



SOC 2 Type 2 Report

Draftspotting Technologies Private Limited

July 20, 2022 to January 17, 2023

Next Report Issue Date: February 20, 2024

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security,
Confidentiality, and Availability



AUDIT AND ATTESTATION BY



AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

The next report would be issued on February 20, 2024 subject to observation and examination by Prescient Assurance.

Table of Contents

Management's Assertion	6
Independent Service Auditor's Report	9
Scope	9
Service Organization's Responsibilities	9
Service Auditor's Responsibilities	10
Inherent Limitations	10
Opinion	11
Restricted Use	11
System Description	13
DC 1: Company Overview and Types of Products and Services Provided	14
DC 2: Principal Service Commitments and System Requirements	15
DC 3: The Components of the System Used to Provide the Services	17
3.1 Primary Infrastructure	17
3.2 Primary Software	17
3.3 People	19
3.4 Data	19
3.5 Procedures and Policies	21
DC 4: Disclosures about Identified Security Incidents	22
DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements Were Achieved	23
5.1 Integrity and Ethical Values	23
5.2 Commitment to Competence	24
5.3 Senior Management Oversight	24
5.4 Organizational Structure and Assignment of Authority and Responsibility	24
5.5 Risk Assessment	25
5.6 Integration with Risk Assessment	27
5.7 Physical Access and Environmental Controls	27
5.8 Incident Management	28
5.9 Change Management	29
5.10 Information and Communication	30
5.11 Monitoring Controls	31
DC 6: Complementary User Entity Controls	32
DC 7: Complementary Subservice Organization Controls	33
DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant	34
DC 9: Disclosures of Significant Changes In Last 1 Year	35

Testing Matrices	36
Tests of Operating Effectiveness and Results of Tests	37
Scope of Testing	37
Types of Tests Generally Performed	37
General Sampling Methodology	38
Reliability of Information Provided by the Service Organization	39
Test Results	39

SECTION 1

Management's Assertion



SPOTDRAFT

Management's Assertion


We have prepared the accompanying description of SpotDraft's system throughout the period July 20, 2022 to January 17, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about SpotDraft's system that may be useful when assessing the risks arising from interactions with SpotDraft's system, particularly information about system controls that SpotDraft 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, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

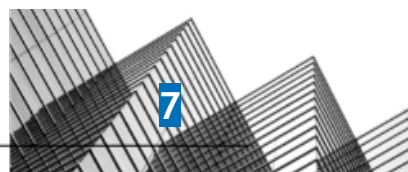
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at SpotDraft, to achieve SpotDraft's service commitments and system requirements based on the applicable trust services criteria. The description presents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

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

- a. The description presents SpotDraft's system that was designed and implemented throughout the period July 20, 2022 to January 17, 2023 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period July 20, 2022 to January 17, 2023, to provide reasonable assurance that SpotDraft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of SpotDraft's controls during that period.
- c. The controls stated in the description operated effectively throughout the period July 20, 2022, to January 17, 2023, to provide reasonable assurance that SpotDraft's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of SpotDraft's controls operated effectively throughout the period.

DocuSigned by:

-----607Q17378F1D4BB-----

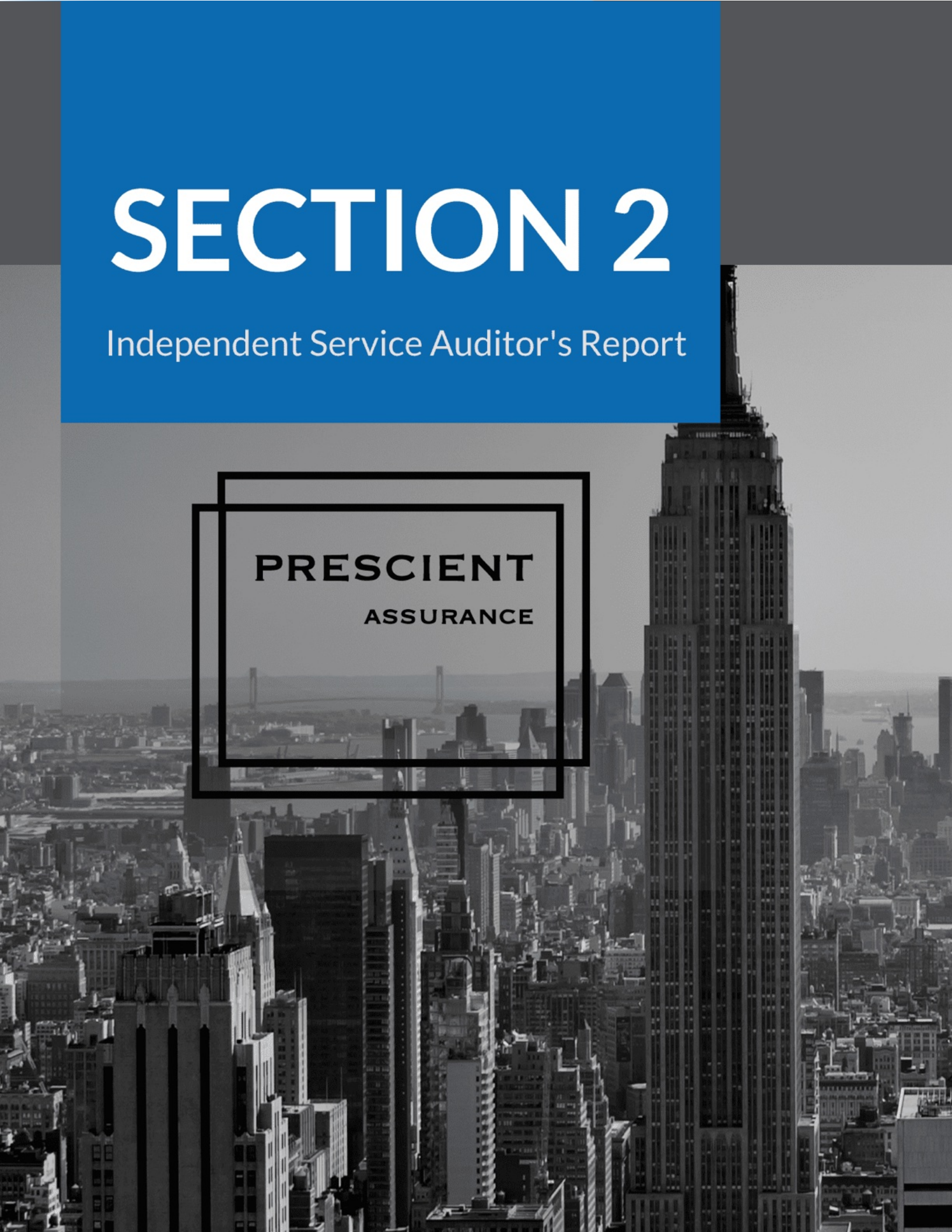
Rohith Salim
Chief Product Officer
Draftspotting Technologies Private Limited



SECTION 2

Independent Service Auditor's Report

PRESCIENT
ASSURANCE



Independent Service Auditor's Report

To: Draftspotting Technologies Private Limited

Scope

We have examined Draftspotting Technologies Private Limited's ("SpotDraft") accompanying description of its SpotDraft system found in Section 3, titled SpotDraft System Description throughout the period July 20, 2022, to January 17, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 20, 2022, to January 17, 2023, to provide reasonable assurance that SpotDraft's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

Service Organization's Responsibilities

SpotDraft 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 SpotDraft's service commitments and system requirements were achieved. In Section 1, SpotDraft has provided the accompanying assertion titled "Management's Assertion of SpotDraft" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. SpotDraft 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 AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects:

- a. The description presents SpotDraft's system that was designed and implemented throughout the period July 20, 2022, to January 17, 2023, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period July 20, 2022, to January 17, 2023, to provide reasonable assurance that SpotDraft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of SpotDraft's controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period July 20, 2022, to January 17, 2023, to provide reasonable assurance that SpotDraft'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 SpotDraft's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of SpotDraft, user entities of SpotDraft's system during some or all of the period July 20, 2022 to January 17, 2023, business partners of SpotDraft 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 of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. 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.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

Prescient Assurance LLC

DocuSigned by:
John D Wallace
-----F5ADF3569EA450-----

John D. Wallace, CPA
Chattanooga, TN
February 20, 2023

SECTION 3

System Description



DC 1: Company Overview and Types of Products and Services Provided

SpotDraft is a cloud-hosted software application built by DraftSpotting Technologies Pvt Ltd's ("DraftSpotting").

SpotDraft is an end-to-end contract lifecycle management & automation platform that helps in-house legal teams process contracts faster & more efficiently. SpotDraft has customers from 15+ countries around the world and has processed 1M+ contracts on the platform.

SpotDraft's aim is to eliminate repetitive, mundane work and automate high volume business contracts.

Any other services provided by DraftSpotting are not in the scope of this report.

DC 2: Principal Service Commitments and System Requirements

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

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- The fundamental design of DraftSpotting's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role;
- DraftSpotting implements various procedures and processes to control access to the production environment and the supporting infrastructure;
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics;
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

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

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between DraftSpotting and user entities.

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

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in DraftSpotting'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. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies,

Standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

DC 3: The Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures

3.1 Primary Infrastructure

The SpotDraft is hosted in Google Cloud Platform (GCP) in their US, Europe and India region. SpotDraft software application uses a virtual and secure network environment on top of GCP infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. SpotDraft software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through an GCP Internet Gateway, over to a virtual private cloud that:

- Houses the entire application runtime
- Protects the application runtime from any external networks

The internal networks of GCP are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

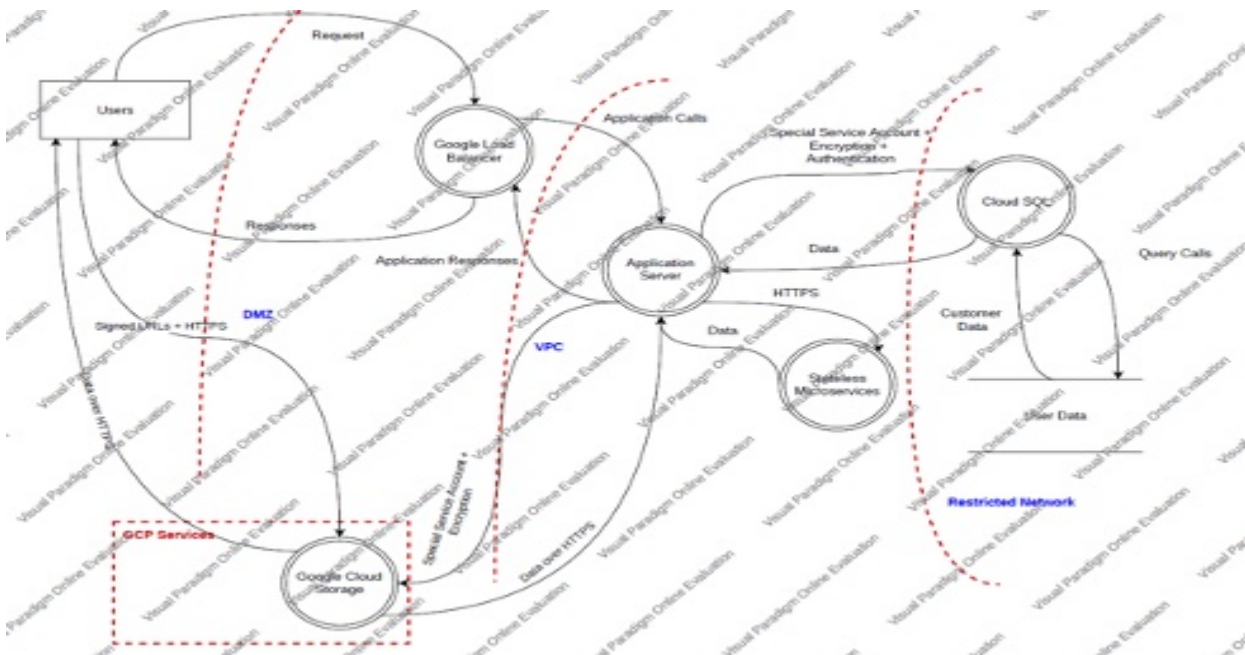
3.2 Primary Software

DraftSpotting is responsible for managing the development and operation of the SpotDraft platform including infrastructure components such as servers, databases, and storage systems. The in-scope SpotDraft infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	Business Function / Description	OS DB	Physical Location
SpotDraft Main Web App	SpotDraft's aim is to eliminate repetitive, mundane work and automate high volume business contracts. Access to the SpotDraft SaaS application is through a web interface and user authentication.	PostgreSQL (Google Cloud SQL)	GCP europe-west4 GCP asia-south1 GCP us-east4

Primary Infrastructure and Software			
System / Application	Business Function / Description	OS DB	Physical Location
GCP IAM	Identity and access management console for AWS resources.	Google Proprietary	GCP
GCP Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	Google Proprietary	GCP
Github	Source code repository, version control system, and build software.	Github	Github Cloud
Google Workspace	Identity/Email provider for all DraftSpotting employees	Google Proprietary	GCP(Gmail)

Network Architecture Diagram



3.3 People

DraftSpotting's staff have been organized into various functions like Sales, Support, Engineering, Product Management etc. The personnel have also been assigned the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, vulnerabilities, and adding controls to mitigate this risk. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

3.4 Data

Data, as defined by DraftSpotting, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Output reports are available and include data and files systematically generated from the system. The availability of these reports is limited by job function. Reports delivered externally are only sent using a secure method—encrypted email, secure FTP, or secure websites to customer users.

All data that is managed, processed and stored as a part of the SpotDraft software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	<ul style="list-style-type: none">• Customer system and operating data• Customer PII• Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally, or was entrusted to DraftSpotting by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	<ul style="list-style-type: none">• DraftSpotting's PII• Unpublished financial information• Documents and processes explicitly marked as confidential• Unpublished goals, forecasts, and initiatives marked as confidential• Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	<ul style="list-style-type: none">• Press releases• Public website

Customer data is retained per agreements with customers and disposed of upon request by customers. A confirmation is sent back to the customer to notify them that the disposal is complete.

3.5 Procedures and Policies

Formal policies and procedures have been established to support the SpotDraft software application. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

DraftSpotting also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the SpotDraft software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

DC 4: Disclosures about Identified Security Incidents

There were no system incidents as of August 27th, 2022, requiring disclosure that either:

- Were the result of controls failing; or,
- Resulted in a significant impairment to the achievement of system requirements or service commitments to customers.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements Were Achieved

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of DraftSpotting's description of the system. This section provides information about the five interrelated components of internal control at DraftSpotting, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

Control Environment

5.1 Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of DraftSpotting's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of DraftSpotting's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

DraftSpotting and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

5.2 Commitment to Competence

DraftSpotting's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

5.3 Senior Management Oversight

DraftSpotting's control awareness is significantly influenced by its senior management. Attributes that define "tone at the top" include senior management's experience of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company's operations and information security posture.

Management Philosophy and Operating Style

DraftSpotting's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information. DraftSpotting's control environment reflects the philosophy of management. DraftSpotting's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities DraftSpotting has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high severity security incidents annually.
- Senior management meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap.

5.4 Organizational Structure and Assignment of Authority and Responsibility

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

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

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and updated as required.

Human Resources

DraftSpotting's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top quality personnel who ensure the service organization is operating at maximum efficiency.

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

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

5.5 Risk Assessment

DraftSpotting regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the applicable trust services criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

DraftSpotting's risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. DraftSpotting identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the SpotDraft software application, and management has implemented various measures designed to manage these risks.

- DraftSpotting believes that effective risk management is based on the following principles:
- Senior management's commitment to the security of SpotDraft software application
- The involvement, cooperation, and insight of all DraftSpotting staff
- Initiating risk assessments with discovery and identification of risks
- Thorough analysis of identified risks
- Commitment to the strategy and treatment of identified risks
- Communicating all identified risks to the senior management
- Encouraging all DraftSpotting staff to report risks and threat vectors

Scope

The risk assessment and management program apply to all systems and data that are a part of the SpotDraft software application. The DraftSpotting risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of DraftSpotting's Information Security Officer and the department or individuals responsible for the area being assessed. All DraftSpotting staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

DraftSpotting uses a number of vendors to meet its business objectives. DraftSpotting understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

DraftSpotting employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, DraftSpotting assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support DraftSpotting's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, DraftSpotting management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

5.6 Integration with Risk Assessment

As part of the design and operation of the system, DraftSpotting identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. DraftSpotting's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity and mitigating action.

Control Activities

DraftSpotting's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

The SpotDraft software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

DraftSpotting has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

Administrator access to the production console is restricted to authorized system and security administrators. Powerful service/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.

Staff members must use complex passwords, wherever possible, for all of their accounts that have access to DraftSpotting customer data. Staff are encouraged to use passwords which have at least 10 characters, randomly generated, alphanumeric and special-character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems requires multi-factor authentication (MFA). Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

5.7 Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted by GCP. As such, GCP is responsible for the physical security controls of the in-scope system. DraftSpotting reviews the SOC 2 report provided by

GCP on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the DraftSpotting software application.

5.8 Incident Management

DraftSpotting has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact DraftSpotting via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of DraftSpotting being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.
- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between virtual private cloud (VPC) environments to help ensure only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from the security utilities are reviewed by DraftSpotting management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

DraftSpotting only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to DraftSpotting's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to DraftSpotting web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit.

5.9 Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the DraftSpotting are reviewed, deployed, and managed. The policy covers all changes made to the SpotDraft software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the SpotDraft software application can be initiated by a staff member with an appropriate role. DraftSpotting uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Customer content and personal information are not used in non-production environments.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented

inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. DraftSpotting uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

System Hardening, Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

- Email attachments entering the organization's email gateway are scanned for viruses; and,
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Availability

DraftSpotting has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

5.10 Information and Communication

DraftSpotting maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, DraftSpotting also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Information about the system and services are maintained and made available to users on the company website.

5.11 Monitoring Controls

DraftSpotting's management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.



DC 6: Complementary User Entity Controls

DraftSpotting's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for DraftSpotting customers.

For customers to rely on the information processed through the SpotDraft's software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for managing their organization's SpotDraft's software application account as well as establishing any customized security solutions or automated processes through the use of setup features
- User entities are responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the SpotDraft's software application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the SpotDraft's software application.
- User entity is responsible for removing terminated employee access to the SpotDraft's software application.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the SpotDraft's software application.
- User entity is responsible for sending data to SpotDraft's software application via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying SpotDraft's software application if they detect or suspect a security incident related to the DraftSpotting.
- User entity is responsible for reviewing email and other forms of communications from DraftSpotting, related to changes that may affect DraftSpotting customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.
- User entity is responsible for developing their own business continuity and disaster recovery plan

DC 7: Complementary Subservice Organization Controls

DraftSpotting uses subservice organizations in support of its system. DraftSpotting's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the user entities to be achieved solely by DraftSpotting. Therefore, user entity controls must be evaluated in conjunction with DraftSpotting'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 organization as described below.

DraftSpotting periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Applicable Criteria	Subservice Organization	Control Activity Expected to be Implemented by Subservice Organization
CC6.1, CC6.2, CC6.3, CC6.5, CC7.2	GCP	Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.
CC6.4, CC6.5	GCP	Physical access to the data center facility is restricted to authorized personnel.
CC6.4, A1.2	GCP	Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.
A1.3	GCP	Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.
A1.2	GCP	Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.
C1.1	GCP	A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.
C1.2	GCP	A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

The system services are measured for Security, Availability, and Confidentiality. None of the criteria of the applicable trust services are irrelevant.

DC 9: Disclosures of Significant Changes In Last 1 Year

Not applicable given that this is the first SOC 2 Type 2.



SECTION 4

Testing Matrices

PRESCIENT
ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to SpotDraft provided by Draftspotting Technologies Private Limited. The scope of the testing was restricted to SpotDraft, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period July 20, 2022 to January 17, 2023.

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: <ul style="list-style-type: none">• Examination / Inspection of source documentation and authorizations to verify transactions processed.• Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.• Examination / Inspection of systems documentation, configurations, and settings; and• Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.

Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2

Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices.

Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity.

Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	Criteria	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Entity establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet	Inspected the Code of Business Conduct, which outlines the expectations regarding employee behavior, to determine that the entity establishes behavioral standards defined in the Code of Business Conduct and makes them available to all staff members on the company intranet. Observed through Sprinto that all policies are available and accessible for all employees.	No exceptions noted.
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Entity requires that new employees review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	Inspected the Code of Business Conduct to determine that the company's staff is expected to follow the Code of Business Conduct in all matters pertaining to their work. Inspected the System Description to determine that the new employees are required to acknowledge company policy upon hire and annually thereafter. Observed the new hire policy acknowledgement logs within Sprinto to determine that all in-scope new hires during the observation period have accepted policies within the SLA as part of onboarding.	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.	Entity's Senior Management reviews and approves all company policies annually.	Observed through Sprinto that the company's policies have been approved and reviewed on August 2, 2022, to determine that the entity's senior management reviews and approves all the policies annually.	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.	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the management meeting minutes dated July 26, 2022, which define the agenda of a review of the annual risk assessment, vendor risk management procedures, information security controls, and administrator access to critical systems by senior	No exceptions noted.

			management of staff members to determine that Senior Management reviews and approves the state of the Information Security program annually.	
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Observed through Sprinto that organizational structure has been reviewed on August 18, 2022, to determine that senior management reviews and approves the organizational chart for all employees annually.	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.	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the management meeting minutes dated July 26, 2022, which document the review of the annual risk assessment to determine that senior management reviews and approves the risk assessment report annually.	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.	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the management meeting minutes dated July 26, 2022, which document a review of the vendor management procedures to determine that senior management reviews and approves the "Vendor Risk Assessment Report" annually. Inspected the System Description to determine that senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high-severity security incidents annually.	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.	Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities	Observed through Sprinto which lists all employees, their assigned roles, and managers, to determine that the entity has documented its organizational structure.	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.	Entity ensures clarity in job responsibilities for client serving, IT and engineering positions (via OKRs, Job Descriptions etc.) to increase the operational effectiveness of the organization	Observed through Sprinto which shows the job description of Account Executive, Account Manager, Associate Director of Engineering, and others to determine that the company maintains job description to increase the operational effectiveness of employees within the organization.	No exceptions noted.

CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Entity ensures that new hires have been duly evaluated for competence in their expected job responsibilities.	<p>Observed the screenshot of the hiring evaluation report to determine that newly hired employees are evaluated for their technical expertise, skills, and self-learning ability.</p> <p>Observed screenshots of the hiring evaluations for 5 sampled new hires to determine that the company evaluates new hires to ensure competence in job responsibilities.</p>	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Entity ensures that new hires go through a background check as part of their onboarding process	<p>Inspected a sample of employee background verification reports available on Sprinto to determine that the company conducts background checks for new hires.</p> <p>Observed the background check logs from Sprinto to determine that the company has completed background checks for all in-scope full-time employees.</p>	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Entity has established an Information Security Awareness training, and its contents are available for all staff on the company intranet.	<p>Inspected the Information Security Awareness training presentation by Infosec Training, distributed to employees through the Sprinto platform to determine that the entity has established an Information Security Awareness training program, and its contents are available for all staff on the company intranet.</p> <p>Inspected the System Description to determine that annual security awareness training is provided to all staff and focuses on maintaining the security of the proprietary and customer-servicing systems and related data.</p>	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually	<p>Observed the new hire infosec training logs and periodic infosec training logs exported through Sprinto to determine that all of the new employees have completed the information security awareness training.</p> <p>Inspected the Information Security</p>	No exceptions noted.

			Policy to determine that all staff are expected to complete information security training within 30 days of joining the company and annually thereafter.	
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their Job responsibilities	Observed an employee peer feedback form sample to determine that the company is required to perform performance evaluations. Observed 2 completed samples of employee feedback forms to determine that the company evaluates employees regarding their job responsibilities.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Entity requires that all staff members review and acknowledge company policies annually	Inspected the system description to determine that new employees are required to acknowledge the company's policies upon hire and annually thereafter. Observed the periodic policy acknowledgement logs within Sprinto to determine that all in-scope active personnel have accepted policies as part of the annual acknowledgement.	No exceptions noted.
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Inspected the production infrastructure monitoring data exported through Sprinto, which shows various monitoring alerts enabled on the infrastructural assets, including GCP Cloud SQL CPU utilization monitoring to determine that systems generate information that is reviewed and evaluated to determine the impacts on the functioning of internal controls.	No exceptions noted.
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Entity makes all policies and procedures available to all staff members via the company intranet	Observed that all the information security policies are available to the staff through the Sprinto platform. Inspected the system description to determine that all policies are required to be available to all staff members via Sprinto.	No exceptions noted.
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information	Entity displays the most current information about its services on its website, which is accessible to its customers.	Observed the company's website (https://www.spotdraft.com/) to determine that the description of the most current products and solutions is	No exceptions noted.

	to support the functioning of internal control.		provided to customers through the website.	
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.	Entity establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet	<p>Inspected the Code of Business Conduct, which outlines the expectations regarding employee behavior, to determine that the entity establishes behavioral standards defined in the Code of Business Conduct and makes them available to all staff members on the company intranet.</p> <p>Observed through Sprinto that all policies are available and accessible for all employees.</p>	No exceptions noted.
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.	Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually	<p>Observed the new hire infosec training logs and periodic infosec training logs exported through Sprinto to determine that all of the new employees have completed the information security awareness training.</p> <p>Inspected the Information Security Policy to determine that all staff are expected to complete information security training within 30 days of joining the company and annually thereafter.</p>	No exceptions noted.
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.	Entity requires that all staff members review and acknowledge company policies annually	<p>Inspected the system description to determine that new employees are required to acknowledge the company's policies upon hire and annually thereafter.</p> <p>Observed the periodic policy acknowledgement logs within Sprinto to determine that all in-scope active personnel have accepted policies as part of the annual acknowledgement.</p>	No exceptions noted.
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.	Entity makes all policies and procedures available to all staff members via the company intranet	<p>Observed that all the information security policies are available to the staff through the Sprinto platform.</p> <p>Inspected the system description to determine that all policies are required to be available to all staff members via Sprinto.</p>	No exceptions noted.

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.	Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the Information Security Policy to determine that staff members are required to report issues, or other complaints directly to their manager/supervisor, or to the Information Security Officer or CEO if the manager is not immediately available.	No exceptions noted.
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.	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	<p>Inspected the system description to determine that all employees are required to acknowledge their understanding of policies upon hire.</p> <p>Observed the new hire policy acknowledgement logs within Sprinto to determine that all in-scope new hires during the observation period have accepted policies within the SLA as part of onboarding.</p>	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Entity displays the most current information about its services on its website, which is accessible to its customers.	Observed the company's website (https://www.spotdraft.com/) to determine that the description of the most current products and solutions is provided to customers through the website.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	<p>Observed the contact page (https://www.spotdraft.com/requestfor-demo) to determine that the company has provided a form that users can use to report issues.</p> <p>Inspected the Privacy Policy (https://www.spotdraft.com/privacy) to determine that the company has provided an email (romit@spotdraft.com) where users can report privacy-related issues.</p>	No exceptions noted.
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Entity has formally documented policies and procedures to govern risk management.	Inspected the Risk Management Policy to determine that the risk assessment procedures and mitigation strategies for identified risks have been documented.	No exceptions noted.
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management	Inspected the periodic risk assessment data exported through Sprinto, which shows the results of a recent risk assessment, including a list of risks,	No exceptions noted.

	identification and assessment of risks relating to objectives.	Policy, to identify threats that could impair systems' security commitments and requirements	their mitigation checks, impact score, likelihood, residual risk, and risk treatment decision, to determine that the company performs risk assessments at least annually.	
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.	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	Inspected the periodic risk assessment data exported through Sprinto, which shows the results of a recent risk assessment, including a list of risks, their mitigation checks, impact score, likelihood, residual risk, and risk treatment decision, to determine that the company performs risk assessments at least annually.	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.	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment data exported through Sprinto, showing the results of a recent risk assessment, including an impact score and likelihood for each identified risk to determine that the company assesses the impact and likelihood of risks as part of the risk assessment process. Inspected the Risk Assessment and Management Policy to determine that a mechanism for quantifying risk impact using a relative measure on a scale of 0 to 10 and mitigation strategies for identified risks have been defined.	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.	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	Inspected the system description to determine that all employees are required to acknowledge their understanding of policies upon hire. Observed the new hire policy acknowledgement logs within Sprinto to determine that all in-scope new hires during the observation period have accepted policies within the SLA as part of onboarding.	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	Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are	Inspected the vendor risk assessment report which shows the company's vendors, their categories, internal owners, risk levels, and remediation measures to determine that the entity performs a formal vendor risk	No exceptions noted.

	determining how the risks should be managed.	critical to the systems' security commitments and requirements	assessment exercise annually.	
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Inspected the risk assessment data exported through Sprinto which shows the results of a recent risk assessment, including entries for fraud risks, to determine that the entity evaluates the potential for fraud when assessing risks.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	Inspected the periodic risk assessment data exported through Sprinto, which shows the results of a recent risk assessment, including a list of risks, their mitigation checks, impact score, likelihood, residual risk, and risk treatment decision, to determine that the company performs risk assessments at least annually.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment data exported through Sprinto, showing the results of a recent risk assessment, including an impact score and likelihood for each identified risk to determine that the company assesses the impact and likelihood of risks as part of the risk assessment process. Inspected the Risk Assessment and Management Policy to determine that a mechanism for quantifying risk impact using a relative measure on a scale of 0 to 10 and mitigation strategies for identified risks have been defined.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements	Inspected the vendor risk assessment report which shows the company's vendors, their categories, internal owners, risk levels, and remediation measures to determine that the entity performs a formal vendor risk assessment exercise annually.	No exceptions noted.
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the	Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning,	Observed through Sprinto that the company has designated a Chief Technology Officer with the responsibility for planning, assessing,	No exceptions noted.

	components of internal control are present and functioning.	assessing, implementing and reviewing the internal control environment.	implementing, and reviewing the internal control environment.	
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.	Entity appoints an owner of Infrastructure, who is responsible for all assets in the inventory	Observed through Sprinto that the company has assigned an owner for infrastructure operations to determine that all assets in the inventory are managed by the infrastructure owner.	No exceptions noted.
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.	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the results of an internal audit assessment which includes information about owners, controls, and performance of controls to determine that the entity uses Sprinto to continuously monitor, track, and report the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
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.	Entity's Senior Management reviews and approves all company policies annually.	Observed through Sprinto that the company's policies have been approved and reviewed on August 2, 2022, to determine that the entity's senior management reviews and approves all the policies annually.	No exceptions noted.
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.	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the management meeting minutes dated July 26, 2022, which define the agenda of a review of the annual risk assessment, vendor risk management procedures, information security controls, and administrator access to critical systems by senior management of staff members to determine that Senior Management reviews and approves the state of the Information Security program annually.	No exceptions noted.
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.	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Observed through Sprinto that organizational structure has been reviewed on August 18, 2022, to determine that senior management reviews and approves the organizational chart for all employees annually.	No exceptions noted.

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.	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the management meeting minutes dated July 26, 2022, which document the review of the annual risk assessment to determine that senior management reviews and approves the risk assessment report annually.	No exceptions noted.
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.	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	<p>Inspected the management meeting minutes dated July 26, 2022, which document a review of the vendor management procedures to determine that senior management reviews and approves the "Vendor Risk Assessment Report" annually.</p> <p>Inspected the System Description to determine that senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high-severity security incidents annually.</p>	No exceptions noted.
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.	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met	Inspected the Vendor Risk Assessment report consisting of the assessment details of vendors including the criticality of the risk to the company's business and the recommended approach to mitigate that risk to determine that the entity reviews and evaluates all sub-service organizations periodically.	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.	Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the Information Security Policy to determine that staff members are required to report issues, or other complaints directly to their manager/supervisor, or to the Information Security Officer or CEO if the manager is not immediately available.	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	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the results of an internal audit assessment which includes information about owners, controls, and performance of controls to determine that the entity uses Sprinto to continuously monitor, track, and report the health of the information security	No exceptions noted.

	board of directors, as appropriate.		program to the Information Security Officer and other stakeholders.	
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.	Entity's Senior Management reviews and approves all company policies annually.	Observed through Sprinto that the company's policies have been approved and reviewed on August 2, 2022, to determine that the entity's senior management reviews and approves all the policies annually.	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.	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the management meeting minutes dated July 26, 2022, which define the agenda of a review of the annual risk assessment, vendor risk management procedures, information security controls, and administrator access to critical systems by senior management of staff members to determine that Senior Management reviews and approves the state of the Information Security program annually.	No exceptions noted.
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.	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the Information Security Policy, which summarizes the requirements for information security training, incident management, vulnerability management, data classification, backup, retention, encryption, and physical security to determine that the entity has developed a set of policies that establish expected behavior with regard to the control environment.	No exceptions noted.
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.	Entity has a documented Acceptable Usage Policy, and makes it available for all staff on the company intranet	Inspected the Acceptable Usage Policy to determine that the company has a policy in place stating the secure and acceptable use of the information assets.	No exceptions noted.
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.	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers	Inspected the organizational structure of the company which lists all the employees, their assigned roles, and managers to determine that responsibilities and duties are segregated across the organization to mitigate risks to the services provided to customers.	No exceptions noted.

CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the results of an internal audit assessment which includes information about owners, controls, and performance of controls to determine that the entity uses Sprinto to continuously monitor, track, and report the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity's Senior Management reviews and approves all company policies annually.	Observed through Sprinto that the company's policies have been approved and reviewed on August 2, 2022, to determine that the entity's senior management reviews and approves all the policies annually.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the management meeting minutes dated July 26, 2022, which define the agenda of a review of the annual risk assessment, vendor risk management procedures, information security controls, and administrator access to critical systems by senior management of staff members to determine that Senior Management reviews and approves the state of the Information Security program annually.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Observed through Sprinto that organizational structure has been reviewed on August 18, 2022, to determine that senior management reviews and approves the organizational chart for all employees annually.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the management meeting minutes dated July 26, 2022, which document the review of the annual risk assessment to determine that senior management reviews and approves the risk assessment report annually.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity's Infosec officer reviews and approves the list of people with access to production console annually	Inspected the User Access Reviews for Critical Systems exported through Sprinto, which shows that access privileges for GCP, GitHub, and G Suite accounts are tracked by the ISO to determine that the Infosec Officer reviews and approves the list of people with access to the production console annually.	No exceptions noted.

CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	<p>Inspected the management meeting minutes dated July 26, 2022, which document a review of the vendor management procedures to determine that senior management reviews and approves the "Vendor Risk Assessment Report" annually.</p> <p>Inspected the System Description to determine that senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high-severity security incidents annually.</p>	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met	Inspected the Vendor Risk Assessment report consisting of the assessment details of vendors including the criticality of the risk to the company's business and the recommended approach to mitigate that risk to determine that the entity reviews and evaluates all sub-service organizations periodically.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the Information Security Policy, which summarizes the requirements for information security training, incident management, vulnerability management, data classification, backup, retention, encryption, and physical security to determine that the entity has developed a set of policies that establish expected behavior with regard to the control environment.	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.	Entity makes all policies and procedures available to all staff members via the company intranet	<p>Observed that all the information security policies are available to the staff through the Sprinto platform.</p> <p>Inspected the system description to determine that all policies are required to be available to all staff members via Sprinto.</p>	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in	Entity requires that all staff members review and acknowledge company policies annually	Inspected the system description to determine that new employees are required to acknowledge the company's policies upon hire and annually thereafter.	No exceptions noted.

	procedures that put policies into action.		Observed the periodic policy acknowledgement logs within Sprinto to determine that all in-scope active personnel have accepted policies as part of the annual acknowledgement.	
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.	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	<p>Inspected the system description to determine that all employees are required to acknowledge their understanding of policies upon hire.</p> <p>Observed the new hire policy acknowledgement logs within Sprinto to determine that all in-scope new hires during the observation period have accepted policies within the SLA as part of onboarding.</p>	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.	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the Information Security Policy, which summarizes the requirements for information security training, incident management, vulnerability management, data classification, backup, retention, encryption, and physical security to determine that the entity has developed a set of policies that establish expected behavior with regard to the control environment.	No exceptions noted.
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.	Entity has developed an Access Control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	Inspected the Access Control Policy to determine that the procedures for granting access to users based on the principle of least privilege have been documented.	No exceptions noted.
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.	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.	<p>Inspected the Role-Based System Access Matrix which lists staff roles and their access privileges to G Suite, GitHub, and GCP to determine that the entity maintains a matrix that outlines the access rights of staff members.</p> <p>Inspected the Access Control Policy to determine that access to the systems is to be granted on a need basis, dependent on the roles and responsibilities of the staff member.</p>	No exceptions noted.

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.	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed	Observed the user access reviews of GCP, GSuite, and GitHub user accounts through Sprinto to determine that the company uses Sprinto to continuously monitor the access privileges of the employees, and alerts are sent to the Director of IT to update the access levels.	No exceptions noted.
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.	Entity's Senior Management or the Information Security Officer periodically reviews and approves the list of people with access to the entity's system	Inspected the user access reviews for critical systems through Sprinto to determine that access privileges for GCP, GSuite, and GitHub user accounts are tracked by the Senior Management.	No exceptions noted.
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.	Entity's Senior Management or the Information Security Officer periodically reviews and approves the list of people with Administrative access to the entity's system	Inspected the user access reviews for critical systems through Sprinto to determine that access privileges for GCP, GSuite, and GitHub user accounts are tracked by the Senior Management.	No exceptions noted.
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.	Entity has developed an Access Control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	Inspected the Access Control Policy to determine that the procedures for granting access to users based on the principle of least privilege have been documented.	No exceptions noted.
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.	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.	<p>Inspected the Role-Based System Access Matrix which lists staff roles and their access privileges to G Suite, GitHub, and GCP to determine that the entity maintains a matrix that outlines the access rights of staff members.</p> <p>Inspected the Access Control Policy to determine that access to the systems is to be granted on a need basis, dependent on the roles and responsibilities of the staff member.</p>	No exceptions noted.

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.	Staff access to Entity's systems are made inaccessible in a timely manner as a part of the offboarding process.	Observed a list of employees and contractors who have been offboarded and their associated accounts have been deactivated to determine that the company revokes staff access to the systems as part of the offboarding process. Interviewed the company to determine that they Need to keep several account IDs active due to business reasons.	No exceptions noted.
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.	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Inspected the Role-Based System Access Matrix which lists staff roles and their access privileges to G Suite, GitHub, and GCP to determine that the entity maintains a matrix that outlines the access rights of staff members. Inspected the Access Control Policy to determine that access to the systems is to be granted on a need basis, dependent on the roles and responsibilities of the staff member.	No exceptions noted.
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.	Staff access to Entity's systems are made inaccessible in a timely manner as a part of the offboarding process.	Observed a list of employees and contractors who have been offboarded and their associated accounts have been deactivated to determine that the company revokes staff access to the systems as part of the offboarding process. Interviewed the company to determine that they Need to keep several account IDs active due to business reasons.	No exceptions noted.
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.	Entity ensures that access to the Infrastructure provider's environment (production console) is restricted to only those individuals who require such access to perform their job functions	Observed a list of GCP users with their access levels based on roles in the GCP console to determine that the entity restricts privileged access to the GCP console to users who require such access to perform their jobs. Inspected the system description to determine that the company restricts administrator access to the production console to the authorized system and security administrators.	No exceptions noted.

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.	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Observed a list of GCP users with their access levels based on roles in the GCP console to determine that the entity restricts privileged access to the GCP production databases to users who require such access to perform their jobs. Inspected the system description to determine that the company restricts administrator access to the production console to the authorized system and security administrators.	No exceptions noted.
CC6.4	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.	Entity relies on an infrastructure provider for hosting the systems supporting its production environment. As a result there is no physical access available to its staff members	Observed through Sprinto that the entity uses GCP as its infrastructure provider, due to which physical access is not available to its staff members.	No exceptions noted.
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.	Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.	Inspected the Media Disposal Policy to determine that the steps to permanently dispose of the company's media are described stating that the company is required to use the recommended disposal methods for critical and sensitive data.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multi Factor-authentication	Observed through Sprinto that all users of GCP, GitHub, and Google Workspace have MFA protection enabled on the console to determine that MFA is enabled on critical systems.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity requires that all endpoints with access to production systems are protected by malware-protection software	Interviewed the company to determine that Falcon software is used as an antivirus. Observed an output report from Falcon to determine that endpoints are protected with Falcon antivirus.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access	Observed the list of staff devices and their encryption status through Sprinto to determine that all of the	No exceptions noted.

	sources outside its system boundaries.		company-owned devices have hard drive encryption enabled. Observed a screenshot of a recently hired employee's device settings to determine that disk encryption is enabled.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Observed the list of staff devices and their OS auto update status through Sprinto to determine that all of the company-owned devices have auto updates enabled. Observed screenshots of 10 sample employee computers via Sprinto to determine that all devices have auto updates enabled.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity	Observed screenshots of JAMF password policy configurations to determine that maximum auto-lock is set for 3 minutes and maximum grace period for computer lock is set for 5 minutes.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Inspected the documentation published by GCP the company's cloud infrastructure provider to determine that GCP uses VPC firewall rules that deny all inbound and outbound traffic by default.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity has a documented Endpoint Security Policy, and makes it available for all staff on the company intranet	Observed that the company has documented the Endpoint Security Policy and made it available for all staff on Sprinto along with all other policies.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity has a documented Password Policy and makes it available to all staff members on the company intranet	Observed that the company has documented the Password Policy and made it available for all staff on Sprinto along with all other policies.	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.	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access	Observed the list of staff devices and their encryption status through Sprinto to determine that all of the company-owned devices have hard drive encryption enabled. Observed a screenshot of a recently hired employee's device settings to	No exceptions noted.

			determine that disk encryption is enabled.	
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.	All production database[s] that store customer data are encrypted at rest.	Observed through Sprinto that all GCP cloud storage buckets are encrypted at rest to determine that all data stores are encrypted. Inspected the system description to determine that the company requires all data at rest to be encrypted using the AES-256 bit standard.	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.	User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.	Observed that the security certificate of the company's website (https://app.spotdraft.com/auth/login) is valid till April 14, 2023, to determine that the entity's application is secured using HTTPS (TLS algorithm) and industry-standard encryption.	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.	Entity maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.	Inspected a list of infrastructure assets exported through Sprinto to determine that the company ensures production and non-production assets are required to be marked separately for identification.	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.	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment	Inspected a list of infrastructure assets exported through Sprinto to determine that the company ensures production and non-production assets are required to be marked separately for identification.	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.	Entity has a documented Encryption Policy, and makes it available for all staff on the company intranet	Observed that the company has documented the Encryption Policy and made it available for all staff on Sprinto along with all other policies.	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.	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Observed the list of staff devices and their OS auto update status through Sprinto to determine that all of the company-owned devices have auto updates enabled. Observed screenshots of 10 sample employee computers via Sprinto to determine that all devices have auto updates enabled.	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.	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Inspected the documentation published by GCP the company's cloud infrastructure provider to determine that GCP uses VPC firewall rules that deny all inbound and outbound traffic by default.	No exceptions noted.
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.	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed through Sprinto that the company uses Dependabot for scanning and vulnerability checks are enabled on the relevant repositories to determine that the entity has configured its system to perform regular vulnerability scans.	No exceptions noted.
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.	Entity tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	Inspected the vulnerability logs exported through Sprinto to determine that all vulnerabilities are identified by Dependabot, assigned severity level and tracked from the date of reporting to the resolution date.	No exceptions noted.
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.	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Inspected the production infrastructure monitoring data exported through Sprinto to determine that monitoring alerts are enabled for various activities including GCP/Cloud SQL, GCP/Compute Instance, and GCP VPC Subnet flow logs.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative	Entity identifies vulnerabilities on the Company platform through	Observed through Sprinto that the company uses Dependabot for scanning and vulnerability checks are enabled on the relevant repositories to determine	No exceptions noted.

	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.	the execution of regular vulnerability scans.	that the entity has configured its system to perform regular vulnerability scans.	
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.	Entity tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	Inspected the vulnerability logs exported through Sprinto to determine that all vulnerabilities are identified by Dependabot, assigned severity level and tracked from the date of reporting to the resolution date.	No exceptions noted.
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.	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Inspected the production infrastructure monitoring data exported through Sprinto to determine that monitoring alerts are enabled for various activities including GCP/Cloud SQL, GCP/Compute Instance, and GCP VPC Subnet flow logs.	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.	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the results of an internal audit assessment which includes information about owners, controls, and performance of controls to determine that the entity uses Sprinto to continuously monitor, track, and report the health of the information security program to the Information Security Officer and other stakeholders.	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.	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Observed the list of staff devices and their OS auto update status through Sprinto to determine that all of the company-owned devices have auto updates enabled. Observed screenshots of 10 sample employee computers via Sprinto to	No exceptions noted.

			determine that all devices have auto updates enabled.	
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.	Entity maintains a record of information security incidents.	Inspected the Incident Management Policy to determine that the company is required to maintain a record of security, availability, and confidentiality incidents. Disclosure: There have not been any security incidents reported.	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.	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed through Sprinto that the company uses Dependabot for scanning and vulnerability checks are enabled on the relevant repositories to determine that the entity has configured its system to perform regular vulnerability scans.	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.	Entity tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	Inspected the vulnerability logs exported through Sprinto to determine that all vulnerabilities are identified by Dependabot, assigned severity level and tracked from the date of reporting to the resolution date.	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.	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Inspected the production infrastructure monitoring data exported through Sprinto to determine that monitoring alerts are enabled for various activities including GCP/Cloud SQL, GCP/Compute Instance, and GCP VPC Subnet flow logs.	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.	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the results of an internal audit assessment which includes information about owners, controls, and performance of controls to determine that the entity uses Sprinto to continuously monitor, track, and report the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to	Entity has established an Incident Management & Response Policy, which includes guidelines and	Inspected the Incident Management Policy to determine that the company has established the procedures for responding to a discovered security	No exceptions noted.

	understand, contain, remediate, and communicate security incidents, as appropriate.	procedures to be undertaken in response to information security incidents. This is available to all staff members via the company intranet.	incident through several steps documented in the policy. Observed that all policies are available to the staff via Sprinto.	
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.	Entity maintains a record of information security incidents.	Inspected the Incident Management Policy to determine that the company is required to maintain a record of security, availability, and confidentiality incidents. Disclosure: There have not been any security incidents reported.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy to determine that the company has documented the procedures to be followed in case of an incident.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Entity has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	Inspected the Data Backup Policy, available on Sprinto, which states that the company periodically performs a complete backup of all critical data stored by the company, to determine that the entity has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	No exceptions noted.
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.	Entity has a documented Change Management Policy, which is available to all Staff Members via the company intranet	Inspected the Change Management Policy, available on Sprinto, which lists the principles applied to handle changes regarding software changes and production environment changes to determine that the company has a documented Change Management Policy, and makes it available for all staff on the company intranet.	No exceptions noted.
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.	Entity uses a change management system to track, review and log all changes to the application code.	Observed the Change Management Repositories showing GitHub repositories through Sprinto to determine that the company uses GitHub as a change management system to track, review, and log all changes to the application code.	No exceptions noted.

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.	Entity maintains a list of infrastructure assets and segregates production assets from its staging/development assets.	Inspected the list of infrastructure assets exported through Sprinto, which shows that production assets are marked separately to determine that the entity maintains a list of infrastructure assets and segregates production assets from its staging/development assets.	No exceptions noted.
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.	Entity's change management system is configured to enforce peer reviews for all planned changes. For all code changes, the reviewer must be different from the author.	Observed through Sprinto that peer reviews are enabled for the GitHub control repositories to determine that the entity's change management system is configured to enforce peer reviews for all planned changes.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Entity has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Assessment and Management Policy to determine that the guidelines for identifying and mitigating risks to the business by identifying the sources of risk, assessing the threats, and treating risks have been described.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	Inspected the periodic risk assessment data exported through Sprinto, which shows the results of a recent risk assessment, including a list of risks, their mitigation checks, impact score, likelihood, residual risk, and risk treatment decision, to determine that the company performs risk assessments at least annually.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment data exported through Sprinto, showing the results of a recent risk assessment, including an impact score and likelihood for each identified risk to determine that the company assesses the impact and likelihood of risks as part of the risk assessment process. Inspected the Risk Assessment and Management Policy to determine that a mechanism for quantifying risk impact	No exceptions noted.

			using a relative measure on a scale of 0 to 10 and mitigation strategies for identified risks have been defined.	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Entity has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Assessment and Management Policy to determine that the guidelines for identifying and mitigating risks to the business by identifying the sources of risk, assessing the threats, and treating risks have been described.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Entity has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.	Inspected the Vendor Management Policy to determine that the company has documented the process for managing vendor relationships, with an aim to reduce risks associated with using third-party services.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements	Inspected the vendor risk assessment report which shows the company's vendors, their categories, internal owners, risk levels, and remediation measures to determine that the entity performs a formal vendor risk assessment exercise annually.	No exceptions noted.
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Inspected the production infrastructure monitoring data exported through Sprinto to determine that monitoring alerts are enabled for various activities including GCP/Cloud SQL, GCP/Compute Instance, and GCP VPC Subnet flow logs.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Entity has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	Inspected the Data Backup Policy, available on Sprinto, which states that the company periodically performs a complete backup of all critical data stored by the company, to determine that the entity has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	No exceptions noted.

A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Entity backs-up their production databases periodically.	Observed through Sprinto that backup is enabled on all GCP/Cloud SQL databases to determine that the entity backs up its production databases periodically. Inspected the Data Backup Policy to determine that the company is required to perform a complete backup of all critical data on a periodic basis.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Entity's data backups are restored and tested annually	Inspected the Database Backup Restore Exercise Notes which document the restoration and testing activities performed during the exercise to determine that the entity's data backups are restored and tested annually. Inspected the Backup Policy to determine that the company is required to restore and test the backups on a periodic basis.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy to determine that the company has documented the procedures to be followed in case of an incident.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy to determine that the company has documented the procedures to be followed in case of an incident.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Entity ensures that the Disaster Recovery Plan is tested periodically and learnings documented	Inspected the notes from a disaster recovery exercise dated July 22, 2022, to determine that a relevant team tests the disaster recovery plan periodically and is required to document learnings from the exercise if any. Disclosure: No learnings were documented in the disaster recovery test exercise.	No exceptions noted.

A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Entity's data backups are restored and tested annually	<p>Inspected the Database Backup Restore Exercise Notes which document the restoration and testing activities performed during the exercise to determine that the entity's data backups are restored and tested annually.</p> <p>Inspected the Backup Policy to determine that the company is required to restore and test the backups on a periodic basis.</p>	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Entity has a documented Confidentiality Policy, and makes it available for all staff on the company intranet.	Inspected the Confidentiality Policy, uploaded on Sprinto, which describes the steps to ensure the confidentiality of sensitive data to determine that the entity has a documented Confidentiality Policy, and makes it available for all staff on the company intranet.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	<p>Inspected the system description to determine that all employees are required to acknowledge their understanding of policies upon hire.</p> <p>Observed the new hire policy acknowledgement logs within Sprinto to determine that all in-scope new hires during the observation period have accepted policies within the SLA as part of onboarding.</p>	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Entity requires that all staff members review and acknowledge company policies annually	<p>Inspected the system description to determine that new employees are required to acknowledge the company's policies upon hire and annually thereafter.</p> <p>Observed the periodic policy acknowledgement logs within Sprinto to determine that all in-scope active personnel have accepted policies as part of the annual acknowledgement.</p>	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Entity has a documented Data Classification Policy, and makes it available for all staff on the company intranet.	Inspected the Data Classification Policy uploaded on Sprinto, which outlines a framework for classifying data based on its sensitivity, value, and criticality to the organization, to determine that the entity has a documented Data Classification Policy and makes it	No exceptions noted.

			available for all staff on the company intranet.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	All production database[s] that store customer data are encrypted at rest.	Observed through Sprinto that all GCP cloud storage buckets are encrypted at rest to determine that all data stores are encrypted. Inspected the system description to determine that the company requires all data at rest to be encrypted using the AES-256 bit standard.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorized access	Observed the list of staff devices and their encryption status through Sprinto to determine that all of the company-owned devices have hard drive encryption enabled. Observed a screenshot of a recently hired employee's device settings to determine that disk encryption is enabled.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Entity has a documented Data Retention Policy, and makes it available for all staff on the company intranet.	Inspected the Data Retention Policy uploaded on Sprinto, which describes the company's policy for retaining and disposing of data, to determine that the entity has a documented Data Retention Policy and makes it available for all staff on the company intranet.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.	Inspected the Media Disposal Policy to determine that the steps to permanently dispose of the company's media are described stating that the company is required to use the recommended disposal methods for critical and sensitive data.	No exceptions noted.