THOUGHTSPOT, INC.

ThoughtSpot Cloud Platform

System and Organization Controls (SOC) for Service Organizations Report for the period of January 1, 2023, to August 31, 2023

Report of Independent Service Auditor issued by Aprio LLP

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

Table of Contents

I. Report of Independent Service Auditor

We have examined ThoughtSpot, Inc.'s (the "Company" or "ThoughtSpot") accompanying assertion titled *ThoughtSpot, Inc.'s Assertion* (the "Assertion") indicating that the controls within the ThoughtSpot Cloud Platform (the "System") were effective for the period of January 1, 2023 to August 31, 2023 (the "Specified Period") to provide reasonable assurance that ThoughtSpot's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, and Confidentiality ("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*).

The Company uses Amazon Web Services' (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. In addition, the Company uses AWS Simple Storage (S3) as a Platform-as-a-Service. The Company also uses Google Cloud Platform (GCP) for its third-party hosting of servers and equipment in a Platform-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. In addition, the Company uses Hurricane Electric for its third-party hosting of development servers and equipment, including the restriction of physical access to the defined system, including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses Intercom, Inc. as an in-application communications platform. Lastly, the Company uses Radical HQ Limited t/a Cord (Cord) as an in-application collaboration platform. Certain AICPA Applicable Trust Services Criteria specified in the section titled *ThoughtSpot, Inc.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled *ThoughtSpot, Inc.'s Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to 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

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *ThoughtSpot, Inc.'s Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting and identifying in its assertion, the Applicable Trust Services Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that the controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the controls were not effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services Criteria.

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

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other matters

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *ThoughtSpot, Inc.'s Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Basis for Qualified Opinion

The Company states in ThoughtSpot, Inc.'s Assertion that controls related to background checks and terminated employee access were not operating effectively throughout the period January 1, 2023 to August 31, 2023 to achieve the following trust services criteria:

- Common Criteria CC 1.4: *COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives,*
- Common Criteria CC 6.1: *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;*
- Common Criteria CC 6.2: *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;* and

- Common Criteria CC 6.3: *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.*

Qualified Opinion

In our opinion, except for the matters described in the paragraph above, ThoughtSpot's assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects, is fairly stated.

Aprio, LLP

Aprio, LLP

Atlanta, Georgia
November 17, 2023

II. ThoughtSpot, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over ThoughtSpot, Inc.'s (the "Company" or "ThoughtSpot") ThoughtSpot Cloud Platform (the "System") for the period of January 1, 2023, to August 31, 2023 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, Processing Integrity, and Confidentiality were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, and Confidentiality (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*). The Company's objectives for the system in applying the Applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the Applicable Trust Services Criteria. The principal service commitments and system requirements related to the Applicable Trust Services Criteria are specified in the section titled *ThoughtSpot, Inc.'s Description of the Boundaries of its System*.

The Company uses Amazon Web Services' (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. In addition, the Company uses AWS Simple Storage (S3) as a Platform-as-a-Service. The Company also uses Google Cloud Platform (GCP) for its third-party hosting of servers and equipment in a Platform-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. In addition, the Company uses Hurricane Electric for its third-party hosting of development servers and equipment, including the restriction of physical access to the defined system, including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses Intercom, Inc. as an in-application communications platform. Lastly, the Company uses Radical HQ Limited t/a Cord (Cord) as an in-application collaboration platform. Certain AICPA Applicable Trust Services Criteria specified in the section titled *ThoughtSpot, Inc.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *ThoughtSpot, Inc.'s Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by User Entities.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Controls related to background checks and terminated employee access were not operating effectively throughout the period January 1, 2023, to August 31, 2023 to achieve the following trust services criteria:

- Common Criteria CC 1.4: *COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives;*

- Common Criteria CC 6.1: *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,*
- Common Criteria CC 6.2: *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;* and
- Common Criteria CC 6.3: *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.*

Except for the matters described in the paragraph above, we assert that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. ThoughtSpot, Inc.'s Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of ThoughtSpot, Inc. (the "Company" or "ThoughtSpot") as it relates to its ThoughtSpot Cloud Platform (the "System") for the period January 1, 2023 to August 31, 2023 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, Processing Integrity, and Confidentiality (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

B. Company Overview and Background

TS Cloud Platform's search engine allows users to ask questions, analyze data, build reports, and generate liveboards. Searches automatically generate visualizations. Customers can pin visualizations to the liveboards and share them with other users within their organization. As customers' users continue to search in their company's ThoughtSpot instance, the system learns over time to make more customized search suggestions. Data is analyzed in real-time, providing fresh information every time the client refreshes or opens their application.

As of August 2023, TS Cloud Platform's search capabilities are further enhanced by an updated ThoughtSpot Sage, a new artificial intelligence (AI)-powered natural language search experience that leverages generative pre-trained transformers (GPT) with the large language models (LLM) of Microsoft Azure OpenAI Service. Customers can choose to enable this option for their instance. As a note, ThoughtSpot Sage AI feature is currently only live in Beta upon customer request, and therefore, was not included in the scope of this report.

ThoughtSpot continually updates its corporate website with various offerings of the TS Cloud Platform and ThoughtSpot Everywhere product line, describing the features and limitations that customers can choose from. ThoughtSpot also offers TS Visual Embed Software Development Kit (SDK) as part of the ThoughtSpot Everywhere product for the customer's developer community for TS Cloud features embedding into their applications. The TS Cloud Platform also provides various application programming interface (API) integrations and connectors to the customers within its application. For the mobile experience of TS Cloud, the ThoughtSpot Mobile App is available on the Google Play Store and Apple App Store.

ThoughtSpot product documentation websites are continually updated with the latest product release content tailored to the respective audiences. ThoughtSpot maintains terms of use, privacy policy, and other digital trust-relevant documentation on its corporate website.

Customer-facing training for TS Cloud administrators is available via ThoughtSpot U, and instructor-led classes and training credits are provided for these classes, which go toward payment for the product. Certifications for the product, such as ThoughtSpot Professional, ThoughtSpot Architect, ThoughtSpot Data Expert, etc., are also available.

A cluster of AWS and/or GCP instances is created upon the customer's initiation. Clients can choose the cloud and regions where they want to set up their clusters. After the cluster is presented to the client, Salesforce sends the client an activation email that informs clients how to activate and interact with the clusters and how to interact with TS Cloud Software-as-a-Service (SaaS). Sales personnel provide clients with a walkthrough explaining how to create additional clusters, upload data and connect to their data sources, prevent the TS Cloud site from being blocked by their firewall, add users, and set up the single sign-on capabilities.

Clients are assigned a Client Success Manager/Account Executive responsible for managing the relationship with the client and acting as the client's point of contact. Contracts are also completed with all clients, including service-level agreements (SLAs). Information collected from clients includes email, company name, and username. The administrator adds users after the initial setup. To initiate client offboarding, a ticket is entered into Salesforce to terminate the account. The client environment is decommissioned, and data is purged per the customer subscription agreement.

C. System Overview

Infrastructure

TS Cloud is a hosted and managed SaaS offering. TS Cloud is available on AWS and GCP. Customers can choose the cloud and region where they would like their TS Cloud Platform deployed.

ThoughtSpot’s infrastructure comprises servers, workstations, firewalls, and other networking and telecommunications devices. To illustrate this infrastructure, the company maintains Network General Overview Diagrams (Figures 1 & 2) that the Director of IT is responsible for reviewing and updating annually and as needed.

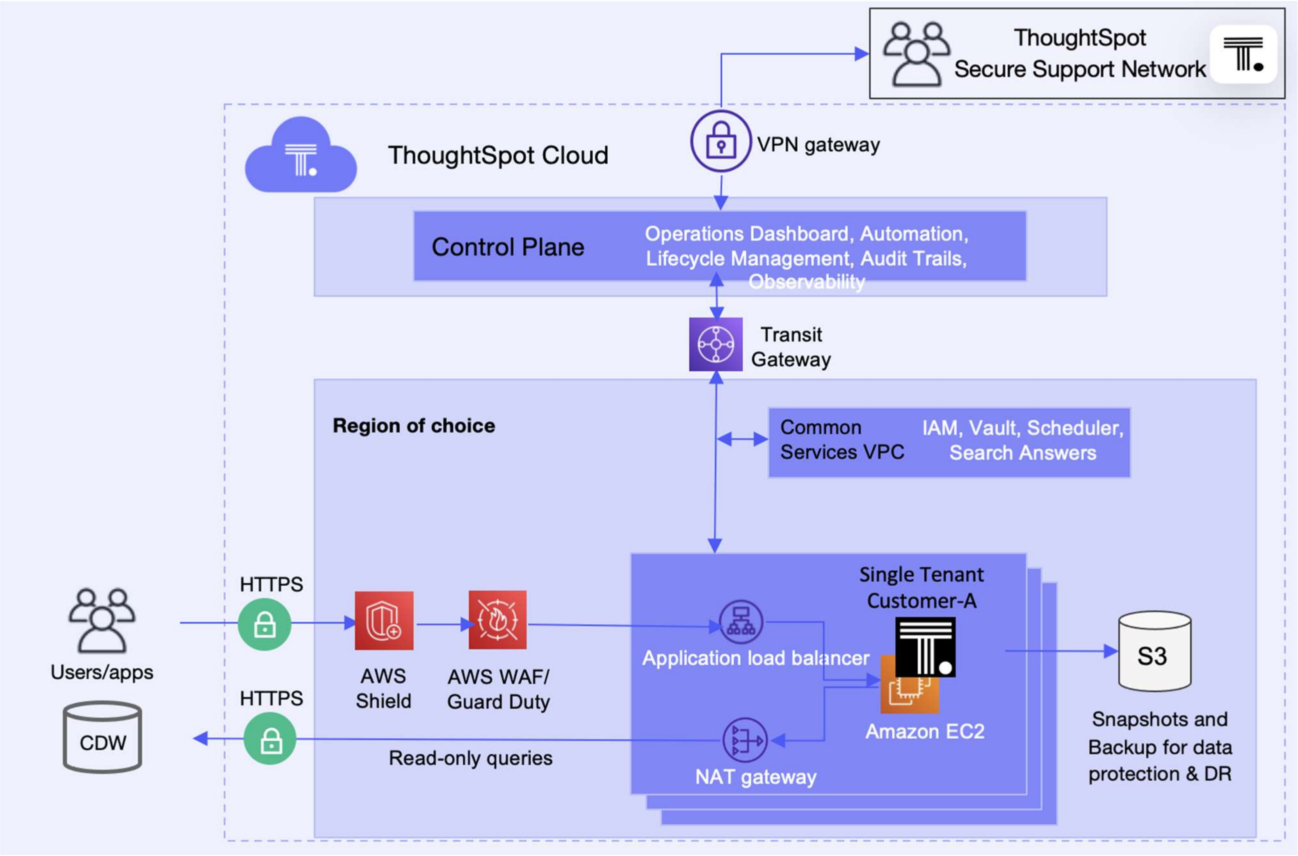

Figure 1: ThoughtSpot’s Network General Overview Diagram (TS Cloud’s AWS typical setup)

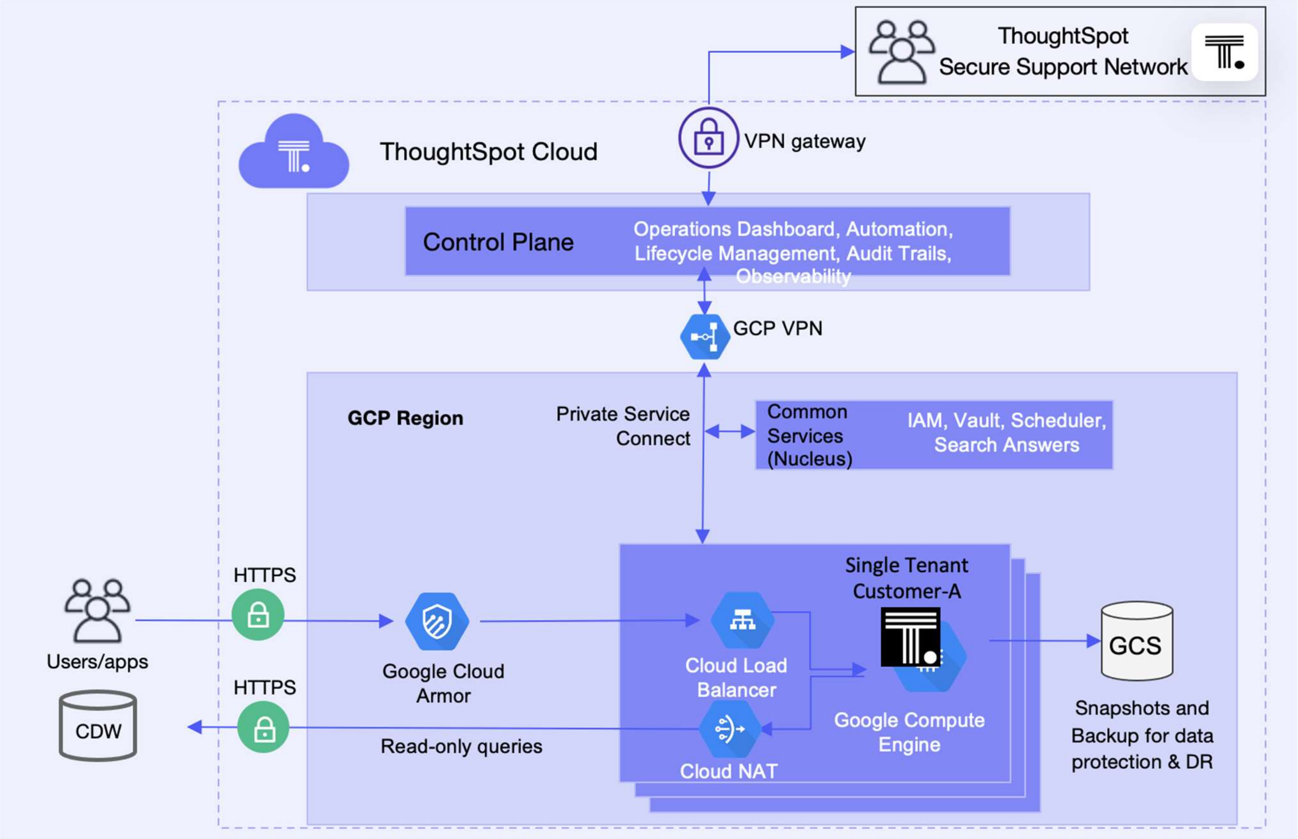

Figure 2: ThoughtSpot's Network General Overview Diagram (TS Cloud GCP typical setup)

ThoughtSpot also uses several systems and tools to manage inventories of all its physical, mobile, and virtual systems, assets, and devices, and these inventories include a description of the function and use of each device, system, or asset.

Software

ThoughtSpot maintains a software inventory of all its critical software in use, including the documentation and tracking of applicable software licenses. The Company's critical software in use includes the following:

- CentOS
- macOS
- Postgres
- Terraform
- Tomcat
- Vault
- Windows

D. Principal Service Commitments and System Requirements

ThoughtSpot designs its processes and procedures to meet its objectives for its TS Cloud Platform. Those objectives are based on the service commitments that ThoughtSpot makes to user entities, the laws and regulations that govern the provision of TS Cloud Platform, and the operational and compliance requirements that ThoughtSpot has established for the services.

Security, availability, processing integrity, and confidentiality commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the service offering provided online. Security, availability, processing integrity, and confidentiality commitments are standardized and include, but are not limited to, the following:

- The use of security and confidentiality principles that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- The use of encryption technologies to protect customer data in transit over untrusted networks;
- The use of reasonable precautions to protect the security and confidentiality of the information that is collected;
- The use of availability principles that are designed to help ensure the availability of the systems supporting TS Cloud;
- Make commercially reasonable efforts that controls are in place to automatically filter certain personal information collected from the System, such as passwords or other non-relevant personal information;
- Make commercially reasonable efforts that controls are in place to destroy or encrypt any information that is not filtered automatically; and
- Make commercially reasonable efforts that controls are in place to help ensure complete and accurate processing of the in-scope system(s) transactions.

ThoughtSpot establishes operational requirements that support the achievement of security, availability, processing integrity, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ThoughtSpot's system policies and procedures, system design documentation, and customer contracts. Information security policies define an organization-wide approach to protecting systems and data.

E. Subservice Organizations

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

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

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services (AWS)	The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses AWS Key Management Services (KMS) and AWS Simple Storage Service (S3) as a Platform-as-a-Service. Amazon S3 provides object storage through	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4* CC 6.5*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	a web service interface. The following control activities are critical to achieving the Applicable Trust Services Criteria: ● Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; ● Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; ● Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; ● Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS; ● Controls over incident monitoring, response, and follow up; ● Controls over managing the Platform-as-a-Service components for Amazon KMS and S3 such as physical servers and operating systems including applying critical patching for this infrastructure; ● Controls over Amazon KMS and S3 including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; ● Controls over AWS S3 redundancy, including controls over data replication; and ● Controls over the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform (KMS and S3) components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: ● On an annual basis, management performs a vendor risk assessment to evaluate third parties and determine the vendor's risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* PI 1.2* PI 1.3* PI 1.4* PI 1.5*
Google Cloud Platform (GCP)	The Company uses Google Cloud Platform (GCP) for its third-party hosting of servers and equipment in a Platform-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control activities are critical to achieving the Applicable Trust Services Criteria: ● Controls around the underlying infrastructure and Data Centers supporting the in-scope production environment including	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4* CC 6.5* CC 6.6* CC 6.7*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	environmental safeguards such as UPS, backup generators, and fire suppression; - Controls around storage redundancy, including controls over data replication; - Controls over incident monitoring, response, and follow up; - Controls over the prevention, detection, and follow up upon the introduction of malicious software; - Controls over the logical access to supporting infrastructure such as underlying physical servers and related operating systems; - Controls around various encryption settings including encryption keys and encryption of the databases; - Controls around various networking devices such as firewalls; - Controls over managing infrastructure such as physical servers and physical access to backups and facilities; - Controls around the data storage, including controls around physical access to the backup servers and facilities, high availability replication, physical access to storage systems, operating system installation and patches, database software installation and patches, and system configuration; - Controls over the databases including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; - Controls over managing GCP Platform-as-a-Service components such as physical servers and operating systems including applying critical patching for this infrastructure; and - Controls around the change management processes for the GCP Platform-as-a-Service components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: - On an annual basis, management performs a vendor risk assessment to evaluate third parties and determine the vendor's risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* PI 1.2* PI 1.3* PI 1.4* PI 1.5*
Hurricane Electric	The Company uses Hurricane Electric for its third-party hosting of development servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control activities are critical to achieving the Applicable Trust Services Criteria:	CC 6.4* A 1.2* A 1.3* C 1.2* PI 1.5*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; and • Controls over physical access to the Data Centers hosting the in-scope production environment. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management performs a vendor risk assessment to evaluate third parties and determine the vendor's risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	
Intercom	The Company uses Intercom, Inc. as an in-application communications platform. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the encryption methods for communication within the application to ensure that customer PII is protected. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management performs a vendor risk assessment to evaluate third parties and determine the vendor's risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	PI 1.2* PI 1.3* PI 1.4*
Radical HQ Limited t/a Cord	The Company uses Radical HQ Limited t/a Cord as an in-application communications platform. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the encryption methods for communication within the application to ensure that customer PII is protected. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management performs a vendor risk assessment to evaluate third parties and determine the vendor's risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations.	PI 1.2* PI 1.3* PI 1.4*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	
Azure OpenAI	The Company uses Azure OpenAI for its large language model (LLM) data processing services. As of the date of this report, Azure OpenAI was not released in the production environment. It was only available via Beta release and upon customer request. The following control activities are critical to achieving the Applicable Trust Services Criteria: ● Controls over REST API access to OpenAI's language models. In addition, the Company has identified the following control activity to help monitor the subservice organization: On an annual basis, management performs a vendor risk assessment to evaluate third parties and determine the vendor's risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.4 CC 6.5 CC 6.6 CC 6.7 CC 6.8 CC 7.1 CC 7.2 CC 7.3 CC 7.4 CC 7.5 CC 8.1 CC 9.1 CC 9.2 A 1.1 A 1.2 A 1.3 C 1.1 C 1.2 PI 1.2 PI 1.3 PI 1.4 PI 1.5

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

F. User Entity Controls

ThoughtSpot, Inc.'s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary user entity controls identified within the table below, where applicable.

As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. For user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
User Entities are responsible for adhering to the terms and conditions stated within their contracts with ThoughtSpot.	CC 2.2 CC 2.3 PI 1.1
User Entities are responsible for reporting any security, availability, processing integrity, and confidentiality incidents while accessing TS Cloud Platform to the ThoughtSpot support team in a timely manner.	CC 2.3 CC 4.2 CC 5.3 CC 7.3 CC 7.4
User Entities are responsible for reporting to ThoughtSpot in a timely manner any material changes to their overall control environment that may adversely affect services being performed by ThoughtSpot.	CC 2.3 CC 4.2 CC 5.3 CC 7.3 CC 7.4
User Entities are responsible for establishing their external database connection via the ThoughtSpot Connections (Embrace) option of TS Cloud Platform.	CC 5.2* CC 6.1* CC 6.6* CC 6.7* CC 6.8*
User Entities are responsible for implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user entity components associated with the use of the TS Cloud Platform.	CC 5.2 CC 6.1 CC 6.6 CC 6.7 CC 6.8
User Entities are responsible for provisioning and deprovisioning access to the TS Cloud Platform.	CC 6.2* CC 6.3*

User Entity Control	Associated Criteria
User Entities are responsible for notifying ThoughtSpot in a timely manner of any changes to personnel directly involved with services performed by ThoughtSpot. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by ThoughtSpot.	CC 6.2* CC 6.3*
User Entities are responsible for authorizing transactions relating to the TS Cloud Platform are sent securely, timely, and completely.	CC 6.7*
User Entities are responsible for developing their own business continuity (BC) and disaster recovery (DR) plans that address their inability to access or use the TS Cloud Platform.	CC 7.5 CC 9.1 A 1.3 C 1.1 PI 1.5
User Entities are responsible for verifying that the Tenant component of the TS Cloud Platform is set up in specific availability zones and regions as purchased and determined by them during setup.	A 1.2* A 1.3*
User Entities are responsible for implementing controls requiring additional approval procedures for critical transactions relating to TS Cloud Platform.	PI 1.2* PI 1.3* PI 1.4*

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

Aprio®