	1	1	1
Quarterly	2	2	1
Monthly	3	2	2
Weekly	8	5	3
Transactional	See Table 1	See Table 1	See Table 1
Daily	See Table 1	See Table 1	See Table 1

Non-occurrences

There may be instances where a control activity did not occur as the reason for the control activity did not happen during the Specified Period (a "non-occurrence" of the control activity). If such a situation occurred, the Service Auditor noted that these control activities did not operate during the Specified Period and could not be tested for operating effectiveness. These non-occurrences are not considered exceptions.

B. Trust Services Category, Criteria, Control Activities, and Testing Provided by the Service Auditor

The trust services criteria relevant to Security address that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the Availability, Processing Integrity, Confidentiality, and Privacy of Information of systems and affect the Company's ability to achieve its service commitments and system requirements.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-05	The Company requires employees to acknowledge the Code of Conduct and information security policies at the time of hire. Employees who violate the Code of Conduct or information security policies are subject to disciplinary actions in accordance with the Code of Conduct.	Inspection: Inspected the Code of Conduct to determine that the Code of Conduct documented that employees who violated the Code of Conduct or information security policies would be subjected to disciplinary actions.	No exceptions noted.
		Inspection: Inspected the Information Security and Code of Conduct Acknowledgement forms related to a sample of new employees to determine that each selected new employee signed a statement signifying that they had acknowledged the Code of Conduct and information security policies at the time of hire.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-06	The Company requires contractors with access to customer data to comply with confidentiality and data protection requirements, including the Code of Conduct.	Inspection: Inspected the signed contractor agreements related to a sample of new contractors with access to customer data to determine that the agreement for each selected new contractor with access to customer data included confidentiality and data protection requirements, including the Code of Conduct. Inspection/Inquiry: Inspected a system generated listing of new contractors with access to customer data during the Specified Period to determine that there were no new contractors with access to customer data during the Specified Period. Further, inquired of the Director of Audit Risk and Compliance to determine that there were no new contractors with access to customer data during the Specified Period.	No exceptions noted. The Service Auditor noted that this Control Activity did not operate during the Specified Period, as there were no new contractors with access to customer data during the Specified Period. Therefore, this Control Activity could not be tested for operating effectiveness.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-07	The Company requires contractors with access to customer data to sign a confidentiality agreement at the time of engagement.	Inspection: Inspected the confidentiality agreements related to a sample of new contractors with access to customer data to determine that each selected new contractor with access to customer data signed a confidentiality agreement at the time of engagement. Inspection/Inquiry: Inspected a system generated listing of new contractors with access to customer data during the Specified Period to determine that there were no new contractors with access to customer data during the Specified Period. Further, inquired of the Director of Audit Risk and Compliance to determine that there were no new contractors with access to customer data during the Specified Period.	No exceptions noted. The Service Auditor noted that this Control Activity did not operate during the Specified Period, as there were no new contractors with access to customer data during the Specified Period. Therefore, this Control Activity could not be tested for operating effectiveness.
CC 1.1-08	The Company requires employees to sign a confidentiality agreement during onboarding.	Inspection: Inspected the confidentiality agreements related to a sample of new employees to determine that each selected new employee signed a confidentiality agreement during onboarding.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-09	Performance reviews are performed for employees of the Engineering Department on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities.	Inspection: Inspected the annual performance reviews related to a sample of current employees of the Engineering Department to determine that performance reviews were performed during the Specified Period for each selected current employee of the Engineering Department to help ensure that each employee's skill set matched his/her job responsibilities.	No exceptions noted.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC 1.2-01	Management maintains the Company's organizational structure dynamically within the Company's HR Portal. The organizational chart is available to internal users via the Company's HR Portal.	Observation/Inquiry: Observed the Company's HR Portal to determine that management maintained the Company's organizational structure dynamically within the HR Portal and that the organizational chart was available to internal users via the Company's HR Portal. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Organizational Chart was available to internal users via the HR Portal throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.2-02	The Company's Board of Directors meets at least annually and maintains formal meeting minutes.	Inspection: Inspected the Annual Board Minutes and the listing of Board members to determine that the Company's Board of Directors met during the Specified Period and maintained formal meeting minutes.	No exceptions noted.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.
CC 1.2-01	Management maintains the Company's organizational structure dynamically within the Company's HR Portal. The organizational chart is available to internal users via the Company's HR Portal.	Observation/Inquiry: Observed the Company's HR Portal to determine that management maintained the Company's organizational structure dynamically within the HR Portal and that the organizational chart was available to internal users via the Company's HR Portal. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Organizational Chart was available to internal users via the HR Portal throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.3-01	The Company has written agreements in place with critical vendors and third parties. These agreements include security commitments applicable to that entity.	Inspection: Inspected the agreements with vendors and third parties related to a sample of new critical vendors and third parties to determine that the Company had written agreements in place with each selected new critical vendor and/or third party and that each selected agreement included security commitments applicable to that entity.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.
CC 1.1-05	The Company requires employees to acknowledge the Code of Conduct and information security policies at the time of hire. Employees who violate the Code of Conduct or information security policies are subject to disciplinary actions in accordance with the Code of Conduct.	Inspection: Inspected the Code of Conduct to determine that the Code of Conduct documented that employees who violated the Code of Conduct or information security policies would be subjected to disciplinary actions.	No exceptions noted.
		Inspection: Inspected the Information Security and Code of Conduct Acknowledgement forms related to a sample of new employees to determine that each selected new employee signed a statement signifying that they had acknowledged the Code of Conduct and information security policies at the time of hire.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.4-01	The Company performs background checks and/or reference checks on new employees and contractors with access to the in-scope systems at the time of hire.	Inspection: Inspected the completed background checks and/or reference checks related to a sample of new employees and contractors with access to the in-scope systems to determine that each selected new employee and contractor with access to the in-scope systems was subjected to a background check and/or reference check at the time of hire.	No exceptions noted.
CC 1.4-02	The Company requires employees to complete security awareness training within thirty business days of hire and at least annually thereafter.	Inspection: Inspected the Security Awareness Acknowledgments related to a sample of current employees to determine that each selected current employee completed the security awareness program during the Specified Period.	No exceptions noted.
		Inspection: Inspected the Security Awareness Acknowledgments related to a sample of new employees to determine that each selected new employee completed the security awareness program within thirty business days of hire.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-05	The Company requires employees to acknowledge the Code of Conduct and information security policies at the time of hire. Employees who violate the Code of Conduct or information security policies are subject to disciplinary actions in accordance with the Code of Conduct.	Inspection: Inspected the Code of Conduct to determine that the Code of Conduct documented that employees who violated the Code of Conduct or information security policies would be subjected to disciplinary actions.	No exceptions noted.
		Inspection: Inspected the Information Security and Code of Conduct Acknowledgement forms related to a sample of new employees to determine that each selected new employee signed a statement signifying that they had acknowledged the Code of Conduct and information security policies at the time of hire.	No exceptions noted.
CC 1.2-01	Management maintains the Company's organizational structure dynamically within the Company's HR Portal. The organizational chart is available to internal users via the Company's HR Portal.	Observation/Inquiry: Observed the Company's HR Portal to determine that management maintained the Company's organizational structure dynamically within the HR Portal and that the organizational chart was available to internal users via the Company's HR Portal. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Organizational Chart was available to internal users via the HR Portal throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-01	The Company has a Data Protection Policy in place to help ensure that confidential data is properly secured and restricted to appropriate personnel.	Inspection: Inspected the Data Protection Policy to determine that the Company had a documented policy in place to help ensure that confidential data was properly secured and restricted to appropriate personnel.	No exceptions noted.
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the on-premise Bidtellect production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC 2.1-06	The Company utilizes a log management tool to identify events that may have a potential impact on the Company's ability to achieve its security objectives. The logs are maintained and protected from alteration, and access is restricted to appropriate personnel based on job function.	Observation/Inquiry: Observed the log management tool's configuration settings to determine that the Company utilized a log management tool to identify events that could have a potential impact on the Company's ability to achieve its security objectives and that the logs were maintained and protected from alteration. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the log management tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection/Inquiry: Inspected the listing of users with access to the logs within the log management tool and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-07	The Company maintains a formal inventory of production system assets.	Observation/Inquiry: Observed the master list of system components/assets within Vanta to determine that the Company maintained a formal inventory of production system assets. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the master list of system components/assets was maintained throughout the Specified Period.	No exceptions noted.
		Observation/Inquiry: Observed the master list of system components/assets for the on-premise Bidtellect production environment to determine that the Company maintained a formal inventory of production system assets. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the master list of system components/assets was maintained throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-05	The Company requires employees to acknowledge the Code of Conduct and information security policies at the time of hire. Employees who violate the Code of Conduct or information security policies are subject to disciplinary actions in accordance with the Code of Conduct.	Inspection: Inspected the Code of Conduct to determine that the Code of Conduct documented that employees who violated the Code of Conduct or information security policies would be subjected to disciplinary actions.	No exceptions noted.
		Inspection: Inspected the Information Security and Code of Conduct Acknowledgement forms related to a sample of new employees to determine that each selected new employee signed a statement signifying that they had acknowledged the Code of Conduct and information security policies at the time of hire.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-06	The Company requires contractors with access to customer data to comply with confidentiality and data protection requirements, including the Code of Conduct.	Inspection: Inspected the signed contractor agreements related to a sample of new contractors with access to customer data to determine that the agreement for each selected new contractor with access to customer data included confidentiality and data protection requirements, including the Code of Conduct. Inspection/Inquiry: Inspected a system generated listing of new contractors with access to customer data during the Specified Period to determine that there were no new contractors with access to customer data during the Specified Period. Further, inquired of the Director of Audit Risk and Compliance to determine that there were no new contractors with access to customer data during the Specified Period.	No exceptions noted. The Service Auditor noted that this Control Activity did not operate during the Specified Period, as there were no new contractors with access to customer data during the Specified Period. Therefore, this Control Activity could not be tested for operating effectiveness.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-07	The Company requires contractors with access to customer data to sign a confidentiality agreement at the time of engagement.	Inspection: Inspected the confidentiality agreements related to a sample of new contractors with access to customer data to determine that each selected new contractor with access to customer data signed a confidentiality agreement at the time of engagement. Inspection/Inquiry: Inspected a system generated listing of new contractors with access to customer data during the Specified Period to determine that there were no new contractors with access to customer data during the Specified Period. Further, inquired of the Director of Audit Risk and Compliance to determine that there were no new contractors with access to customer data during the Specified Period.	No exceptions noted. The Service Auditor noted that this Control Activity did not operate during the Specified Period, as there were no new contractors with access to customer data during the Specified Period. Therefore, this Control Activity could not be tested for operating effectiveness.
CC 1.1-08	The Company requires employees to sign a confidentiality agreement during onboarding.	Inspection: Inspected the confidentiality agreements related to a sample of new employees to determine that each selected new employee signed a confidentiality agreement during onboarding.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.4-02	The Company requires employees to complete security awareness training within thirty business days of hire and at least annually thereafter.	Inspection: Inspected the Security Awareness Acknowledgments related to a sample of new employees to determine that each selected new employee completed the security awareness program within thirty business days of hire.	No exceptions noted.
		Inspection: Inspected the Security Awareness Acknowledgments related to a sample of current employees to determine that each selected current employee completed the security awareness program during the Specified Period.	No exceptions noted.
CC 2.2-01	The Company's network is segmented to prevent unauthorized access to customer data. The Company’s network diagram is available to IT Security personnel via GitHub.	Observation/Inquiry: Observed the network configurations for the Simpli.fi Demand Side Platform's production environment to determine that the Company's network was segmented to prevent unauthorized access to customer data. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Observation/Inquiry: Observed the network diagrams in GitHub to determine that the network diagrams were available to IT Security personnel via GitHub. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the network diagrams were available in GitHub throughout the Specified Period.	No exceptions noted.
CC 2.2-02	The Company has established an internal communication channel for users to report potential security issues or fraud concerns. Each report is reviewed by the appropriate management personnel, based on the nature of the potential security issue or fraud concern.	Observation/Inquiry: Observed the Slack to determine that an internal communication channel was in place for users to report potential security issues or fraud concerns. Further, inquired of the Director of Audit Risk and Compliance to determine that the internal communication channel was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets related to a sample of internally reported security incidents and fraud concerns to determine that each selected incident and/or fraud concern was reviewed by the appropriate management personnel, based on the nature of the potential security issue or fraud concern.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC 2.3-01	The Company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. Each report is reviewed by the appropriate management personnel, based on the nature of the reported system information on failures, incidents, concerns, and other complaints.	Observation/Inquiry: Observed the external-facing support system to determine that the Company had an external-facing support system in place that allowed users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. Further, inquired of the Director of Audit Risk and Compliance to determine that the external-facing support system was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets related to a sample of externally reported system information on failures, incidents, concerns, and other complaints to determine that each selected report was reviewed by the appropriate management personnel, based on the nature of the reported system information on failures, incidents, concerns, and/or other complaints.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.3-02	The Company provides a description of its products and services to internal and external users.	Observation/Inquiry: Observed the Company's website to determine that the Company provided a description of its products and services to internal and external users on the website. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the description of the Company's products and services was on the website throughout the Specified Period.	No exceptions noted.
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.
CC3.2 - COSO Principle 7: 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.			
CC 1.3-01	The Company has written agreements in place with critical vendors and third parties. These agreements include security commitments applicable to that entity.	Inspection: Inspected the agreements with vendors and third parties related to a sample of new critical vendors and third parties to determine that the Company had written agreements in place with each selected new critical vendor and/or third party and that each selected agreement included security commitments applicable to that entity.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 3.2-01	The Company has a vendor management program in place which includes the following: • critical third-party vendor inventory, • vendor's security requirements, and • review of critical third-party vendors at least annually.	Observation/Inquiry: Observed the Company's critical vendor listing in Vanta to determine that the Company maintained an inventory of critical third-party vendors as part of the Company's vendor management program. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Company maintained an inventory of critical third-party vendors throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Third-Party Risk Management Policy to determine that the Company had a documented vendor management program in place.	No exceptions noted.
		Inspection: Inspected the annual third-party reviews related to a sample of current critical third parties and vendors to determine that the Company reviewed the security requirements of each selected vendor during the Specific Period as part of the Company's vendor management program.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.2-01	Management maintains the Company's organizational structure dynamically within the Company's HR Portal. The organizational chart is available to internal users via the Company's HR Portal.	Observation/Inquiry: Observed the Company's HR Portal to determine that management maintained the Company's organizational structure dynamically within the HR Portal and that the organizational chart was available to internal users via the Company's HR Portal. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Organizational Chart was available to internal users via the HR Portal throughout the Specified Period.	No exceptions noted.
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.
CC 3.2-01	The Company has a vendor management program in place which includes the following: • critical third-party vendor inventory, • vendor's security requirements, and • review of critical third-party vendors at least annually.	Inspection: Inspected the Third-Party Risk Management Policy to determine that the Company had a documented vendor management program in place.	No exceptions noted.
		Observation/Inquiry: Observed the Company's critical vendor listing in Vanta to determine that the Company maintained an inventory of critical third-party vendors as part of the Company's vendor management program. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Company maintained an inventory of critical third-party vendors throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the annual third-party reviews related to a sample of current critical third parties and vendors to determine that the Company reviewed the security requirements of each selected vendor during the Specific Period as part of the Company's vendor management program.	No exceptions noted.
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC 1.1-05	The Company requires employees to acknowledge the Code of Conduct and information security policies at the time of hire. Employees who violate the Code of Conduct or information security policies are subject to disciplinary actions in accordance with the Code of Conduct.	Inspection: Inspected the Code of Conduct to determine that the Code of Conduct documented that employees who violated the Code of Conduct or information security policies would be subjected to disciplinary actions.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the Information Security and Code of Conduct Acknowledgement forms related to a sample of new employees to determine that each selected new employee signed a statement signifying that they had acknowledged the Code of Conduct and information security policies at the time of hire.	No exceptions noted.
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC 4.2-01	The Company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's Incident Response Plan.	Inspection: Inspected the Incident Response Plan to determine that the Incident Response Plan documented requirements for the Company to log, track, resolve, and communicate security incidents to affected or relevant parties by management.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the system tickets related to a sample of security incidents to determine that each selected security incident was logged, tracked, resolved, and communicated to affected or relevant parties by management in accordance to the Company's Incident Response Plan.	No exceptions noted.
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.
CC 1.2-01	Management maintains the Company's organizational structure dynamically within the Company's HR Portal. The organizational chart is available to internal users via the Company's HR Portal.	Observation/Inquiry: Observed the Company's HR Portal to determine that management maintained the Company's organizational structure dynamically within the HR Portal and that the organizational chart was available to internal users via the Company's HR Portal. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Organizational Chart was available to internal users via the HR Portal throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-06	The Company utilizes a log management tool to identify events that may have a potential impact on the Company's ability to achieve its security objectives. The logs are maintained and protected from alteration, and access is restricted to appropriate personnel based on job function.	Observation/Inquiry: Observed the log management tool's configuration settings to determine that the Company utilized a log management tool to identify events that could have a potential impact on the Company's ability to achieve its security objectives and that the logs were maintained and protected from alteration. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the log management tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection/Inquiry: Inspected the listing of users with access to the logs within the log management tool and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC 5.2-01	Administrative access to GCP, including super administrator access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to GCP, including super administrator access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-02	Virtual Private Network (VPN) access, including administrative access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with VPN access, including administrative access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-03	Access to the unique Secure Shell (SSH) Keys is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to the unique SSH Keys and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-04	Access to GCP requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for GCP to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-05	Super administrator access to GCP requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for super administrator access to GCP to determine that access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-06	Access to Okta requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device.	Observation/Inquiry: Observed the authentication process for access to Okta to determine that access required MFA, which required users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-07	Direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid Secure Shell (SSH) key.	Observation/Inquiry: Observed the authentication process for direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid SSH key. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-08	Administrative access to Okta is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to Okta and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-09	Administrative access to the Simpli.fi Demand Side Platform's databases is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the Simpli.fi Demand Side Platform's databases and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-10	The Company restricts access to migrate changes to the production environment to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to migrate changes into the production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-11	The production environment's infrastructure is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers are hardened against security threats.	Inspection: Inspected the system tickets related to a sample of infrastructure deployments for the Simpli.fi Demand Side Platform's production environment to determine that the Company had production infrastructure patched for each selected infrastructure deployment as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers were hardened against security threats.	No exceptions noted.
		Observation/Inquiry: Observed Patch Manager Plus to determine that patches for the production infrastructure were configured to be applied automatically as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers were hardened against security threats. Further, inquired of the Director of Audit Risk and Compliance to determine that patches for the production infrastructure were configured to be automatically applied throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-12	The Company has a formal Secure Development Policy (SDP) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspection: Inspected the SDP methodology to determine that the Company had a formal SDP methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC 5.2-13	Prior to implementation, all changes to the Simpli.fi Demand Side Platform are tested in a development environment separate from the production environment.	Observation/Inquiry: Observed the development and production environments to determine that the development and production environments were separated. Further, inquired of the Director of Audit, Risk, and Compliance to determine that separate development and production environments were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets related to a sample of changes to the Simpli.fi Demand Side Platform to determine that each selected change was tested prior to promotion into production.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-14	All changes to the Bidders application in the on-premise production environment must be approved by a member of management prior to promotion into production.	Inspection: Inspected the system tickets related to a sample of changes to the Bidders application in the on-premise production environment to determine that each selected change was approved by a member of management prior to promotion into production.	No exceptions noted.
CC 5.2-15	Administrative access to the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-16	Administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-17	Direct access to the on-premise Bidtellect production environment, including servers, databases, and the Bidder application, requires VPN access and multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for direct access to the Bidtellect production environment, including servers, databases, and the Bidder application, to determine that authentication required remote access via VPN and access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-18	Prior to implementation, all changes to the Bidders application in the on-premise production environment are tested in a staging environment separate from the production environment.	Observation/Inquiry: Observed the Bidders application's staging and production environments to determine that the staging and production environments were separated. Further, inquired of the Director of Audit, Risk, and Compliance to determine that separate staging and production environments were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets related to a sample of changes to the Bidders application in the on-premise production environment to determine that each selected change was tested prior to promotion into production.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC 1.1-01	The Company has incident response policies and procedures which collectively address the security of the system. These policies and procedures are documented and communicated to appropriate users.	Observation/Inquiry: Observed Confluence to determine that the Company had incident response policies and procedures that were communicated to appropriate users. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the Operations Security Policy, Information Security Policy, and Incident Response Plan to determine that the Company had incident response policies and procedures, which collectively addressed the security of the system and were documented.	No exceptions noted.
CC 1.1-02	The Company has information security policies and procedures which cover vulnerability management and system monitoring. These policies and procedures are documented and reviewed at least annually.	Inspection: Inspected the Operations Security Policy and Incident Response Plan to determine that the Company's information security policies and procedures were documented and reviewed during the Specified Period and that the policies included documentation over vulnerability management and system monitoring.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 1.1-03	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in each selected job description and/or the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 1.1-04	The Company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspection: Inspected the written job descriptions specifying the responsibilities of and professional requirements for personnel related to a sample of job positions and inspected the Information Security Roles and Responsibilities Policy to determine that Company management had established defined roles and responsibilities for each selected job position to oversee the design and implementation of information security controls.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC 4.2-01	The Company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's Incident Response Plan.	Inspection: Inspected the Incident Response Plan to determine that the Incident Response Plan documented requirements for the Company to log, track, resolve, and communicate security incidents to affected or relevant parties by management.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the system tickets related to a sample of security incidents to determine that each selected security incident was logged, tracked, resolved, and communicated to affected or relevant parties by management in accordance to the Company's Incident Response Plan.	No exceptions noted.
CC6.0 - Logical and Physical Access Controls			
CC6.1 - 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.			
CC 2.1-07	The Company maintains a formal inventory of production system assets.	Observation/Inquiry: Observed the master list of system components/assets within Vanta to determine that the Company maintained a formal inventory of production system assets. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the master list of system components/assets was maintained throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.2-01	The Company's network is segmented to prevent unauthorized access to customer data. The Company's network diagram is available to IT Security personnel via GitHub.	Observation/Inquiry: Observed the network configurations for the Simpli.fi Demand Side Platform's production environment to determine that the Company's network was segmented to prevent unauthorized access to customer data. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
		Observation/Inquiry: Observed the network diagrams in GitHub to determine that the network diagrams were available to IT Security personnel via GitHub. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the network diagrams were available in GitHub throughout the Specified Period.	No exceptions noted.
CC 5.2-01	Administrative access to GCP, including super administrator access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to GCP, including super administrator access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-02	Virtual Private Network (VPN) access, including administrative access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with VPN access, including administrative access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-03	Access to the unique Secure Shell (SSH) Keys is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to the unique SSH Keys and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-04	Access to GCP requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for GCP to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-05	Super administrator access to GCP requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for super administrator access to GCP to determine that access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-06	Access to Okta requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device.	Observation/Inquiry: Observed the authentication process for access to Okta to determine that access required MFA, which required users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-07	Direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid Secure Shell (SSH) key.	Observation/Inquiry: Observed the authentication process for direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid SSH key. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-08	Administrative access to Okta is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to Okta and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-09	Administrative access to the Simpli.fi Demand Side Platform's databases is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the Simpli.fi Demand Side Platform's databases and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-15	Administrative access to the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-16	Administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-17	Direct access to the on-premise Bidtellect production environment, including servers, databases, and the Bidder application, requires VPN access and multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for direct access to the Bidtellect production environment, including servers, databases, and the Bidder application, to determine that authentication required remote access via VPN and access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 6.1-01	Access to the backup tool is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to the backup tool for the Bidtellect on-premise production environment databases and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the listing of users with access to the backup tool for the Simpli.fi Demand Side Platform and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 6.1-02	Password parameters for Okta are configured as follows: • Minimum password length: 15 characters, • Password history: 24 passwords, and • Password complexity: enabled.	Observation/Inquiry: Observed the password parameters for Okta to determine that the password parameters were configured as follows: • Minimum password length: 15 characters, • Password history: 24 passwords, and • Password complexity: enabled. Further, inquired of the Director of Audit Risk and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.1-03	Password parameters for GCP are configured as follows: • Minimum password length: 15 characters and • Password complexity: enabled.	Observation/Inquiry: Observed the password parameters for GCP to determine that the password parameters were configured as follows: • Minimum password length: 15 characters and • Password complexity: enabled. Further, inquired of the Director of Audit Risk and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC 6.1-04	The Company's legacy on-premise databases housing sensitive customer data utilize application-layer encryption to protect data at rest.	Inspection/Inquiry: Inspected the source code for the application-layer encryption configurations for the legacy on-premise databases to determine that the Company's databases housing sensitive customer data were encrypted at rest. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC 6.1-05	Access to the system components for the in-scope production environments is removed or disabled according to Service Level Agreements (SLAs).	Inspection: Inspected the termination tickets related to a sample of terminated employees with access to the system components for the in-scope production environments to determine that the Company removed or disabled access for each selected terminated employee according to SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.1-06	The backup tool is configured to automatically protect backups of the production environment utilizing Advanced Encryption Standards (AES) or a Secure Hash Algorithm (SHA).	Observation/Inquiry: Observed the script for the backup tool's configurations for the on-premise environment to determine that the tool was configured to automatically protect backups with AES and SHA. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC 6.1-07	Company-owned endpoint devices are configured to enforce hard drive encryption to access the Company's network.	Observation/Inquiry: Observed the Vanta configurations to determine that endpoint devices were configured to enforce hard drive encryption. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.1-08	Server builds leverage a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform.	Observation/Inspection/Inquiry: Observed the build process and inspected the applicable source code for server implementations to determine that server builds leveraged a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC 6.1-09	Server builds leverage a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment.	Observation/Inquiry: Observed the build process to determine that server builds leveraged a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC6.2 - 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.			
CC 6.1-05	Access to the system components for the in-scope production environments is removed or disabled according to Service Level Agreements (SLAs).	Inspection: Inspected the termination tickets related to a sample of terminated employees with access to the system components for the in-scope production environments to determine that the Company removed or disabled access for each selected terminated employee according to SLAs.	No exceptions noted.
CC 6.2-01	Requests to add and/or modify access to the system components for the Simpli.fi System are approved by each user's manager or other appropriate personnel prior to access being granted.	Inspection: Inspected the system tickets/corresponding documentation related to a sample of requests to add and/or modify access to the system components for the in-scope systems to determine that each selected request was approved by each user's manager prior to access being granted.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC6.3 - 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.			
CC 6.1-05	Access to the system components for the in-scope production environments is removed or disabled according to Service Level Agreements (SLAs).	Inspection: Inspected the termination tickets related to a sample of terminated employees with access to the system components for the in-scope production environments to determine that the Company removed or disabled access for each selected terminated employee according to SLAs.	No exceptions noted.
CC 6.2-01	Requests to add and/or modify access to the system components for the Simpli.fi System are approved by each user's manager or other appropriate personnel prior to access being granted.	Inspection: Inspected the system tickets/corresponding documentation related to a sample of requests to add and/or modify access to the system components for the in-scope systems to determine that each selected request was approved by each user's manager prior to access being granted.	No exceptions noted.
CC6.4 - 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.			
CC 6.4-01	N/A – The Company's hosting provider, Google Cloud Platform (GCP) and Equinix, and Software-as-a-Service provider, Okta, are responsible for physical security controls. The Company does not maintain any hard copy data or store any customer information physically.	N/A	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC6.5 - 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.			
CC 6.5-01	Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time.	Inspection: Inspected the formal data retention and destruction standards to determine that the standards included guidelines for the retention of data for required periods of time and the data destruction requirements.	No exceptions noted.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC 5.2-01	Administrative access to GCP, including super administrator access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to GCP, including super administrator access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-02	Virtual Private Network (VPN) access, including administrative access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with VPN access, including administrative access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-03	Access to the unique Secure Shell (SSH) Keys is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to the unique SSH Keys and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-04	Access to GCP requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for GCP to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-05	Super administrator access to GCP requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for super administrator access to GCP to determine that access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-06	Access to Okta requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device.	Observation/Inquiry: Observed the authentication process for access to Okta to determine that access required MFA, which required users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-07	Direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid Secure Shell (SSH) key.	Observation/Inquiry: Observed the authentication process for direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid SSH key. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-15	Administrative access to the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-17	Direct access to the on-premise Bidtellect production environment, including servers, databases, and the Bidder application, requires VPN access and multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for direct access to the Bidtellect production environment, including servers, databases, and the Bidder application, to determine that authentication required remote access via VPN and access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.6-01	The Company uses firewalls and configures them to prevent unauthorized access.	Observation/Inquiry: Observed the virtual network devices (firewalls) for the Simpli.fi Demand Side Platform and related configurations to determine that the Company used firewalls and configured them to prevent unauthorized access. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
		Observation/Inquiry: Observed the Cisco Secure firewalls for the on-premise Bidtellect production environment and related configurations to determine that the Company used firewalls and configured them to prevent unauthorized access. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the network diagram to determine that the network diagram documented the Company's use of firewalls to prevent unauthorized access.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.6-02	The Company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspection: Inspected the annual review of firewall rulesets and if applicable, the system tickets related to a sample of firewall changes, to determine that the Company reviewed its firewall rulesets during the Specified Period and that a change request was documented and tracked to completion for each selected change as a result of the review.	No exceptions noted.
CC6.7 - 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.			
CC 5.2-01	Administrative access to GCP, including super administrator access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to GCP, including super administrator access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-02	Virtual Private Network (VPN) access, including administrative access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with VPN access, including administrative access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-03	Access to the unique Secure Shell (SSH) Keys is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to the unique SSH Keys and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-15	Administrative access to the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 6.1-07	Company-owned endpoint devices are configured to enforce hard drive encryption to access the Company's network.	Observation/Inquiry: Observed the Vanta configurations to determine that endpoint devices were configured to enforce hard drive encryption. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.7-01	The Company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Observation/Inquiry: Observed the Simpli.fi Demand Side Platform production environment's transmission configurations to determine that the Company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these encryption transmission configurations were in place throughout the Specified Period.	No exceptions noted.
		Observation/Inquiry: Observed the on-premise Bidtellect production environment's transmission configurations to determine that the Company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these encryption transmission configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.7-02	The Company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. To protect mobile devices supporting the service, the Company has implemented protections such as remote wipe, remote lock, encryption, and patch management.	Observation/Inquiry: Observed the MDM system configurations to determine that the Company had a MDM system in place to centrally manage mobile devices supporting the service and that the Company had implemented protections such as remote wipe, remote lock, encryption, and patch management to protect mobile devices supporting the service. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC 5.2-01	Administrative access to GCP, including super administrator access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to GCP, including super administrator access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-02	Virtual Private Network (VPN) access, including administrative access, is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with VPN access, including administrative access, and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-03	Access to the unique Secure Shell (SSH) Keys is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to the unique SSH Keys and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-04	Access to GCP requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for GCP to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-05	Super administrator access to GCP requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for super administrator access to GCP to determine that access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-06	Access to Okta requires multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device.	Observation/Inquiry: Observed the authentication process for access to Okta to determine that access required MFA, which required users to enter a password and to confirm authentication via a token, push notification, security key, or biometrics to a mobile device. Further, inquired of the Director of Audit Risk and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.
CC 5.2-07	Direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, requires multi-factor authentication (MFA) and Single-Sign-On (SSO) through deployment of Okta, which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid Secure Shell (SSH) key.	Observation/Inquiry: Observed the authentication process for direct access to the Simpli.fi Demand Side Platform's production environment and related databases, including remote access via VPN, to determine that access required MFA and SSO through deployment of Okta, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device, and to enter a valid SSH key. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-08	Administrative access to Okta is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to Okta and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit Risk and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-09	Administrative access to the Simpli.fi Demand Side Platform's databases is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the Simpli.fi Demand Side Platform's databases and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-10	The Company restricts access to migrate changes to the production environment to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to migrate changes into the production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-15	Administrative access to the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-16	Administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment is restricted to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with administrative access to the databases (SQL and Vertica) supporting the on-premise Bidtellect production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.
CC 5.2-17	Direct access to the on-premise Bidtellect production environment, including servers, databases, and the Bidder application, requires VPN access and multi-factor authentication (MFA), which requires users to enter a password and to confirm authentication via a token or push notification to a mobile device.	Observation/Inquiry: Observed the authentication process for direct access to the Bidtellect production environment, including servers, databases, and the Bidder application, to determine that authentication required remote access via VPN and access required MFA, which required users to enter a password and to confirm authentication via a token or push notification to a mobile device. Further, inquired of the Director of Audit, Risk, and Compliance to determine that this process was in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.1-08	Server builds leverage a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform.	Observation/Inspection/Inquiry: Observed the build process and inspected the applicable source code for server implementations to determine that server builds leveraged a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC 6.1-09	Server builds leverage a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment.	Observation/Inquiry: Observed the build process to determine that server builds leveraged a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.8-01	Antivirus software is in place on all Company-owned endpoint devices. Virus definitions are automatically downloaded and deployed to Company-owned endpoint devices each business day.	Observation/Inquiry: Observed the anti-virus application's configurations console to determine that antivirus software was in place on all Company-owned endpoint devices and that virus definitions were automatically downloaded and deployed to Company-owned endpoint devices each business day. Further, inquired of the Director of Audit Risk and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC7.0 - System Operations			
CC7.1 - 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.			
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC 6.6-02	The Company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspection: Inspected the annual review of firewall rulesets and if applicable, the system tickets related to a sample of firewall changes, to determine that the Company reviewed its firewall rulesets during the Specified Period and that a change request was documented and tracked to completion for each selected change as a result of the review.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC7.2 - 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.			
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-06	The Company utilizes a log management tool to identify events that may have a potential impact on the Company's ability to achieve its security objectives. The logs are maintained and protected from alteration, and access is restricted to appropriate personnel based on job function.	Observation/Inquiry: Observed the log management tool's configuration settings to determine that the Company utilized a log management tool to identify events that could have a potential impact on the Company's ability to achieve its security objectives and that the logs were maintained and protected from alteration. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the log management tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection/Inquiry: Inspected the listing of users with access to the logs within the log management tool and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.6-02	The Company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspection: Inspected the annual review of firewall rulesets and if applicable, the system tickets related to a sample of firewall changes, to determine that the Company reviewed its firewall rulesets during the Specified Period and that a change request was documented and tracked to completion for each selected change as a result of the review.	No exceptions noted.
CC7.3 - 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.			
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC 4.2-01	The Company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's Incident Response Plan.	Inspection: Inspected the Incident Response Plan to determine that the Incident Response Plan documented requirements for the Company to log, track, resolve, and communicate security incidents to affected or relevant parties by management.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the system tickets related to a sample of security incidents to determine that each selected security incident was logged, tracked, resolved, and communicated to affected or relevant parties by management in accordance to the Company's Incident Response Plan.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC 2.1-04	The Company's penetration testing over the Bidtellect on-premise production environment and the Simpli.fi Demand Side Platform's production environment is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical vulnerabilities in accordance with Service Level Agreements (SLAs).	Inspection: Inspected management's review of the annual third-party penetration test for the Simpli.fi Demand Side Platform's production environment and if applicable, the remediation plans related to a sample of critical vulnerabilities, to determine that the Company's penetration testing was performed during the Specified Period and that a remediation plan was developed and changes were implemented to remediate each selected critical vulnerability in accordance with SLAs.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection/Inquiry: Inspected the corresponding documentation related to the annual third-party penetration test for the Bidtellect on-premise production environment to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was scheduled to be next conducted in Q4 2026, which was outside of the Specified Period. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the annual third-party penetration test for the Bidtellect on-premise production environment was last conducted in Q4 2022, which was outside of the Specified Period, and was scheduled to be conducted next in Q4 2026, which was outside of the Specified Period.	The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as the annual third-party penetration test for the Bidtellect on-premise production environment was not scheduled to be completed until Q4 2026, which was outside of the Specified Period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Observation/Inquiry: Observed the vulnerability remediation SLAs in Vanta to determine that the Company had documented timelines in place for the remediation of critical vulnerabilities. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these SLAs were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.
CC 4.2-01	The Company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's Incident Response Plan.	Inspection: Inspected the Incident Response Plan to determine that the Incident Response Plan documented requirements for the Company to log, track, resolve, and communicate security incidents to affected or relevant parties by management.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the system tickets related to a sample of security incidents to determine that each selected security incident was logged, tracked, resolved, and communicated to affected or relevant parties by management in accordance to the Company's Incident Response Plan.	No exceptions noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC 2.1-05	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. Any potential risks that are identified are logged and investigated.	Observation/Inspection/Inquiry: Observed the configuration settings of the infrastructure monitoring tool for the Simpli.fi Demand Side Platform's production environment and inspected an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the infrastructure monitoring tool was in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the corresponding documentation related to a sample of infrastructure events to determine that each selected event was logged and investigated.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 7.5-01	Backups of the production environment and related databases of the Simpli.fi Demand Side Platform are configured to be performed at least daily. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved.	Observation/Inspection/Inquiry: Observed the backup configurations for the production environment and related databases of the Simpli.fi Demand Side Platform and inspected an example alert to determine that the backups were configured to be performed at least daily and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets/corresponding documentation related to a sample of backup failure alerts received to determine that each selected backup failure alert was investigated and resolved, if applicable.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 7.5-02	Backups of the production environment and related databases of the on-premise Bidtellect production environment are configured to be performed at least daily. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved.	Observation/Inspection/Inquiry: Observed the backup configurations for the on-premise Bidtellect production environment's databases and inspected an example alert to determine that the backups were configured to be performed at least daily and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets/corresponding documentation related to a sample of backup failure alerts received to determine that each selected backup failure alert was investigated and resolved, if applicable. Inspection/Inquiry: Inspected a system generated listing of backup failure alerts during the Specified Period to determine that there were no backup failure alerts during the Specified Period. Further, inquired of the Director of Audit Risk and Compliance to determine that there were no backup failure alerts during the Specified Period.	No exceptions noted. The Service Auditor noted that this portion of the Control Activity did not operate during the Specified Period, as there were no backup failure alerts during the Specified Period. Therefore, this portion of the Control Activity could not be tested for operating effectiveness.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 7.5-03	A Business Continuity and Disaster Recovery Plan has been developed and is documented.	Inspection: Inspected the Business Continuity and Disaster Recovery Plan to determine that the Business Continuity and Disaster Recovery Plan was developed and documented.	No exceptions noted.
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC 2.1-07	The Company maintains a formal inventory of production system assets.	Observation/Inquiry: Observed the master list of system components/assets within Vanta to determine that the Company maintained a formal inventory of production system assets. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the master list of system components/assets was maintained throughout the Specified Period.	No exceptions noted.
CC 5.2-10	The Company restricts access to migrate changes to the production environment to appropriate personnel based on job function.	Inspection/Inquiry: Inspected the listing of users with access to migrate changes into the production environment and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-11	The production environment's infrastructure is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers are hardened against security threats.	Inspection: Inspected the system tickets related to a sample of infrastructure deployments for the Simpli.fi Demand Side Platform's production environment to determine that the Company had production infrastructure patched for each selected infrastructure deployment as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers were hardened against security threats.	No exceptions noted.
		Observation/Inquiry: Observed Patch Manager Plus to determine that patches for the production infrastructure were configured to be applied automatically as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that production servers were hardened against security threats. Further, inquired of the Director of Audit Risk and Compliance to determine that patches for the production infrastructure were configured to be automatically applied throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-12	The Company has a formal Secure Development Policy (SDP) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspection: Inspected the SDP methodology to determine that the Company had a formal SDP methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC 5.2-13	Prior to implementation, all changes to the Simpli.fi Demand Side Platform are tested in a development environment separate from the production environment.	Observation/Inquiry: Observed the development and production environments to determine that the development and production environments were separated. Further, inquired of the Director of Audit, Risk, and Compliance to determine that separate development and production environments were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets related to a sample of changes to the Simpli.fi Demand Side Platform to determine that each selected change was tested prior to promotion into production.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 5.2-14	All changes to the Bidders application in the on-premise production environment must be approved by a member of management prior to promotion into production.	Inspection: Inspected the system tickets related to a sample of changes to the Bidders application in the on-premise production environment to determine that each selected change was approved by a member of management prior to promotion into production.	No exceptions noted.
CC 5.2-18	Prior to implementation, all changes to the Bidders application in the on-premise production environment are tested in a staging environment separate from the production environment.	Observation/Inquiry: Observed the Bidders application's staging and production environments to determine that the staging and production environments were separated. Further, inquired of the Director of Audit, Risk, and Compliance to determine that separate staging and production environments were in place throughout the Specified Period.	No exceptions noted.
		Inspection: Inspected the system tickets related to a sample of changes to the Bidders application in the on-premise production environment to determine that each selected change was tested prior to promotion into production.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 6.1-08	Server builds leverage a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform.	Observation/Inspection/Inquiry: Observed the build process and inspected the applicable source code for server implementations to determine that server builds leveraged a "golden image" during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the Simpli.fi Demand Side Platform. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.
CC 6.1-09	Server builds leverage a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment.	Observation/Inquiry: Observed the build process to determine that server builds leveraged a defined template during infrastructure builds to provide consistency when building, implementing, and upgrading servers supporting the on-premise Bidtellect production environment. Further, inquired of the Director of Audit, Risk, and Compliance to determine that these configurations were in place throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 8.1-01	Version control software is in place to manage current versions of source code for the in-scope production environments. The ability to modify the source code of the production environments is restricted to appropriate personnel based on job function.	Observation/Inquiry: Observed the version control software to determine that the software was in place to manage the current versions of source code of the in-scope production environments. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the version control software was in place throughout the Specified Period.	No exceptions noted.
		Inspection/Inquiry: Inspected the listing of users with the ability to modify the source code of the in-scope production environments and the corresponding job titles related to a sample of those users to determine that the selected users' access was appropriate based on job function. Further, inquired of the Director of Audit, Risk, and Compliance to determine that access was appropriate based on job function for each selected user.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 8.1-02	A peer review, including a review of the Simpli.fi Demand Side Platform code for vulnerabilities, is performed on the source code change prior to migration into the production environment. Any issues identified as a result of the review must be resolved before the change is moved into the production environment.	Inspection: Inspected the change tickets related to a sample of source code changes promoted into the Simpli.fi Demand Side Platform production environment to determine that a peer review was performed on each selected source code change to detect potential vulnerabilities prior to migration into the production environment and that any issues identified as a result of the review of each selected change were resolved before each selected change was moved into the production environment.	Exceptions noted. During testing, the Service Auditor noted that for two out of the 40 sampled changes to the Simpli.fi Demand Side Platform, a peer review, including a review of the code for vulnerabilities, was not performed.
CC 8.1-03	All changes to the Simpli.fi Demand Side Platform must be approved by a member of management prior to promotion into production.	Inspection: Inspected the system tickets related to a sample of changes to the Simpli.fi Demand Side Platform to determine that each selected change was approved by a member of management prior to promotion into production.	Exceptions noted. During testing, the Service Auditor noted that two out of the 40 sampled changes to the Simpli.fi Demand Side Platform were not approved by a member of management prior to promotion into production.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 8.1-04	All infrastructure changes to the on-premise production environment (server, operating system, and databases) must be approved by a member of management prior to promotion into production.	Inspection: Inspected the system tickets related to a sample of infrastructure changes to the on-premise production environment (server, operating system, and databases) to determine that each selected change was approved by a member of management prior to promotion into production.	Exception noted. During testing, the Service Auditor noted that the Company was unable to provide a complete and accurate population of the infrastructure changes to the on-premise production environment (server, operating system, and databases). Therefore, the Service Auditor was unable to verify that all infrastructure changes to the on-premise production environment (server, operating system, and databases) were approved by a member of management prior to promotion into production.
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC 1.2-02	The Company's Board of Directors meets at least annually and maintains formal meeting minutes.	Inspection: Inspected the Annual Board Minutes and the listing of Board members to determine that the Company's Board of Directors met during the Specified Period and maintained formal meeting minutes.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.
CC 7.5-03	A Business Continuity and Disaster Recovery Plan has been developed and is documented.	Inspection: Inspected the Business Continuity and Disaster Recovery Plan to determine that the Business Continuity and Disaster Recovery Plan was developed and documented.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 9.1-01	The Company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspection: Inspected the Insurance Certificates to determine that the Company maintained cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC 1.3-01	The Company has written agreements in place with critical vendors and third parties. These agreements include security commitments applicable to that entity.	Inspection: Inspected the agreements with vendors and third parties related to a sample of new critical vendors and third parties to determine that the Company had written agreements in place with each selected new critical vendor and/or third party and that each selected agreement included security commitments applicable to that entity.	No exceptions noted.
CC 2.1-02	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspection: Inspected the Risk Management Policy to determine that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
CC 2.1-03	The Company's risk assessment is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspection: Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the Specified Period, which included the identification of threats and changes (environmental, regulatory, and technological) to service commitments and the formal assessment of the risks, and that the risk assessment included a consideration of the potential for fraud and how fraud might impact the achievement of objectives.	No exceptions noted.
CC 3.2-01	The Company has a vendor management program in place which includes the following: • critical third-party vendor inventory, • vendor's security requirements, and • review of critical third-party vendors at least annually.	Inspection: Inspected the Third-Party Risk Management Policy to determine that the Company had a documented vendor management program in place.	No exceptions noted.
		Observation/Inquiry: Observed the Company's critical vendor listing in Vanta to determine that the Company maintained an inventory of critical third-party vendors as part of the Company's vendor management program. Further, inquired of the Director of Audit, Risk, and Compliance to determine that the Company maintained an inventory of critical third-party vendors throughout the Specified Period.	No exceptions noted.

Control Activities		Tests Performed by Aprio LLP	Results of Testing
		Inspection: Inspected the annual third-party reviews related to a sample of current critical third parties and vendors to determine that the Company reviewed the security requirements of each selected vendor during the Specific Period as part of the Company's vendor management program.	No exceptions noted.

V. Other Information Provided by Simplifi Holdings, LLC

A. Management's Responses to Testing Exceptions

The information in this section is presented by the Company to provide additional information to its user entities, business partners, and other specified parties and is not part of the Company's description of its system and controls included in Section III. The information in this section has not been subjected to the procedures applied in the examination of the description of the Company's Simpli.fi Demand Side Platform and Bidtellect Platform and the suitability of design and operating effectiveness of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, and accordingly, Aprio LLP expresses no opinion on it.

Applicable Trust Services Criteria	Control Activities	Tests Performed by Aprio LLP	Results of Testing
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC 8.1-02	A peer review, including a review of the Simpli.fi Demand Side Platform code for vulnerabilities, is performed on the source code change prior to migration into the production environment. Any issues identified as a result of the review must be resolved before the change is moved into the production environment.	Inspection: Inspected the change tickets related to a sample of source code changes promoted into the Simpli.fi Demand Side Platform production environment to determine that a peer review was performed on each selected source code change to detect potential vulnerabilities prior to migration into the production environment and that any issues identified as a result of the review of each selected change were resolved before each selected change was moved into the production environment.	Exceptions noted. During testing, the Service Auditor noted that for two out of the 40 sampled changes to the Simpli.fi Demand Side Platform, a peer review, including a review of the code for vulnerabilities, was not performed.

Applicable Trust Services Criteria	Control Activities	Tests Performed by Aprio LLP	Results of Testing
CC 8.1-03	All changes to the Simpli.fi Demand Side Platform must be approved by a member of management prior to promotion into production.	Inspection: Inspected the system tickets related to a sample of changes to the Simpli.fi Demand Side Platform to determine that each selected change was approved by a member of management prior to promotion into production.	Exceptions noted. During testing, the Service Auditor noted that two out of the 40 sampled changes to the Simpli.fi Demand Side Platform were not approved by a member of management prior to promotion into production.
CC 8.1-04	All infrastructure changes to the on-premise production environment (server, operating system, and databases) must be approved by a member of management prior to promotion into production.	Inspection: Inspected the system tickets related to a sample of infrastructure changes to the on-premise production environment (server, operating system, and databases) to determine that each selected change was approved by a member of management prior to promotion into production.	Exception noted. During testing, the Service Auditor noted that the Company was unable to provide a complete and accurate population of the infrastructure changes to the on-premise production environment (server, operating system, and databases). Therefore, the Service Auditor was unable to verify that all infrastructure changes to the on-premise production environment (server, operating system, and databases) were approved by a member of management prior to promotion into production.

Management's Response to Exceptions Noted:

CC 8.1-02: Peer Review Prior to Production Migration

During testing, the Service Auditor found that for two of the 40 sampled changes to the Simpli.fi Demand Side Platform, a peer review, including a review of the code for vulnerabilities, was not performed. Management agrees with this finding. For one of these changes, two engineers provided substantive review comments prior to merge, but no formal approval was recorded. The other change was merged with no review recorded. Automated pull request approvals were not enforced on these two repositories due to conflicting release workflows, leaving peer reviews reliant on manual compliance.

Several controls lowered the risk of these changes:

- Both changes passed automated safety checks before merge, including security vulnerability scans.
- Access to migrate changes to production was restricted to appropriate personnel (CC 5.2-10).
- The ability to modify production source code was restricted (CC 8.1-01).
- Sampled DSP changes were tested before production (CC 5.2-13).
- Production access required Okta SSO with MFA (CC 5.2-07).
- Infrastructure monitoring and log management were in place (CC 2.1-05, CC 2.1-06).

No system incidents related to these changes were identified during the period. Management reviewed the two changes eliciting exceptions and confirmed they did not introduce vulnerabilities.

To fix the issue permanently, management will:

1. Enforce a branch protection rule on all in-scope DSP repositories that requires at least one approving review before changes are merged to production.
2. Grant release automation bypass permission only where a workflow requires it.
3. Put in place an automated detective control that flags any overrides of production branch protection, with each flagged change reviewed and documented by engineering management.

CC 8.1-03: Approval Prior to Production Promotion

During testing, the Service Auditor found that two of the 40 sampled changes to the Simpli.fi Demand Side Platform were not approved prior to promotion into production. Management agrees with this finding. These were the same two changes noted for CC 8.1-02. The root cause was the same as for CC 8.1-02: approval was not enforced by the system on the affected repositories due to release workflows that were considered incompatible with approval-based branch protection.

Applicable Trust Services Criteria	Control Activities	Tests Performed by Aprio LLP	Results of Testing

The mitigating controls described for CC 8.1-02 also applied to these changes, including automated security scanning, restricted production migration access (CC 5.2-10), restricted source code modification (CC 8.1-01), and MFA-protected production access (CC 5.2-07). To fix the issue permanently, management will implement the additional measures noted in the management response for CC 8.1-02.

CC 8.1-04: Approval of On-Premise Infrastructure Changes

During testing, the Service Auditor found that the Company was unable to provide a complete and accurate population of infrastructure changes to the on-premise production environment (server, operating system, and databases). As a result, the Service Auditor was unable to verify that these changes were approved by an authorized reviewer prior to promotion into production. Management agrees with this finding. The root cause was that on-premise infrastructure changes were recorded across several separate systems, some of which had limited log retention during the period. No single, system-generated list of changes covering the full period could be produced.

Several controls that operated effectively during the period lowered the risk:

- Administrative access to the on-premise environment was restricted to appropriate personnel (CC 5.2-15, CC 5.2-16).
- Direct access required VPN and MFA (CC 5.2-17).
- Server builds followed a defined template (CC 6.1-09).
- Patching was automated (CC 5.2-11).
- Infrastructure monitoring was in place for the on-premise environment (CC 2.1-05).

To fix the issue permanently, management will:

1. Require every on-premise infrastructure change to be recorded in the organization’s ticketing system (Jira) as the single system of record, with documented approval from an authorized reviewer before implementation.
2. Increase log retention on change sources to at least 13 months.
3. Perform a quarterly reconciliation of system-detected changes (for example, vCenter events and configuration diffs) against approved tickets, so the population can be shown to be complete.


Aprio