WHITE PAPER

Zscaler — Compliance with Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

Introduction

In March 2023, the Securities and Exchange Board of India (SEBI) published the "Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)" (Framework). The Framework provides Governance, Baseline Security, Legal and Regulatory requirements that REs should adopt to effectively manage their cloud service providers (CSPs), key risks, and mandatory control measures which REs need to put in place before adopting cloud computing.

Zscaler is not a RE which is bound to the principles and requirements of the Framework. This whitepaper describes the security controls and processes that Zscaler has in place, and REs may, subject to the Disclaimer below, utilize this information to conduct their due diligence on how they may use Zscaler Products whilst meeting the Framework requirements .

Key Principles of the SEBI Framework

The SEBI Framework consists for 9 Principles of

Governance, Risk and Complliance	Selection of CSPs	Data Ownership and Localization
Responsibility of the RE (to CSPs)	Due Diligence by the RE (CSPs)	Security Controls
Contractual Obligations	BCP, DR & Cyber Resilience	Concentration Risk Management

What does Zscaler do?

Zscaler's Zero Trust Exchange is a purpose-designed, cloud-based SASE platform that securely connects users, devices, and apps using business policies over any network. Zscaler provides RE with cloud based secure web gateway with multiple inline security capabilities for securing their web traffic, replacing the archaic traditional network security solutions.

Zscaler does not host any infrastructure, Deployment (VM/ containers) or managed application services for the RE on its Zero trust platform cloud and Zscaler does not manage a customer enterprise's security controls directly. The control of the cloud platform is retained by the RE itself. All requests, configurations, log meta data are owned and managed by the RE.

Further, a few key questions about Zscaler company, our customers, our technology, and products are answered here: zscaler.com/company/faqs

RE's Compliance with SEBI Framework

Subject to the Disclaimer below, RE may utilize the information below to assess how it may fulfill its obligations under the SEBI Framework when using Zscaler Products.

Principle 1: Governance, Risk and Compliance Sub-Framework

REs (Customers) are responsible for developing and implementing their Cloud Governance, Cloud risk management and compliance management programs and processes to identify, monitor, measure, and manage the reporting of their internal risks assessments.

Zscaler is a publicly traded company. Our financial or fiscal year is from August 1 to July 31. We demonstrate consistent, strong revenue growth. For more information related to our financials and corporate governance, please refer:

ir.zscaler.com

ir.zscaler.com/corporate-governance/governance-documents

Zscaler has in place an extensive risk assessment and risk treatment plan. A formally documented risk assessment process is in place to help guide the risk assessment and treatment processes. Zscaler uses a risk assessment methodology based on the NIST 800-30 standard.

Principle 2: Selection of Cloud Service Providers

Our Public service edges in India are in Delhi, Mumbai, and Chennai.

The latest Zscaler global Data centers map can be sighted at – trust.zscaler.com/zscaler.net/data-center-map

Zscaler uses our Third-Party Risk Management Program, including process to conduct due diligence and contractual diligence, to manage our vendors (e.g., subcontractors, sub processors) that has safeguards in place to guarantee that our security policies and standards are met by these vendors used to deliver the contracted services.

Zscaler maintains a current list of its sub-processors at www.zscaler.com/legal subprocessors

Principle 3: Data Ownership and Data Localization

The RE (Customers) retain complete data ownership for all their data. With all Zscaler solutions, the customer owns the data and is the data controller. REs shall manage their accounts and security configuration for their organization via their admin portals.

As a "data processor" under GDPR, Zscaler process and/or store limited personal data (e.g., IP addresses, URLs, user groups and departments from a corporate directory) only.

We do not process or store any special or sensitive categories of personal or non-public data (e.g., credit card, financial, or PHI). For more information, see Exhibit A of Zscaler's Data Processing Agreement: www.zscaler.com/privacy/dpa.

In case the RE might be required to forward web traffic to Public Service Edges in a specific region only (in this case India), note that if a remote user has traveled outside of specific region, then web traffic might be forwarded to a ZIA Public Service Edge located outside of your selected region. In such a case, RE can configure a subcloud to ensure that traffic is forwarded to your preferred ZIA Public Service Edges.

The customer web request data is stored in the form of transaction logs by Zscaler. The logs are tokenized, rendered unreadable, and thus do not contain any string identifiers. The token dictionary is stored on separate systems from the log files and requires different access privileges.

RE in India can opt for storing logs in Zscaler's India Hosted In-Country Logging Hub Site by requesting the same during the contracting phase and adding the location-based Log SKU's in their contracts.

These logs can be streamed to SIEM solution/ Server as desired by the RE by using the Nanolog streaming service (NSS) for ZIA and log streaming services (LSS) for ZPA. The NSS and LSS services need to be subscribed to and configured by the RE. This helps the RE have all the logs available in their preferred location that is managed by them in India and helps meet SEBI regulation for Data Localization and Retention.

Principle 4: Responsibility of the Regulated Entity

Zscaler has a standard clickthrough terms EUSA document for their customers.

The Roles and responsibilities (for customer and Zscaler) are defined in our End User Subscription Agreement in Section 4.5 and 4.6. Please refer: www.zscaler.com/legal/end-user-subscription-agreement

Further legal documents such as acceptable use policy, Data privacy and protection template can be found at www.zscaler.com/legal/overview

Our public Service Level agreements can be found at SLAs on our public-facing SLA web page: www.zscaler.com/legal/sla-support

Principle 5: Due Diligence by the RE:

Zscaler is a publicly traded company. Our financial or fiscal year is from August 1 to July 31. We demonstrate consistent, strong revenue growth. For more information related to our financials and corporate governance, please refer:

ir.zscaler.com

ir.zscaler.com/corporate-governance/governance-documents

The Zscaler Compliance team supports a wide variety of International compliance programs and government certification programs designed to certify that our cloud operations meet the highest standards for security and compliance. For example, Zscaler is certified for both ISO 27001 and ISO 27018 as well as SOC 2 Type II. For a full list of our certifications, please visit our compliance web page: www.zscaler.com/compliance/overview

Principle 6: Security Controls

Security of the Cloud

Zscaler has comprehensive security mechanisms in place that cross over many areas such as our cloud infrastructure, products, admin portals, data centers, and customer data to ensure Security of its zero trust Cloud.

Vulnerability and patch management programs are reviewed and part of our annual ISO and SOC2 type II reviews which are conducted by an external auditor.

Zscaler performs quarterly vulnerability assessments and annual penetration tests to identify any weakness or deficiencies in our environment that could affect the performance of the cloud platform and/or affect the security, availability, and confidentiality of the system. RE can obtain confidential reports (e.g., pen test results, vulnerability scan reports, etc.) after agreeing to an NDA through your designated Zscaler Account team, who will place a request on your behalf through our internal compliance web page

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/NOC personnel when predefined thresholds are exceeded. Real time monitoring stats can be viewed at – trust.zscaler.com

For security of the cloud the as a first step the Zscaler zero trust exchange confirms that the user is who they say they are. Once validated, access rights are verified based on context and the principles of least-privileged access to ensure users only have access to the applications for which they have been authorized. Zscaler's Zero Trust Exchange enhances known access control principles (least privilege, segregation of duties) them through its robust identity and access management capabilities:

1. **Least Privilege:** ZTE offers role-based access control (RBAC), allowing REs to define and enforce access policies based on users' roles, department, and responsibilities. Users are granted access only to the resources necessary for their tasks, adhering to the principle of least privilege.

2. **Segregation of Duties:** ZTE's RBAC system enables RE to define and separate roles and responsibilities within the platform. This ensures that users and administrators are not granted conflicting permissions that could compromise security.

3. **Timely Detection of Incidents:** ZTE incorporates advanced monitoring and analytics features, enabling RE to monitor user activity in real-time. Suspicious or anomalous behaviour triggers alerts, facilitating swift incident detection and response.

In addition to these principles, ZTE provides robust authentication and authorization mechanisms, including integration with multi-factor authentication (MFA) and single sign-on (SSO) capabilities. These features enhance identity security, ensuring that only authorized users gain access to sensitive resources.

Zscaler integrates with leaders in identity and access management (IAM) as well as identity governance and administration (IGA), Please check our support for all leading identity and access providers at: www.zscaler.com/partners/technology/identity-access-management

The Zscaler data security model uses data segregation as the key mechanism to ensure security. Zscaler security model ensures separation of data elements to minimize information leakage if a single component is compromised. Information in Zscaler logs cannot be extracted without access to multiple cloud components (Nanolog, Public Service Edge, and Central Authority). No single employee has privileged access to all three components. Further all Administrative level access is protected using several layers of security:

- The cloud is only accessible through jump systems located inside the Zscaler Network which are logically and physically segregated from the production cloud.
- Access to the restricted jump systems requires multi-factor authentication (MFA)
- Each node is protected by a built-in firewall and administrative traffic is protected by AES 128, or AES 256 encryption.
- Once the Network access has been granted, the administrators are authenticated with a username and password and an individual certificate (public key authentication)

Security in the Cloud

RE will configure, manage and maintain security, hardening and access control for all its infrastructure, applications and endpoints deployed by them in the cloud / on their premises.

Zscaler provides protection against advanced threats by using multiple inspection techniques for identifying web threats. Zscaler Internet Access (ZIA) scans all traffic bi-directionally for malware/spyware that passes through its cloud and offers an SLA that states the service will capture 100% of all known viruses transmitted. In addition to detecting malware, Zscaler provides protection against advanced threats that would typically not be blocked by traditional anti-malware engines. For example: Botnet Communications, Browser Exploitation, Phishing Sites, Cookie Theft, Anonymizer Sites, Use of Vulnerable ActiveX controls, Injected Code (zero-pixel iframes, obfuscated code, etc.)

Zscaler helps RE maintain the security posture in the cloud by replacing their legacy network security solutions to stop advanced attacks and prevent data loss with a comprehensive zero trust approach that includes:

- Zero Trust Network Access: Replace legacy VPNs with a secure, direct connection to private apps, not the network, for better security and a superior user experience via native integration with Zscaler Private Access
- Cloud Access Security Broker: Secure cloud apps with integrated CASB to protect data, stop threats, and ensure compliance across your SaaS and IaaS environments.

- Cloud Data Loss Prevention: Protect data in motion with full inline inspection, including Exact Data Match (EDM), Indexed Document Matching (IDM), and machine learning.
- Firewall & IPS: Extend industry-leading protection to all ports and protocols and replace edge and branch firewalls with a cloud native platform.
- Sandbox: Stop never-before-seen malware in line with shared protections sourced from 360+ billion daily transactions per day and 500+ trillion daily signals, including quarantine of zero-day threats, for AI/ML cloud effect.
- Cloud Browser Isolation: Make web-based attacks obsolete and prevent data loss by creating a virtual air gap between users, the web, and SaaS.
- Digital Experience Monitoring: Reduce IT operational overhead and speed up ticket resolution with a unified view of application, Cloud Path, and endpoint performance metrics for analysis and troubleshooting.

Principle 7: Contractual and Regulatory Obligations

Zscaler has a standard clickthrough terms EUSA document for their customers.

The roles and responsibilities (for customer and Zscaler) are defined in our End User Subscription Agreement in Section 4.5 and 4.6.
Please refer: www.zscaler.com/legal/end-user-subscription-agreement

Further legal documents such as acceptable use policy, Data privacy and protection template can be found at www.zscaler.com/legal/overview

RE should leverage our ISO and SOC 2 Type II compliance to satisfy audit requirements. Reports can be shared with a customer under NDA. Zscaler adheres to The National Institute of Standards and Technology NIST 800-53 ensuring sufficient protection of confidentiality, integrity, and availability of information and information systems. Zscaler also has several Global government certifications which include FEDRAMP (USA), C5 (Germany), ARPA (Australia), MTSCS Level 3 (Singapore)

Principle 8: BCP, Disaster Recovery & Cyber Resilience

Zscaler tests our formal Business Continuity/ Disaster Recovery Plan (BCP/DR) at least annually. Third-party auditors also verify our BC/DR Plan and test results annually as part of our ISO 27001 and SOC 2 Type II certifications. Our ISO 27001 and SOC 2 Type II attestation reports are available to customers (upon request and with an NDA) through a request form on our public-facing compliance web page: www.zscaler.com/compliance/overview

At Zscaler, we understand how critical Zscaler is to our customers' organizations and make the reliability, availability, and serviceability (RAS) of our products a top priority for the company. Zscaler products have a long history of near-perfect uptime and are backed by best-in-class service level agreements (SLAs)

Zscaler provides Zscaler's Disaster Recovery Solution – a customer-controlled business continuity solution to keep organizations operational even during a catastrophic event that might interrupt the global Zscaler cloud.

With Zscaler's Disaster Recovery solution, customers can control what business-critical private, or SaaS applications users can access even during a black swan event by the switch of operations from normal mode to DR mode through a single click and configure option. Refer www.zscaler.com/blogs/product-insights/zscaler-strengthens-sse-offering-disaster-recovery

Zscaler features several measures for resiliency, high availability and minimal downtime. Our Public Service Edges have significant fault tolerance capabilities. They are deployed in active-active mode to ensure availability and redundancy and Zscaler monitors and maintains its Public Service Edges to ensure continuous availability. Our recommended deployment approach has our customers' users and locations using a primary and secondary Public Service Edge, with automatic failover.

Mature operational procedures allow for cloud updates with no operational effect on customers. With data centers in many countries across the world, combined with our ability to handle any user on any node, Zscaler can provide a 99.999% SLA.

For additional information about our resilience approach, please read our resilience whitepaper at www.zscaler.com/resources/solution-briefs/zscaler-disaster-recovery.pdf

Principle 9: Vendor Lock-In and Concentration Risk Management

RE shall evaluate the concentration risks associated with cloud services. Zscaler does not provide/ host any Infrastructure, VM's, Containers, applications for customers in the cloud and does not store any customer data on its cloud. The log data can be readily streamed to any location / SIEM the customer selects. Zscaler ZTA is a cloud/ network agnostic solution, hence concentration risks are not applicable.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com