Hootsuite Inc.

System and Organization Controls (SOC) 3 Report on Hootsuite Dashboard, Amplify, and Mobile Application System Relevant to Security

December 15, 2021

Hootsuite®

Contents

Section 1: Independent Service Auditor's Report

Deloitte.

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Hootsuite Inc.

Scope

We have been engaged to report on Hootsuite's accompanying statement titled "Statement by Management of Hootsuite" (statement) that the controls within Hootsuite Dashboard, Amplify, and Mobile Application system (system) were effective throughout the period November 1, 2020 to October 31, 2021 to provide reasonable assurance that Hootsuite's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

The accompanying statement and the Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Hootsuite, to achieve Hootsuite's service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system presents the complementary user entity controls assumed in the design of Hootsuite's controls. Our engagement did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Hootsuite uses Amazon Web Services ("AWS") to host its cloud infrastructure, and MongoDB Atlas Cloud Service to host its MongoDB deployment (collectively referred to as "subservice organizations"). The accompanying statement and the Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system indicate that certain service commitments and system requirements based on the applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. The Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system presents the types of complementary subservice organization controls assumed in the design of Hootsuite's controls. Our engagement did not include the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2020 to October 31, 2021.

Service Organization's Responsibilities

Hootsuite 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 Hootsuite's service commitments and system requirements were achieved. Hootsuite has also

provided the accompanying statement about the effectiveness of controls within the system. When preparing its statement, Hootsuite is responsible for selecting, and identifying in its statement, the applicable trust services criteria and for having a reasonable basis for its statement by performing an assessment of the effectiveness of the controls within the system.

Our Independence and Quality Control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, *Qualify Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion, based on the evidence we have obtained, on whether management's statement 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 engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whethermanagement's statement 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 reasonable assurance engagement 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 Hootsuite'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 Hootsuite's service commitments and system requirements based on the applicable trust services criteria
- 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 ineffective because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's statement that the controls within Hootsuite Enterprise, Amplify, and Mobile Application system were effective throughout the period November 1, 2020 to October 31, 2021 to provide reasonable assurance that Hootsuite's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte LLP

DELOITTE LLP
Chartered Professional Accountants
Vancouver, BC

December 15, 2021

Section 2: Hootsuite's Management Statement

HOOTSUITE INC.

STATEMENT BY MANAGEMENT OF HOOTSUITE

We are responsible for designing, implementing, operating, and maintaining effective controls within Hootsuite Dashboard, Amplify, and Mobile Application system (system) throughout the period November 1, 2020 to October 31, 2021 to provide reasonable assurance that Hootsuite's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system is presented in Section 3 and identifies the aspects of the system covered by our statement.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2020 to October 31, 2021 to provide reasonable assurance that Hootsuite's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Hootsuite'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 3.

We use Amazon Web Services ("AWS") to host our cloud infrastructure, and MongoDB Atlas Cloud Service to host our MongoDB deployment (collectively referred to as "subservice organizations"). This statement and the Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with Hootsuite's controls, to achieve Hootsuite's service commitments and system requirements related to the Hootsuite services based on the applicable trust services criteria. The accompanying Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system presents the types of complementary subservice organization controls assumed in the design of Hootsuite's controls. The actual controls at the subservice organizations are not disclosed.

This statement and the Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Hootsuite, to achieve Hootsuite's service commitments and system requirements related to the Hootsuite Dashboard, Amplify, and Mobile Application system, based on the applicable trust services criteria. The accompanying Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application system presents the complementary user entity controls assumed in the design of Hootsuite's controls.

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 confirm that the controls within the system were effective throughout the period November 1, 2020 to October 31, 2021 to provide reasonable assurance that Hootsuite's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 3: Hootsuite's Description of the Boundaries of Hootsuite Dashboard, Amplify, and Mobile Application System Relevant to Security

Company Background

Hootsuite is a widely adopted platform for managing social media, used by over 18 million people around the globe, including more than 800 of the Fortune 1000 companies. With Hootsuite, brands harness the power of social. Our platform brings together customers' social networks and integrates with hundreds of business applications in one place. We help customers build relationships with customers, stay connected to the needs of the market, and grow your revenue. We are the core platform for managing social media, helping customers support and drive their business with an ecosystem that plugs directly into existing, and future, needs.

Brands trust Hootsuite as their centralized hub for all things social: managing social media campaigns, marketing, and advertising; engaging audiences; scheduling and publishing messages, and analyzing results. Hootsuite offers a complete set of offerings for every need, whether it is an individual, small business, or large organization. People all around the world are using Hootsuite to get more out of social, and we're here to make them as successful as possible, regardless of how big or small their goals are.

Hootsuite helps brands of all sizes and any industry around the globe to build and sustain relationships with their audiences and drive their social media goals. Hootsuite offers an ecosystem of external tools and services and a web and mobile platform to manage all social media activities. Hootsuite also offers broad enterprise integrations so that social directly plugs into the business.

Hootsuite's headquarters is based in Vancouver, British Columbia, Canada, and has close to 1,000 employees located in Vancouver, San Francisco, New York, London, Sydney, Toronto, and other countries.

Description of Services Provided

Dashboard

Hootsuite Dashboard can be used to manage multiple social media channels, schedule posts, track mentions and traffic. It allows businesses and teams to collaboratively execute campaigns across social networks such as Instagram, Twitter, Facebook, and LinkedIn and enables organizations to securely manage social media accounts, engage audiences, and measure business results.

While using existing, preauthorized social media accounts, Dashboard allows users to effectively define, authorize and schedule their social media interactions. Due to their interoperability and versatility, enterprise social tools can be deployed in a variety of configurations to suit different businesses. Hootsuite Analytics is an integrated feature of Dashboard. It provides the easiest way for customers to measure social media contents and learn about fans and followers, all in one place. Customers can generate social media analytics reports, get a clear understanding of their social post performance, and measure the impact of their social media campaigns and conversations across multiple channels. Hootsuite also offers the Ow.ly shortening services, which is a built-in URL shortener that customers can access via their Hootsuite account. Using the Ow.ly shortening services to manage URLs provides businesses and organizations with important statistical analysis to see which Twitter messages generate click-throughs.

Hootsuite Dashboard is a cloud-based Software as a Service (SaaS) application that is resident with Amazon Web Services (AWS), as outlined in the diagram below. The Dashboard is hosted on Linux servers within the AWS environment, linked to SQL and NoSQL databases.

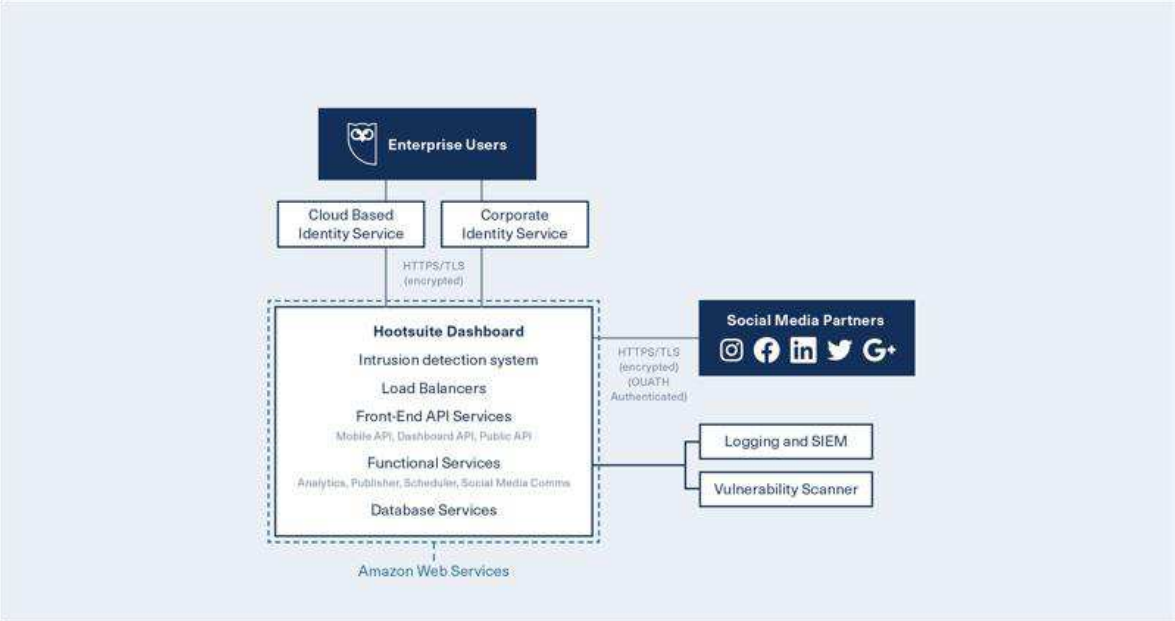

FIGURE 1: OVERVIEW OF THE HOOTSUITE DASHBOARD

Amplify

Hootsuite Amplify allows organizations to grow their business using their employees' organic social networks. It can be used to manage a central location for organizations to provide a feed of messages to their employees. Employees acting as advocates for their organization, or as social selling looking to grow sales on social media channels can publish any of these messages onto their own social network accounts. Hootsuite Amplify is an effective tool either in place of, or alongside, paid revenue channels such as advertising.

Hootsuite Amplify is a cloud-based Software as a Service (SaaS) application that is resident with Amazon Web Services (AWS), as outlined in the diagram below. All environments are hosted on Linux servers linked to NoSQL databases.

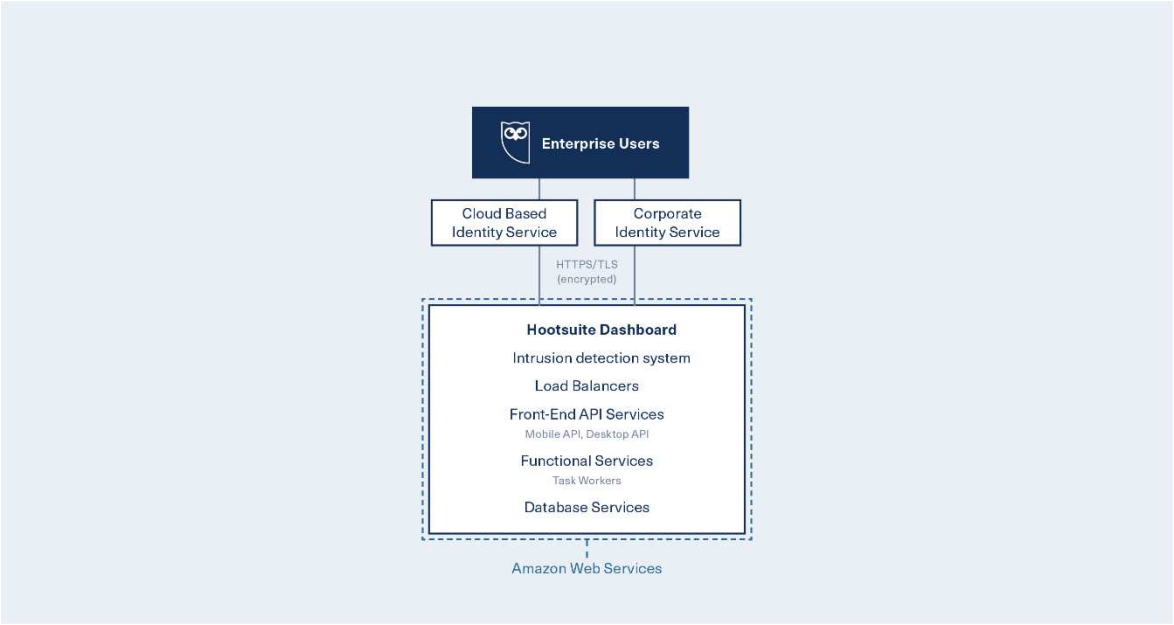

FIGURE 2: OVERVIEW OF THE HOOTSUITE AMPLIFY

Mobile Application

Hootsuite mobile application for iOS and Android is a complementary product to the Hootsuite web experience, enabling Hootsuite customers to accomplish their social media tasks on the go. The mobile application allows Hootsuite customers to:

- Schedule or send their messages to social media using the mobile Composer.
- Plan their outgoing social media messages using the mobile Publisher.
- Monitor incoming social media activities and engage with customers using the mobile Streams.
- Manage conversations with customers using the mobile Inbox.

The mobile application is written using native Android and iOS SDKs in Kotlin/Java and Swift/Obj-C programming languages respectively. They are delivered to user devices through Google Play and Apple Store. All traffic to Hootsuite APIs is encrypted using TLS 1.2+. The mobile application also supports getting push notifications via cloud messaging services. Urban Airship is the service provider we currently use for cloud messaging as outlined in the diagram below.

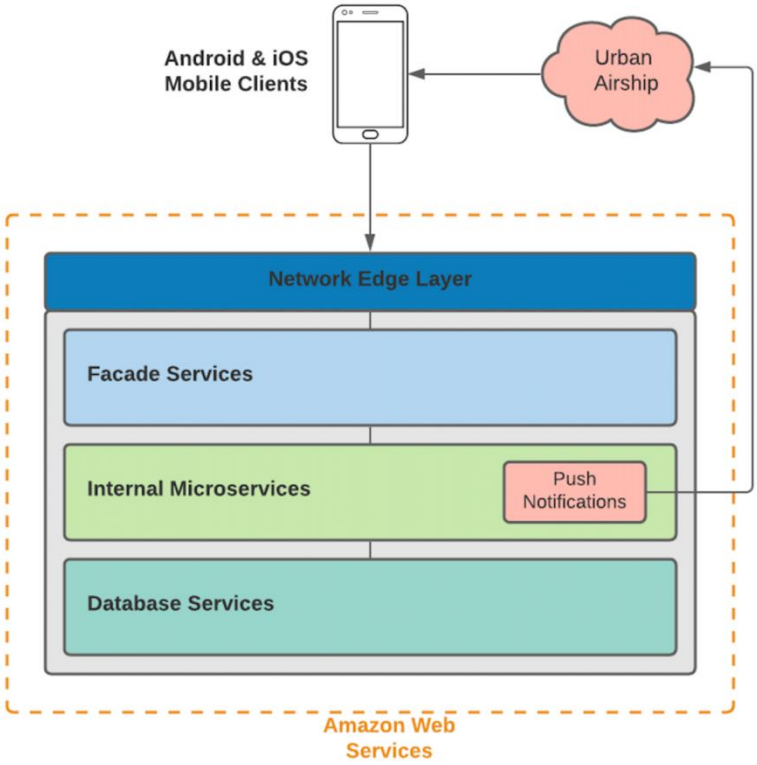

FIGURE 3: OVERVIEW OF THE HOOTSUITE MOBILE APPLICATION

Scope definition

The scope of this report addresses the security controls related to the Dashboard (including Analytics), Amplify, and Mobile Application system provided by Hootsuite. This covers Hootsuite's infrastructure in both EC2 and Kubernetes environments hosted in AWS.

Controls related to services provided by Hootsuite to customers using the following products are not included in the scope of this report:

- Hootsuite Ads
- Hootsuite Impact
- Hootsuite Insights
- SparkCentral

Principal Service Commitments and System Requirements

Hootsuite's Service Commitments to our user entities are communicated using either our Master Services Agreement (MSA) or our online Enterprise Terms of Service. Our principal service commitments are to:

- Maintain the security and confidentiality of the data that our user entities store in the Hootsuite Dashboard, Amplify, and Mobile Application services.
- Closely monitor our systems and data for any indication of a security event, incident, or breach.
- Maintain the availability of the system, as per our Service Level Agreement (SLA).
- Hootsuite's System Requirements are contained in our Information Security Management System (ISMS), and include:
    - A suite of Information Security related policies, with supporting procedures, to support our control environment.
    - Mandatory Information Security Awareness Training and Policy Acknowledgement for all employees.
    - Identity and Access Management processes that are based on a Roles Based Access Control (RBAC) matrix to enforce least privilege access to systems that contain user entity (customer) data.
    - 24x7 monitoring of all alerts generated by our systems, including system and security events.
    - Incident Management processes to detect, triage, and respond to security events.
    - A resilient design and architecture to ensure that our products are highly available, and recoverable in the event of a disaster.

Operational Overview

Hootsuite operates in three business segments: Security, Technology and Operations. Their responsibilities are defined as such:

- Security and Compliance – the Security team is committed to helping our customers protect their brand by ensuring that Hootsuite provides industry-leading security controls on its social relationship platform.
- Software Development – the Technology teams at Hootsuite build elegant solutions and lead the way in pioneering new social technologies.
- Production Operations and Delivery (POD) – the POD team is responsible for the administration and service management of Hootsuite systems worldwide.

Chief Technology Officer (CTO), in conjunction with the Security and Compliance team, helps to guide the strategic direction of security. Each segment is responsible for ensuring the confidentiality, availability, and integrity of Hootsuite's production systems.

Subservice Organizations

Hootsuite uses Amazon Web Services ("AWS") to host its cloud infrastructure, and MongoDB Atlas Cloud Service to host its MongoDB deployment. AWS is responsible for providing flexible, scalable, and secure datacenter infrastructure. This includes computing power, storage and other application services delivered over the Internet. AWS operates data centers across the world and is also responsible for the physical security and environmental controls within these data centers. MongoDB Atlas is a cloud-hosted Database-as-a-Service (DaaS) offering that is available on-demand. MongoDB Atlas enables users to set up, operate, and scale a MongoDB deployment in the cloud; therefore, allowing developers to focus on their core development while leaving database operations such as scaling, security, high availability, and other operations to be managed by MongoDB. MongoDB Atlas is hosted within the Amazon Web Services (AWS).

Customers can obtain further details of compliance and security of AWS and MongoDB Atlas Cloud Service via their websites at:

- https://www.mongodb.com/cloud/trust
- https://aws.amazon.com/compliance/
- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/gdpr-center/
- https://aws.amazon.com/compliance/shared-responsbility-model/
- https://aws.amazon.com/compliance/programs/

Complementary Subservice Organization Controls

Listed below are the Trust Services Criteria and illustrative controls that Hootsuite expects to be in place at AWS and MongoDB. Those complementary subservice organization controls, along with controls at Hootsuite, are necessary to achieve Hootsuite's service commitments and system requirements based on applicable trust services criteria.

TRUST SERVICES CRITERIA REF. (2017)	SUBSERVICE ORGANIZATION	EXPECTED CONTROLS
CC6.4, CC6.5, CC7.2	AWS, MongoDB	The subservice organization is responsible for maintaining controls over physical access to the facilities supporting Hootsuite's services. Additionally, it is responsible for maintaining controls for Hootsuite that address environmental threats including natural disasters and man-made threats.
CC7.2	AWS	The subservice organization is responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers and servers.
CC6.1, CC6.2, CC6.3, CC6.6, CC7.1, CC8.1	AWS	The subservice organization is responsible for maintaining controls that restrict access to the IaaS environment to authorized personnel.
CC8.1	AWS	The subservice organization is responsible for maintaining controls over the change management processes within the IaaS environment.
CC6.5, CC6.7	AWS	The subservice organization is responsible for maintaining controls over data management processes within the IaaS environment, including data redundancy and data protection.
CC6.5	AWS	The subservice organization is responsible for deleting information on the instances of the virtual server when the virtual server is terminated.
CC6.1, CC6.2, CC6.3, CC6.6	MongoDB	The subservice organization is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the services supporting Hootsuite.
CC8.1	MongoDB	The subservice organization is responsible for the maintenance and change management of the infrastructure and supporting systems that support its platform as a service where Hootsuite's MongoDB is hosted.
CC6.1, CC6.6, CC6.8, CC7.1, CC7.2	MongoDB	The subservice organization is responsible for antimalware protection related to Hootsuite's systems hosted on the subservice organization's platform.
CC6.1, CC6.6, CC6.7	MongoDB	The subservice organization is responsible for the encryption of data at rest and data in motion for Hootsuite's systems hosted on the subservice organization's platform.

TRUST SERVICES CRITERIA REF. (2017)	SUBSERVICE ORGANIZATION	EXPECTED CONTROLS
CC6.6, CC6.7	MongoDB	The subservice organization is responsible for the encryption of the Remote Desktop Connection used for administrator access to Hootsuite's systems hosted on the subservice org's platform services.
CC6.6, CC6.7	MongoDB	The subservice organization is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.
CC7.2	MongoDB	The subservice organization is responsible for geographic replication and backups for Hootsuite's systems hosted on the subservice org's platform services.
CC6.7	MongoDB	The subservice organization is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Hootsuite's system resides.

TABLE 1: COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Control Environment

Corporate governance

An experienced Board of Directors (hereafter referred to as “The Board”) governs Hootsuite’s strategic direction and operations. The Board is made up of independent members with a diverse portfolio of skills, knowledge and expertise in business and finance, and an understanding of the technology and social media landscapes to effectively guide andcontribute to Hootsuite’s continued development.

Employee commitment to Hootsuite’s values and ethics

Employees must acknowledge key policies or guidelines, such as the following:

- Code of Ethics – principles to guide employees on how to conduct business honestly and with integrity, and behaviors that embrace the organization’s core values and culture.
- Respectful Workplace Guidelines – outlines how employees must contribute to an environment of mutual respect, free of discrimination and harassment, in which all employees can advance and grow.
- Data Management Policy – enables consistent corporate-wide management of all information created, collected, stored, processed, transmitted, or disposed of by Hootsuite.

Operational management

Hootsuite’s Product, Development, and Technology (PDT) organization have adopted Operational Key Results (OKRs) to track ongoing progress against strategic goals.

Commitment to training and growth

The management of the PDT team has committed to ensuring that all staff have access to professional development opportunities. These include external training courses and conferences, as well as internal courses.

Executive support for security

Hootsuite is committed to information security management to ensure the confidentiality, integrity and availability of its data and systems. Management actively supports information security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.

This commitment is demonstrated through Hootsuite's establishment of a dedicated Security & Compliance team led by the Senior Director of Information Security. Further guidance is provided by the Information Security Steering Committee (ISSC), which is composed of Senior Executive Management. This council includes the following personnel and their delegates:

- Chief Financial Officer
- Senior Director of Information Security
- Chief Legal Officer
- Chief People & Diversity Officer
- Chief Technology Officer

The ISSC meets regularly and is governed by a formal charter. The committee's responsibilities include:

- Review and approval of Information Security/IT Policies
- Review of critical strategic and operational information security risks
- Monitoring of Security and Compliance KPIs
- Provide oversight and guidance for Information Security projects and initiatives
- Review of any security incidents

Security management

The Director of Information Security leads Hootsuite's Security & Compliance team. There are four distinct sub-teams:

- Security Architecture
- Security Development
- Security Incident Responses
- Security Governance, Risk, and Compliance (GRC)

Security Architecture

The Security Architecture team is responsible for reviewing new and current feature sets, network and application architectural designs, and vendor and partner risk review. The Architecture team works closely with various internal Hootsuite teams to ensure security is built into Hootsuite's product and platform.

Security Development

The Security Development team is responsible for the development, deployment and maintenance of security applications and tools. The team is also in charge of performing regular vulnerability reviews of Hootsuite's information technology infrastructure and deployed applications.

Security Incident Response

The Security Incident Response team handles the day-to-day monitoring and response of security incidents, including incident triage, investigation, documentation, and communication.

Security Governance, Risk, and Compliance (GRC)

The Security GRC team is responsible for defining, implementing, and managing the overall information security governance, risk management framework, and security policies for Hootsuite. The team maintains security compliance programs for various jurisdictions and coordinates the internal and external security audits.

Security Team Requirements

Employee positions related to security are supported by job descriptions that are defined and/or approved by the Director of Information Security. During the hiring process, Hootsuite's People Operations (Human Resources) and the Security & Compliance team will evaluate candidates on their ability to meet the requirements specified in the related job descriptions.

Human Resource Security

In the hiring process, candidates are evaluated for their abilities to perform the role described in the job description. This includes assessing candidates' information security knowledge and postures.

Criminal background checks are performed on new employees for the positions within the PDT organization or at above certain management levels as defined in the HR policies.

Communication and Information

Hootsuite uses various methods of internal communication to help employees understand their individual roles and responsibilities, and to communicate significant events in a timely manner. These methods include:

Our IT team is responsible for providing new employees with a general IT induction session.

The Security & Compliance team provides employees with general security and privacy awareness as part of their new hire orientation and is responsible for providing the detailed technical security orientation to newly hired employees joining Hootsuite's technical teams, such as Development and Operations.

The Security and Compliance team maintains pages on Hootsuite's internal collaboration platforms, using them to share links to general and role specific security guidance. These platforms, along with our corporate instant messaging tool, can be used to broadcast notifications to the entire company or select groups. Our staff can also use these tools to ask for advice or get help from the Security and Compliance team.

Hootsuite maintains a dynamic incident response team. In the event of a serious security incident, this team can be contacted by a variety of electronic means such as mobile alerts, email messages, and instant messaging channels. The Incident Response Team notifies and coordinates with any Customers whose account or access is affected. The Incident Response Team also establishes what level of wider internal notification is required.

Risk Assessment

The Hootsuite Security GRC team has placed into operation a risk assessment process to identify and manage risks that could affect Hootsuite's ability to provide services for its customers. The Risk Management process is defined in the Security Risk Management Policy and the accompanying Risk Framework.

Monitoring Activities

The Security GRC Team monitors the health of Hootsuite's security controls. This process, known as the Continuous Assessment Program (CAP), requires control owners to assess the performance of their security controls on a semi-annual basis.

The GRC team also supports internal testing of key controls related to security, operations, and development to validate adherence with the controls and policies relevant to the trust services criteria relevant to security set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Control Activities

Overview of governance, risk, and compliance

Hootsuite's internal controls are a set of processes and procedures with oversight by its board of directors, executive management team, and other personnel to provide reasonable assurance regarding the achievement of Hootsuite's objectives in security, operations, and governance, risk, and compliance.

The Hootsuite Security GRC team includes dedicated personnel whose mission is to provide objective assurance and consulting activities designed to add value and improve Hootsuite's operations. The scope of its charter is to determine whether Hootsuite's arrangement of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning as intended for all business units which includes Hootsuite's operations.

User access

User administration control processes and procedures exist and are followed to manage the authentication, authorization, and
appropriateness of users to key systems and applications including the set-up, maintenance, and termination of access privileges.

Network access

Inbound traffic to production networks is managed by Production Operations and Delivery personnel using Amazon EC2 Security Groups. For clarity, "inbound traffic" refers to IP network communication from the Internet addressed to our computing infrastructure.

Remote access via VPN to the production environment is restricted to only certain roles within Hootsuite.

Physical access

Hootsuite uses AWS to host its cloud infrastructure. Refer to the Complementary Subservice Organization Controls section for more details on AWS and physical access controls.

Secure configuration

Hootsuite's production servers, databases, and AWS Configuration is hardened in line with our internal configuration guidelines.

System performance monitoring

Hootsuite utilizes various tools, technologies, and procedures to monitor and evaluate the performance of our production services. The responsibility for ongoing monitoring, and acting on exceptions, is shared amongst various teams.

Security incident monitoring

Hootsuite has developed and deployed multiple security-monitoring tools which provide coverage and visibility over Hootsuite's technology infrastructure. A combination of commercial and customized tools is deployed to ensure the security and integrity of the Hootsuite production environment.

Software code changes

Hootsuite operates in an agile environment to develop, modify, test and release code into the production environment. Code change processes are based on the Change Management Policy. These processes are documented and communicated to necessary personnel by Development teams.

Infrastructure changes

Hootsuite has adopted DevOps practices, which help increase the number of new features and fixes that can be deployed to our product daily. DevOps practices allow us to remove some of the

bottlenecks associated with a traditional Operations environment.

Vendor risk assessments

Hootsuite has implemented a robust procurement process that ensures vendors are formally engaged and reviewed. This process, which is coordinated by the Procurement Team, includes risk assessments from the Security GRC Team, IT Team, and additional advice from the Legal Team.

Complementary User-Entity Controls (CUEC)

User organizations are responsible for establishing their own system of internal control and enforcing those controls within their environment. Those complementary user-entity controls, along with controls at Hootsuite, are necessary to achieve Hootsuite's service commitments and system requirements based on applicable trust services criteria. User organizations should review the complementary user-entity controls and their importance in meeting the applicable Trust Services criteria to which they relate.

CUEC REF	COMPLEMENTARY USER-ENTITY CONTROLS	TRUST SERVICES CRITERIA REF. (2017)
1	The user organization is responsible for ensuring the use of Hootsuite Dashboard, Amplify, and Mobile Application complies with the organization's internal policies and procedures, applicable laws and regulations. Further, the user organization is responsible for the accuracy, quality, integrity and legality of the information posted via Hootsuite Dashboard, Amplify, and Mobile Application.	CC1.3, CC1.5, CC2.3, CC6.7, CC8.1
2	The user organization is responsible for adhering to the terms and conditions of the Supported Third-Party platforms, including but not limited to the user organization's social network accounts, social network sites that it connects to through Hootsuite Dashboard, Amplify, and Mobile Application.	CC2.2, CC2.3, CC6.1, CC6.2
3	The user organization is responsible for ensuring that internal processes are in place for requesting account creations and account upgrades performed during Hootsuite's customer onboarding.	CC2.3, CC6.1, CC6.2
4	The user organization is responsible for ensuring that internal processes are in place to make requests for password resets, account creations, modifications, and terminations. These requests can only be submitted to Hootsuite by authorized and current user organization's contacts recorded in Hootsuite's customer management system.	CC6.1, CC6.2, CC6.3, CC8.1
5	The user organization is responsible for ensuring that any credentials (usernames, passwords, API Keys) used to access the Hootsuite Dashboard are kept secure. This includes access to the dashboard via Single Sign-On (authentication using the customer's internal corporate credentials) or through Social Login (authentication that uses a customer's, or their users', social media credentials). Multifactor authentication (MFA) should be used to further secure user access to the Hootsuite Dashboard.	CC6.1
6	The user organization is responsible for ensuring that access to the Hootsuite Dashboard, Amplify, and Mobile Application is restricted to authorized users. This includes ensuring that access of terminated employees is removed on a timely basis and that periodic review of access is performed. The user organization is responsible for submitting any changes to the list of authorized users to Hootsuite, if needed.	CC6.1, CC6.2, CC6.3, CC6.6, CC8.1

CUEC REF	COMPLEMENTARY USER-ENTITY CONTROLS	TRUST SERVICES CRITERIA REF. (2017)
7	The user organization is responsible through their use of the administrative functions on the Hootsuite Dashboard, Amplify, and Mobile Application for ensuring the configuration is reviewed on a periodic basis. This includes periodic review of any applications (for example, applications from the Hootsuite App Store) authorized for use via the Hootsuite Dashboard, Amplify, and Mobile Application, and managing the multi-factor authentication settings.	CC6.1, CC6.2, CC6.3, CC6.6, CC6.8
8	The user organization is responsible for promptly notifying their Hootsuite Customer Success Manager, or Hootsuite Support of a suspected or actual security breach including loss, theft or unauthorized disclosure or use of the customer's (or, an authorized user's) password or account.	CC2.2, CC2.3, CC7.3
9	The user organization is responsible for ensuring its employees attend the provided training on how to use Hootsuite Dashboard, Amplify, and Mobile Application.	CC1.4
10	The user organization is responsible for imposing appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. For clarity, the user organization understands and agrees that persons authorized to post or otherwise process Customer Content on the user organization's instance of Hootsuite Dashboard, Amplify, and Mobile Application have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality with respect to that Customer Content[1].	CC1.1
11	The user organization has taken steps to understand how the use of a social media management platform may affect their risk management practices, and adjusted their control environment appropriately.	CC3.2, CC3.3, CC4.1, CC4.2, CC5.1, CC5.2, CC7.2, CC8.1
12	The user organization is responsible for ensuring they are using a supported Web Browser with all current security patches and updates applied.	CC7.2, CC8.1
13	The user organization is responsible for promptly notifying their Hootsuite Customer Success Manager or Hootsuite support of any security flaws or vulnerabilities it identifies in any Hootsuite product or service.	CC2.2, CC2.3, CC8.1

TABLE 2: COMPLEMENTARY USER ENTITY CONTROLS

[1] Please see the Hootsuite SaaS Agreement for the complete definition of "Customer Content"