



## **SOC 2 REPORT**

FOR

ZSCALER CLOUD PLATFORM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS  
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

FEBRUARY 1, 2018, TO MARCH 31, 2019

Attestation and Compliance Services



This report is intended solely for use by the management of Zscaler, Inc., user entities of Zscaler, Inc.'s services, and other parties who have sufficient knowledge and understanding of Zscaler, Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

# TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT .....	1
SECTION 2	MANAGEMENT'S ASSERTION .....	5
SECTION 3	DESCRIPTION OF THE SYSTEM .....	7
SECTION 4	TESTING MATRICES .....	26

# **SECTION I**

## **INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Zscaler, Inc.:

### Scope

We have examined Zscaler, Inc.'s ("Zscaler" or the "service organization") accompanying description of its Zscaler Cloud Platform system, in Section 3, throughout the period February 1, 2018, to March 31, 2019, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2018, to March 31, 2019, to provide reasonable assurance that Zscaler's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

### Service Organization's Responsibilities

Zscaler 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 Zscaler's service commitments and system requirements were achieved. Zscaler has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Zscaler is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

### Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;

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

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

### *Inherent Limitations*

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

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

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

### *Description of Test of Controls*

The specific controls we tested and the nature, timing, and results of those tests are presented in section 4 of our report titled "Testing Matrices."

### *Opinion*

In our opinion, in all material respects,

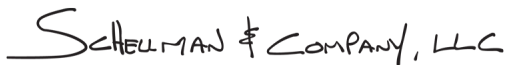
- a. the description presents Zscaler's Cloud Platform system that was designed and implemented throughout the period February 1, 2018, to March 31, 2019, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period February 1, 2018, to March 31, 2019, to provide reasonable assurance that Zscaler's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Zscaler's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period February 1, 2018, to March 31, 2019, to provide reasonable assurance that Zscaler's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Zscaler's controls operated effectively throughout that period.

### *Restricted Use*

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Zscaler; user entities of Zscaler's Cloud Platform system during some or all of the period February 1, 2018, to March 31, 2019, business partners of Zscaler subject to risks arising from interactions with the Zscaler Cloud Platform system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

SCHILLMAN & COMPANY, LLC

Tampa, Florida  
May 30, 2019

## **SECTION 2**

### **MANAGEMENT'S ASSERTION**



## MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Zscaler's Cloud Platform system, in Section 3, throughout the period February 1, 2018, to March 31, 2019, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Zscaler Cloud Platform system that may be useful when assessing the risks arising from interactions with Zscaler's system, particularly information about system controls that Zscaler has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

- a. the description presents Zscaler's Cloud Platform system that was designed and implemented throughout the period February 1, 2018, to March 31, 2019, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period February 1, 2018, to March 31, 2019, to provide reasonable assurance that Zscaler's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations assumed in the design of Zscaler's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period February 1, 2018, to March 31, 2019, to provide reasonable assurance that Zscaler's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Zscaler's controls operated effectively throughout that period.

# SECTION 3

## DESCRIPTION OF THE SYSTEM

## OVERVIEW OF OPERATIONS

### Company Background

Zscaler, Inc. (“Zscaler” or “the Company”) was incorporated in 2007, during the early stages of cloud adoption and mobility, based on a vision that the internet would become the new corporate network as the cloud becomes the new data center.

Enterprise applications are rapidly moving to the cloud to achieve greater information technology (IT) agility, a faster pace of innovation, and lower costs. Organizations are increasingly relying on internet destinations for a range of business activities, adopting new external Software as a Service (SaaS) applications for critical business functions and moving their internally managed applications to the public cloud, or Infrastructure as a Service (IaaS). Enterprise users now expect to be able to seamlessly access applications and data, wherever they are hosted, from any device, anywhere in the world. Zscaler believes these trends are indicative of the broader digital transformation agenda, as businesses increasingly succeed or fail based on their IT outcomes.

Zscaler believes that securing the on-premises corporate network to protect users and data is becoming increasingly irrelevant in a cloud and mobile-first world where organizations depend on the Internet, a network they do not control and cannot secure, to access critical applications that power their businesses. Zscaler pioneered a new approach to security that connects the right user to the right application, regardless of network. Zscaler’s Cloud Platform, which delivers security as a service, eliminates the need for traditional on-premises security appliances that are difficult to maintain and require compromises between security, cost, and user experience. Zscaler’s cloud platform incorporates the security functionality needed to enable users to safely utilize authorized applications and services based on an organization’s policies. Zscaler’s solution is a purpose-built, multi-tenant, distributed cloud security platform that secures access for users and devices to applications and services, regardless of location.

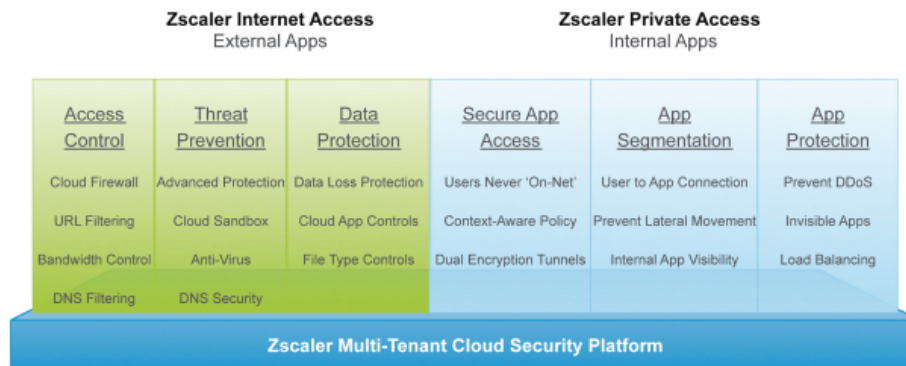
### Description of Services Provided

The Zscaler Cloud Platform consists of Zscaler Internet Access (“ZIA”), Zscaler Private Access (“ZPA”), and Zscaler Shift (collectively referred to as the “Cloud Platform”).

Zscaler is a cloud-based information security platform, which is distributed across more than 100 data centers around the world, that helps organizations accelerate their IT transformation to the cloud. This enables the secure migration of applications from the corporate data center to the cloud and from a legacy “hub-and-spoke” network to a modern direct-to-cloud architecture. Zscaler’s approach applies policies set by an organization to securely connect the right user to the right application, regardless of the network. Unlike traditional “hub-and-spoke” architectures, where traffic is backhauled over dedicated wide area networks (WANs) to centralized gateways, Zscaler’s solution allows traffic to be routed locally and securely to the Internet over broadband and cellular connections.

#### Zscaler Cloud Platform

Zscaler’s purpose-built cloud security platform offers two principal services built natively in the cloud.



## Secure Access to the Internet and Applications



### Zscaler Internet Access

Zscaler's ZIA solution securely connects users to externally managed applications, including SaaS applications and internet destinations, regardless of device, location or network. Zscaler's ZIA solution sits between users and the Internet and is designed to ensure malware does not reach the user and valuable corporate data does not leak out. Zscaler's ZIA solution enforces access based on granular access control policies, inspects unencrypted and encrypted internet traffic inline for malware and advanced threats, and prevents data leakage.

Policies follow the user to provide identical protection on any device, regardless of location; any policy changes are enforced for users worldwide. Zscaler's cloud security platform provides full inline content inspection of webpages to assess and correlate the risk of webpage objects, continuously discovering and blocking sophisticated threats.

Zscaler's ZIA solution includes broad functionality, which Zscaler categorize by three areas:

#### *Access Control*

The access control functionality of Zscaler's ZIA solution enforces access and usage policies to externally managed applications, including SaaS application and internet destinations. This provides functionality that has traditionally been provided by stand-alone point products, such as:

- **Cloud Firewall:** Zscaler's cloud firewall was designed to protect users by inspecting internet traffic on all ports and protocols, and it offers user level policies, application identification with deep packet inspection and intrusion prevention.
- **URL Filtering:** Zscaler's URL filtering capabilities enable customers to enforce acceptable usage policies and protects organizations from users visiting unauthorized websites or illegally downloading content that can increase liability and impact their brand.
- **Bandwidth Control:** Zscaler's bandwidth control and traffic shaping capabilities ensure that business critical applications are prioritized over non-business critical applications, improving productivity and user experience. By enforcing quality of service in the cloud, Zscaler's platform can optimize "last-mile" utilization of a customer's network, providing significant value.
- **Domain Name System (DNS) Filtering:** Zscaler's DNS filtering solution provides a local DNS resolver and enforces acceptable use policies.

## Threat Prevention

Zscaler's second area of functionality, threat prevention, protects users from threats using a range of approaches and techniques. Zscaler's threat prevention capabilities provide multiple layers of protection to prevent cyberattacks. Zscaler provides functionality that has traditionally been offered by disparate, stand-alone products, which are summarily described below:

- **Advanced Threat Protection:** Zscaler's advanced protection solution delivers real-time protection from malicious internet content like browser exploits, scripts, zero-pixel iFrames, malware and botnet callbacks. Over 120,000 unique security updates are performed each day to the Zscaler cloud to keep users protected. Once Zscaler detects a new threat to a user, Zscaler block it for all users. Zscaler calls this the "cloud security effect." Advanced threat protection features include:
  - **Botnet Protection:** protection against botnets that could be secretly installed on user devices to perform malicious tasks at the instruction of command and control servers.
  - **Malicious Active Content Protection:** protection against websites that attempt to download dangerous content to a user's web browser.
  - **Fraud Protection:** protection against phishing sites that mimic legitimate sites, such as banking and e-commerce sites, in order to steal confidential information.
  - **Cross-Site Scripting (XSS) Protection:** protection against XSS, in which malicious code injected into websites is downloaded to a user's web browser from compromised web servers.
  - **Suspicious Destinations Protection:** block requests to any country based on ISO3166 mapping of countries to their IP address space. Websites are blocked based on the location of the web server.
  - **Unauthorized Communication Protection:** protection against communications like internet relay chat (IRC) tunneling applications and "anonymizer" sites that are used to bypass firewall access and proxy security controls.
  - **P2P Anonymizer Protection:** block anonymizing applications such as Tor, an application that enables users to bypass policies controlling what websites they may visit or internet resources they may access.
- **Cloud Sandbox:** Zscaler's cloud sandbox enables enterprises to block zero-day exploits and advanced persistent threats (APTs), by analyzing unknown files for malicious behavior, and can scale to every user regardless of location. Zscaler's sandbox was designed and built to be multi-tenant and allows customers to determine which traffic should be sent to the cloud sandbox. As an integrated cloud security platform, customers can set policies by users and destinations to prevent patient-zero scenarios by holding, detonating and analyzing suspicious files in the sandbox before being sent to the user.
- **Anti-Virus:** Zscaler's anti-virus technology uses a signature database of files and objects on the Internet known to be unsafe and runs traffic through multiple anti-virus engines in a single pass.
- **DNS Security:** Zscaler's DNS security blocks access to known malicious sites, including command and control sites, and routes suspicious traffic to Zscaler's threat detection engines for content inspection.

## Data Protection

Zscaler's third area of functionality, data protection, prevents unauthorized sharing or exfiltration of confidential information, reducing Zscaler's customers' business and compliance risk.

- **Data Loss Protection:** Zscaler's data loss protection enables enterprises to use standard or custom dictionaries using efficient pattern-matching algorithms to easily scale to all users and traffic, including compressed or encrypted traffic, to prevent, monitor or block unauthorized or sensitive data exfiltration.
- **Cloud Application Control:** Zscaler's cloud application control allows enterprises to discover and granularly control user access to known and unknown cloud applications. By doing secure sockets layer (SSL) interception at scale, Zscaler provide malware protection, data loss prevention and similar cloud access security broker (CASB), functions that can be performed inline, for specific sanctioned applications. Business policies can be defined with granular access control for specified cloud applications, such as the ability to upload or download files or post comments or videos based on

different user or group identity. Zscaler partners with specific CASB vendors to extend their policy controls and visibility of out-of-band cloud applications.

- File Type Controls: Zscaler's file type control allows policies to be defined that control which file types are allowed to be downloaded and uploaded based on application, user, location, and destination.

### Zscaler Private Access

Zscaler's ZPA solution offers authorized users secure and fast access to internally managed applications hosted in enterprise data centers or the public cloud. Zscaler's ZPA solution's architecture does not expose the identity or location of these applications and provides only the necessary and appropriate levels of access. While traditional remote access solutions, such as Virtual Private Networks (VPNs), connect a user to the corporate network, Zscaler's ZPA solution connects a specific user to a specific application, without bringing the user on the network, resulting in better security. Zscaler's ZPA Solution was designed around Zscaler's key tenants that fundamentally change the way users access internal applications:

- Connect users to applications without bringing users on the network;
- Never expose applications to the Internet;
- Segment access to applications without relying on traditional approach of network segmentation; and
- Provide remote access over the Internet without VPNs.

Zscaler's ZPA solution enforces a global policy engine that manages access to internally managed applications regardless of location. If access is granted to a user, Zscaler's ZPA solution connects the user's device only to the authorized application without exposing the identity or location of the application. Hence applications are not exposed to the Internet, further limiting threat exposure. This results in reduced cost and complexity, while offering better security and an improved user experience. ZPA functionality falls in three major areas:

- Secure Application Access: Zscaler's ZPA Solution delivers seamless connectivity to internally managed applications and assets whether they are in the cloud, enterprise data center, or both. Administrators can set global policies from a single console, enabling policy-driven access that is agnostic to the network the users are on. By creating seamless access to applications regardless of a user's network, Zscaler's ZPA solution subsumes the need for traditional remote access VPNs, SSL VPNs, reverse proxies and other similar products.
- Application Segmentation: This architecture provides capabilities that enables user and application level segmentation. As each user-to-application connection is segmented with micro-tunnels, each of which is a temporary session between a specific user and a specific application, lateral movement across the network is prevented which significantly reduces security risk. Similar to CASB application discovery reports for internet applications, Zscaler's ZPA Solution provides granular discovery of internally managed applications to aid the creation of segmentation policies. Because Zscaler's ZPA solution sits on the application layer and is name or domain-based, organizations can quickly and easily identify the internally-managed applications that are running and then easily provision appropriate policies. Micro-tunnels subsume the need for internal firewalls, which are required for protecting against lateral malware propagation from machine to machine, and traditional network access control functionality since users are granted access only to applications for which they have permission and are not granted full access to the network.
- Application Protection: Zscaler's ZPA solution initiates and connects together outbound-only links between authenticated users and internally managed applications using micro-tunnels. Access is provided to users without bringing them onto the corporate network and without exposing applications to the Internet. Internally managed applications are not discoverable or identifiable. With no inbound connections and no public IP addresses, there is no inbound attack surface and therefore no threat of distributed denial of service (DDoS) attacks. With Zscaler's approach, Zscaler subsumes the need for a next-generation firewall. Similarly, by completely removing the need for an exposed IP address or DNS to the Internet, Zscaler subsumes the functionality of DDoS mitigation systems.

### Zscaler Shift

Zscaler's Zscaler Shift solution provides carrier-grade security and compliance for guest networks and open public wi-fi access. Zscaler's Shift solution offers multiple security features including content filtering, threat

security, safe search, and SSL inspection. Additionally, Zscaler's Shift solution intelligently routes suspicious traffic to the Zscaler Cloud Platform for full in-line content inspection. Zscaler's Advanced Threat Protection blocks malicious active content, such as browser exploits, vulnerable ActiveX controls, malicious JavaScript, and cross-site scripting.

Security Features provided by Shift to implement an enterprise's policies include the following:

- Content Filtering
- Threat Security
- Safe Search
- SSL Inspection
- Whitelisting and Blacklisting URLs
- Shift Administration

---

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Zscaler designs its processes and procedures related to the Zscaler Cloud Platform system to meet its objectives for its Zscaler Cloud Platform services. Those objectives are based on the service commitments that Zscaler makes to user entities, the laws and regulations that govern the provision of the Zscaler Cloud Platform services, and the financial, operational, and compliance requirements that Zscaler has established for the services. The Zscaler Cloud Platform services are subject to the relevant regulatory and industry information and data security requirements in which Zscaler operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the following Zscaler documents which are available online: End User Subscription Agreement (EUSA) along with the accompanying Products Sheets and Service Level Agreements (SLAs) and Data Processing Agreement (DPA).

The principal security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Maintain administrative, physical, and technical safeguards designed for the protection, confidentiality, and integrity of customer data.
- Complete annual third-party security and compliance audits of the environment, including, but not limited to, the following:
  - Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) examinations.
  - International Organization for Standardization (ISO) 27001:2013 certification reviews.
- Maintain an availability service level agreement for customers of 99.999% measured monthly.

Additionally, Zscaler maintains the following procedures, policies, and controls as part of the Zscaler Cloud Platform services:

- Maintain multiple, geographically-separated data centers providing data mirroring, disaster recovery, and failover capabilities.
- Continuously monitor the production environment via network security controls designed to identify malicious traffic.
- Performance of region specific mandatory background screening and segregation of duties.
- Transmission of users' unique login credentials, as well as data in the resultant connection, via encrypted connections.



- Implemented role-based access permissions for customers.
- Retain customer data for the duration of contracted services and as needed to fulfill the applicable business purposes and securely disposes of customer data as set forth in the EUSA and DPA.

Zscaler establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. This includes the use of encryption technologies to protect system user data both at rest and in transit; database management processes to ensure databases are maintained and monitored for performance; and necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Zscaler Cloud Platform.

In accordance with Zscaler's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system, and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

---

## COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

### System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

### Infrastructure and Software

#### *Zscaler's Technology and Architecture*

Zscaler built a highly scalable, multi-tenant, globally distributed cloud capable of providing inline inspection that offers a full range of enterprise network security services. Zscaler designed a purpose-built three-tier architecture starting with Zscaler's core operating system and adding layers of security and networking innovations over time. Zscaler's Cloud Platform is protected by more than 100 issued and pending patents.

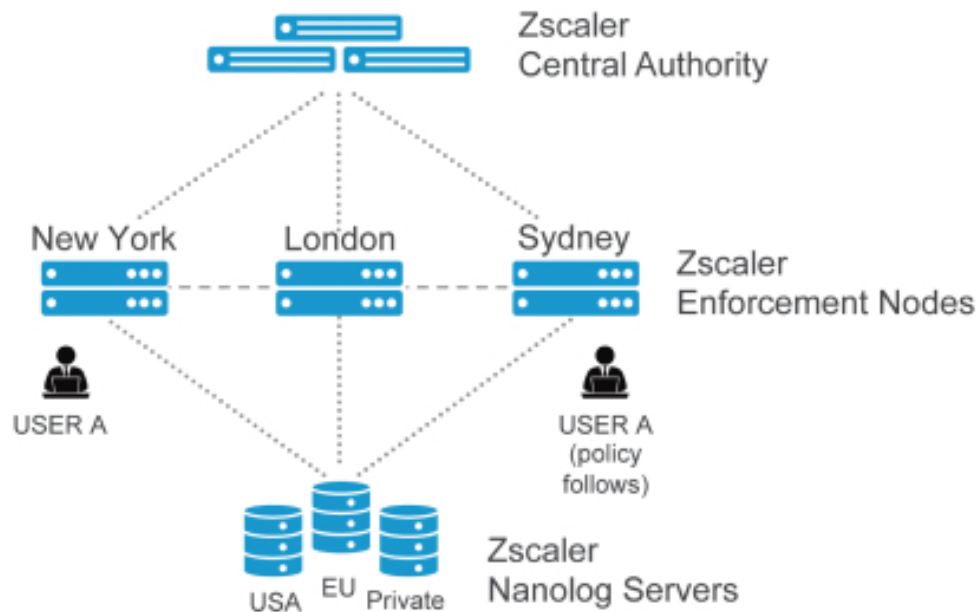
#### *Proprietary Multi-tenant Global Cloud Architecture:*

Zscaler developed a proprietary security cloud that provides policy-based access to internet, SaaS and internally managed applications. Zscaler's cloud is distributed across more than 100 data centers on five continents. The platform is designed to be resilient, redundant, and high-performing.

[Intentionally Blank]



Zscaler's platform is built as software modules that run on standard x86 platforms without any dependency on custom hardware. The platform modules are split into the control plane (Zscaler Central Authority), the enforcement plane (Zscaler Enforcement Nodes) and the logging and statistics plane (Zscaler Nanolog Servers) as described below:

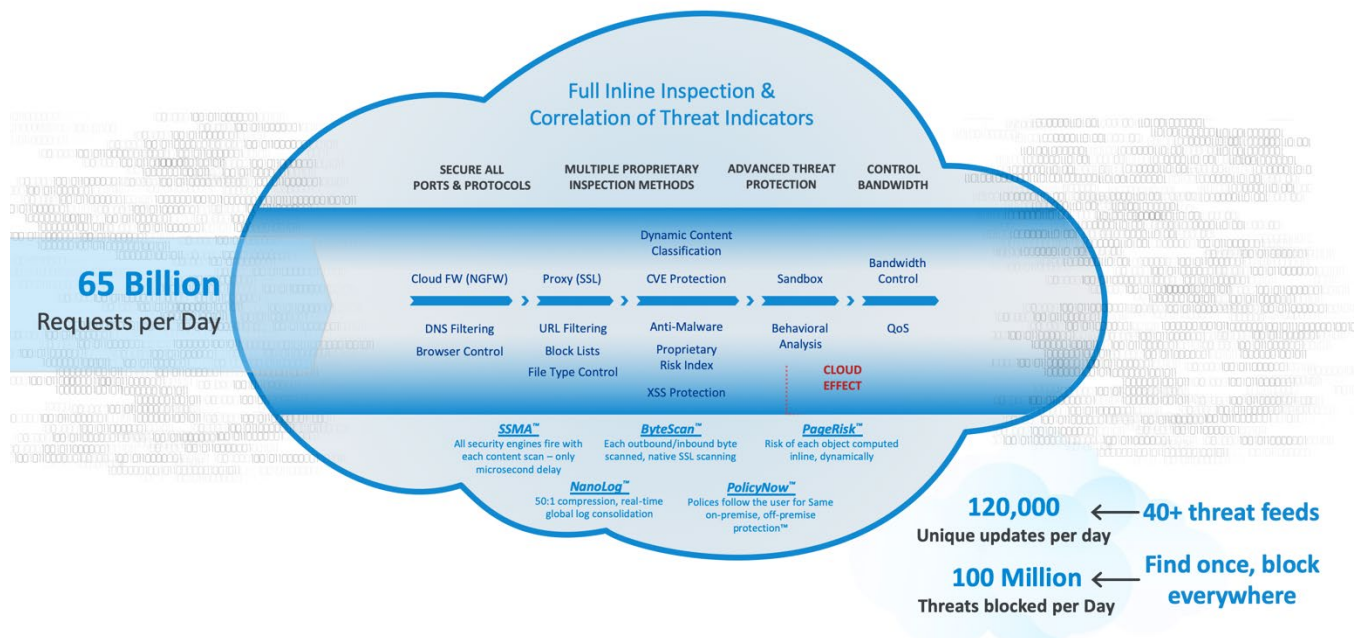


#### Zscaler Proprietary Multi-Tenant Global Cloud Architecture

- **Zscaler Central Authority:** The Zscaler Central Authority monitors Zscaler's security cloud and provides a central location for software and database updates, policy and configuration settings and threat intelligence. The collection of Zscaler Central Authority instances together act like the brain of the cloud, and they are geographically distributed for redundancy and performance.
- **Zscaler Enforcement Nodes:** Customer traffic gets directed to the nearest Zscaler Enforcement Node, where security, management and compliance policies served by the Zscaler Central Authority are enforced. The Zscaler Enforcement Node also incorporates Zscaler's differentiated authentication and policy distribution mechanism that enables any user to connect to any Zscaler Enforcement Node at any time to ensure full policy enforcement. The Zscaler Enforcement Node utilizes a full proxy architecture and is built to ensure data is not written to disk to maintain the highest level of data security. Data is scanned in random access memory (RAM) only and then erased. Logs are continuously created in memory and forwarded to Zscaler's logging module.
- **Zscaler Nanolog Servers:** Zscaler's Nanolog technology is built into the Zscaler Enforcement Node to perform lossless compression of logs, enabling Zscaler's platform to collect over 30 terabytes of unique raw log data every day. Logs are transmitted to Zscaler's Nanolog Servers over secure connections and multicast to multiple servers for redundancy. Zscaler's dashboards provide visibility into Zscaler's customer's traffic to enable troubleshooting, policy changes and other administrative actions. Zscaler's analytics capabilities allow customers to interactively mine billions of transaction logs to generate reports that provide insight on network utilization and traffic. Zscaler does not rely on batch reporting. Zscaler continuously updates Zscaler's dashboards and reporting and can stream logs to a third-party security information and event management (SIEM) system as they arrive. Regardless of where users are located, customers can choose to have logs stored in the United States, the European Union, or Switzerland.

[Intentionally Blank]

## Advanced Cloud-Based Security Capabilities



### Single-Pass, Inline Multi-Action Architecture for Better Security

- **ByteScan™ Technology:** ByteScan provides fast content scanning for detection of malicious sites and content, zero-day attacks and data loss prevention. Zscaler's proprietary network stack enables interception of SSL traffic and can be integrated with a customer's public key infrastructure service, which manages encryption policies. ByteScan does not rely on traditional signature analysis.
- **SSMA™ Technology:** Zscaler's Single-Scan, Multi-Action (SSMA) technology allows inspection engines to scan content in a single pass. This approach is starkly different from the chained model of physical or virtual appliances, whereby each security service independently processes packets, adding incremental latency at each hop. Due to Zscaler's SSMA technology, Zscaler's platform is able to apply policy-based security measures on a variety of security engines with minimal latency. SSMA also enables Zscaler's solution to be an extensible platform to add new technologies as security intelligence and research advances.
- **PageRisk™ Technology:** Beyond identifying known or zero-day threats, Zscaler's PageRisk technology generates a Page Risk Index, which is a dynamically computed risk score based on potential indicators of compromise on objects in a file or a webpage. Zscaler dynamically computes the risk of webpage objects inline, checking for threats such as injected scripts, vulnerable ActiveX objects and zero-pixel iFrames, among others, as well as domain information. This ensures that unknown malware on well-reputed sites can be identified before harming users.
- **PolicyNow™ Technology:** PolicyNow technology ensures that policies follow the user. Any user of any organization can connect to a node in any geography. This provides protection regardless of the user location and also ensures global resiliency for Zscaler's cloud. Even if multiple data centers lose power or become unavailable, users can connect to the next closest node, and Zscaler's platform can continue to provide uninterrupted services.

All hub data centers are certified as ISO 27001, SOC 2 or a similar local certification as applicable. The Cloud Platform servers consist of Linux and Unix based Operating Systems.

[Intentionally Blank]

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
Z-admin Portal	Customer access management tool	Zscaler Operating System (ZOS) and Linux-based OS	Multiple third-party data center providers
Atlantic	Customer access management tool		
Amazon Web Services (AWS) Identity and Access Management (IAM) Console	Allows system administrators to manage and maintain the in-scope servers, database, and services		AWS
Production Servers	Linux servers supporting the in-scope systems		Multiple third-party data center providers
Databases Servers	Databases supporting the logics of the in-scope systems		
Zscaler Private Access technology for remote Administration	Provide remote access to the in-scope systems with multi-factor authentication		

## People

Employees supporting day-to-day activities include the following:

- **Management** – Management is responsible for overall security, ensuring enforcement of controls, change approvals, risk assessment, selection and prioritization for mitigation, and providing oversight of the Zscaler Cloud Platform control environment. Management's role is to ensure personnel are appropriately trained, and that systems and processes are in place to meet system uptime, system-wide security, and consistent service execution. This includes the chief technology officer who oversees all engineering organizations, the Senior vice president of operations who is responsible for all operational aspects of the service, and the Senior vice president of engineering who is responsible for the development of the service. Management is responsible for ensuring risk assessments are performed annually and periodically review the status of cloud security posture based on inputs from internal auditing and event-based activities.
- **Network Operations Center (NOC)** – The NOC is responsible for monitoring operations of the Zscaler Cloud Platform environment. They are also responsible for responding to alerts generated by monitoring systems based on operational triggers and first tier response to incidents. The NOC is responsible for monitoring problems or incidents and ensuring that they are resolved in a timely manner. The NOC team is manned 24x7 with employees across the globe.
- **Security Operations Center** – Zscaler's global Security Operations Center consists of a Computer Emergency Readiness Team (CERT) and a ThreatLabZ team (Zscaler's research and development security lab). The CERT Team and ThreatLabZ team are responsible for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.
- **Operations** – The Operations team consists of system engineering, networking, and program management teams responsible for provisioning and deploying the cloud environment to its production ready state before turning it over to the NOC for continuous monitoring. This includes all aspects of deployment to production as per the design for both public and private service deployments. The Operations team is also responsible for access management to the cloud production environment.

- Cloud Deployment and Change Management – Cloud Deployment and Change management teams are responsible for managing changes to the production environment. Changes to the production environment follow standard Zscaler service continuity customer notification protocol and production changes are documented, reviewed, approved, and tracked via the internal ticketing system before implementation.
- Engineering – The Engineering team is responsible for development of core services, applications, and service patches, as well as third tier response to service issues.
- Customer Care – The Customer Care team is responsible for fielding customer calls regarding cloud environments, triaging of customer reported issues, and initiating internal tickets for resolution by engineering and operations as required and communicating with customers regarding any scheduled or unscheduled outages or issues through the Zscaler Technical Assistance Center (ZTAC).

## **Procedures**

### *Access Authentication and Authorization*

Access to system information, including confidential information, is protected by authentication and authorization mechanisms. The operations and security teams are responsible for assigning and maintaining access rights to the production environment. In order to gain access to the production environment, a user must authenticate first via VPN, then via secure shell (SSH) in order to enforce public-private key authentication. In addition, administrative access privileges within the production environment are restricted to authorized personnel. ZPA production resources are AWS security rulesets designed to filter unauthorized Internet traffic and to deny any activity not previously defined. Furthermore, AWS Elastic Cloud Compute (EC2) security groups are utilized to filter unauthorized inbound and outbound network traffic from the Internet.

### *Access Requests and Access Revocation*

Management has established controls to ensure that access to confidential data is restricted to those who require access. A formal process has been established for managing user accounts and controlling access to Zscaler's resources within the production environment. New employees are granted a standard level of access based on their job role. Prior to granting an individual access above the standard level of access provided upon employment, the access request must be reviewed and approved by the employee's manager.

Upon notification of an employee termination, human resources (HR) personnel create a termination checklist which is shared with the IT department to ensure that employees do not retain system access subsequent to their termination date. Management requires access requests and access revocations to be formally documented to ensure activities are completed for the addition, modification, and revocation of system and software access privileges. On a quarterly basis, Zscaler security and IT teams perform a user access review to verify users with access to the production systems are authorized.

### *Change Management*

Zscaler maintains documented application and infrastructure change management policies and procedures to communicate the company's expectations regarding the change management process to Zscaler personnel, and to ensure that any unauthorized changes are not made to production systems. The cloud engineering teams meet on a weekly basis to discuss and communicate current and upcoming changes and their effects on the system. The change management process adds oversight, visibility, and control of changes to the Zscaler production environment.

Changes are documented and tracked using an automated ticketing system which serves as the system of record for managing the change process. These changes may impact systems, applications, systems software, network, or any other aspect of the information processing environment. Source code is stored within a version control system and access to the source code is restricted to authorized personnel. Changes must follow a formal approval process prior to implementation. Changes to operating systems, and system/application software are authorized, tested and approved by authorized personnel prior to implementation. Changes to system infrastructure and system/application software are developed and tested in a separate environment before being implemented into staging or production. The ability to migrate changes into production environments is restricted to authorized personnel. Emergency changes are subject to the same change management requirements related

to peer review, quality assurance (QA) testing, and approval; however, a postmortem approval may be required depending on the severity of the change.

File integrity monitoring tools are utilized to monitor, detect, and alert the information security team, and track alerts through to resolution when unauthorized software installations or configuration changes to certain production systems occur. In an effort to protect production data, production data is not utilized for change development and testing efforts.

#### *Data Backup and Disaster Recovery*

Production servers supporting the ZIA are hosted and replicated across global third-party data center providers. ZPA production servers are hosted within AWS. Documented policies and procedures are in place governing data backup and restoration processes.

#### *Realtime Replications*

Automated replication systems are configured to perform near real-time replication of client data from the production application servers to replication data storage servers distributed across global third-party data center facilities (for ZIA), and AWS (for ZPA). The automated replication systems are configured to send e-mail notifications to operations personnel regarding the site replication when replication issues are identified. Operations personnel review the replication e-mail notifications for any issues through to resolution. Physical access to the aforementioned third-party data centers are restricted to authorized personnel based on their job responsibilities via a badge access card system. IT and operations management are responsible for approving access requests to the data centers.

#### *Data Restorations and Disaster Recovery*

As a part of Zscaler's business continuity and disaster recovery program for the production environment and platforms, Zscaler maintains an up-to-date business continuity and disaster recovery plan and conducts disaster recovery exercises at least once per year. Operations personnel perform data restoration tests on an annual basis to help ensure the recoverability of production data which are done in tandem with the disaster recovery process. Internal production data is used for restoration tests and is intended to simulate real situations as much as practical. Upon completion of the restore, the operations personnel test and verify that the data restoration is successful. Results of the data restoration efforts are maintained within the automated ticketing system. The testing includes confirming that the account and its data can be accessed, is validated against the source, and appears accurate once restored.

#### *System Availability and Uptime*

Zscaler has documented incident response procedures in place to address operational requirements for the response and resolution of incidents. Internal and external monitoring tools are configured to monitor production servers and network devices for unplanned downtimes which may be the result of various system performance and availability metrics related to network and firewall availability, central processing units (CPUs), process load, and server utilization. The enterprise monitoring tools are configured to send alert notifications in the event that predefined thresholds are exceeded. An incident ticketing system is utilized to log and track system incidents through to resolution. Details are captured within the incident ticket to include service impact, root cause, and steps taken to resolve the issue. Support personnel may also generate incident reports to support post-incident responsibilities and review preventative measures for recurrence and monitoring. A NOC team is in place to monitor the enterprise monitoring applications for any events 24 hours per day, seven days a week, 365 days per year.

In addition to receiving the incident reports from support, internal and external monitoring systems are configured to monitor and notify operations personnel of unplanned downtime events. An external system is employed to check connectivity and application responsiveness. Internally implemented monitoring tools are configured to monitor for server responsiveness and notify operations personnel in the event of an unplanned downtime. Additionally, external users (i.e. customers) have the ability to report incidents on a public-facing portal which feeds into Zscaler's automated ticketing system to track resolution efforts.

System status, including scheduled maintenance and known issues, are displayed on the Zscaler trust page available at [trust.zscaler.com](https://trust.zscaler.com).



*Incident Response*

Incident response and escalation policies and procedures are documented to manage unexpected incidents that interrupt normal business functions. Events are tracked using a ticketing system and follow the same general process of classification, prioritization and remediation.

*System Monitoring*

Zscaler monitors the daily business and operational activities, including the internal control environment, as a routine part of business. Zscaler has implemented a set of logging and monitoring tools that are configured to collect data from system infrastructure components to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT operations upon detection of unusual system activity or service requests.

The in-scope systems are monitored using enterprise monitoring applications that track system performance, responsiveness, availability and vulnerabilities. The enterprise monitoring applications are monitored by IT personnel in real time and are configured to send alert notifications to IT personnel when predefined thresholds are exceeded.

Zscaler performs weekly vulnerability assessments and annual penetration tests to identify any weakness or deficiencies in their environment that could affects the performance of the cloud platform and/or affect the security, availability, and confidentiality of the system.

**Data**

Customers retain the ownership and control of their own company policy and data including information about their firewall rules, configurations and strategies. The Operations team is responsible for managing operational data such as system analytics and logs stored in databases and data files within the system as well as managing the associated infrastructure and log storage necessary to support the service. The Company has deployed secure methods and protocols for transmission of confidential and/or sensitive information over public networks. Proprietary customer metadata is secured and tokenized via patented methods.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Proprietary customer metadata	May include items Unique User ID (UUID) and Session Authentication tokens, Transactions logs in encrypted/ tokenized form	Confidential

**Significant Changes During the Review Period**

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period. No relevant changes to the Zscaler Cloud Platform system occurred during the review period.

**Subservice Organizations**

The data center services provided by multiple third-party data center services providers and the cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at the third-party data center services providers and AWS, alone or in combination with controls at Zscaler, and the types of controls expected to be implemented at the third-party data center services providers and AWS to achieve Zscaler's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Third-party Data Center Services Providers and AWS	Applicable Trust Services Criteria
The third-party data center providers, and AWS, are responsible for restricting physical access to data center facilities, backup media, and other system components including routers and servers.	CC6.4, CC6.5, CC7.2
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside.	CC6.1 – CC6.3 CC6.5 – CC6.6
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Zscaler systems reside.	CC6.7
AWS is responsible for notifying Zscaler of unusual activity, violations, and/or security breaches identified that impact Zscaler systems and customers.	CC2.1 – CC2.3, CC4.1, CC7.3 – CC7.5
Data center and cloud hosting service providers are responsible for ensuring the data center facilities are equipped with environmental security safeguards.	A1.2

## CONTROL ENVIRONMENT

The control environment at Zscaler is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

### Integrity and Ethical Values

The Company has developed a Code of Conduct and an Employee Handbook that is available to all employees on the Zscaler Intranet. The Code of Conduct and the Employee Handbook address the acceptable business practices, conflicts of interest and expected standards of ethical and moral behavior. These documents are provided to all new employees prior to commencement of employment. Prior to the commencement of employment, U.S. employees are required to sign an acknowledgement form that they agree to abide by the Employee Handbook and Code of Conduct. There is an established "tone at the top", and accountability is maintained through the leadership team to provide guidance on acceptable behavior within the organization. This tone is communicated and practiced by executives and management throughout the organization. The importance of high ethics and controls is discussed with newly hired employees throughout both the interview and orientation processes.

### Board of Directors and Audit Committee Oversight

The Company has a board of directors, comprised of a majority of independent members, that meets at least once quarterly and is consulted and involved in all significant business decisions, including providing oversight on risk matters.

### Organizational Structure and Assignment of Authority and Responsibility

The Company has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. The

Company has an organization chart that sets forth the Company's lines of reporting. The organization chart is updated as necessary and made available to all Zscaler personnel via the corporate intranet.

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

### **Commitment to Competence**

Zscaler management defines competence as the knowledge and skills necessary to accomplish tasks that define employee's roles and responsibilities. Zscaler's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that Zscaler has implemented in this area are described below:

- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An information system security and management policy is formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.
- U.S. based new employees must sign an employee handbook acknowledgement form after reviewing the employee handbook indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate security policies.

### **Accountability**

Zscaler's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks; and management's attitudes toward information processing, accounting functions, and personnel. Specific control activities that Zscaler has implemented in this area are described below:

- Management formally documents an organizational strategy within its information security management system (ISMS) policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives.
- Internal audits are performed annually in accordance with ISO 27001 requirements. The audit results are documented and reviewed by management.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- Board of Director meetings are held on an annual basis to review internal control performance.
- An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.

Zscaler's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Zscaler has implemented in this area are described below:

- Management has established pre-hire screening procedures to govern the new hire process for employees.
- Management has established employee termination procedures to govern the termination process.



---

## RISK ASSESSMENT

### Objective Setting

The risk assessment process involves a dynamic process that includes identification and analyzation of risks that pose a threat the organization's ability to perform the in-scope services. The process first starts with determining the organization's objectives as these objectives are key to understanding the risks and allows identification and analyzation of those risks relative to the objectives. Management formally documents organizational strategy within ISMS policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives. Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with company's mission and are utilized as part of the annual risk assessment process. Additionally, management holds quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.

### Risk Identification and Analysis

The Company identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. The Company's risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives. Appropriate levels of management are involved in the risk assessment process. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. The Company's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate or share the risk.

### Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

#### *External Factors*

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

#### *Internal Factors*

- Significant changes in policies, processes or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

## Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that is performed on an annual basis, considers the potential for fraud.

## Risk Mitigation

Policies and procedures are in place to guide personnel in risk mitigation activities, including: monitoring processes and development of policies, procedures, and communications to meet the entity's objectives during response, mitigation, and recovery efforts. Internal audit personnel perform a risk assessment on an annual basis that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved annually based on the business impact analysis during the annual risk assessment process.

Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties. The compliance team reviews vendor audit reports on at least an annual basis to ensure that third-party providers are in compliance with the organization's requirements. Internal audit periodically performs monitoring in the form of onsite visits, or conducting risk assessments of third-party vendors with whom confidential information was shared, including whether the third party is complying with agreed upon confidentiality commitments.

---

## TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

### Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

### Selection and Development of Control Activities

Zscaler assigns owners to each risk identified during the annual risk assessments and those owners are responsible for selecting and developing the control activities to mitigate those risks. These identified controls are documented within the risk assessment mitigation plans and are communicated to personnel via documented policies and procedures.

The applicable trust criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Zscaler's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

### **Trust Services Criteria Not Applicable to the In-Scope System**

All criteria within the security, availability, and confidentiality are applicable to the Zscaler Cloud Platform system.

---

## **INFORMATION AND COMMUNICATION SYSTEMS**

Pertinent information must be identified, captured and communicated in a form and timeframe that enables personnel to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

### *Internal Communications*

Zscaler has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include training for new employees on company policy and commitments, security awareness training for employees, and the use of e-mail messages and internal collaboration tools to communicate time-sensitive information. Employees are encouraged to communicate to their manager and/or Senior Management.

### *External Communications*

Zscaler has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include the public-facing website to communicate relevant information regarding the design and operation of the system and Zscaler's commitments to external customers. The website also features a portal where customers can communicate with Zscaler for support of the system or to report any incidents or concerns related to the operation or security of the system. When communicating with vendors, Zscaler requires that third parties sign a nondisclosure agreement of confidentiality before sharing any confidential information.

---

## **MONITORING**

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

### Ongoing Monitoring

Zscaler utilizes both manual and automated monitoring tools. Management personnel are involved in the day-to-day functioning of each department and provide hands on training, coaching, and correction. The management team holds meetings on a periodic basis within functional departments to discuss changes to the organization, changes to the production environment, and incidents or events identified by personnel or user entities. Additionally, system configured alerting logs are set up in order to alert the team in the case of real time incidents.

### Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the competence and authority. As a result of management's risk analysis process, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Management has determined that each risk assignment or category, will require structured inquiry, observation, inspection, or sample testing, or a combination of the aforementioned, based on the assigned risk level and the nature of the control, whether automated or manual, and the frequency of application (e.g. constant, daily, weekly, quarterly, etc.).

### Subservice Organization Monitoring

The services provided by third-party vendors are monitored on a regular basis as part of the day-to-day operations. As they become available, Zscaler personnel receive and review documentation (SOC reports and/or security certifications) to help ensure security practices are being followed.

### Internal and External Auditing

Zscaler monitors the requirements of certifications and regulatory demands, primarily by obtaining and maintaining an ISO compliance. Additionally, Zscaler performs internal audits of the control environment on an annual basis.

Zscaler supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. Zscaler has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including ISO/IEC 27001:2013.

### **Evaluating and Communicating Deficiencies**

The nature, timing and extent of the self-assessment tests and results are documented for management review. Deviations or deficiencies associated with controls with a risk assignment of high are immediately escalated for corrective action. Other self-assessment results are reviewed within a week of the self-assessment test procedures, and corrective action, if required, is assigned to an individual and documented once those required actions are complete. Management reviews the deviations and corrective actions are tracked through the year and revisited during the annual risk assessment meeting.

---

## **COMPLEMENTARY CONTROLS AT USER ENTITIES**

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria.