ThoughtSpot, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, and Confidentiality categories for the period of February 1, 2021 through January 31, 2022.

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF THOUGHTSPOT, INC. MANAGEMENT 1

INDEPENDENT SERVICE AUDITOR'S REPORT 3

Scope 4

Service Organization's Responsibilities 4

Service Auditor's Responsibilities 4

Inherent Limitations 5

Opinion 5

THOUGHTSPOT, INC.'S DESCRIPTION OF ITS HOSTED DATA ANALYTICS SOFTWARE-AS-A-SERVICE PLATFORM SYSTEM 6

Section A: ThoughtSpot, Inc.'s Description of the Boundaries of Its Hosted Data Analytics Software-As-A-Service Platform System 7

Services Provided 7

Locations 7

Infrastructure 7

Software 8

People 8

Data 8

Data Classification 8

Data Encryption and Retention 8

Processes and Procedures 9

Section B: Principal Service Commitments and System Requirements 10

Regulatory Commitments 10

Contractual Commitments 10

System Design 10

ASSERTION OF THOUGHTSPOT, INC. MANAGEMENT

ASSERTION OF THOUGHTSPOT, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within ThoughtSpot, Inc.'s hosted data analytics software-as-a-service platform system (system) throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that ThoughtSpot, Inc.'s service commitments and system requirements relevant to Security, Availability, Processing Integrity, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that ThoughtSpot, Inc.'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*). ThoughtSpot, Inc.'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 presented in section B.

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.

We assert that the controls within the system were effective throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that ThoughtSpot, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Sudheesh Nair
CEO
ThoughtSpot, Inc.
1900 Camden Ave, Suite 101
San Jose, CA 95124

Scope

We have examined ThoughtSpot, Inc.'s accompanying assertion titled "Assertion of ThoughtSpot, Inc. Management" (assertion) that the controls within ThoughtSpot, Inc.'s hosted data analytics software-as-a-service platform system (system) were effective throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that ThoughtSpot, Inc.'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*).

Service Organization's Responsibilities

ThoughtSpot, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ThoughtSpot, Inc.'s service commitments and system requirements were achieved. ThoughtSpot, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ThoughtSpot, Inc. 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 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 controls were not effective to achieve ThoughtSpot, Inc.'s service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ThoughtSpot, Inc.'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.

Opinion

In our opinion, management's assertion that the controls within ThoughtSpot, Inc.'s hosted data analytics software-as-a-service platform system were effective throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that ThoughtSpot, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

February 21, 2022

THOUGHTSPOT, INC.'S DESCRIPTION OF ITS HOSTED DATA ANALYTICS SOFTWARE-AS-A-SERVICE PLATFORM SYSTEM

SECTION A:
THOUGHTSPOT, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS HOSTED DATA ANALYTICS SOFTWARE-AS-A-SERVICE PLATFORM SYSTEM

Services Provided

ThoughtSpot, Inc. (ThoughtSpot) provides a Business Intelligence (BI)-hosted data analytics software-as-a-service (SaaS) platform, ThoughtSpot Cloud. ThoughtSpot Cloud's search engine allows users to ask questions, analyze data, and build reports and liveboards. Searches automatically generate visualizations, and customers can pin visualizations to liveboards and share them with others. 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.

Upon initiation of the free trial, a cluster of AWS instances is created. Clients can choose what regions in which 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 ThoughtSpot. Sales personnel provide clients with a walkthrough explaining how to create additional clusters, how to upload data and connect to the database, how prevent the site from being blocked by the firewall, how add users, and how to use Security Assertion Markup Language (SAML).

All clients are assigned a Client Success Manager responsible for managing the relationship with the client and acting as the client's point of contact. Contracts are also completed with all clients, and these contracts include service-level agreements (SLAs) that the client can monitor via the company's website.

Locations

The following locations are in scope for this audit:

- Engineering Location
  - Bellevue, WA, USA
- Engineering and Support Locations
  - Bangalore, IN
  - **San Jose, CA, USA—Headquarters**
- Support Locations
  - Addison, TX, USA
  - London, UK

Infrastructure

ThoughtSpot's infrastructure is composed of servers, workstations, firewalls, and other networking and telecommunications devices. To illustrate this infrastructure, the company maintains a Network General Overview Diagram that the Senior Manager of Network Systems is responsible for reviewing and updating annually and as needed.

The company 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, and this inventory includes 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

People

ThoughtSpot maintains a hierarchical and flat structure that consists of functional departments. The company maintains an organizational chart that illustrates its structure, functional departments, and clear reporting lines.

ThoughtSpot maintains a Board of Directors responsible for overseeing governance, product development, sales, marketing, and legal and compliance departments, as well as fulfilling their fiduciary responsibilities. The Board of Directors meets quarterly with company officers, and documentation used during these meetings are provided to all personnel for review via an intranet.

Data

ThoughtSpot's Cloud service processes client data that may include personally identifiable information (PII), and this service includes controls in place used to protect this data. Client data is stored in client service instances and network clusters, and client data can be submitted to these clusters by clients or ThoughtSpot personnel. A SaaS Data Flow Diagram is maintained that illustrates the flow of client and internal data throughout services and systems, and this diagram is reviewed, maintained, and updated by the Principal Engineer as needed.

Data Classification

ThoughtSpot's Privacy Policy specifies the type of information ThoughtSpot obtains and how it is used; the Privacy Policy is available on the company's public website for third-party review. All data handled is required to be classified as Public, Confidential, or Restricted to determine the data's handling and retention requirements, and data owners use this classification model to identify and classify the assets they own.

Data Encryption and Retention

ThoughtSpot's Cryptography and Key Management Policy dictates industry-accepted encryption best practices algorithms to ensure the security of its data. The use of encryption keys and Transport Layer Security (TLS) v1.2 or v1.3 is required for the transmission and storage of

data on systems, networks, assets, devices, and applications. The company has identified an encryption key custodian that is responsible for the management of its cryptographic keys and uses the AWS Key Management to automatically rotate encryption keys annually. All user passwords are encrypted at rest and in transit using various tools and cryptographic methods.

ThoughtSpot complies with GDPR and Privacy Shield regarding data retention and retains its data accordingly.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

ThoughtSpot is subject to the General Data Protection Regulation (GDPR) and similar privacy regulations. The Privacy Policy details how the organization uses the data collected for its clients and how the company complies with applicable privacy laws, such as GDPR and the California Consumer Privacy Act (CCPA).

Additionally, ThoughtSpot complies with the AICPA Trust Services Criteria and ISO 27001:2013 security frameworks and employs an independent auditing firm to conduct independent audits of its internal controls annually to ensure its compliance with these frameworks.

Contractual Commitments

Contractual materials are maintained that define the scope of services provided to customers. The Cloud Subscription Agreement sets important expectations, such as permissions, billing periods, and expectations for client data use. The organization uses a Subscription Contract to acquire customers, and the service offered to clients is a managed cloud data warehouse, which supports natural language queries. The agreement also addresses the following categories:

- Purchasing
- Permissions and limitations
- Customer data
- Warranties
- Priority rights
- Third-party claims
- Limitations of liability
- Term and termination
- General

ThoughtSpot describes its service commitments and system requirements in the ThoughtSpot Support and Maintenance Program Guide, in marketing materials, and on the organization's public website. As described in the guide, the organization commits to providing support at all times, and the organization executes the following documented response times:

- P0 – Response time within one hour
- P1 – Response time within two hours
- P2 – Response time within four hours
- P3 – Response time next business day

System Design

ThoughtSpot designs its hosted data analytics SaaS platform system to meet its regulatory and contractual commitments. These commitments are based on the services that ThoughtSpot provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that ThoughtSpot has established for its services. ThoughtSpot establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in ThoughtSpot's system policies and procedures, system design documentation, and contracts with clients.