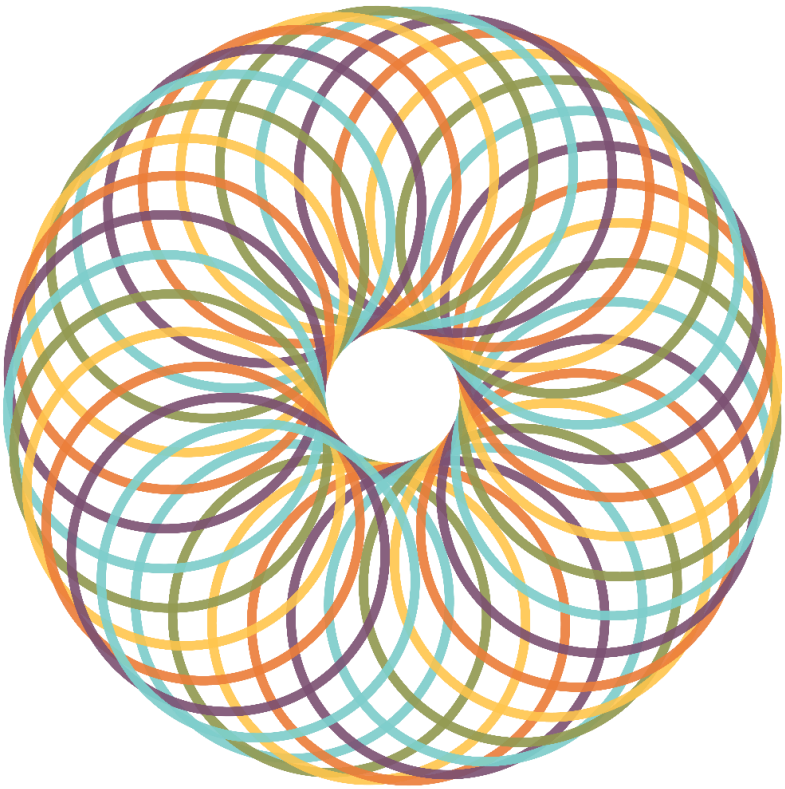
Deloitte Haskins & Sells LLP

ZOHO



SSAE 18 and ISAE 3402 – Type 2 Examination

Zoho Corporation Private Limited ('Zoho')

Report (SSAE 18 and ISAE 3402 – Type 2) on the Description system of Zoho related to Application Development, Production Support and the related General Information Technology Controls hosted in datacenters located at USA, India, Europe, Australia and Japan for services provided to its customers and Suitability of the Design and Operating Effectiveness of controls for the period December 01, 2023 to September 30, 2024.

Table of Contents

SECTION - 1:

Independent Service Auditor's Report

Deloitte
Haskins & Sells LLP

Chartered Accountants
ASV N Ramana Tower
52, Venkatnarayana Road
T. Nagar
Chennai - 600017
Tamil Nadu, India

Tel: +91 44 66885000

Section 1. Independent Service Auditor's Report

Independent Service Auditor's Report on the Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

To the Management of Zoho Corporation Private Limited

Scope

We have examined the description of the system of Management of Zoho Corporation Private Limited ('Zoho' or 'Company' or 'Service Organization') related to the Application Development, Production Support and the related General Information Technology Controls hosted in datacenters located at USA, India, Europe, Australia and Japan, for the services provided to its customers ('User Organizations' or 'User Entities' or 'Clients'), from Zoho locations ("ODCs" or "Facilities") at Chennai, Tenkasi, Renigunta in India and Austin in USA throughout the period December 01, 2023 to September 30, 2024, included in Section 3, "Management of Zoho's Description of Its System" (the "Description") and the suitability of the design and operating effectiveness of controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in management of Zoho's assertion. The controls and control objectives included in the Description are those that management of Zoho believes are likely to be relevant to user entities' internal control over financial reporting and the Description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

Zoho uses Sabey Data Center Properties LLC, Databank Holdings Limited, CtrlS Datacenters Limited, Digital Realty Trust Inc., Equinix Inc. B.V., Equinix Asia Pacific Pte. Ltd and Colt Technology Service Co. Ltd for Datacenter Co-Location Services ("subservice organizations"). The Description in Section 3 includes only the controls and related control objectives of Zoho and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by Zoho can be achieved only if complementary subservice organization controls assumed in the design of the Zoho's controls are suitably designed and operating effectively, along with the related controls at Zoho. Our examination did not extend to controls of the subservice organizations or their functions, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Zoho's controls are suitably designed and operating effectively, along with related controls at Zoho. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 2, "Management of Zoho's Assertion", management of Zoho has provided an assertion about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. Management of Zoho is responsible for preparing the Description and its assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives 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 ('AICPA') and International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization, issued by the International Auditing and Assurance Standards Board ('IAASB'). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the Description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period December 01, 2023 to September 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on the criteria in management's assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved.
- Evaluating the overall presentation of the Description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and therefore may not include every aspect of the system that each individual user entities may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in

processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4, "Management of Zoho's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results."

Opinion

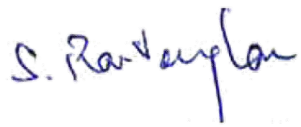
In our opinion, in all material respects, based on the criteria described in management of Zoho's assertion:

a. The description fairly presents the system related to the Application Development, Production Support and the related General Information Technology Controls (GITCs) for services provided by Zoho to customers that was designed and implemented throughout the period December 01, 2023 to September 30, 2024.
b. The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period December 01, 2023 to September 30, 2024 and subservice organization and User entities applied the complementary controls assumed in the design of Zoho's controls throughout the period December 01, 2023 to September 30, 2024.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period December 01, 2023 to September 30, 2024, and if complementary subservice organization and user entity controls assumed in the design of Zoho's controls operated effectively throughout the period December 01, 2023 to September 30, 2024.

Restricted Use

This report, including the description of tests of controls and results in Section 4, is intended solely for the information and use of management of Zoho, user entities of the Zoho's system related to the Application Development, Production Support and the related General Information Technology Controls for services provided by Zoho to its user entities during some or all of the period December 01, 2023 to September 30, 2024, and their auditors who audit and report on user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte Haskins & Sells LLP
Chartered Accountants
(ICAI Registration No.: 117366W/W-100018)



S. Ravi Veeraraghavan
Partner
M. No. 029935

January 30, 2025

SECTION - 2

Management of Zoho's Assertion

Section 2. Management of Zoho's Assertion

Management of Zoho Corporation Private Limited's Assertion

For the period from December 01, 2023 through September 30, 2024

The signed Management assertion has been provided by Zoho Corporation Private Limited's Management via letter dated January 30, 2025. The extract of the letter is as under:

We have prepared the description of the system of Management of Zoho Corporation Private Limited ('Zoho' or 'Company' or 'Service Organization') related to the Application Development, Production Support and the related General Information Technology Controls hosted in datacenters located at USA, India, Europe, Australia and Japan, for the services provided to customers ('User Organizations' or 'User Entities'), from Zoho locations ("ODCs" or "Facilities" or "Clients") at Chennai, Tenkasi, Renigunta in India and Austin in USA throughout the period December 01, 2023 to September 30, 2024, included in Section 3, "Management of Zoho's Description of Its System" (the "Description") for user entities of the system during some or all of the period December 01, 2023 to September 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by Subservice organization and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Zoho uses Sabey Data Center Properties LLC, Databank Holdings Limited, CtrlS Datacenters Limited, Digital Realty Trust Inc., Equinix Inc. B.V., Equinix Asia Pacific Pte. Ltd and Colt Technology Service Co. Ltd for Datacenter Co-Location Services ("subservice organizations"). The Description in Section 3 includes only the controls and related control objectives of Zoho and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by Zoho can be achieved only if complementary subservice organization controls assumed in the design of Zoho's controls are suitably designed and operating effectively, along with the related controls at Zoho. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of the Zoho's controls are suitably designed and operating effectively, along with related controls at Zoho. The description does not extend to controls of the user entities.

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

1. The Description fairly presents the Zoho's Application Development, Production Support and the related General Information Technology Controls for services provided to its user entities of the system during some or all of the period December 01, 2023 to September 30, 2024. as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description.

a. Presents how the system made available to user entities was designed and implemented to process relevant user entity's transactions, including, if applicable:

   i. The types of services provided including, as appropriate, the classes of transactions processed.
   ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
   iii. The information used in the performance of procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
   iv. How the system captures and addresses significant events and conditions other than transactions.
   v. The process used to prepare reports and other information provided for user entities.
   vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
   vii. The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
   viii. Other aspects of our control environment, risk assessment process, information and communications including the related business processes, control activities, and monitoring activities that are relevant to the services provided.

b. Includes relevant details of changes to Zoho's system during the period covered by the Description.

c. Does not omit or distort information relevant to the service organization's system, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the system that each individual user entity of the system and its user auditor may consider important in its own particular environment.

2. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period December 01, 2023 to September 30, 2024 to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of Zoho's controls throughout the period December 01, 2023 to September 30, 2024. The criteria we used in making this assertion were that:

   a. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of Zoho.
   b. Controls identified in our description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in our description from being achieved.
   c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

For Zoho Corporation Private Limited

Sd/-

Name – N Jai Anand
Designation – Chief Financial Officer
Date – January 30, 2025

SECTION - 3
Management of Zoho's Description of Its System

Section 3. Management of Zoho's Description of Its System

3.1. Overview

Applicability & Purpose of Report

The review of controls for Type 2 in accordance with ISAE 3402 and SSAE 18 examination describes the control environment and features control objectives and underlying controls of Zoho Corporation Private Limited. This report is prepared to provide information on the Application Development, Production Support and the related General Information Technology Controls hosted in USA, India, Europe, Australia and Japan by Zoho to its user entities from the following Offshore Development Centers ("facilities" or "premises" or "ODCs") for the period from December 01, 2023 to September 30, 2024:

ODC	Address
Chennai, India	Estancia IT ParkGST Road, Chengalpattu, Tamilnadu, India.
Tenkasi, India	Silaraipuravu Village, Mathalamparai, Tamilnadu, India.
Renigunta, India	Srikalahasti Road, Renigunta Pillapalem, Andhra Pradesh, India.
Austin, USA	Springdale Rd, Austin, United States of America.

This report has been prepared to provide information for use by Zoho's user entities and their independent auditors in obtaining an understanding of the control structure relating to Application Development, Production Support and the related General Information Technology Controls performed by Zoho. The user entities and their independent auditors should consider the results of this report within the context of the user entities' overall control environment. Controls relating to Zoho are not designed, nor are they likely to compensate for any weaknesses in user entities' control environment.

Zoho's System has been designed for providing services to its user entities in a controlled environment. The System comprises of policies and procedures implemented to support consistent maintenance of the client service delivery.

The scope of this report is limited to those controls set out in section 3, "Management of Zoho's Description of Its System". Internal applications are used to support Zoho's Application Development, Production Support and the related General Information Technology Controls operations. This report does not cover the controls relating to IT General Controls of the internal applications except as mentioned in Description of system.

As this report provides assurance on internal controls, it does not encompass all aspects of the services provided or procedures followed by Zoho. Additionally, in their Service Level Agreements ('SLA'), user entities may stipulate additional control activities to be undertaken. Therefore, section 3 "Management of Zoho's Description of Its System", may not be a comprehensive listing of all controls relating to Application Development, Production Support and the related General Information Technology Controls operations for all user entities, nor would all controls listed may be of relevance to all user entities.

This report covers services provided by Zoho and focuses on control objectives that may be relevant to the internal controls for financial reporting by Zoho's user entities. The scope of the report covers significant processes that Zoho have determined as material to its user entities from a financial reporting perspective.

The report has been developed to cover the Application Development, Production Support and the related General Information Technology Controls of Zoho, which are in scope. It focuses on processes and controls applicable to the common processes supported by Zoho for the user entities.

3.2. Zoho – Overview

Incorporated in 1996, Zoho Corporation provides SaaS solutions, IoT platform and IT management software (on premise) to organizations of all sizes across the globe. Zoho comes with a suite of software that brings together collaboration, productivity, and communications tools and integrates them into other business processes. From network, and IT infrastructure management applications, software maintenance and support services for enterprise IT, networking, and telecom clients to enterprise IT management software for network performance management, IT service desk and desktop management, datacenter and server management, and log analysis and security management.

Zoho's primary facilities are based from India-Chennai, Tenkasi and Renigunta and USA-Austin. The development and support activities are entirely based on India locations. Zoho also has a global presence in Netherlands (Utretch), Singapore (Cecil Street), China, Japan, Mexico and Australia (Varsity Lakes). The sales, marketing and customer support activities are specifically carried out in secondary facilities in Netherlands, Australia, China, Japan and Singapore.

Zoho hosts the data in datacenters across the globe. When an organization (customer who wants to subscribe to Zoho) signs up with Zoho, the default datacenter location is chosen by Zoho based on the user/organization's IP address. The customer does not have the option to choose the hosting location. In order to make it easier for the organization, that field is selected by default based on the organizations IP address. Based on the country chosen there, the corresponding datacenter is chosen for the organization's account. Listed below are the locations Zoho services and their associated datacenters (including the primary and secondary DCs):

- United States Of America – Quincy, Dallas (www.zoho.com)
- Europe – Amsterdam, Dublin (www.zoho.eu)
- India – Mumbai, Chennai (www.zoho.in)
- Australia – Sydney, Melbourne (www.zoho.com.au)
- Japan – Tokyo, Osaka (www.zoho.jp)
- China – Shanghai, Beijing (www.zoho.com.cn)
- Canada – Toronto, Montreal (www.zohocloud.ca)
- Saudi Arabia – Riyadh, Jeddah (www.zoho.sa)

Zoho's range of products are internally classified under the following verticals:

- Zoho - offers a comprehensive suite of online business, productivity & collaboration applications to assist user entities manage their business processes and information.
- ManageEngine - offers enterprise IT management software for service management, operations management, Active Directory and security needs.
- Qntrl – A workflow orchestration software that helps gain visibility and control over business processes by automating them.
- TrainerCentral - A comprehensive platform to help build engaging online courses, nurture a learning community and turn expertise into a successful training business.
- Zakya - Running a retail business is easier with Zakya. We help sell better, manage entire business, and join the digital revolution.

- MedicalMine - chARMHealth Suite of Products are used by healthcare professionals in the Ambulatory Clinic Care. The chARMHealth helps to providers to manage Electronic Health Record, Patient Health Record, Medical Billing, etc.,

System Overview

Zoho operates in a well-defined system to provide services to its user entities. This system consists of multiple components such as policies and procedures, governance structure, support functions, and application systems. The policies and procedures provide guidance to the users regarding the process to be followed for providing the services and assistance in the consistent implementation of the same. The governance structure establishes a structure for operating the system and assists in demonstrating Management's commitment towards the same. The defined processes for information systems including Software development, Quality and Security testing, Incident Management, Change Management, and Service Delivery are implemented by Zoho to support the processes followed for providing services to its user entities. Zoho has established an internal controls framework that reflects:

- The overall control environment within the organization and its various processes
- The Risk Assessment procedure
- Information and communication and
- Monitoring components of internal control

The components mentioned above are described in detail in the succeeding sections. There is synergy and linkage amongst these components, forming an integrated system that responds dynamically to changing conditions. The internal control system is intertwined with Zoho's operating activities and exists for fundamental business reasons.

Overview of Teams and Roles within Zoho

Zoho products are developed, maintained and supported by the following teams:

a. Product Teams

Product teams perform the following activities:

- Development, design, research and analysis of new features and enhancements
- Application Patch management
- Issue fixing
- Quality and security testing before deploying in production environment.
- Release management (where applicable)
- Overall management of product (including assessments, documentation, training programs for associates etc.).

b. Customer Support Team

Zoho Customer Support has several tiers of Customer support depending upon the support plan the customer is entitled to. Zoho does provide both complementary and paid customer support. User entities report clarifications or bugs via phone/chat/email to the Customer Support team. The team coordinates with Product teams to resolve reported issues.

c. Server Operations and NOC team

The Server Operations team handles the management of components such as servers, databases and network devices within the data center hosting Cloud services and the servers.

The Network Operations Center (NOC) team monitors Local Area Networks (LAN) / Wide Area Networks (WAN) and network devices for faults, failures, errors, usage and performance from a centralized location based out of Zoho's Corporate Office in Estancia, Chennai. The scope of work for NOC and Server Operations team includes- analyzing problems in network devices, troubleshooting issues, reporting incidents, communicating with site technicians and tracking problems to resolution.

d. Sysadmin team

The Sysadmin team is responsible for management of Zoho's internal Corporate Infrastructure components such as servers, databases and network devices. Corporate Infrastructure supports non-production instances of Zoho products used for development and testing purposes, and other internal tools used by teams to support the Zoho products.

e. Compliance team

The Compliance team is responsible for managing the organization's Information Security governance framework and ensuring compliance with relevant regulatory and internal standards. They also manage all internal and external audits for all the applicable standards and regulations. This includes the continuous monitoring of policies, procedures, and practices to mitigate risks. Additionally, the team oversees the coordination and execution of various audits, including second-party and third-party audits ensuring that all audit activities align with establish organization objectives.

f. Legal team

Legal team works jointly with the internal teams to achieve company's objectives and also ensures that the company's activities are in conformity with the applicable laws and regulations. Legal Team assists the sales and product teams in reviewing and drafting contracts, provides legal consultation and advise with regards to law enforcements requests, customer account disputes. It takes care of trademark filings and renewal, reviews licenses of third party open source and commercial software.

The Compliance team is responsible for the overall Information Security Governance and compliance within the organization and also ensuring the service commitments and system requirements as per the Master Service agreement and Terms of Service or any other agreements between Zoho and the user entities.

g. Security and privacy team

Zoho has have dedicated security and privacy teams that implements and manages security and privacy programs. They engineer and maintain defense systems, develop review processes for security, and constantly monitor networks to detect suspicious activity. They provide domain-specific consulting services and guidance to engineering teams.

h. Configuration Management Team

Zoho has a centralized Configuration Management team. They are responsible for maintaining the source code and enforce code check standards for the builds which needs to be deployed.

i. Service Delivery team

The Service Delivery team is responsible for the deployment of builds into production environments for Zoho products. The service delivery team takes care of SD tool, which in turn takes care of automation related activities related to deployment of builds into production environments.

Zoho Products

The below products are categorized based on the scale of usage and complexity of the product. The below products are internally classified as Large, Medium and Small based on the scale of usage and complexity of the product. The following products are scoped-in for the report hosted in the following data centers:

- United States of America – Dallas, Washington (www.zoho.com)
- Europe – Amsterdam, Dublin (www.zoho.eu)
- India – Mumbai, Chennai (www.zoho.in)
- Australia – Sydney, Melbourne (www.zoho.com.au)
- Japan – Tokyo, Osaka (www.zoho.jp)

Small	Medium	Large
• Zoho Payroll • Zoho People	• Zoho Invoice • Zoho Expense • Zoho Inventory • Zoho Billing • Zoho Checkout • Zepto Mail • Zakya	• Zoho CRM • Zoho Campaigns • Zoho Books • Zoho Creator • Zoho Mail • Zoho Projects and Bug Tracker

3.3. Overview of Services

Zoho provides Application Development, Production Support and the related General Information Technology Controls services to its user entities from the following Zoho locations:

- Chennai India
- Tenkasi, India
- Renigunta, India
- Austin, USA

3.3.1. Control Environment

Zoho's control environment reflects the position taken by management, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods and organizational structure.

3.3.1.1 Integrity and Ethical Values

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure.

Zoho has programs and policies defined and documented to promote integrity and ethical values in their environment. Zoho has adopted a code of ethics, referred to as "Employee Code of Conduct". This code of conduct applies to Zoho. Newly joined associates at Zoho are required to sign the Employee Code of Conduct which denotes their acceptance and agreement to abide by the same.

Training

The Training and Development Group plays a key role to facilitate meeting the following objectives of training:

- To enable utilization of manpower resources
- To improve the workforce skills in line with emerging business requirements. The following training programs are mandatory:
    - HR Induction Program
    - Information Security Management System (ISMS) Awareness Workshop
- General Data Protection Regulation (GDPR) and Privacy Awareness Program.

Zoho has launched new programs for associates with respect to the changes and developments in the use of technology. It has enhanced hands-on assessments to facilitate enhanced reach of the enablement program across the organization.

Upon joining Product teams, associates undergo training by designated individuals within the team via product training materials and practical exercises. Product related training materials are made available on Zoho Intranet for their respective teams.

Employee Code of Conduct and Ethics

Zoho has framed a Code of Conduct and Ethics ('the code') which is applicable to the member of the Board, the Executive officers, and associates of the Company and its subsidiaries. Zoho has adopted the Code of Conduct and Ethics which forms the foundation of its ethics and compliance program and is available to all associates on its Intranet portal. It includes global best practices with an interactive resource making it easier for associates to understand while also trying in the elements of the code to Zoho's corporate culture.

Zoho has adopted a Whistle blower policy mechanism for Directors and associates to report concerns about unethical behavior, actual or suspected fraud, or violation of the Company's code of conduct and ethics. Upon initial employment, all associates are issued the Whistle blower policy which is part of the Code of Ethics document and are required to read and accept the policy.

3.3.1.2 Commitment to Competence

Zoho's Management defines competence as the knowledge and skills necessary to accomplish tasks that define employee's roles and responsibilities. Roles and responsibilities and job descriptions are defined in collaboration by HR and respective Team Managers. Management's commitment to competence includes Management's consideration of the job descriptions, roles and responsibilities for performing specific jobs and ensuring recruitment activities are in line with these requirements. Associates undergo training activities in the form of classroom trainings, training exercises and simulations, and are evaluated on an on-going basis by product teams.

Zoho has adopted ISO 27001, ISO 27701, ISO 27017, ISO 27018 International Standard to establish, document, implement, operate, monitor, review and maintain an Information Security and Privacy Management Systems to demonstrate its ability to provide services in line with the business activities and any applicable statutory, regulatory, legal and other requirements. Its aim is to enhance client satisfaction by continually improving the system. The validity of this existing certification is until August 21, 2025.

3.3.1.3 Management's Philosophy and Operating Style

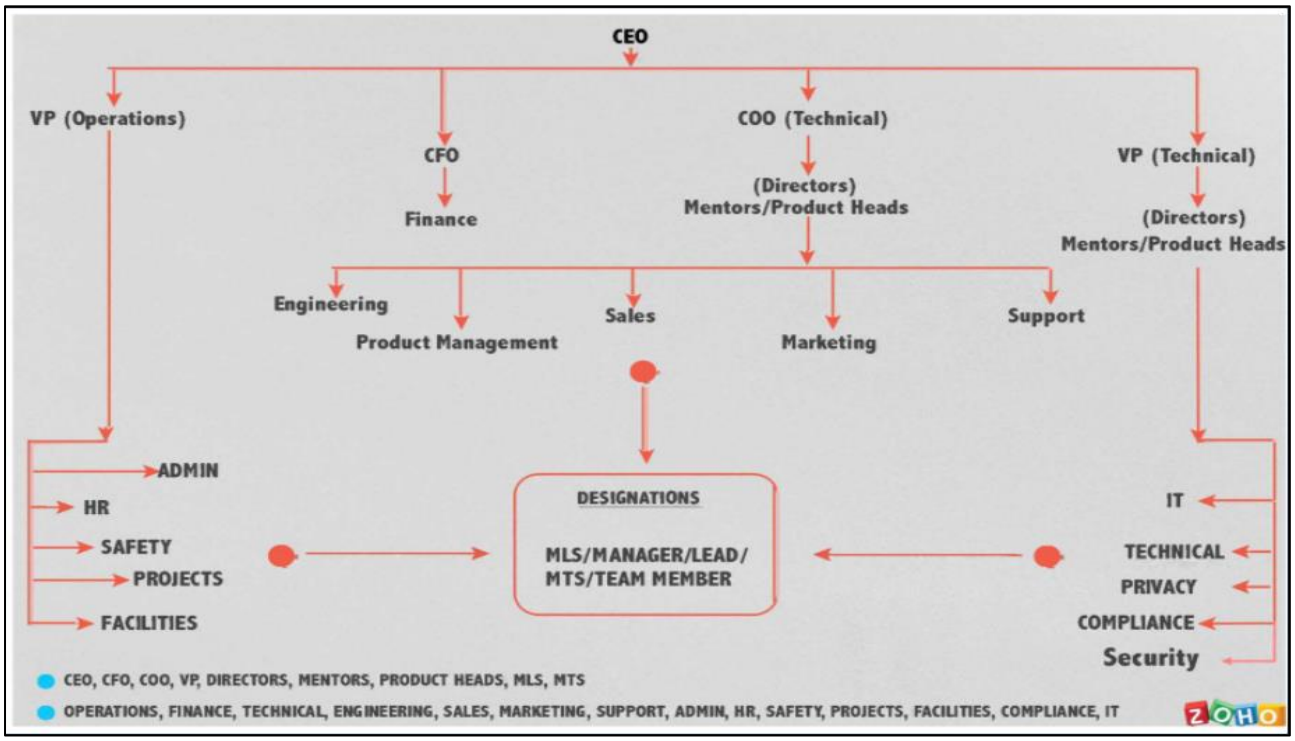
Zoho Management's philosophy and operating style encompass a broad range of characteristics including Management's approach to taking and monitoring business risks, and Management's attitudes toward information processing, accounting functions, and personnel. Specific control activities that Zoho has implemented in this area are described below:

• Management is periodically briefed on regulatory and industry changes affecting the services provided,
• Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

3.3.1.4 Zoho Organization Structure

Zoho has defined its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process to meet its commitments and requirements.

Zoho's organizational structure establishes the key areas of authority and responsibility, appropriate lines of reporting, defined roles, and responsibilities. Roles, responsibilities and authorities associated with the roles that constitute Zoho's organizational structure are defined and documented by Zoho Management. Zoho's Security team is responsible for defining, implementing, and monitoring of policies and procedures related to information security and availability, which are made available to associates through internal portal.



3.3.1.5 Board of Directors or Audit Committee

Zoho operates under the direction of Directors and other stakeholders, as the case may be, who meet and conduct the respective meetings in compliance with the law and for the growth and benefit of the company.

The Board of Directors has established a number of committees for addressing specific areas with well-defined objectives and activities like- Corporate Social Responsibility (CSR) Committee which oversees the implementation of CSR projects and CSR Spending's and Vigil (Whistle Blower) mechanism committee, which provides a channel to the associates and Directors to report to the management the concerns about unethical behavior, actual or suspected fraud or violation of the Codes of conduct or policy.

The Board of Directors meet at least once each quarter and perform the following functions regularly including but not limited to:

- Oversight of the selection, evaluation, development and compensation of senior management;
- Overseas management's functions and protects the long-term interest of the organization's stakeholders;
- Reviewing, approving and monitoring fundamentals financial and business strategies and major corporate actions;
- Assessing major risks facing the Company and reviewing options for their mitigation; and
- Ensuring that processes are in place for maintaining the integrity of the Company, the financial statements, compliance with law and ethics, relationship with user entities and suppliers and relationship with other stakeholders.

3.3.1.6 Assignment of Authority and Responsibility

Following are the roles and responsibilities of personnel within Zoho:

Role	Responsibility and Authority
Chief Executive Officer (CEO)	Responsible for handling Operations, Resource Management, Point of Communication for Directions
Chief Financial Officer (CFO)	Responsible for operations relating to Finance, Tax, Billing, Collections and Treasury.
Chief Operating Officer (COO)	Responsible for end-to-end handling Product Management and Operations
Vice President (VP)	Responsible for General Management, Administration and Product Management
Directors (Mentors / Product Heads)	Responsible for handling specific Zoho Products and Division Specific Management
Member Leadership Staff (MLS) / Member Technical Staff (MTS) / Team Member / Lead	- Responsible for handling specific product related roles - Responsible for handling product specific Internal Teams/Divisions/Stream based roles/Product based roles
Information Security Head	- Define the Information Security Policy - Ensure the communication and understanding of the Information Security Policy throughout the organization. - Monitor the implementation of security policy established under the Integrated ISPIMS.
Director of Compliance	- Accomplishes compliance business objectives by producing value added employee results; offering information and opinion as a member of senior management; integrating objectives with other business units; directing staff. - Develops compliance organizational strategies by contributing information, analysis, and recommendations to strategic thinking and direction, establishing functional objectives in line with organizational objectives. - Establishes compliance operational strategies by evaluating trends; establishing critical measurements; determining production, productivity, quality, and customer-service strategies; designing systems; accumulating resources; resolving problems; implementing change.

Role	Responsibility and Authority
	- Monitor the implementation of privacy policy established under the Integrated ISPIMS. - Protects assets by establishing compliance standards; anticipating emerging compliance trends; designing improvements to internal control structure.
Information Security Compliance Manager	- Document and maintain the policies related to security of Organizational Information and information handled as a CSP. - Ensure that the Information Security Management System is established, implemented, monitored and maintained. - Co-ordinate improvements to the Information Security Management System. - Perform periodic tests, Implement and act as per the Information Security Continuity Plan. - Facilitate implementation of corrective actions pertaining to Integrated ISPIMS. - Perform periodic test, Implement and act as per Business Continuity Plan. - Plan and conduct internal audits. - Ensure the planning and execution of external audits. - Measure, track and analyse trends in metrics. - Implement and act per the Integrated ISMS policies that are applicable. - Periodic review of Integrated ISMS documents. - Review policies and documents in consultation with System Administrator before release. - Ensure that selected controls are documented in the Statement of Applicability and are implemented. - Monitor the implementation of Integrated ISMS on a continual basis and report discrepancies to the DOC. - Facilitate risk assessment using cross functional teams. - Identify training needs of Integrated ISMS and coordinate with training department to ensure that the training is completed. - Verify the implemented corrective actions.
Member Technical Staff - Compliance Tools & Support	- Establish, designing and implementing the process and tools to make the organization adhere to the compliance. - Analyze the compliance requirements, designing the solutions and implementing the same. - Responding to the compliance related questions raised by the customers. - Attending the conference calls with the customers on compliance. - Conducting meetings with the internal teams and steering.
Product / Department Head / Internal Audit Coordinators	- Implement the Integrated Information Security Management System and Cloud security best practices within product / Department. - Product / Department heads act as risk owners & will have the authority take decisions on risk, for their respective departments. - Obtain and communicate customer requirements to the appropriate personnel or functional organizations. - Ensure that qualified, skilled, and trained personnel and other resources are available to implement the Integrated Information security Management System. - Ensure integrity, quality, safety, optimal cost, schedule, performance, reliability, accuracy and maintainability of products and services in order to satisfy customer requirements.

Role	Responsibility and Authority
	- Ensure that the personnel comply with applicable standards, regulations, specifications, and documented procedures. - Provide the corrective actions.
Product Data Protection Officer (P-DPO)	- Heads & oversees the privacy implementation in their respective products/business units. - Maintains the Data inventory (Information Asset Register) for their respective product/business unit. - Reviews the documents pertaining to the common privacy practices, IAR in their respective teams. - Provides oversight and guidance to the PIMs in privacy related tasks, implementations in their respective products/business unit. - Co-ordinates with the Privacy Steering Committee on various activities related to privacy and compliance within their product/business unit. - Heads, authorizes and reviews the RCA of privacy incidents. - Serves as the first point of contact in case of any privacy incidents or escalations. - Report to the Head of the Business Function/Product.
Member- Compliance Audit	- Establish and execute compliance monitoring programs around information technology. Participate in internal security assessments, internal audits, customer audits, compliance certifications (external audit), and customer security questionnaire responses. - Assists in creating policies and procedures to help reduce risk, meet regulatory requirements and best business practices. - Performs Information security assessments and prepares findings and remediation reports. - Assists in updating and maintain policies, standards and procedures documents. - Evaluate security controls to ensure effectiveness and compliance, including managing the security control remediation efforts. - Coordinate with various teams in the organization regarding standards, regulations. - Coordinate with teams for Information Security awareness training. - Mapping and analyzing the adherence level with the applicable standards. - Performs other job-related duties as assigned.
Data Protection Officer (DPO)	- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the data privacy regulations. - To monitor compliance with this the applicable data protection laws, and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. - To provide advice were requested as regards the data protection impact assessment and monitor its performance - To cooperate with the supervisory/data protection regulatory authorities - To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation of certain types of processing of personally identifiable information (as maybe required by the laws) and to consult, where appropriate, with regard to any other matter related to it.

Role	Responsibility and Authority
Privacy Implementation Member (PIM)	- Implements or assist in implementing the privacy controls and features - Provides reports of the consistency to the P-DPO on request. - Consults with the Privacy Team and/or Legal team on new activities or processes. - Conducts the Risk Assessment (DPIA) for their team's activities processes and products/features. - Co-operate during Privacy incidents by finding the root cause and works to fix it on priority. - Conduct privacy awareness trainings and exercises during team member on-boarding and periodically. - Ought to report directly to the P-DPO. - Provide suggestions to the P-DPO on how to address privacy risks in a better way, proactively.
Lead - Privacy Operations & Management	- Establish and maintain the Privacy Program, which addresses the personal data management of both customers and employees. - Aids the ISH in defining the Information Privacy Policy of the organization. - Serve as the internal point of contact for the organisation's information privacy initiatives. - Co-ordinate with the Services and Operations teams to operationalize the program across all the applicable business units. - Facilitate Privacy Risk & Impact assessments as per the scope defined in the DPIA policy. - Initiate, facilitate and promote activities to foster information privacy awareness within the organization. - Perform ongoing monitoring of the compliance with the organisation's policies related to information privacy. - Work with the Legal team on negotiation of contracts with customers, vendors and other third parties. - Review the organisation's policies pertaining to the Information Privacy Program. - Work with the Incident Management team during incident analysis and investigations that have effect on the privacy of the applicable parties. - Provide consultation to business personnel on methods to mitigate the risks identified. - Conduct trainings to internal auditors on PIMS. - Work with the Compliance team during internal and external audits to assess and review the implementation of the privacy controls and the maturity. - Review third party's privacy posture during vendor on-boarding especially when the third party processes personal data on behalf of the organization or its products - Convert stakeholders' requirements into action plans for the organization, based on the applicable laws and lead the compliance program that follows
Data Privacy Analyst	- Work as part of the Privacy team and assist in the administration, management, of the Zoho's Privacy Program and related projects, such as the EU GDPR compliance program. - Assist the DPO & the Privacy Lead in the handling and coordination of daily firm-wide data privacy exceptions, including but not limited to, response, investigation, logging, reporting and coordination.

Role	Responsibility and Authority
	- Assist in the management and coordination of other on-going compliance, and projects. - Continuously assess Zoho's operations to develop policies, processes, and procedures related to Zoho's privacy practices and programs. - Remain well-informed and support the team members with questions related to Information Privacy Concepts. - Work closely with internal stakeholders, such as legal teams and other corporate functions to analyze and respond to privacy related issues, in co-operation with the Privacy Lead. - Work with internal stakeholders to implement and to maintain privacy best practices, such as conducting Data Protection Impact Assessments. - Assist Information Security team in responding to customer related surveys and questionnaires regarding the Zoho's compliance initiatives. - Evaluate vendor's privacy stature during vendor on-boarding process, especially if the vendor processes personal data on behalf of the organization or its products.
Director of IT (DOIT)	- Reviews and approves procedures pertaining to handling some of the privacy and security compliance related processes. - Advises on ways to achieve intended outcomes with respect to addressing risks in processing data. - Enables / spearheads some operations to improve the overall working of the GRC program and serves as an important person in the privacy steering committee.
Central Security Team	- Accountable for the overall Information Security and Cloud security Program. - Initiate, facilitate and promote activities related to security awareness in the organization. - Conduct Security Risk & Impact assessments for any new product, technology and architecture component. - Assist and guide the product security engineers on secure coding standards and security assessments guidelines within the product scope. - Responsible for identifying and building security tools and frameworks to assist the development and operations teams. - Evaluate evolving new technologies in the context of information security and provide guidance on secure adoption to the product teams. - Closely work with the Incident management team during incident analysis and investigations.

3.3.1.7 Human Resource Policies and Practices

Zoho has defined policies and procedures on the intranet portal consisting the HR processes covering the employee life cycle. These policies cover on-boarding, joining formalities, credential and reference checks, payroll processing, travel, leave and attendance management, rewards and recognition, performance review, employee benefits and employee separation. Third party service provider performs background checks for Zoho associates. The checks carried out include verification of educational qualifications and criminal checks as applicable for the associates.

Upon joining Zoho, newly joined associates are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.

The associates are also required to sign a Non- Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media policy on their first day of employment as part of the employee handbook acknowledgement formalities.

3.4. Risk Assessment

Zoho's risk assessment process identifies and manages risks that could potentially affect Zoho's ability to provide services to user entities. This ongoing process requires that Management identify significant risks inherent in products or services as they oversee their areas of responsibility. Zoho identifies the underlying sources of risk, measures the impact to organization, measures the likelihood, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks. This process has identified risks resulting from the nature of the services provided by Zoho. Management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel.
- Security risk – Security related vulnerabilities in the Corporate and IDC infrastructure which may impact confidentiality of client data and availability of services.
- Strategic risk - new technologies, changing business models, and shifts within the industry.
- Compliance - legal and regulatory changes.

3.5. Information and Communication

Internal and External Communication

Zoho has procedures in place for user entities to report incidents and reach out for support. Roles and responsibilities of Zoho and Client are communicated to all the stake holders. Any upgrades, planned downtimes are communicated to the user entities in advance.

Zoho Intranet channels are an important medium for associate communication to know the policies and procedures. Dedicated portal for GRC (Governance, risk and compliance) is in place for policies and procedures. The internal communication from the Senior Management or the support groups comes in the form of Blogs, emails, Newsletters, Zoho Connect Portal etc. The communication includes messages related to Security policies and procedures, new initiatives and tools, performance management, rewards and recognitions etc.

Zoho communicates its commitment to security as a top priority for its customers via Master Service Agreement and Terms of Service. Mock drill for BCP/DR is initiated on an annual basis at Zoho facilities and the results are communicated to the Top management (CEO, CFO & Directors) personnel.

Zoho Privacy team communicates changes to confidentiality commitments through Zoho Code of ethics, whenever applicable. Zoho security commitments to users and required security obligations are communicated to users during the induction program.

3.6. Monitoring

Zoho has developed an organization-wide Integrated Information Security & Privacy Manual (IISPM) based on the ISO27001 standard. The Information Security ('IS') Policy is structured and is made available to the Zoho associates through a Portal on the Intranet.

The Compliance team is responsible for monitoring compliance with the IISPM policy at Zoho. Internal audits are conducted by the Compliance team at half yearly intervals to monitor compliance with the policy. Any deviation from the laid down policies and procedures is noted as an exception and accordingly reported to Management for corrective action.

3.7. Processes and Controls

Zoho's control objectives and related controls are included in Section 4 of this report "Management of Zoho's Description of its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results". The Description of controls includes controls encompassing the following domains:

- Change Management
- Information Security
- Logical Access Security
- Physical and Environmental Security
- Manage Human Resources
- Incident Management
- Backup and Restoration Management Services
- Third Party Management

3.7.1 Change Management

Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.

Change management policy of Zoho is defined by the compliance team. The document is review by compliance manager and approved by the web master – project manager on an annual basis.

Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.

Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.

Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.

Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.

Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.

Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.

IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.

The control objectives and control activities related to 'Change Management' in scope are as below:

CO1: Control provides reasonable assurance that segregation of environments is maintained.	
CA1.01	Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.

The control objectives and control activities related to 'Change Management' in scope are as below:

CO2: Controls provide reasonable assurance that application and server changes are documented, tested and approved as per the procedures.	
CA2.01	Change management policy of Zoho is defined by the compliance team. The document is review by compliance manager and approved by the web master – project manager on an annual basis.
CA2.02	Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.
CA2.03	Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.
CA2.04	Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.
CA2.05	Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.
CA2.06	Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.
CA2.07	IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.

3.7.2 Information Security

Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis.

Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.

For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.

For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.

The control objectives and control activities related to 'Information Security' are as below:

CO3: Controls provide reasonable assurance that Information Security policies and procedures are documented, approved and communicated to associates.	
CA3.01	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA3.02	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA3.03	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA3.04	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.

3.7 3 Logical Access Security

Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.

For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining.

For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date.

For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.

For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.

For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.

For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes

access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.

For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.

For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM.

For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.

Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.

IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any)

For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.

For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.

Administrative access to Jump Server of Zoho is restricted to Server Operations team.

For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People. For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.

For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.

The control objectives and control activities related to ‘Logical Access Security’ in scope are as below:

CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	
CA4.01	Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.
CA4.02	For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining.
CA4.03	For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date.

CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	
CA4.04	For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.
CA4.05	For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.
CA4.06	For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.
CA4.07	For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.
CA4.08	For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.
CA4.09	For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.
CA4.10	Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.
CA4.11	IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any)
CA4.12	For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.
CA4.13	For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.
CA4.14	Administrative access to Jump Server of Zoho is restricted to Server Operations team.
CA4.15	For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.
CA4.16	For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.

CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	
CA4.17	For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.

3.7.4 Network Security

Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.

For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.

For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager. For changes to network device configuration, the request is raised in Zoho SDP.

For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.

Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.

Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.

Penetration testing is performed for External IP of Zoho on a annual basis. Vulnerabilities identified if any are tracked to closure.

IDC servers of Zoho are restricted from accessing internet and mounting removable device.

Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.

Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.

[Space left blank intentionally]

The control objectives and control activities related to 'Network Security' in scope are as below:

CO5: Controls provide reasonable assurance that logical access to Zoho network is protected from unauthorized access and viruses.	
CA5.01	Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA5.02	For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA5.03	For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA5.04	For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA5.05	Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.
CA5.06	Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.
CA5.07	Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure.
CA5.08	IDC servers of Zoho are restricted from accessing internet and mounting removable device.
CA5.09	Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA5.10	Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.

3.7.5 Physical and Environmental Security

Physical Access Security:

Physical Security policy of Zoho is defined by Admin team. The policy document is reviewed and approved by Head of safety and security on an annual basis. The policy document defines the physical access restrictions for Zoho associates.

For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.

For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.

For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.

Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance.

Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.

Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.

Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.

Environmental Security:

Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis (For Austin location the environmental controls are managed by building maintenance vendor):

- Cooling system
- UPS
- DG
- Fire suppression system

Mock fire drill is conducted by Admin team of Zoho on an annual basis.

Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.

Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness. Data copy restriction is imposed for IDC servers of Zoho.

The control objectives and control activities related to 'Physical Security' in scope are as below:

CO6: Controls provide reasonable assurance that physical access to Zoho facilities is restricted to authorized individuals and is monitored for detecting unauthorized access.	
CA6.01	Physical Security policy of Zoho is defined by Admin team. The policy document is reviewed and approved by Head of safety and security on an annual basis. The policy document defines the physical access restrictions for Zoho associates.
CA6.02	For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.

CO6: Controls provide reasonable assurance that physical access to Zoho facilities is restricted to authorized individuals and is monitored for detecting unauthorized access.	
CA6.03	For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.
CA6.04	For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.
CA6.05	Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance.
CA6.06	Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.
CA6.07	Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.
CA6.08	Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.

The control objectives and control activities related to 'Environmental Security' in scope are as below:

CO7: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.	
CA7.01	Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system
CA7.02	Mock fire drill is conducted by Admin team of Zoho on an annual basis.
CA7.03	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA7.04	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.

3.7.6 Manage Human Resource

Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.

Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.

For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining. For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining.

Third party vendor performs background verification (Educational Verification, Employment Verification, Criminal Record Verification, Address Verification and Database Verification) and provides the report. For negative background verification results, HR team performs follow-up action.

Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates. Disciplinary complaints (if any) are raised to Zoho's HR team for appropriate action as per Zoho Disciplinary action policy.

Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.

Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.

The control objectives and control activities related to 'Human Resource' in scope are as below:

CO8: Controls provide reasonable assurance that policies and procedures for hiring and separation of the associates are adhered to.	
CA8.01	Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.
CA8.02	Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.
CA8.03	For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA8.04	For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA8.05	Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.

CO8: Controls provide reasonable assurance that policies and procedures for hiring and separation of the associates are adhered to.	
CA8.06	Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.
CA8.07	Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.

3.7.7 Incident Management

Zoho Incident management team has defined an incident management policy. The document is reviewed and approved by the Information security manager on an annual basis.

Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.

Site 24x7 tool is the inhouse developed application availability monitoring tool of Zoho. Log of activities performed by users in Zoho Cloud products are stored using Zoho logs application. Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.

An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.

The control objectives and control activities related to 'Incident Management' in scope are as below:

CO9: Controls provide reasonable assurance that incident tickets are recorded, analyzed and resolved.	
CA9.01	Zoho Incident management team has defined an incident management policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA9.02	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA9.03	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA9.04	An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.

3.7.8 Backup and Restoration Management Services

Backup of IDC servers are performed using ZAC tool on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool. Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.

Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.

Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.

Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.

The control objectives and control activities related to 'Backup and Restoration Management Services' in scope are as below:

CO10: Controls provide reasonable assurance that data, network configurations are backed up and restored based on the request received.	
CA10.01	Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.
CA10.02	Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA10.03	Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.
CA10.04	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.
CA10.05	Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.

3.7.9 Third Party Management

Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.

On an annual basis Risk assessment is performed by Privacy Team to assess the risk of sub processors and third party vendors identified by them and identify suitable risk treatment plan on an annual basis.

Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.

The control objectives and control activities related to 'Third Party Management' in scope are as below:

CO11: Controls provide reasonable assurance that services performed by third party vendors are monitored as per defined contract.	
CA11.01	Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.
CA11.02	On an annual basis Risk assessment is performed by Privacy Team to assess the risk of sub processors and third party vendors identified by them and identify suitable risk treatment plan on an annual basis.
CA11.03	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.

3.8. Complementary User Entity Controls ('CUECs')

The controls at Zoho, relating to the services provided to user entities cover only a portion of the overall internal control structure of Zoho. The control objectives cannot be achieved without taking into consideration the design of controls at Zoho as well as controls at user entities. Therefore, User entities' internal control structure must be evaluated in conjunction with Service Organization's control policies and procedures.

This section highlights those internal control structure responsibilities that Zoho believe should be present at user entities, and which Zoho has considered in developing its control structure policies and the procedures described in this report. In order to rely on the control structure policies and procedures reported herein, user entities and their auditors must evaluate user entities' internal control structure to determine if the Complementary User Entity Controls mentioned below or similar procedures are in place.

The CUECs mentioned below are as explained and provided by Zoho management:

3.8.1 User entities are responsible for providing and managing the access of with their associates having access to Zoho products including access provisioning, de-provisioning, periodical access review and restriction of administrative access (CA4.01, CA4.02, CA4.03 and CA4.11)

3.8.2 User entities are responsible for communicating any security or privacy incidents to Zoho on a timely basis. (CA9.02)

3.8.3 User entities are responsible for raising any backup restoration request to Zoho. (CA10.03)

User entities are responsible for defining and implementing CUECs provided in sub-section 3.8. These controls address the interface and communication between User entities and Zoho and are not intended to be a complete listing of the controls related to the financial statements of User entities.

3.9. Vendor v/s Subservice Organization (SSO) analysis

Zoho utilizes subservice organizations to support complete, accurate and timely processing of client transactions which are identified in table 1 below. Zoho management assesses the risks associated with these subservice organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner. These include, but are not limited to, the review of third-party service auditors reports, holding discussions with subservice organization management, participating on the client advisory committees, and performing periodic assessments of subservice organizations' facilities, processes, and controls.

Additionally, Zoho utilizes certain vendors in performing controls related to its services.

Zoho's controls relating to the Application development, Production Support and the related General Information Technology Controls relevant to the process covers only a portion of overall internal control for each user entity of Zoho. It is not feasible for the control objective related to Application development, Production Support and the related General Information Technology Controls to be achieved solely by Zoho. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with Zoho's controls and the related tests and results described in section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Table 1: Subservice Organizations

Name of Subservice Organization	Nature of Services Provided
- Sabey Data Center Properties LLC - Databank Holdings Limited - CtrlS Datacenters Limited - Digital Realty Trust Inc. - Equinix Inc. B.V. - Equinix Asia Pacific Pte. Ltd - Colt Technology Service Co. Ltd	Datacenter Co-Location Services

Subservice organizations are responsible for defining and implementing CSOCs provided in sub-section 3.9.

3.9.1 Subservice organizations are responsible for supporting the physical security and environmental safeguard controls for the datacenter. (CA6.02, CA6.03, CA6.04, CA6.05, CA6.06, CA6.07, CA6.08, CA7.01 and CA7.02)

Table 2: Vendors

Organizations that provide services to a service organization that are not considered subservice organizations are referred to as vendors. As Zoho's controls alone are sufficient to meet the needs of the user entities' internal control over financial reporting (that is, achievement of the control objectives is not dependent on the vendor's controls), management has concluded that the entity is not a subservice organization. Zoho uses the vendors in the table below to support the specified functions related to the control objectives in section 4 of this report. However, the activities performed by these vendors are not required to meet the assertions specified in the control objectives, and as a result, no additional procedures are required to be evaluated related to the activities of these vendors.

Name of Vendor	Description of Service(s) Provided
- Powerica Limited - HVAC Space air Pvt ltd - Ardelisys Technologies Private Limited - SVE Energy Private Limited	Environmental equipment maintenance
- G4S Secure Solutions India Private Limited	Physical Security Agency for Security Personnel
- KPMG Assurance and Consulting Services LLP	Background Verification Services

Name of Vendor	Description of Service(s) Provided
- Matrix Business Services India Private Limited	
- Amazon Web Services, Inc.	Content Delivery Network
- Easy Post: Simpler Postage Inc.	Shipping Services
- Google translate: Google LLC	Translation Service
- Litmus Software Inc.	Email Marketing Service

(Space left intentionally blank)

SECTION - 4
Management of Zoho's Description of its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

Section 4. Management of Zoho's Description of its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

4.1 Description of Testing Procedures Performed

Deloitte Haskins & Sells LLP performed a variety of tests relating to the controls listed in this section throughout the period from December 01, 2023 to September 30, 2024. Our tests of controls were performed on controls as they existed during the period of December 01, 2023 to September 30, 2024 and were applied to those controls specified by Zoho.

In determining the nature, timing, and extent of testes, we considered (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the assessed level of control risk, (d) the expected effectiveness of the test, and (e) our understanding of the control environment.

In addition to the tests listed below, we ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of documentation/inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities of manual controls	Obtained documents used in the monitoring activity or manual control activity, independently reperformed the procedures, and compared any discrepancies identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

4.2 Testing of tools supporting control activities

For the tools used in the performance of control activities in Section 4, we performed procedures to address the risks associated with their use. While these procedures were not specifically included in the test procedures listed in Section 4, they were completed as part of the testing to support our conclusions.

4.3 Reliability of information produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information in response to ad hoc requests from the service auditor (e.g., population lists), and (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Our procedures to evaluate whether this information was sufficiently reliable included procedures to address (a) the accuracy and completeness of source data, and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by the Service Organization.

4.4 Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of control tests because Deloitte Haskins & Sells LLP does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, Deloitte Haskins & Sells LLP reports all exceptions.

(Space left intentionally blank)

4.5 Test Procedures performed by Service Auditors

4.5.1 Change Management

Control Objective 01: Controls provide reasonable assurance that segregation of environments is maintained.

In addition to the tests listed below for control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUECs/CSOC	Results of Tests
CA1.01	Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.	Inspected for sample cloud products the production and local page for aspects such as 'Product name', 'Product page URL' and 'Local page URL' to ascertain whether Zoho Cloud products maintained dedicated development and test environment in local Zoho and whether the local Zoho environment was segregated from production environment of Zoho Cloud products.	None	No Exception Noted

(Space left blank intentionally)

Control Objective 02: Controls provide reasonable assurance that application and server changes are documented, tested and approved as per the procedures.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUECs/CSOC	Results of Tests
CA2.01	Change management policy of Zoho is defined by the compliance team. The document is review by compliance manager and approved by the web master – project manager on an annual basis.	Inspected the change management policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether change management policy of Zoho was defined by the compliance team and whether the document was review by compliance manager and approved by the web master – project manager on an annual basis.	None	No Exceptions Noted
CA2.02	Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.	Inspected Hardening guidelines of IDC servers for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether hardening guidelines for onboarding IDC Servers of Zoho was defined by server operations team and whether the guidelines document was reviewed and approved by Server Operations Manager on an annual basis.	None	No Exceptions Noted

#	Control Activity	Tests Performed	CUECs/CSOC	Results of Tests
CA2.03	Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.	Inspected for sample products the software development life cycle document for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether software development life cycle document of Zoho Cloud products was defined by the product team and whether the document was reviewed and approved by Product manager on an annual basis and whether the document defined the change testing and deployment process for the product.	None	No Exceptions Noted.
CA2.04	Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.	Inspected for sample changes made to Cloud/On-Prem product the deployment logs for aspects such as 'Build URL', 'Date of local deployment', 'Date of production deployment'; Further inspected for sample changes made to Cloud product the testcases and testing signoff record for aspects such as 'Tested by', 'Tested on' and 'Testcases' to ascertain whether changes made to Cloud products were deployed using inhouse SD tool to production and local environment and whether the build generated were tested in local Zoho and signoff was provided by product manager before deployment in production environment/publishing in website.	None	Exception Noted. Refer Exception #1

#	Control Activity	Tests Performed	CUECs/CSOC	Results of Tests
CA2.05	Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.	Inspected for sample changes made to Cloud product the hacksaw report and exceptional approval records for aspects such as 'Build URL', 'Number of blocking issue', 'Exceptional approval provided by' and 'Exceptional approval provided on' to ascertain whether changes made to Cloud products were reviewed for code vulnerabilities using inhouse Hacksaw tool and whether exceptional approval was provided by the product manager if the changes were deployed in production environment/publishing in website with blocking issue.	None	No Exceptions Noted.
CA2.06	Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.	Inspected for sample products the support process document for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether Support process document of Zoho Cloud products was defined by the product team and whether the document was reviewed and approved by Product manager on an annual basis and whether the document defined the support process and data flow of the product.	None	No Exceptions Noted.
CA2.07	IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.	Inspected for sample IDC patches the ticket for aspects such as 'Patch ID', 'Tested by', 'Tested on', 'Approved by', 'Approved on' and 'Deployed on' to ascertain whether operating system of IDC servers were patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.	None	Exception Noted. Refer Exception #2

4.5.2 Information Security

Control Objective 03: Controls provide reasonable assurance that Information Security policies and procedures are documented, approved and communicated to associates.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA3.01	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.	Inspected Information Security Management System policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether Information Security Management System policy of Zoho was defined by Information security compliance Manager and whether the policy document was reviewed and approved by Chief Information Security Officer on an annual basis and whether the policy document defined the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.	None	No Exceptions Noted
CA3.02	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.	Inspected the Integrated Management System Manual in Zoho portal for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on', and 'Availability in intranet portal' to ascertain whether Zoho's management committee was responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis and whether policies and procedures related to information security were made available to associates through the intranet portal.	None	No Exceptions Noted

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA3.03	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.	Inspected for sample new joiners the Induction Training records in Zoho People for aspects such as 'associate's date of joining', 'date of training completion', 'attendance status', 'training completion status' and 'content of induction training material' to ascertain whether induction training was completed by the associate on the date of joining and the induction training covered the information security and privacy commitments of Zoho and also whether the attendance for completion of induction training is captured in Zoho People.	None	Exception Noted. Refer Exception #3
CA3.04	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.	Inspected for sample active associates the annual refresher training records in Zoho Learn for aspects such as 'Associate ID', 'Associate name', 'date of training completion', 'training completion status' and 'content of induction training material' to ascertain whether annual refresher training was completed by the associate and the annual refresher training covers the information security and privacy commitments of Zoho and whether the attendance for completion of annual refresher training was captured in Zoho Learn.	None	No Exceptions Noted.

4.5.3 Logical Access Security

Control Objective 04: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA4.01	Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.	Inspected Zoho password policy and password configuration of Active directory, Zoho Directory and IAM for aspects such as 'Password configuration', 'Account lockout configuration' and 'Password guidelines as per policy' to ascertain whether security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account were defined as per Zoho password policy.	3.8.1	Exception Noted. Refer Exception #4
CA4.02	For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining.	Inspected for sample joiners the IAM account creation log for aspects such as 'associate's date of joining', 'access created on' and 'access created by' to ascertain whether the HR team created the IAM account in Zoho people for the associate on their date of joining.	3.8.1	No Exceptions Noted.
CA4.03	For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date.	Inspected for sample leavers the IAM account revocation LOG for aspects such as 'Associate ID', 'Associate name', 'Associate's last working date' 'Access revoked on' 'Access revoked by' 'Email sent by' 'to ascertain whether the HR team revoked the IAM account in Zoho people for the associate on their last working date.	3.8.1	Exception Noted. Refer Exception #5

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA4.04	For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.	Inspected the SDP integration and for sample new joiners the domain account creation log and email relating to domain account creation for aspects such as 'Associate's date of joining ' 'Access created on' 'Access created by' 'Email sent by' 'Email sent to' 'Email sent on' to ascertain whether the HR team notified the sysadmin team for domain account creation and whether an automated SDP ticket was created and closed by the sysadmin team upon creation of the domain ID.	None	No Exception Noted.
CA4.05	For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.	Inspected for sample leavers the domain account revocation log and ticket relating to domain account revocation for aspects such as ‘Access name’, ‘Associate ID’, 'Associate's last working date' 'Access revoked on' 'Access revoked by', ‘Ticket ID', Email sent by' 'Email sent to' 'Email sent on' to ascertain whether the HR team notified the sysadmin team for domain account revocation and also whether an automated SDP ticket was created and closed by the sysadmin team upon deletion of the domain ID.	None	No Exception Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA4.06	For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.	Inspected for sample access creation to network operations tools the SDP ticket for aspects such as 'Associate joining date', 'Ticket ID', 'Approved by', 'Approved on', 'Access created by', 'Access created to' and 'Access created on' to ascertain whether for creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request was raised in Zoho SDP and whether network operations team created access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.	None	No Exception Noted.
CA4.07	For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.	Inspected for sample access revocation to network operations tools the SDP ticket for aspects such as 'Associate last working date', 'Ticket ID', 'Approved by', 'Approved on', 'Access revoked by', 'Access revoked to' and 'Access revoked on' to ascertain whether for creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request was raised in Zoho SDP and whether network operations team created access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.	None	No Exception Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA4.08	For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.	Inspected for sample access creation to server operation tools the SDP ticket for aspects such as 'Associate joining date', 'Ticket ID', 'Approved by', 'Approved on', 'Access created by', 'Access created to' and 'Access created on' to ascertain whether for creation of access to Server Operation tools (ZAC and Server Operations Passman), the request was raised in Zoho SDP and whether server operations team created access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.	None	No Exception Noted.
CA4.09	For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.	Inspected the passman tool and IAM integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the access to Server Operations Passman tool was revoked based on the integration with IAM. Further inspected the ZAC tool and Zoho people integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the access to ZAC was revoked based on the integration with Zoho People.	None	No Exception Noted.
CA4.10	Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.	Inspected authentication configuration of VPN application for aspects such as 'Tool name' and 'Integration' to ascertain whether security setting for authentication to Zoho Corporate VPN was managed by Active Directory.	None	No Exception Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA4.11	IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any)	Inspected the IAM role review report for aspects such as 'Content of report', 'Date of review', 'Reviewed on', 'Approval details' and 'Corrective action taken' to ascertain whether IAM roles access to Zoho associates were reviewed on an annual basis and whether the extension of IAM roles were based on approval provided by the associate and associate's manager and whether corrective action was performed by IAM team for discrepancies identified (if any)	3.8.1	Exception Noted. Refer Exception #6
CA4.12	For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.	Inspected for sample access creation to jump server the SDP ticket for aspects such as 'Ticket ID', 'Associate name', 'Associate date of joining', 'Approved by', 'Approved on', 'Access created by' and 'Access created on' to ascertain whether for creation of access to Jump server, the request was raised in Zoho SDP and whether server operations team created access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.	None	No Exceptions Noted.
CA4.13	For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.	Inspected for sample access revocation to jump server the SDP ticket for aspects such as 'Ticket ID', 'Associate name', 'Associate last working date', 'Access revoked by' and 'Access revoked on' to ascertain whether for revocation of access to jump server, the request was raised in Zoho SDP and whether server operations team revoked access to Jump server and IDC server account for the associate and whether for associates leaving from Zoho, the access to Jump server and IDC server account was revoked on the associate's last working date.	None	Exceptions Noted. Refer Exception #7

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA4.14	Administrative access to Jump Server of Zoho is restricted to Server Operations team.	Inspected the user access list of jump server for aspects such as 'User listing' and 'Team name' to ascertain whether administrative access to Jump Server of Zoho was restricted to Server Operations team.	None	No Exceptions Noted.
CA4.15	For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.	Inspected the Zero Trust and Zoho people integration aspects such as 'Tool name' and 'Integration' to ascertain whether for associates joining Zoho, the Zero Trust account was created based on the integration with Zoho People.	None	No Exceptions Noted.
CA4.16	For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.	Inspected the Zero Trust and Zoho people integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the Zero Trust account was revoked based on the integration with Zoho People.	None	No Exceptions Noted.
CA4.17	For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.	Inspected for sample zero trust policy access creation the ticket for aspects such as 'Policy name', 'Approved by', 'Approved on', 'Access created by', 'Access created on' and 'Hardening agent version' to ascertain whether for creation of access to Zero Trust policy, the request was raised in Zero trust application by the associate and whether SPM team created access to the associate based on the report from hardening agent installed at the associate's endpoint.	None	No Exceptions Noted.

Control Objective 05: Controls provide reasonable assurance that logical access to Zoho network is protected from unauthorized access and viruses.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA5.01	Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.	Inspected for sample workstations the CrowdStrike EDR console for aspects such as 'Host name', 'Type of OS', 'Location' and 'Status of EDR' to ascertain whether workstations of Zoho were installed with CrowdStrike EDR. Further inspected for sample EDR alerts the service desk plus ticket for aspects such as 'Ticket ID', 'Opened on', 'Closed on' and 'Corrective action performed' to ascertain whether system administration team performed follow-up action for anomalies identified.	None	No Exceptions Noted.
CA5.02	For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.	Inspected for sample VLAN setup/modification request the SDP ticket for aspects such as 'Ticket ID', 'Date of ticket opening', 'Date of ticket closing', 'Approved by', 'Approved on' to ascertain whether for setup/modification to segregated VLAN, the request was raised in Zoho SDP and whether Network Operations team created/modified segregated VLAN for the request based on the approval provided by Network Operations Manager.	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA5.03	For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.	Inspected for sample firewall ruleset changes the SDP ticket for aspects such as 'Ticket ID', 'Date of ticket opening', 'Date of ticket closing', 'Approved by', 'Approved on' to ascertain whether for addition/modification for firewall ruleset, the request was raised in Zoho SDP and whether Network Operations team added/modified firewall ruleset for request based on the approval provided by Network Operations Manager.	None	No Exceptions Noted.
CA5.04	For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.	Inspected for sample network device configuration changes the SDP ticket for aspects such as 'Ticket ID', 'Date of ticket opening', 'Date of ticket closing', 'Approved by', 'Approved on' to ascertain whether for changes to network device configuration, the request was raised in Zoho SDP and whether network Operations team changed network device configuration based on approval provided by Network Operations Manager.	None	No Exceptions Noted.
CA5.05	Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.	Inspected for sample half year the firewall rule review ticket for aspects such as 'Ticket ID', 'Scope', 'Date of review', 'Reviewed by' and 'Follow-up action performed' to ascertain whether rules of Zoho wide area network and local area network was reviewed by Network Operations team on a half yearly basis and whether network operations team performed follow-up action for anomalies identified.	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA5.06	Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.	Inspected for sample weeks the vulnerability assessment report for aspects such as 'Scope', 'Scan result' and 'follow-up performed' to ascertain whether vulnerability assessment was performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis and whether vulnerabilities identified if any are notified to relevant team for closure.	None	Exception Noted. Refer Exception #8
CA5.07	Penetration testing is performed for External IP of Zoho on a annual basis. Vulnerabilities identified if any are tracked to closure.	Inspected the penetration testing report for aspects such as 'Scope', 'Scan result' and 'closure action performed' to ascertain whether penetration testing was performed for External IP of Zoho on an annual basis and whether vulnerabilities identified if any were tracked to closure.	None	Exception Noted. Refer Exception #9
CA5.08	IDC servers of Zoho are restricted from accessing internet and mounting removable device.	Inspected for sample IDC servers the ping configuration for aspects such as 'Host name', ‘removable device block’ and 'Internet access block' to ascertain whether IDC servers of Zoho were restricted from accessing internet.	None	No Exceptions Noted.
CA5.09	Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.	Inspected for sample network devices the monitoring configuration for aspects such as 'Hostname', 'Parameters monitored' and 'monitoring tool'; Further inspected for sample NOCMON alerts the tickets for aspects such as 'Ticket ID', 'Date of incident opening', 'Date of incident closing', 'Closure action performed' to ascertain whether Firewall, Router and Managed Switches were monitored for downtime and process utilization using NOCMON tool and whether Network Operations team performed follow-up action for anomalies identified.	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA5.10	Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.	Inspected network diagram for aspects such as 'Scope', 'Content of network diagram', 'Reviewed by' and 'Date of review' to ascertain whether network diagram of Zoho was defined by the Network operations team and whether the network diagram was reviewed and approved by Network operations team on an annual basis and whether the network diagram defined the components and connections within Zoho network.	None	No Exceptions Noted.

[Space left blank intentionally]

4.5.4 Physical and Environmental Security

Control Objective 06: Controls provide reasonable assurance that physical access to Zoho facilities is restricted to authorized individuals and is monitored for detecting unauthorized access.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA6.01	Physical Security policy of Zoho is defined by Admin team. The policy document is reviewed and approved by Head of safety and security on an annual basis. The policy document defines the physical access restrictions for Zoho associates.	Inspected the physical security policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether physical Security policy of Zoho was defined by Admin team and the policy document was reviewed and approved by Head of safety and security on an annual basis and whether the policy document defined the physical access restrictions for Zoho associates.	None	No Exceptions Noted.
CA6.02	For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.	Inspected for sample new joiners the physical access creation log and email relating to access creation for aspects such as 'Associate ID', 'Associate name', 'associate's date of joining', 'access creation email sent on', 'access creation email sent from', 'access creation email sent to', 'access created on', 'access created by' and 'email configuration' to ascertain whether the HR team enters the joining date in Zoho people and whether the admin team created physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.	3.9.1	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA6.03	For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.	Inspected for sample leavers the physical access revocation log and email relating to access revocation for aspects such as 'Associate ID', 'Associate name', 'associate's last working date', 'access revocation email sent on', 'access revocation email sent from', 'access revocation email sent to', ' access revoked on', 'access revoked by' and 'email configuration' to ascertain whether the HR team enters the last working date in Zoho people and whether admin team revoked physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.	3.9.1	Exception Noted. Refer Exception #10
CA6.04	For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.	Inspected for sample access card lost cases the physical access logs and ticket from Zoho People for aspects such as 'associate's access card lost date', 'access recreation email sent on', 'access recreation email sent from', 'access recreation email sent to', 'old access revoked on', 'new access created on', 'access recreated by', 'access revoked by' and 'email configuration' to ascertain whether the associate raise request in Zoho People and whether admin team revoked physical access for the lost card and created physical access for the new card based on the automatic email triggered from Zoho People on the date of request.	3.9.1	No Exceptions Noted.
CA6.05	Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance.	Inspected for sample dates the security guard registry for aspects such as entry and exit points of Zoho Facilities was manned by security guards and security guard registry was maintained by the admin team to track attendance.	3.9.1	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA6.06	Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.	Inspected for sample dates the visitor and vendor registry from visitor management system for aspects such as 'vendor and visitor details', 'date', 'review sign', 'Escort details' and 'location' to ascertain whether visitor and vendors entering Zoho are recorded in visitor management system and the escort details were recorded as part of the registry.	3.9.1	No Exceptions Noted.
CA6.07	Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.	Inspected the Zoho Facilities Server Operations Team and NOC room of Zoho for aspects such as 'Location', 'PIN based access system status' and 'Proximity card system status' to ascertain whether access to facilities, Datacenter, Server Operations Team and NOC room of Zoho was restricted by proximity card system and whether in addition, Server Operations Team and NOC room were protected with PIN based access.	3.9.1	No Exceptions Noted.
CA6.08	Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.	Inspected the Zoho Facilities, Server Operations Team and NOC room of Zoho for aspects such as 'Location', 'Availability of CCTV' and 'CCTV retention period' to ascertain whether Facilities, Server Operations Team and NOC room of Zoho was monitored by CCTV and whether the CCTV recordings are retained for a period of 60 days.	3.9.1	No Exceptions Noted.

[Space left blank intentionally]

Control Objective 07: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA7.01	Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system	Inspected the Planned Preventive Maintenance reports of Zoho facilities for aspect such as 'Date of service', 'Location' 'Service report output' to ascertain whether Facilities, Datacenter, Server Operations Team and NOC room of Zoho were installed with the following environmental safeguards and also whether the equipment was serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system	3.9.1	No Exceptions Noted.
CA7.02	Mock fire drill is conducted by Admin team of Zoho on an annual basis.	Inspected the annual mock fire drill report of Zoho facilities for aspects such as 'Date of drill' 'Drill participants ' 'Drill outcome' to ascertain whether mock fire drill was conducted by Admin team of Zoho on an annual basis.	3.9.1	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA7.03	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.	Inspected Business continuity plan of Zoho for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether business continuity plan of Zoho was defined by Information security compliance Manager and whether the plan document was reviewed and approved by BCP Head on an annual basis and whether the plan document outlines how a business would continue to operate during an unplanned disruption in Zoho.	None	No Exceptions Noted.
CA7.04	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.	Inspected the Disaster recovery readiness report for aspects such as 'Datacenter ID', 'Date of test' and 'Test outcome' to ascertain whether server operations team on an annual basis switched service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.	None	Exception Noted. Refer Exception #11

[Space left blank intentionally]

4.5.5 Manage Human Resources

Control Objective 08: Controls provide reasonable assurance that policies and procedures for hiring and separation of the associates are adhered to.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA8.01	Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.	Inspected Job Description of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Job Description of Zoho was defined by Senior Manager TA and HR operations and the policy document was reviewed and approved by the Associate Director TA and HR operations on an annual basis and whether the policy document defined the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.	None	No Exception Noted.
CA8.02	Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.	Inspected Background Verification policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Background Verification Policy of Zoho was defined by HR team and the policy document was reviewed and approved by the Deputy Manager HR on an annual basis and whether the policy document defined the background verification process for Zoho associates.	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA8.03	For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.	Inspected for sample new joiners the background verification report for aspects such as 'associate ID', 'associate name', 'associate's date of joining', 'date of BGV initiation', 'date of BGV completion', 'BGV result' to ascertain whether background verification was initiated by HR team within 2 days from date of joining and whether third party vendor performed background verification and provides the report; also ascertained whether for negative background verification results, HR team performed follow-up action.	None	No Exceptions Noted.
CA8.04	For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.	Inspected for sample new joiners the Non Disclosure Agreement for aspects such as 'associate's date of joining', 'Signatory', 'date of signature' and 'content' to ascertain whether Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy were signed by the associate before date of joining.	None	No Exceptions Noted.
CA8.05	Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.	Inspected code of ethics document of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'contents' to ascertain whether code of ethics document of Zoho was defined by HR team and the policy document was reviewed and approved by the Deputy Manager HR on an annual basis and whether the policy document defined the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA8.06	Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.	Inspected Hiring and Separation policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether hiring and separation policy of Zoho was defined by HR team and the policy document was reviewed and approved by Deputy Manager HR on an annual basis and whether the policy document defined the onboarding and offboarding process for Zoho associates.	None	No Exceptions Noted.
CA8.07	Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.	Inspected Organization chart of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Organization chart was defined by HR team and the policy document was reviewed and approved by Senior Manager HR on an annual basis and whether the organization chart defined the departments and internal structure of Zoho.	None	No Exceptions Noted.

4.5.6 Incident Management

Control Objective 09: Controls provide reasonable assurance that incident tickets are recorded, analyzed and resolved.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA9.01	Zoho Incident management team has defined an incident management policy. The document is reviewed and approved by the Information security manager on an annual basis.	Inspected the incident management policy for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Zoho Incident management team had defined an incident management policy and whether the document was reviewed and approved by the Information security manager on an annual basis	None	No Exceptions Noted.
CA9.02	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.	Inspected for sample incidents, the ticket from creator tool for aspects such as 'Incident ID', 'Incident Title', 'Description of the incident', 'RCA available', 'Raised By' 'Incident Cause', 'Incident Category' and 'Incident start time' and 'Status' to ascertain whether incidents raised from customer were raised as ticket in Zoho Desk Portal which was assigned to the Zoho incident management team for resolution and whether the relevant product team performed root cause analysis (RCA) and updates the incident in the Zoho creator tool.	3.8.2	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA9.03	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.	Inspected for sample products the site 24x7 dashboard for aspects such as 'Product name', 'DC Name' and 'Monitoring status'; Further inspected for sample incidents the 'Incident ID', 'Date of incident opening' and 'Date of incident closing', 'Incident closed by' to ascertain whether Zoho cloud products were monitored for downtime using Site 24x7 tool and whether anomalies (if any) were tracked to closure by incident management team.	None	No Exceptions Noted.
CA9.04	An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.	Inspected the incident report for aspects such as 'Reviewed by', 'Reviewed on', 'Name of report', 'Report uploaded by', 'Date of report' and 'Content of report' to ascertain whether An Incident report was reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal and whether the report included the categories of incidents, downtime details (in case of availability incident) and the incident description.	None	No Exceptions Noted.

4.5.7 Backup and Restoration Management Services

Control Objective 10: Controls provide reasonable assurance that data, network configurations are backed up and restored based on the request received.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA10.01	Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.	Inspected for sample IDC servers the backup configuration for aspects such as 'Host name', 'Type of backup' and 'Backup frequency' to ascertain whether backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) were configured using ZAC tool by Server Operations team.	None	No Exceptions Noted.
CA10.02	Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.	Inspected for sample network devices the backup configuration for aspects such as 'Hostname', 'Type of backup' and 'backup frequency'; Further inspected for sample dates the backup logs for aspects such as 'Backup status' and 'Corrective action performed' to ascertain whether backup of Network device configurations (Firewall, Router and Managed Switches) were performed using Network Configuration Manager tool on a daily basis (Full Backup) and whether in case of a backup failure, an automated email was triggered and remediation action was taken by Network Operations team.	None	No Exceptions Noted

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA10.03	Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.	Inspected for sample backup restoration request the restoration tickets for aspects such as 'Ticket ID', 'Date of request', 'Date of closure' and 'Restoration status' to ascertain whether restoration of backup of IDC servers were performed using ZAC tool based on request from customer.	3.8.3	No Exceptions Noted.
CA10.04	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.	Inspected for sample IDC servers the cluster configuration for aspects such as 'Host name' and 'implementation of redundant cluster' to ascertain whether data stored in IDC network were set up with redundant database clusters to ensure mirroring of customer data.	None	No Exceptions Noted.
CA10.05	Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.	Inspected for sample assets disposed the approval records and asset disposal registry for aspects such as 'Asset ID', 'Disposed on', 'Approved by', 'Approved on' and 'Parameters in registry' to ascertain whether server operations team maintained an asset disposal registry at Zoho Datacenter and whether the assets were degaussed and disposed based on the approval provided by Server operations manager.	None	No Exceptions Noted.

[Space left blank intentionally]

4.5.8 Third Party Management

Control Objective 11: Controls provide reasonable assurance that services performed by third party vendors are monitored as per defined contract.

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period December 01, 2023 to September 30, 2024

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA11.01	Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.	Inspected reports relating to review of third party report for aspects such as 'Datacenter ID', 'Vendor name', 'Exceptions identified', 'Relevance to Zoho' and 'Follow-up action performed' to ascertain whether Network Operations team reviewed the third party reports of co location datacenter on an annual basis and whether follow-up action was performed by compliance team for exceptions identified.	None	No Exceptions Noted.
CA11.02	On an annual basis Risk assessment is performed by Privacy Team to assess the risk of sub processors and third party vendors identified by them and identify suitable risk treatment plan on an annual basis.	Inspected for sample vendors/sub processors the risk assessment report for aspects such as 'Date of risk assessment', 'Assessment scope' and 'Risk assessment outcome' to ascertain whether on an annual basis risk assessment was performed by Privacy Team to assess the risk of sub processors and third party vendors identified by them and identify suitable risk treatment plan on an annual basis.	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUEC/CSOC	Results of Tests
CA11.03	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	Inspected the master service agreement with co-location vendors for aspects such as 'Datacenter ID', 'Vendor name', 'Signatory details', 'Scope', 'Availability of confidentiality and related clause' and 'Tenure' to ascertain whether master service agreement was signed between Zoho and co location datacenter hosting service vendor and whether any changes to the contracts were agreed by Zoho and the co location datacenter hosting service vendor and whether the contract included the scope of services to be provided, confidentiality and other related commitments / clauses.	None	No Exceptions Noted.

[Space left blank intentionally]

4.6 Management Responses to Exceptions

The examination exceptions presented in the Section 4 of this report were reviewed and discussed on December 12, 2024 during a dedicated Closing Meeting attended by the Service Auditors and Zoho Compliance Team.

The Management Responses to the exceptions noted is as under:

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #1	We noted that for 1 out of 25 sample builds selected, there were no records of testing document maintained.	CA2.04: Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website. CO2: Controls provide reasonable assurance that application and server changes are documented, tested and approved as per the procedures.	We agree with the exception noted. There were no formal documentation maintained for testcases validated as part of the QA process for the identified sample build. However, QA signoff was obtained before pushing build to production. Further, there were no incidents noted from pushing the 1 change to production. Going forward, the management will formally document the testcases validated as part of the QA process.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #2	We noted that 5 out of 25 sample servers run on Unix version whose support life ended in June 2024.	CA2.07: IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager. CO2: Controls provide reasonable assurance that application and server changes are documented, tested and approved as per the procedures.	We agree with the exception noted. The management was in process of selecting the EOL support vendor because of which there was no end of life support for the period July 2024 till September 2024. However, the management performs vulnerability assessment and penetration testing on a periodic basis to identify the vulnerabilities and perform corrective action. Further, the management has purchased end of life support from November 2024. The servers will be migrated to a vendor supported OS by Q3 2025.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #3	We noted that there is no induction training completion record maintained for 3 out of 25 sample associates.	CA3.03: For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People. CO3: Controls provide reasonable assurance that Information Security policies and procedures are documented, approved and communicated to associates.	We agree with the exception noted. The same has been actioned upon with appropriate escalation to our senior management after the completion of examination period. Also we noted that there were no security violations by these 3 employees. In addition to this, management will periodically monitors the completion status of induction training as part of the onboarding process to identify the employees who have not completed. Going forward, the same shall be rigorously monitored by the human resource team to ensure there are very minimal defaults.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #4	We noted that the password history configuration for IAM and ZD, password expiry configuration for AD and account lockout configuration of Zero Trust, IAM and ZD were configured but were not in line with Zoho's password policy.	CA4.01: Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy. CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	We agree with the exception noted. The password configurations mentioned are not in line with the policy. We have initiated the rectification activity for the same. However, to access customer data in IDC network the user has to utilize password from the passman tool. The password in passman tool adheres to Zoho password policy during the examination period.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #5	We noted that the IAM accounts access was revoked after last working date for 7 of 25 sample associates with a delay ranging from 2 to 34 days	CA4.03: For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date. CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	We agree with the exception noted. There was a delay in revocation of access for 7 sample associates. However, upon inspection of the IAM access logs, the associates did not login after the last working date. Hence, no customer data was accessed by the associates after their last working date. In addition to this, there were no security incidents noted due to these associates. Going forward, the management shall implement measures to revoke IAM access as part of the exit clearance process.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #6	We noted that Zoho associates' IAM access/role review was not performed during the examination period.	CA4.11: IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any) CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	We agree with the exception noted. The management is developing a new tool for the review of IAM roles because of which there is a delay in the review process. However, the IAM roles are created and assigned based on the approval from managers and the access to IAM accounts are revoked on the associate's last working date. The previous IAM role access review was completed in June 2023. Further, there were no security incidents identified due to inappropriate IAM roles assigned to Zoho associates. The management has started the IAM role review activity and will complete by Q1 2025.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #7	We noted that there was a delay in access revocation to jump server for 6 out of 25 sample associates ranging from 6 to 43 days	CA4.13: For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date. CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated.	We agree with the exception noted. There was a delay in revocation of access for 6 sample associates. However, the zero trust accounts were disabled on a timely manner. Further, upon inspection of the access logs, it was noted that the associates did not login after the last working date to the jump servers. In addition to this, there were no security incidents noted due to these associates. Going forward, the management shall implement measures to revoke jump servers access as part of the exit clearance process.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #8	We noted that the vulnerability assessment for external IP of product was performed with a delay of for 3 out of 25 samples selected.	CA5.06: Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure. CO5: Controls provide reasonable assurance that logical access to Zoho network is protected from unauthorized access and viruses.	We agree with the exception noted. There was a delay in performing vulnerability scan for the 3 samples selected. However, the management performed scans in the upcoming weeks and no issues were identified. Moving forward, the management shall track the status of vulnerability assessment and ensure timely completion.
Exception #9	We noted that there was no formal documentation maintained for corrective action performed for 178 out of 194 vulnerabilities identified from the PT reports of 5 out of 15 sample products	CA5.07: Penetration testing is performed for External IP of Zoho on a annual basis. Vulnerabilities identified if any are tracked to closure. CO5: Controls provide reasonable assurance that logical access to Zoho network is protected from unauthorized access and viruses.	We agree with the exception noted. The PT report template used for the 5 sample reports did not capture the individual closure status of the vulnerabilities identified. Further, vulnerability scans were performed on a regular basis at a weekly frequency. However, the management has updated the template from Q3 2024 and the PT reports will capture the closure status of the vulnerabilities identified.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #10	We noted that there was a delay in physical access revocation for 3 out of 25 sample associates ranging from 7 to 12 days.	CA6.03: For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date. CO6: Controls provide reasonable assurance that physical access to Zoho facilities is restricted to authorized individuals and is monitored for detecting unauthorized access.	We agree with the exception noted. There was a delay in revocation of access for 3 sample associates. However, upon inspection of the physical access logs, the access cards were not used after the last working date and the logical access to the domain and IAM accounts were revoked on the last working date of the associate. In addition to this, there were no security incidents noted due to these associates. Going forward, the management shall implement measures to revoke physical access to facility as part of the exit clearance process.

Exception Number	Description of Exception	Control Objective and Control Activity Impacted by Exception	Management Response to Exception
Exception #11	We noted that Disaster Recovery (DR) readiness test for India datacenter was performed in a delayed manner	CA7.04: Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness. CO7: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.	We agree with the exception noted. There was a delay in performing Disaster Recovery (DR) readiness test for India datacenter. However, the management performed the test on Q4 2024 and noted no disruptions that could impact the availability of the applications. Further, the previous disaster recovery test was performed in Q2 2023. In addition, backup of servers is also being performed on a daily basis. Going forward, the management will monitor the completion of disaster recovery readiness test and ensure timely completion.

Deloitte
Haskins & Sells LLP

Document Reference No.: RA-TPA-31096388-2024-25-R106