

## 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 for services provided to its customers and Suitability of the Design and Operating Effectiveness of controls for the period December 01, 2021 to November 30, 2022.

This report is intended solely for the information and use of Zoho Corporation Private Limited, user entities and their user auditors and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report.

# Table of Contents

|  |    |
|--|----|
| SECTION 1. INDEPENDENT SERVICE AUDITORS' REPORT .....                  | 1  |
| SECTION 2. MANAGEMENT ASSERTION PROVIDED BY SERVICE ORGANIZATION ..... | 5  |
| SECTION 3. SYSTEM DESCRIPTION PROVIDED BY SERVICE ORGANIZATION .....   | 8  |
| SECTION 4. INFORMATION PROVIDED BY SERVICE AUDITOR .....               | 35 |

# SECTION - 1:

## Independent Service Auditors' Report

# Section 1. Independent Service Auditors' Report

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

**For the period December 01, 2021 to November 30, 2022**

**To the Management of Zoho Corporation Private Limited**

### Scope

We have examined the description of the system 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 (GITC) ("description of the system"), for services provided to customers ('User Organizations' or 'User Entities'), from Zoho Corporation's Offshore Development Centers ('ODC') at Chennai, Tenkasi, Renigunta in India, Austin and Pleasanton in USA throughout the period December 1, 2021 to November 30, 2022 and the suitability of the design and operating effectiveness of controls included in the Description to achieve the related control objectives also included in the Description, based on the criteria identified in Section 2 (the '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 of Zoho that are not likely to be relevant to user entities' internal control over financial reporting.

The Service Organization uses Sabey Data Center Properties LLC, Zayo Group, LLC Colocation Services ("zColo"), Interxion HeadQuarters B.V., Equinix Inc. B.V., CtrlS Datacenters Limited and Equinix Asia Pacific Pte. Ltd; for datacenter co-location services and KPMG, Matrix Business Services India Private Limited and Hire Right LLC for background verification of associates ("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 the Service Organization's controls are suitably designed and operating effectively, along with related controls at the Service Organization. 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 Organizations' Responsibilities**

In Section 2, the Service Organization 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. The Service Organization 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 Auditors' 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 Statement on Standards for Attestation Engagements No. 18 Attestation Standards: Clarification and Recodification ("SSAE 18") established by the American Institute of Certified Public Accountants ('AICPA') and International Standard on Assurance Engagements 3402 ('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 1, 2021 to November 30, 2022. 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.
- We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.

## **Service Auditors' Independence and Quality Control**

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the statements on quality control standards established by the AICPA 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 may not therefore, include every aspect of the system that each individual user entity 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 we tested and the nature, timing, and results of our tests are listed in Section 4 of this report.

## Opinion

In our opinion, in all material respects, based on the criteria described in the Service Organization's assertion in Section 2 of the report:

- a. The Description fairly presents the system related to the Application Development, Production Support and the related GITC provided by Zoho to its user entities that was designed and implemented throughout the period December 1, 2021 to November 30, 2022.
- 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 1, 2021 to November 30, 2022, and user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout the period December 1, 2021 to November 30, 2022.
- c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period December 1, 2021 to November 30, 2022 if complementary user entity controls and complementary subservice organization controls assumed in the design of Zoho's controls operated effectively throughout the period December 1, 2021 to November 30, 2022.

## Emphasis of matter

Zoho states in its description that it had controls in place for physical and environmental security for Zoho premises. However, post March 2021 till date, Employees from Austin and Pleasanton in USA only work remotely and hence the below control activities were not applicable for the afore mentioned locations

Control Objective 6: Controls provide reasonable assurance that physical access to Zoho facilities is restricted to authorized individuals and is monitored for detecting unauthorized access.

Control Objective 7: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.

CA-6.01, CA-6.02, CA-6.03, CA-6.04, CA-6.05, CA-6.06, CA-6.07, CA-7.01, CA7.02, CA-7.03

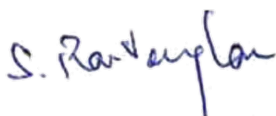
## Restricted Use

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 the Service Organization, user entities of the Service Organization's system related to the Application Development, Production Support and the related General IT Controls provided by Zoho to its user entities throughout the period December 1, 2021 to November 30, 2022, 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 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

March 15, 2023

## SECTION - 2

# Management Assertion provided by Service Organization





# Section 2. Management Assertion provided by Service Organization

## Management Assertion by Zoho Corporation Private Limited

The signed Management assertion has been provided by Service Organization Management via letter dated March 15, 2023. The extract of the letter is as under:

We have prepared the description of the system of Zoho Corporation Private Limited's ('Zoho' or 'Company' or 'Service Organization') related to Application Development, Production Support and the related General Information Technology Controls (GITC) for services provided to customers ('User Organisation' or 'User Entities') from Zoho's Offshore Development Centers located at Chennai, Tenkasi, Renigunta in India, Austin and Pleasanton in USA throughout the period December 1, 2021 to November 30, 2022, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by 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, Zayo Group, LLC Colocation Services ("zColo"), Interxion HeadQuarters B.V., Equinix Inc. B.V., CtrlS Datacenters Limited and Equinix Asia Pacific Pte. Ltd; for datacenter co-location services and KPMG, Matrix Business Services India Private Limited and Hire Right LLC for background verification of associates ("Subservice organizations"). The description includes only the control objectives and related controls 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 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.

### Description Criteria

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 IT Controls provided to its user entities of the system throughout the period December 1, 2021 to November 30, 2022. 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 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.
    - v. The process used to prepare reports or other information provided to user entities of the system.
    - 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. The description includes relevant details of changes to Zoho's system during the period covered by the description when the description covers a period of time.
  - c. The description 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 auditors may consider important in its own particular environment.
2. Except for the effects of the matter described in the following paragraph, the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period December 1, 2021 to November 30, 2022 to achieve those control objectives provided that user entities applied the controls contemplated in the design of the service organization's controls. 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 Zoho.
  - b. Controls identified in our description would, if operating as described, 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.



- d. Zoho states in its description that it had controls in place for physical and environmental security for Zoho premises. However, based on Zoho Management's decision to enable remote working environment from March 13, 2021, the below control activities were not applicable from March 13, 2021 till date for the mentioned locations; Pleasanton (USA).

Control Objective 6: Controls provide reasonable assurance that physical access to Zoho facilities is restricted to authorized individuals and is monitored for detecting unauthorized access.

Control Objective 7: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.

CA-6.01, CA-6.02, CA-6.03, CA-6.04, CA-6.05, CA-6.06, CA-6.07, CA-7.01, CA7.02, CA-7.03.

**For Zoho Corporation Private Limited**

**Sd/-**

Name – N Jai Anand

Designation – Chief Financial Officer

Date – March 15, 2023

## SECTION - 3

# System Description provided by Service Organization

# Section 3. System Description provided by Service Organization

## 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 IT Controls by Zoho to its user entities from the following Offshore Development Centers ('facilities') for the period from December 1, 2021 to November 30, 2022:

| ODC              | Address   |
|------------------|---|
| Chennai, India   | Estancia IT Park, Plot no. 140, 151, GST Road, Vallancheri, Chengalpattu District 603 202 |
| Tenkasi, India   | Silaraipuravu Village, Mathalamparai, Tenkasi District 627 814                            |
| Renigunta, India | 16-237, Srikalahasti Road, Renigunta Pillapalem, Renigunta, Andhra Pradesh 517520         |
| Austin, USA      | 4708 HWY 71 E Del Valle, TX 78617-3216  |
| Pleasanton, USA  | 4141 Hacienda Drive, Pleasanton, CA 94588, USA  |

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 IT 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 Description of Controls provided by Zoho. Internal applications are used to support Zoho’s Application Development, Production Support and the related General IT Controls operations. This report does not cover the controls relating to Information Technology General Controls of the internal applications.

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 Description of Controls provided by Zoho, may not be a comprehensive listing of all controls relating to Application Development, Production Support and the related General IT 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 business 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 IT 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 Corp provides SaaS solutions, IoT platform and IT management software to organizations across the globe. Zoho provides a suite of software that servers for 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 out of India - Chennai, Tenkasi and Renigunta and USA - Austin and Pleasanton. 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 USA, Netherlands, Australia and Singapore.

Zoho hosts the data in datacenters across the globe. When an organization signs up for Zoho, they are given an option to choose the country from which they are signing up from. 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:

- United States of America – Dallas, Washington ([www.zoho.com](http://www.zoho.com))
- Europe – Amsterdam, Dublin ([www.zoho.eu](http://www.zoho.eu))
- India – Mumbai, Chennai ([www.zoho.in](http://www.zoho.in))
- Australia – Sydney, Melbourne ([www.zoho.com.au](http://www.zoho.com.au))

Zoho's 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.
- **Site24x7** - an all-in-one monitoring tool for DevOps and IT Operations from the cloud. Monitor the performance of websites, servers, network, cloud resources, and APM application on-the-go.
- **Qntrl** – A workflow orchestration software that helps you gain visibility and control over your business processes by automating them.
- **TrainerCentral** - A comprehensive platform to help you build engaging online courses, nurture a learning community and turn your expertise into a successful training business.
- **Zakya** - Running a retail business is easier with Zakya. We help you sell better, manage your entire business, and join the digital revolution.
- **MedicalMine** - Charmhealth Suite of Products are developed for MedicalMine Inc. to be 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.,

## Zoho Cloud Applications

Zoho offers a suite of online applications to support business' activities. Zoho includes more than 40 enterprise-level online applications including Mail, CRM, Writer, Workdrive, Cliq, Books to support sales, market business, accounting, communicate with teammates and customers, etc. This plan includes web, mobile, and installed versions of Zoho's applications, as well as browser extensions and other useful extras. Zoho also includes a toolkit to customize, extend, and integrate our software to fit the organization.

## ManageEngine - Enterprise IT Infrastructure Management

The ManageEngine provides suite of application for performing the following:

- **Network Performance Management:** Offers network monitoring solution and is loaded with features that enable IT administrators to resolve network outages quickly and take control of their network.
- **Help Desk & ITIL:** Gain visibility and control over IT and customer support issues with the help of web-based help desk software.
- **Bandwidth Monitoring:** A real-time bandwidth monitoring tool to analyze bandwidth usage patterns and track bandwidth utilization of non-business-critical applications.
- **Server and Application Management:** Application management software that gives deep performance insight into complex, dynamic environments. It reduces troubleshooting time and supports to improve performance of applications
- **Desktop Management:** It is a unified endpoint management (UEM) solution that helps in managing servers, laptops, desktops, smartphones, and tablets from a central location.
- **Mobile Device Management:** A mobile device management solution designed to empower enterprise workforce with the power of mobility, by enhancing employee productivity without compromising on corporate security. It lets user entities manage smartphones, laptops, tablets, and desktops and multiple operating systems such as iOS, Android, Windows, MacOS, and Chrome OS.
- **Security Information Event Management:** Secure organization's information assets against internal and external threats, manage security risks, and improve overall security strategy by gaining real-time visibility into network activity, mitigate potential threats, and resolve issues faster.
- **Password Management:** Password Manager Pro is a secure vault for storing and managing shared sensitive information such as passwords, documents and digital identities of enterprises.

## Site24x7

Site24x7 is an AI-powered performance monitoring solution for DevOps and IT operations from the cloud. Its broad capabilities help monitor and troubleshoot problems with end-user experience, websites, applications, servers, public clouds, and network infrastructure.

## 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
- Control activities that help in meeting the overall applicable trust services criteria.
- 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 Client Support team. The team coordinates with Product teams to resolve reported issues.

### **c. Zorro and NOC team**

The Zorro 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 centralised location based out of Zoho's Corporate Office in Estancia, Chennai. The scope of work for NOC and Zorro team includes- analysing 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 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.

**f. 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.

**g. 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.

**h. 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 SOC 1 report:

| Small   | Medium  | Large  |
|---|---|--|
| <ul style="list-style-type: none"> <li>Zoho Payroll</li> <li>Zakya</li> </ul> | <ul style="list-style-type: none"> <li>Zoho Invoice</li> <li>Zoho Expense</li> <li>Zoho Inventory</li> <li>Zoho Subscriptions</li> <li>Zoho Checkout</li> <li>Zepto Mail</li> <li>Zoho People</li> <li>MedicalMine</li> <li>Division - CharmHealth</li> </ul> | <ul style="list-style-type: none"> <li>Zoho CRM</li> <li>Zoho Books</li> <li>Zoho Mail</li> <li>Zoho Projects and Bug tracker</li> <li>Zoho Creator</li> </ul> |

### 3.3. Overview of Services

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

- Chennai India
- Tenkasi, India
- Renigunta, India
- Austin, USA
- Pleasanton, 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 an Employee Code of Conduct ('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 Employee 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 Employee'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 till 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. Management is periodically briefed on regulatory and industry changes affecting the services provided and executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

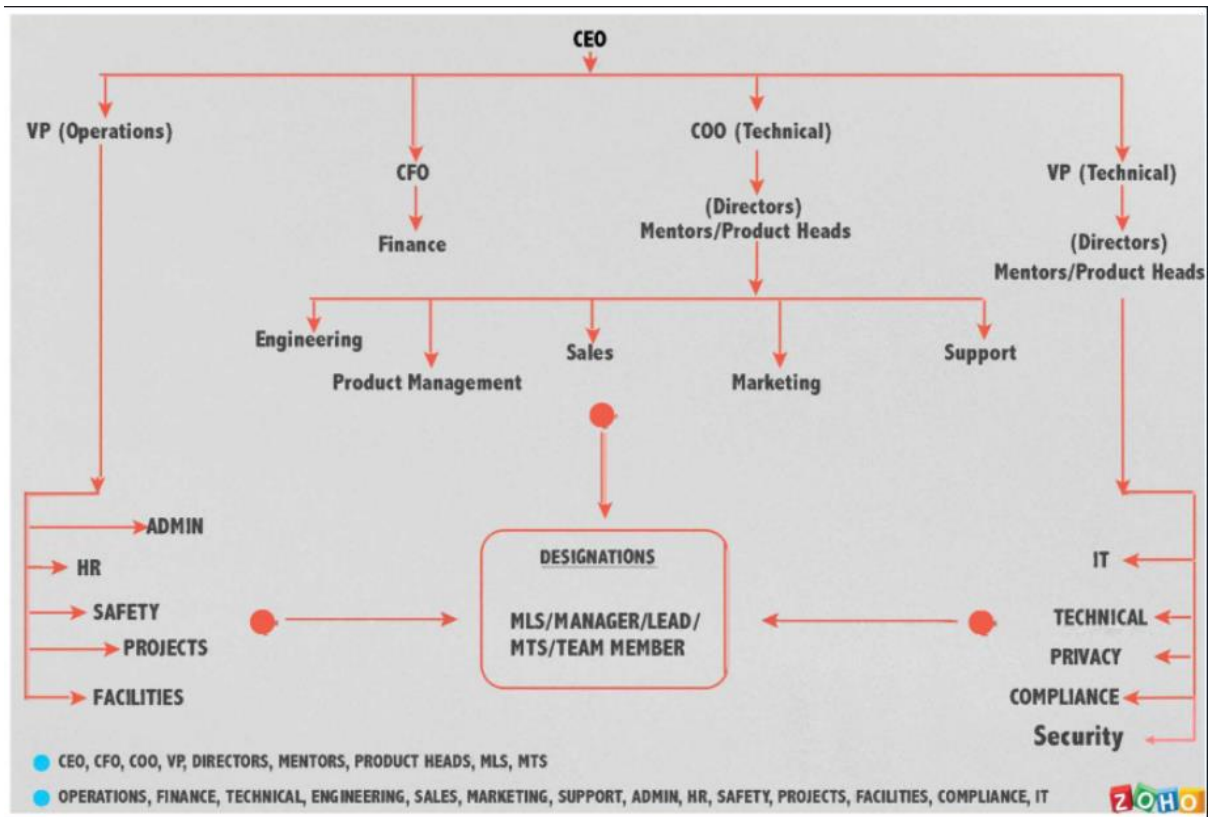
### **3.3.1.4 Zoho Organization Structure**

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.

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.

[Space left blank intentionally]

### Organization Chart – Zoho



#### 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 | <ul style="list-style-type: none"> <li>• Responsible for handling specific product related roles</li> <li>• Responsible for handling product specific Internal Teams/Divisions/Stream based roles/Product based roles</li> </ul>   |
| Information Security Head   | <ul style="list-style-type: none"> <li>• Define the Information Security Policy</li> <li>• Ensure the communication and understanding of the Information Security Policy throughout the organization.</li> <li>• Monitor the implementation of security policy established under the Integrated ISPIMS.</li> </ul>   |
| Director of Compliance  | <ul style="list-style-type: none"> <li>• 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.</li> <li>• Develops compliance organizational strategies by contributing information, analysis, and recommendations to strategic thinking and direction; establishing functional objectives in line with organizational objectives.</li> <li>• 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.</li> <li>• Monitor the implementation of privacy policy established under the Integrated ISPIMS.</li> <li>• Protects assets by establishing compliance standards; anticipating emerging compliance trends; designing improvements to internal control structure.</li> </ul> |

| Role  | Responsibility and Authority  |
|---|---|
| Information Security Compliance Manager                 | <ul style="list-style-type: none"> <li>• Document and maintain the policies related to security of Organizational Information and information handled as a CSP</li> <li>• Ensure that the Information Security Management System is established, implemented, monitored and maintained.</li> <li>• Co-ordinate improvements to the Information Security Management System.</li> <li>• Perform periodic tests, Implement and act as per the Information Security Continuity Plan.</li> <li>• Facilitate implementation of corrective actions pertaining to Integrated ISMIS.</li> <li>• Perform periodic test, Implement and act as per Business Continuity Plan.</li> <li>• Plan and conduct internal audits.</li> <li>• Ensure the planning and execution of external audits.</li> <li>• Measure, track and analyse trends in metrics.</li> <li>• Implement and act per the Integrated ISMS policies that are applicable.</li> <li>• Periodic review of Integrated ISMS documents.</li> <li>• Review policies and documents in consultation with System Administrator before release.</li> <li>• Ensure that selected controls are documented in the Statement of Applicability and are implemented.</li> <li>• Monitor the implementation of Integrated ISMS on a continual basis and report discrepancies to the DOC.</li> <li>• Facilitate risk assessment using cross functional teams.</li> <li>• Identify training needs of Integrated ISMS and coordinate with training department to ensure that the training is completed.</li> <li>• Verify the implemented corrective actions.</li> </ul> |
| Member Technical Staff - Compliance Tools & Support     | <ul style="list-style-type: none"> <li>• Establish, designing and implementing the process and tools to make the organization adhere to the compliance.</li> <li>• Analyze the compliance requirements, designing the solutions and implementing the same.</li> <li>• Responding to the compliance related questions raised by the customers.</li> <li>• Attending the conference calls with the customers on compliance.</li> <li>• Conducting meetings with the internal teams and steering.</li> </ul>   |
| Product / Department Head / Internal Audit Coordinators | <ul style="list-style-type: none"> <li>• Implement the Integrated Information Security Management System and Cloud security best practices within product / Department.</li> <li>• Product / Department heads act as risk owners &amp; will have the authority take decisions on risk, for their respective departments.</li> <li>• Obtain and communicate customer requirements to the appropriate personnel or functional organizations.</li> </ul>   |

| Role                        | Responsibility and Authority   |
|-----------------------------|--|
|                             | <ul style="list-style-type: none"> <li>• Ensure that qualified, skilled, and trained personnel and other resources are available to implement the Integrated Information security Management System.</li> <li>• Ensure integrity, quality, safety, optimal cost, schedule, performance, reliability, accuracy and maintainability of products and services in order to satisfy customer requirements</li> <li>• Ensure that the personnel comply with applicable standards, regulations, specifications, and documented procedures</li> <li>• Provide the corrective actions</li> </ul>  |
| Member-<br>Compliance Audit | <ul style="list-style-type: none"> <li>• 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.</li> <li>• Assists in creating policies and procedures to help reduce risk, meet regulatory requirements and best business practices.</li> <li>• Performs Information security assessments and prepares findings and remediation reports.</li> <li>• Assists in updating and maintain policies, standards and procedures documents.</li> <li>• Evaluate security controls to ensure effectiveness and compliance, including managing the security control remediation efforts.</li> <li>• Coordinate with various teams in the organization regarding standards, regulations.</li> <li>• Coordinate with teams for Information Security awareness training.</li> <li>• Mapping and analyzing the adherence level with the applicable standards.</li> <li>• Performs other job-related duties as assigned.</li> </ul> |
| Director of IT (DOIT)       | <ul style="list-style-type: none"> <li>• Reviews and approves procedures pertaining to handling some of the privacy and security compliance related processes.</li> <li>• Advises on ways to achieve intended outcomes with respect to addressing risks in processing data.</li> <li>• Enables / spearheads some operations to improve the overall working of the GRC program and serves as an important person in the privacy steering committee.</li> </ul>  |
| Central Security<br>Team    | <ul style="list-style-type: none"> <li>• Accountable for the overall Information Security and Cloud security Program</li> <li>• Initiate, facilitate and promote activities related to security awareness in the organization</li> <li>• Conduct Security Risk &amp; Impact assessments for any new product, technology and architecture component.</li> </ul>   |

| Role | Responsibility and Authority  |
|------|---|
|      | <ul style="list-style-type: none"> <li>• Assist and guide the product security engineers on secure coding standards and security assessments guidelines within the product scope</li> <li>• Responsible for identifying and building security tools and frameworks to assist the development and operations teams</li> <li>• Evaluate evolving new technologies in the context of information security and provide guidance on secure adoption to the product teams</li> <li>• Closely work with the Incident management team during incident analysis and investigations.</li> </ul> |

**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 Management System Manual (IMSM) 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 IMSM 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 "Information Provided by Service Auditors". The description of controls includes controls encompassing the following domains:

- Change Management
- 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 has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and application (product) changes. The policy is reviewed and approved on an annual basis. Zoho has also defined support documents including the system flow diagrams and other design documents for the products and the same are made available to the respective team members of Zoho.

Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.

#### Application Changes:

Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the team lead from respective Product Teams on an annual basis.

Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.

The code created by the development team is maintained in a centralised repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team. The code is developed by the developers in the development environment.

The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment and the changes are tracked by the respective product teams through a tool. The Quality testing is performed in the Quality environment by the QA team.

On completion of the quality checks by the Quality Assurance team, a QA report is generated and in case of any issues/errors in the report, it is communicated to the developers for resolution. On resolution, a sign-off is provided by the QA Team and then the code is deployed in the production environment by the respective product team. Once the code is approved the QA team, the code is pushed into the development environment. Hacksaw is an automated scanning tool which scans every build and blocks the update in case of any security violations. It performs a static code analysis for the builds before moving the change to production. The builds are tested in the Hacksaw tool by the respective product teams within Zoho. Hacksaw is an in-house product that ensures secure coding practice, secure configurations of the application and detects vulnerabilities in third-party dependencies. It follows OWASP and SANS standards and scans every release bundle and reports vulnerabilities.

Zorro team has defined OS Hardening Procedure for Operating Systems. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.

Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the International Data Centers (IDCs) are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Zorro Manager. Access to IDC is controlled in the ODC in Chennai location.

Zoho has International Data Centers (IDCs) in USA, Europe, India, Australia. The Data Center where customer data is stored is selected automatically based on the IP address of the customers. The infrastructure of these data centers is managed from India.

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

|  |   |
|--|---|
| <b>CO1: Control provides reasonable assurance that segregation of environments is maintained.</b>  |   |
| <b>CA1.01</b>  | Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.  |
| <b>CO2: Controls provide reasonable assurance that application and infrastructure changes are documented, tested and approved as per the procedures.</b> |   |
| <b>CA2.01</b>  | Zorro team has defined OS Hardening Procedure for Operating Systems. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.  |
| <b>CA2.02</b>  | Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The policy is reviewed by Infosec compliance manager and approved by CIO on an annual basis.                    |
| <b>CA2.03</b>  | Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the team leads from the respective Product Teams on an annual basis.  |
| <b>CA2.04</b>  | The code created by the development team is maintained in a centralised repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool.  |
| <b>CA2.05</b>  | The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests in the build in the local (testing) environment and the changes are tracked by the respective product teams through creator tool.  |
| <b>CA2.06</b>  | On completion of the quality checks by the Quality Assurance team, a QA report is generated and in case of any issues/errors in the report, it is communicated to the developers for resolution. On resolution, a sign-off is provided by the QA Team and then the code is deployed in the production environment by the respective product team. |
| <b>CA2.07</b>  | Support documents including the system flow diagrams and other design documents are maintained and are made available to the respective team members of Zoho.   |
| <b>CA2.08</b>  | Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.  |
| <b>CA2.09</b>  | Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Zorro Manager   |

### 3.7.2 Logical Security

Zoho has defined an organization wide "Integrated Management System Manual" which specifies the information security and privacy requirement and also defines the related roles and responsibilities. It is prepared by Compliance / Privacy Team and approved by the Security Head and is reviewed 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 internal portal.

#### Access Management:

For newly joined associates, trainees, contractors the HR team creates an account in ZohoPeople (Control Panel) and once the account is created, AD account is auto-created by the system. The respective manager also creates a request for providing workstation to the associate in ZohoPeople and the same is assigned and actioned upon by the SysAdmin team.

In case of an associate leaving Zoho, the HR team disables the account in ZohoPeople (Control Panel).

Access to IDC Landing Access Machine and IDC server for new requests are granted by Zorro Team member based on the approval from the reporting manager and Zorro Manager.

Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro Team based on the IDC access revocation process on a timely manner. User Access Review of users with access to IAM Roles that grant access to the application and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on a half-yearly basis. Corrective actions, if any, are taken on a timely manner.

The HR notifies the SysAdmin / Zorro team and the SysAdmin / Zorro team disables the logical access of the associate.

Logical access to the tools (managed by NOC team), Event log analyser, OP Manager plus, Netflow analyser, used for performing NOC's daily operations are granted/revoked by the Senior NOC Member based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member. The tools include Firewall, Switch, Access card, landing Server.

#### Authentication:

Security settings for account lockout, password minimum length and password history are configured for authentication into Domain (AD), IAM (for Zoho accounts), IAN (for Zodoor and IDC) and also for IDC infrastructure. Users are required to use two-factor authentication to connect to the IDC infrastructure from IAN network.

#### Network Security:

The policies and procedures covering the logical access and operations of NOC are defined by the NOC Project Coordinator/ Senior NOC Engineer as part of the Network Operation Center - Policies and Procedures document and is approved by the NOC manager on an annual basis. This policy is hosted on NOC's intranet site with access available to the designated team members.

Network diagram detailing the network devices such as firewalls and switches is maintained by the NOC Manager. Further, access to the network devices are restricted to NOC Team to prevent unauthorized access.

Based on the network monitoring by the NOC team through monitoring (NOCMON) and EventLog Analyzer, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC ServiceDeskPlus Portal. Based on the alerts generated, corrective actions are taken by the NOC team.

Access to Corporate VPN is authenticated with Zoho users' domain account. Client servers and data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho Facility.

Virtual LAN changes are requested by the SysAdmin Team (in the case of Corporate offices) or by the Zorro team (in the case of IDCs) and the same is approved by the Managers/ L3 of the Sysadmin/ Zorro team.

The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the SysAdmin or Zorro team as a second level approval.

On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset and tracks the deviations to closure.

When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager. Privileged access to servers is restricted to authorized personnel from the Zorro

Access to external storage devices and internet are disabled on IDC workstations to prevent data loss

On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken. On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective action is taken.

Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations based on the frequency defined.

Monitoring of Anti Virus console is performed on a real time basis by the IT Team and in case of any alerts, corrective action is taken.

---

**CO3: Controls provide reasonable assurance that Information Security policies and procedures are documented, approved and communicated to associates.**

---

**CA3.01** Zoho has defined an organization wide 'Integrated Management System Manual' which specifies the information security and privacy requirement and also defines the related roles and responsibilities. It is prepared by Compliance / Privacy Team and approved by the Security Head and is reviewed on an annual basis.

---

---

**CO3: Controls provide reasonable assurance that Information Security policies and procedures are documented, approved and communicated to associates.**

---

**CA3.02** Zoho's management committee is responsible for defining, implementing, and monitoring compliance to 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 internal portal.

---



---

**CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated**

---

**CA4.01** Security settings for account lockout, password minimum length and password history are configured for authentication into Domain (AD), IAM (for Zoho accounts), IAN (for Zodoor and IDC) and also for IDC infrastructure. Users are required to use two-factor authentication to connect to the IDC infrastructure from IAN network.

---

**CA4.02** For newly joined associates, trainees, contractors, the HR team creates an account in ZohoPeople (Control Panel) and once the account is created, AD account is auto created by the system. The respective manager also creates a request for providing workstation to the associate and the same is assigned and actioned upon by the SysAdmin team.

---

**CA4.03** In case of an associate leaving Zoho, the HR team disables the account in ZohoPeople (Control Panel). The HR notifies the SysAdmin / Zorro team and the SysAdmin / Zorro team disables the logical access of the associate.

---

**CA4.04** Logical access to the tools (managed by NOC team) used for performing NOC's daily operations are granted/revoked by the Senior NOC Member based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member.

---

**CA4.05** Network diagram detailing the network devices such as firewalls and switches is maintained by the NOC Manager. Further, access to the network devices are restricted to NOC Team to prevent unauthorized access.

---

**CA4.06** Based on the network monitoring by the NOC team through NOCMON and EventLog Analyzer, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC ServiceDeskPlus Portal.

---

**CA4.07** Access to Corporate VPN is authenticated with Zoho users' domain account.

---

**CA4.08** Client servers and data can be accessed through IAN VPN or the dedicated IAN servers in the Zoho facilities.

---

**CA4.09** User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on a yearly basis. Corrective actions, if any, are taken on a timely manner.

---

**CA4.10** Access to IDC Landing Access Machine and IDC server for new requests are granted by Zorro Team member based on the approval from the reporting manager and Zorro Manager.

---

---

**CO4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated**

---

- CA4.11 Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro Team based on the IDC access revocation process on a timely manner.

---

- CA4.12 Privileged access to servers is restricted to authorized personnel from the Zorro

---

---

**CO5: Controls provide reasonable assurance that logical access to Zoho network is protected from unauthorized access and viruses.**

---

- CA5.01 Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations based on the frequency defined.

---

- CA5.02 Monitoring of Anti Virus console is performed on a real time basis by the IT Team and in case of any alerts, corrective action is taken.

---

- CA5.03 Virtual LAN changes are requested by the SysAdmin Team (in the case of Corporate offices) or by the Zorro team (in the case of IDCs) and the same is approved by the Managers/ L3 of the Sysadmin/ Zorro team.

---

- CA5.04 The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the SysAdmin or Zorro team as a second level approval.

---

- CA5.05 On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset and tracks the deviations to closure

---

- CA5.06 When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager.

---

- CA5.07 On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken. On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective action is taken.

---

- CA5.08 Access to external storage devices and internet are disabled on IDC workstations to prevent data loss

---

**3.7.3 Physical and Environmental Security**

**Physical Access Security:**

Zoho has defined and documented Physical Security Policy which is reviewed and approved by the Head of Safety and Security on an annual basis. The Policy includes the physical access restrictions to the NOC / Zorro processing area.

For new associates / trainees / contractors joining Zoho, the Physical Security team /Building Management System Team issues an access card to the associate based on the request raised by HR to grant physical access. Physical Security team also provides photo based ID cards for the Zoho associates. The ID cards / badges are distinguished based on the color of the tags described in the HR policy.

In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team/Building Management System Team deactivates the old ID card and issues a new physical ID card.

Upon an associate or a contractor leaving Zoho or in case of absconding associates, the HR team updates separation details in HRMS application and also sends an e- mail to the Physical Security team notifying the leavers. Based on the email, Physical Security team revokes the physical access card on the last working day.

Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.

Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities and recorded.

Proximity card-based access control system is installed at the entry / exit points within the facility. In addition, access to the Zoho Server room, NOC room, Switch room, Zorro Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system and PIN based authentication.

Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.

Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.

**Environmental Security:**

Environmental safeguards are installed in Zoho facilities comprising of the following:

- Cooling Systems
- UPS with Battery and diesel generator back-up
- Smoke detectors
- Water sprinklers
- Fire resistant floors
- Fire extinguisher

Planned Preventive Maintenance (PPM) is performed on quarterly basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.

Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.

Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a annual basis, the Zorro team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness and also



to perform DC maintenance operations, if required. This is done using the ZAC tool with the approval of the Zorro Manager.

---

**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** For new associates / trainees / contractors joining Zoho, the Physical Security team /Building Management System Team issues an access card to the associate based on the request raised by HR to grant physical access. Physical Security team also provides photo based ID cards for the Zoho associates. The ID cards / badges are distinguished based on the color of the tags described in the HR policy.

---

**CA6.02** In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team/Building Management System Team deactivates the old ID card and issues a new physical ID card.

---

**CA6.03** Upon an associate or a contractor leaving Zoho or in case of absconding associates, the HR team updates separation details in HRMS application and also sends an e-mail to the Physical Security team notifying the leavers. Based on the email, Physical Security team revokes the physical access card on the last working day.

---

**CA6.04** Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.

---

**CA6.05** Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities and recorded.

---

**CA6.06** Proximity card-based access control system is installed at the entry / exit points within the facility. In addition, access to the Zoho Server room, NOC room, Switch room, Zorro Workspace and asset storage room is restricted using proximity card-based access control system and PIN based authentication.

---

**CA6.07** Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.

---



---

**CO7: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.**

---

**CA7.01** Environmental safeguards are installed in Zoho facilities comprising of the following:

- Cooling Systems
- UPS with Battery and diesel generator back-up
- Smoke detectors
- Water sprinklers
- Fire resistant floors
- Fire extinguisher

---

**CA7.02** Planned Preventive Maintenance (PPM) is performed on quarterly basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.

---

**CA7.03** Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.

---

---

**CO7: Controls provide reasonable assurance that Zoho facilities are protected from environmental damage.**

---

**CA7.04** Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.

---

**CA7.05** Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On an annual basis, the Zorro team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness and also to perform DC maintenance operations, if required. This is done using the ZAC tool with the approval of the Zorro Manager.

---

### **3.7.4 Manage Human Resource**

Zoho has a Human Resource Security policy, which is defined by the Assistant Manager - HR Operations and approved by the Senior Manager - HR on an annual basis. The policy is made available to the Zoho associates through Intranet (Zoho People).

Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.

Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions and approved by the Senior Manager-HR on an annual basis.

Upon a new associate joining, an induction training is conducted by the Training Team and HR Team to make the associate aware of the information security practices and various policies of Zoho. The attendance for the training is captured in Zoho people.

Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.

Upon new associates joining Zoho, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.

Upon joining Zoho, the associates are required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.

Zoho has a defined Code of Ethics document that is reviewed and approved by the Manager - HR on an annual basis and it is made available on Intranet to the associates. The Code defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.

**CO8: Controls provide reasonable assurance that policies and procedures for hiring and separation of the associates are adhered to.**

|               |   |
|---------------|---|
| <b>CA8.01</b> | Upon a new associate joining, an induction training is conducted by the Training Team and HR Team to make the associate aware of the information security practices and various policies of Zoho. The attendance for the training is captured in Zoho people.   |
| <b>CA8.02</b> | Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions and approved by the Senior Manager-HR on an annual basis.   |
| <b>CA8.03</b> | Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.   |
| <b>CA8.04</b> | Upon new associates joining Zoho, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.  |
| <b>CA8.05</b> | Upon joining Zoho, the associates are required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.  |
| <b>CA8.06</b> | Zoho has a defined Code of Ethics document that is reviewed and approved by the Manager - HR on an annual basis and it is made available on Intranet to the associates. The Code defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. |
| <b>CA8.07</b> | Zoho has a Human Resource Security policy, which is defined by the Assistant Manager - HR Operations and approved by the Senior Manager - HR on an annual basis. The policy is made available to the Zoho associates through Intranet (Zoho People).  |
| <b>CA8.08</b> | Zoho has a defined organizational structure establishing the key areas of authority and responsibility, lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.  |

**3.7.5 Incident Management**

Zoho has defined an Incident Management Policy, which is prepared by Incident Management team and approved by the Information Security Manager. The policy is reviewed on an annual basis and version history is maintained within the document.

Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyse the potential impact of the security incident. The relevant product team performs root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The appropriate actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.

Based on the alert triggered by the availability monitoring tools, from SITE 24x7, an automated entry of an event is created in the Zoho creator tool and a downtime post is made on Zoho Connect to notify the stakeholders. The relevant product team performs RCA and the action points are identified for implementation. The incident ticket is updated appropriately and tracked for closure.

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.

---

**CO9: Controls provide reasonable assurance that incident tickets are recorded, analyzed and tracked to closure**

---

**CA9.01** Zoho has defined an Incident Management Policy, which is prepared by Manager in Incident Management team and approved by the Information Security Manager. The policy is reviewed on an annual basis and version history is maintained within the document.

---

**CA9.02** Based on the inputs received via service desk, the incident management team coordinates with relevant stakeholders to analyse the potential impact of the security incident raised in Creator application. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool.

---

**CA9.03** Based on the alert triggered by the availability monitoring tools, an automated entry of an event is created in the Zoho creator tool and a downtime post is made on Zoho Connect to notify the stakeholders. The relevant product team performs RCA and the action points are identified for implementation. The incident ticket is updated appropriately and tracked for closure.

---

**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.

---

### **3.7.6 Backup and Restoration Management Services**

The NOC team uses an in-house tool (DeviceExpert) to backup network device configurations on a daily basis (incremental backup) and also on a weekly basis (full backup). In case of a backup failure, an automated email is triggered, and remediation action is taken.

The Zorro team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Zorro team and appropriate corrective action is taken.

Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Zorro team through Zoho Creator tool, who handles the backup restoration.

IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.

The storage devices are disposed securely using secure disposal methods by the Zorro team. The failed hard disk drives (HDD) are degaussed prior to disposal / replacement.

---

**CO10: Controls provide reasonable assurance that data, network configurations are backed up and restored based on the request received.**

---

|                |  |
|----------------|--|
| <b>CA10.01</b> | The NOC team uses an in-house tool (DeviceExpert) to backup network device configurations on a daily basis (incremental backup) and also on a weekly basis (full backup). In case of a backup failure, an automated email is triggered, and remediation action is taken.                   |
| <b>CA10.02</b> | The Zorro team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Zorro team and appropriate corrective action is taken. |
| <b>CA10.03</b> | Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Zorro team through Zoho Creator tool, who handles the backup restoration.   |
| <b>CA10.04</b> | IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.   |
| <b>CA10.05</b> | The failed hard disk drives are degaussed prior to disposal / replacement.   |

### 3.7.7 Third Party Management

On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centres and are reviewed by the Zoho Compliance team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.

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

A contract is defined, documented and approved between Zoho and sub processors/third party vendors for services in relation to hosting of servers. The contract includes the scope of services to be provided and confidentiality clauses.

---

**CO11: Controls provide reasonable assurance that the sub processors, and third party vendors in relation to hosting of servers are monitored by Zoho.**

---

|                |  |
|----------------|--|
| <b>CA11.01</b> | On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centres and are reviewed by the Zoho Compliance team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action. |
| <b>CA11.02</b> | Risk assessment is performed annually by Zoho Privacy Team to assess the risk of sub processors identified by them and identify suitable risk treatment plan on an annual basis.   |
| <b>CA11.03</b> | A contract is defined, documented and approved between Zoho and sub processors/third party vendors for services in relation to hosting of servers. The contract includes the scope of services to be provided and confidentiality 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 shared with their associates on Zoho products (CA-4.01)
- 3.8.2 User entities are responsible for raising any backup restoration request to Zoho. (CA-10.03)
- 3.8.3 User entities are responsible for communicating any security or privacy incidents to Zoho on a timely basis. (CA-9.02)

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 vs 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.

#### Table 1: Subservice Organizations

Zoho’s controls relating to the Application development, Production Support and the related General IT 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 IT 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.

| Name of Subservice Organization  | Nature of Services Provided         |
|--|-------------------------------------|
| <ul style="list-style-type: none"> <li>- Sabey Data Center Properties LLC</li> <li>- Zayo Group, LLC Colocation Services ("zColo")</li> <li>- Interxion HeadQuarters B.V.</li> <li>- Equinix Inc B.V.,</li> <li>- CtrlS Datacenters Limited</li> <li>- Equinix Asia Pacific Pte. Ltd.</li> </ul> | Co-Location Services of IDC Servers |
| <ul style="list-style-type: none"> <li>- KPMG</li> <li>- Matrix Business Services India Private Limited</li> <li>- Hire Right LLC</li> </ul>   | Background Verification Services    |

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

3.9.1 Subservice organizations are responsible for the scope of services covering the co-location data centers including the physical security and environmental security controls. (CA-6.01, CA-6.02, CA-6.03, CA-6.04, CA-6.05, CA-6.06, CA-6.07, CA-7.01, CA-7.02. CA-7.03, CA-11.01, CA-11.03)

3.9.2 Subservice organization is responsible for performing the background verification of Zoho associates, based on request from Zoho HR Teams. (CA-8.04)

**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              |
|---|---|
| <ul style="list-style-type: none"> <li>- Powerica</li> <li>- HVAC</li> <li>- Ardelisys Technologies Private Limited</li> <li>- SVE Energy Private Limited</li> <li>- Pinnacle System</li> </ul> | Environmental equipment maintenance             |
| G4S Secure Solutions India Private Limited  | Physical Security Agency for Security Personnel |

(Space left blank intentionally)

# SECTION - 4

## Information provided by Service Auditors



# Section 4. Information provided by Service Auditors

## 4.1 Introduction

This report is intended to provide user entities with information about the controls at Zoho that may affect the processing of user entities' transactions and also to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user entities, is intended to assist user entities' auditors in (1) planning the audit of user entities' financial statements and in (2) assessing control risk for assertions in user entities' financial statements that may be affected by controls at Zoho.

Our testing of Zoho's controls was restricted to the control objectives and related controls listed in Section 4.3 of the report and were not extended to controls described in system description but not included in the aforementioned section, or to controls that may be in effect at user entities and subservice organizations, as referred in section 3.9. It is user entities auditors' responsibility to evaluate this information in relation to the controls in place at user entities. If certain complementary controls are not in place at user entities, Zoho's controls may not compensate for such weaknesses.

## 4.2 Control Environment elements

In addition to the tests of operating effectiveness of the controls in the matrices in this section of the report, our procedures included tests of the following relevant elements of Zoho's control environment:

- Zoho's Management;
- Human Resources Policies and Practices;
- Corporate Internal Audit Function;
- Risk Management; and
- Monitoring.

Our procedures included testing those relevant elements of the control environment that we considered necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. We have considered the details of the control environment as provided by Zoho in its management assertion, in the tests of operating effectiveness.

Our tests of the control environment included inquiry of appropriate management, supervisory, and staff personnel, and inspection of Zoho's documents and records. The control environment was considered in determining the nature, timing, and extent of the tests of operating effectiveness of controls.

## 4.3 Tests of Operating Effectiveness

Our tests of effectiveness of the controls included such tests as we considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, was sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from December 1, 2021 to November 30, 2022. Our tests of the

operational effectiveness of controls were designed to cover a representative number of transactions throughout the period of December 1, 2021 to November 30, 2022, for each of the controls listed in this section, which are designed to achieve the specific control objectives. In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the audit objectives to be achieved (d) the assessed level of control risk and, (e) the expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of information provided by Zoho is also a component of the testing procedures performed. Information we are utilizing as evidence may include, but is not limited to:

- Standard “out of the box” reports as configured within the system
- Parameter-driven reports generated by Zoho systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- Zoho - prepared analyses, schedules, or other evidence manually prepared and utilized by the Company.

While these procedures are not specifically called out in the test procedures listed in this section, they are 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 Zoho.

**Description of Testing Procedures Performed**

Tests performed for the suitability of the design and operational effectiveness of controls listed in Section 4 are described below:

| Test                         | Description  |
|------------------------------|--|
| Corroborative inquiry        | Made inquiries of appropriate personnel and corroborated responses with other personnel to ascertain the compliance of controls. |
| Observation                  | Observed application of specific controls virtually and remotely.  |
| Examination of documentation | Inspected documents and reports indicating performance of the controls.  |
| Re-performance               | Re-performed application of the controls   |

**Results of Testing Performed**

The results of the testing of the controls were sufficient to conclude that controls were operating effectively and provide reasonable, but not absolute, assurance that the control objectives were achieved during the period from December 1, 2021 to November 30, 2022.

It is user organizations’ responsibility to evaluate this information in relation to internal controls in place at user organizations to assess the total system of internal controls. If it is concluded that the user organizations does not have effective internal controls in place, the controls described in this report may not compensate for the absence of essential user controls.

The following tests were designed to obtain evidence about their effectiveness in achieving control objectives also referenced in section 3.

For each control listed in Section 3, a walk-through was performed to ascertain the controls were designed and implemented. The walk-through consisted of confirming the controls with appropriate personnel at the Zoho.

Observation and inspection procedures were performed as it relates to manually prepared reports, queries, listings and system generated reports to assess the accuracy and completeness (reliability) of the information used in our testing of the controls.

### **Reporting on Results of Testing**

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte Haskins & Sells LLP does not have the ability to determine whether a deviation will be relevant to a particular user organization. Consequently, Deloitte Haskins & Sells LLP reports all deviations.

(Space left intentionally blank)

**4.3.1 Test Procedures performed by Service Auditors**

**4.3.1.1 Change Management**

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

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.

| #      | Control Activity   | Tests Performed   | CUECs/<br>CSOC | Results of Tests   |
|--------|--|---|----------------|--------------------|
| CA1.01 | Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications. | Inspected the segregation of environments for applications for aspects such as ‘Development environment paths/URL’s’, ‘QA environment paths/URL’s’ and ‘Production environment paths/URL’s’ to ascertain whether Zoho maintained a dedicated Development and test environment, which was separate from the Production environment for its applications. | None           | No Exception Noted |

[Space left blank intentionally]

**Control Objective 02: Controls provide reasonable assurance that application and infrastructure 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.

| #      | Control Activity   | Tests Performed   | CUECs/<br>CSOC | Results of Tests   |
|--------|--|---|----------------|--------------------|
| CA2.01 | Zorro team has defined OS Hardening Procedure for Operating Systems. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.   | Inspected Zorro OS Hardening Procedure document for aspects such as 'name of the procedure', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved on' to ascertain whether Zorro team had defined OS Hardening Procedure for Operating Systems and whether the guidelines were prepared by the Zorro team and approved by Manager - Zorro on an annual basis.  | None           | No Exception Noted |
| CA2.02 | Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The policy is reviewed by Infosec compliance manager and approved by CIO on an annual basis. | Inspected Change Management policy document for aspects such as 'name of policy', 'contents of policy', 'prepared by', 'approved by' and 'approved on' to ascertain whether Zoho had defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes which defined the process of initiation, approval, review and implementation and the policy was reviewed and approved on an annual basis. | None           | No Exception Noted |

| #      | Control Activity   | Tests Performed   | CUECs/<br>CSOC | Results of Tests   |
|--------|--|---|----------------|--------------------|
| CA2.03 | Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the team leads from the respective Product Teams on an annual basis.       | Inspected Software Development Life Cycle document for aspects such as 'name of document' 'version no.', 'prepared by', 'approved by, and 'approved on' to ascertain whether Zoho had defined Software Development Life Cycle document prescribing the lifecycle of the software through the stages of design, development, testing and implementation and whether this document was reviewed and approved by the team leads from the respective product Teams on an annual basis.  | None           | No Exception Noted |
| CA2.04 | The code created by the development team is maintained in a centralised repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool.   | Inspected for sample builds, the Code repository details in Configuration Management tool for aspects such as 'details of the URL's/Paths of codes', and 'repository' to ascertain whether the code created by the development team was maintained in a centralised repository by the CM team and the code developed by the Developers was pushed into the CM tool.   | None           | No Exception Noted |
| CA2.05 | The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests in the build in the local (testing) environment and the changes are tracked by the respective product teams through Creator tool. | Inspected for sample builds, the build workflow details and corresponding records in creator tool for aspects such as 'configuration tool Check Date', 'details of the URL's/Paths', 'Test report', 'QA performed by' 'and 'QA tested on' to ascertain whether the Developed code was tested using the in-house CM tool prior to check-in and also to ascertain whether once the code was checked-in, the Quality Assurance (QA) team executed the quality tests in the build in the local (Testing) Environment and the changes were tracked by the respective product teams through creator tool. | None           | No Exception Noted |

| #      | Control Activity  | Tests Performed   | CUECs/<br>CSOC | Results of Tests     |
|--------|---|---|----------------|----------------------|
| CA2.06 | On completion of the quality checks by the Quality Assurance team, a QA report is generated and in case of any issues/errors in the report, it is communicated to the developers for resolution. On resolution, a sign-off is provided by the QA Team and then the code is deployed in the production environment by the respective product team. | Inspected for sample builds, build workflow details, in the Configuration Management tool for aspects such as 'build name', 'date of hacksaw report', 'generated by', 'details of the URL's/Paths' , 'contents of QA report- result', 'resolution of issues or errors', 'signoff provided by', 'signoff provided on' and 'date of implementation in production' to ascertain whether on completion of the quality checks by the Quality Assurance team, a QA report was generated and in case of any issues/errors in the report, it was communicated to the developers for resolution and whether sign-off was provided prior to code was deployed in the production environment by the respective product team. | None           | No Exceptions Noted. |
| CA2.07 | Support documents including the system flow diagrams and other design documents are maintained and are made available to the respective team members of Zoho.   | Inspected for sample products the supporting documents for aspects such as 'Product details', 'Category' and 'availability in SharePoint' to ascertain whether support documents including the system flow diagrams and other design documents were maintained and also whether they were made available to the respective team members of Zoho .   | None           | No Exception Noted   |
| CA2.08 | Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.  | Inspected the availability of coding practices document for sample products for aspects such as 'availability of coding practice', 'Description of Secure coding practices' and 'availability on SharePoint' to ascertain whether secure coding practices were defined and communicated to the respective personnel as part of the Zoho's SDLC process.   | None           | No Exception Noted   |

| #             | Control Activity  | Tests Performed   | CUECs/<br>CSOC | Results of Tests   |
|---------------|---|---|----------------|--------------------|
| <b>CA2.09</b> | Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Zorro Manager | Inspected for sample patches and upgrades the tickets for aspects such as 'patch ticket ID', 'requestor name', 'patch tested by- local environment' 'patch test date', 'deployment date' and 'approval details' to ascertain whether patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs were initially tested in a local environment/ test lab, then moved to a DR DC following which these changes were implemented in the IDC after obtaining approval from the Zorro Manager. | None           | No Exception Noted |

[Space left blank intentionally]



### 4.3.1.2 Logical 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.

| #      | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|---|---|---------------|--------------------|
| CA3.01 | Zoho has defined an organization wide 'Integrated Management System Manual' which specifies the information security and privacy requirement and also defines the related roles and responsibilities. It is prepared by Compliance / Privacy Team and approved by the Security Head and is reviewed on an annual basis. | Inspected Integrated Management System Manual document for aspects such as 'name of the document', 'version no.', 'prepared by', 'approved by', 'reviewed by', 'reviewed on', 'approved on' and 'contents of the policy' to ascertain whether Zoho had defined an organization wide 'Integrated Management System Manual' which specified the information security and privacy requirements and also defined the related roles and responsibilities and whether it was prepared by Compliance / Privacy Team and approved by the Security Head and was reviewed on an annual basis. | None          | No Exception Noted |
| CA3.02 | Zoho's management committee is responsible for defining, implementing, and monitoring compliance to 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 internal portal.                  | Inspected the Integrated Management System Manual in Zoho portal, MOM for the aspects such as 'name of document', 'contents of policy', 'Prepared By', 'Approved By and Date', 'agenda of MOM' and 'whether policy available in portal' to ascertain whether Zoho's management committee was responsible for defining, implementing, and monitoring compliance to 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 Exception Noted |

**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.

| #      | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests                                |
|--------|---|---|---------------|---|
| CA4.01 | Security settings for account lockout, password minimum length and password history are configured for authentication into Domain (AD), IAM (for Zoho accounts), IAN (for Zodoor and IDC) and also for IDC infrastructure. Users are required to use two-factor authentication to connect to the IDC infrastructure from IAN network. | Inspected the account lockout and password configuration in Domain Controller, IAM, IAN and IDC infrastructure for aspects such as 'Password Configuration and Complexity', 'Password history' 'Account lockout settings' and 'authorization upon every logon' and 'Configuration for Multi-factor Authentication' to ascertain whether security settings for account lockout, password minimum length and password history were configured for authentication into Domain (AD), IAM (for Zoho accounts), IAN (for IDC and Zodoor access) and also whether users are required to use two-factor authentication to connect to the IDC infrastructure from IAN network. | 3.8.1         | Exception Noted. Refer Section 4.4 exception #1 |

| #      | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|--|---|---------------|--------------------|
| CA4.02 | <p>For newly joined associates, trainees, contractors, the HR team creates an account in ZohoPeople (Control Panel) and once the account is created, AD account is auto created by the system. The respective manager also creates a request for providing workstation to the associate in ZohoPeople and the same is assigned and actioned upon by the SysAdmin team.</p> | <p>Inspected for sample new joiners the Zoho IT Incident Request ticket for aspects such as 'associate name', 'date of joining', 'date of creation in ZohoPeople', 'requested on' 'request ID', 'requested by', 'requested on' 'subject of Email', 'Actioned by SysAdmin' and 'Date of creation timestamps from AD' to ascertain whether for newly joined associates, trainees, contractors, the HR team created an account in ZohoPeople (Control Panel) and once the account was created, AD account was auto created by the system.</p> <p>Inspected for sample new joiners the Zoho IT Incident Request for aspects such as 'Workstation request ID', 'Request created by' and 'Actioned by SysAdmin Team' to ascertain whether the respective manager created a request for providing workstation to the associate in ZohoPeople and the same was assigned and actioned upon by the SysAdmin team.</p> | None          | No Exception Noted |
| CA4.03 | <p>In case of an associate leaving Zoho, the HR team disables the account in ZohoPeople (Control Panel). The HR notifies the SysAdmin / Zorro team and the SysAdmin / Zorro team disables the logical access of the associate.</p>   | <p>Inspected Zoho People application for sample associates leaving Zoho, the IT Incident Request ticket for aspects such as 'associate name', 'last working day', 'request ID', 'requested by', 'requested on' 'date of leaving' and 'Date of disabling' to ascertain whether when an associate was leaving Zoho, the HR team disabled the account in ZohoPeople (Control Panel) and the HR notified the SysAdmin / Zorro team and the SysAdmin / Zorro team disabled the logical access of the associate.</p>  | None          | No Exception Noted |

| #      | Control Activity  | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|---|--|---------------|--------------------|
| CA4.04 | Logical access to the tools (managed by NOC team) used for performing NOC's daily operations are granted/revoked by the Senior NOC Member based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member. | <p>Inspected for sample access requests, the ticket from Zoho Creator tool for aspects such as 'ID', 'Added time', 'Name', 'Access required to tool', 'Access granted' and 'approver mail ID' and 'Approval status' to ascertain whether logical access to the tools (managed by NOC team) used for performing NOC's daily operations were granted based on the approval of the NOC manager in the Zoho Creator tool where the request was raised by the Senior NOC Member.</p> <p>Inspected for sample access revocation, the ticket from Zoho Creator Tool for aspects such as 'ID', 'Name', 'Access to tool', 'request date', 'approval' 'disabled time' to ascertain whether logical access to the tools (managed by NOC team) used for performing NOC's daily operations were revoked by the Senior NOC Member based on the approval of the NOC Manager in the Zoho Creator tool where the request was raised by the Senior NOC Member.</p> | None          | No Exception Noted |
| CA4.05 | Network diagram detailing the network devices such as firewalls and switches is maintained by the NOC Manager. Further, access to the network devices are restricted to NOC Team to prevent unauthorized access.  | <p>Inspected the network diagram and email communication between Senior Engineer- NOC and Manager- NOC for aspects such as 'scope', 'network devices', 'prepared by', 'approved by' and 'roles provided to the users' to ascertain whether network diagram detailing the network devices such as firewalls and switches was maintained by the NOC Manager.</p> <p>Inspected the user access listing from firewall and switch console for aspects such as 'user having access', 'privileges', 'role granted' and 'rationale for access' to ascertain whether access to the network devices were restricted to NOC Team to prevent unauthorized access.</p>  | None          | No Exception Noted |

| #      | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|---|---|---------------|--------------------|
| CA4.06 | Based on the network monitoring by the NOC team through NOCMON and EventLog Analyzer, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC ServiceDeskPlus Portal. | <p>Inspected the alert configuration in NOCMON and Event Analyzer for aspects such as 'notification sent to', 'alert priority' and 'integration with network device' to ascertain whether based on the network monitoring by the NOC team through NOCMON and EventLog Analyzer, alerts for changes to network configurations and alerts / errors relating to network devices were auto-generated and sent to the NOC ServiceDeskPlus Portal.</p> <p>Inspected the monitoring dashboard for aspects such as 'dashboard contents', 'type of alerts triggered', 'event information captured', 'resolution of alerts' to ascertain whether based on the network monitoring by the NOC team through NOCMON and EventLog Analyzer, alerts for changes to network configurations and alerts / errors relating to network devices were auto-generated and sent to the NOC ServiceDeskPlus Portal.</p> | None          | No Exception Noted |
| CA4.07 | Access to Corporate VPN is authenticated with Zoho users' domain account.   | Inspected the integration settings between VPN and Zoho domain for aspects such as 'authentication configuration in VPN', 'number of authentication layers' and 'remote gateway used' to ascertain whether access to corporate VPN was authenticated with Zoho users' domain account.   | None          | No Exception Noted |
| CA4.08 | Client servers and data can be accessed through IAN VPN or the dedicated IAN servers in the Zoho facilities.  | Inspected the VPN configuration for DC, hosting of production and pre-production servers and network diagram for aspects such as 'authentication configuration for VPN', 'authentication layers' and 'details of network diagram' to ascertain whether client servers and data can be accessed through IAN VPN or the dedicated IAN servers in the Zoho facilities.   | None          | No Exception Noted |

| #      | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests                                |
|--------|---|---|---------------|---|
| CA4.09 | User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on a yearly basis. Corrective actions, if any, are taken on a timely manner. | Inspected the user access review performed for sample products for aspects such as 'review performed by', 'review date', 'user listing', 'review details' and 'follow-up action' to ascertain whether User Access Review of users with access to IAM Roles that granted access to the products and users with access to Zodoor and IDC network were reviewed by the manager / Department Head / Admin on a yearly basis and corrective actions, if any, were taken on a timely manner.  | None          | No Exception Noted                              |
| CA4.10 | Access to IDC Landing Access Machine and IDC server for new requests are granted by Zorro Team member based on the approval from the reporting manager and Zorro Manager.   | Inspected the tickets from Creator application and approval email for sample access creation for aspects such as 'request ID', 'requestor email ID', 'access type', 'Name of the account to be created in IDC landing machine', 'access created by', 'access created on', 'email sent to', 'approved by' and 'subject of email' to ascertain whether access to IDC Landing Access Machine and IDC server for new requests were granted by Zorro Team member based on the approval from the reporting manager and Zorro Manager. | None          | No Exception Noted                              |
| CA4.11 | Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro Team based on the IDC access revocation process on a timely manner.  | Inspected the sample tickets for access revocation for IDC landing machine for the aspects such as 'name', 'team', 'account', 'disabled by' and 'disabled on' to ascertain whether access revocation in IDC Landing Access Machine and IDC server for Zorro associates were done by the designated Zorro Team based on the IDC access revocation process on a timely manner.  | None          | Exception Noted. Refer Section 4.4 Exception #2 |

| #      | Control Activity  | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|---|--|---------------|--------------------|
| CA4.12 | Privileged access to servers is restricted to authorized personnel from the Zorro | Inspected the user listing from the servers for aspects such as 'employee number', 'username', 'compared the list of users with authorized listing' to ascertain whether Privileged access to servers was restricted to authorized personnel from the Zorro. | None          | No Exception Noted |

[Space left blank intentionally]

**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.

| #      | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|--|---|---------------|--------------------|
| CA5.01 | Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations based on the frequency defined.                                  | Inspected for sample workstations the antivirus installation and configuration for aspects such as 'workstation ID', 'AV version', 'Synchronization interval', 'AV last update date' and 'AV release date' to ascertain whether antivirus software was installed in the user work stations and the latest updates and definitions were pushed automatically to the workstations based on the frequency defined.                       | None          | No Exception Noted |
| CA5.02 | Monitoring of Anti Virus console is performed on a real time basis by the IT Team and in case of any alerts, corrective action is taken.   | Inspected Anti Virus console dashboard for aspects such as 'tool name', 'real-time monitoring status', 'alerts', 'device status' and 'action taken' to ascertain whether monitoring of AV console was performed on a real time basis by the IT Team and in case of any alerts, correction action was taken.   | None          | No Exception Noted |
| CA5.03 | Virtual LAN changes are requested by the SysAdmin Team (in the case of Corporate offices) or by the Zorro team (in the case of IDCs) and the same is approved by the Managers/ L3 of the Sysadmin/ Zorro team. | Inspected for sample VLAN changes the change tickets from Creator application for aspects such as 'change ID, 'requestor', 'request type', 'requestor', 'approver email' and 'processing status' to ascertain whether Virtual LAN changes were requested by the SysAdmin Team (in the case of Corporate offices or by the Zorro team in the case of IDCs) and the same was approved by the Managers / L3 of the Sysadmin/ Zorro team. | None          | No Exception Noted |



| #             | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|---------------|--|---|---------------|--------------------|
| <b>CA5.04</b> | The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the SysAdmin or Zorro team as a second level approval. | Inspected for sample firewall rule changes, the firewall rule change tickets from Creator application for aspects such as 'request ID', 'Datacenter', 'requested by', 'request raised to', 'requested on' 'approval by product manager, approval by SysAdmin or Zorro team', 'completion notes', 'firewall change logs', 'approved on' and 'closed date' to ascertain whether the NOC team added / removed / modified firewall rules based on the requests raised by Zoho Product Teams through the Firewall Access Form in the Zoho Creator tool and whether for the changes to the firewall the approval was obtained from the respective Product Manager and from the SysAdmin or Zorro team as a second level approval. | None          | No Exception Noted |
| <b>CA5.05</b> | On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset and tracks the deviations to closure                                    | Inspected the request ticket raised for firewall rule review for sample half year and sample change tickets for aspects such as 'ID', 'ticket type', 'subject', 'approved by', 'approved on', 'deficiencies observed in the review', 'action taken' and 'ticket closed date' to ascertain whether on a half-yearly basis, the NOC Engineers reviewed the existing firewall rules and the same was approved by the NOC Manager and whether in case of any deviations noted during the firewall review, the NOC Engineer made the necessary changes in the firewall ruleset and tracked the deviations to closure.  | None          | No Exception Noted |

| #      | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|--|--|---------------|--------------------|
| CA5.06 | When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager.  | Inspected for sample change requests Change control form for aspects such as 'subject', 'change ID' 'change', 'Backup plan available', 'tested by', 'approved by', 'servers and sites impacted', 'availability of completion notes', 'implementer' and 'close date' to ascertain whether when the NOC team undertook configuration/ device changes, the Senior NOC Engineer raised a request through the Change Control Form in the Zoho Creator tool which was approved by the NOC Manager.   | None          | No Exception Noted |
| CA5.07 | On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken. On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective action is taken. | <p>Inspected for sample weeks the vulnerability report / email containing vulnerability scan details for sample products for aspects such 'scan run by', 'date of scan', 'email sent to', 'email sent on', 'subject', 'corrective action' and 'count of deviations identified' to ascertain whether on a weekly basis, the central security team performed vulnerability scanning to ensure application security for its products and in case of any deviations identified, a corrective action was taken.</p> <p>Inspected for in-scope applications the penetration testing report for aspects such as 'risk category', 'scope', 'test cases handled', 'date performed', 'deviations identified', 'conclusion' and 'action taken' to ascertain whether on a yearly basis, the product security team performed penetration testing to ensure application security for its products and in case of any deviations identified, corrective action was taken.</p> | None          | No Exception Noted |

| #             | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|---------------|---|---|---------------|--------------------|
| <b>CA5.08</b> | Access to external storage devices and internet are disabled on IDC workstations to prevent data loss | Inspected the configuration for IDC workstation in the domain for the aspects such as 'blacklist rule' and 'configuration for USB storage' to ascertain whether access to external storage devices and internet were disabled on IDC workstations to prevent data loss. | None          | No Exception Noted |

[Space left blank intentionally]

**4.3.1.3 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.

| #      | Control Activity   | Tests Performed  | CUEC/C SOC | Results of Tests   |
|--------|--|--|------------|--------------------|
| CA6.01 | For new associates / trainees / contractors joining Zoho, the Physical Security team /Building Management System Team issues an access card to the associate based on the request raised by HR to grant physical access. Physical Security team also provides photo based ID cards for the Zoho associates. The ID cards / badges are distinguished based on the color of the tags described in the HR policy. | <p>Inspected for sample new associates / trainees / contractors, the Zoho HRMS application for aspects such as 'Employee ID', 'associate name', 'date of joining', 'Access request raised by', 'Access Card details updated by' and 'General Access granted on' to ascertain whether for new associates / trainees / contractors joining Zoho, the Physical Security team /Building Management System Team issued an access card to the associate based on the request raised by HR to grant physical access and whether physical security team also provided photo based ID cards for the Zoho associates.</p> <p>Observed the ID card details for the aspects such as 'location' and 'card details' to ascertain whether the ID cards / badges were distinguished based on the color of the tags described in the HR policy.</p> | 3.9.1      | No Exception Noted |

| #      | Control Activity   | Tests Performed   | CUEC/C SOC | Results of Tests   |
|--------|--|---|------------|--------------------|
| CA6.02 | In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team/Building Management System Team deactivates the old ID card and issues a new physical ID card.   | Inspected for sample lost access cards the request in Zoho people and email communication between Zoho associate and HR team / Physical Security team for aspects such as 'email sent by', 'email sent to', 'email subject', 'Date of email' and 'action taken' to ascertain whether in case an access card was lost, the associate raised a request in Zoho people and whether based on the request, the Physical Security team /Building Management System Team deactivated the old ID card and issued a new physical ID card.  | 3.9.1      | No Exception Noted |
| CA6.03 | Upon an associate or a contractor leaving Zoho or in case of absconding associates, the HR team updates separation details in HRMS application and also sends an e- mail to the Physical Security team notifying the leavers. Based on the email, Physical Security team revokes the physical access card on the last working day. | Inspected for sample resigned associates and third party contractors and absconders, the Zoho HRMS application for aspects such as 'HRMS details updated by', 'HRMS details updated on', 'email request sent by', 'email sent to physical security team' 'requested date', 'last working date', 'physical access revoked on' and 'physical access revoked by' to ascertain whether upon an associate or a contractor leaving Zoho or in case of absconding associates, the HR team updated separation details in HRMS application and also sent an e- mail to the Physical Security team notifying the leavers and whether based on the email, Physical Security team revoked the physical access card on the last working day. | 3.9.1      | No Exception Noted |

| #             | Control Activity   | Tests Performed  | CUEC/C<br>SOC | Results of Tests   |
|---------------|--|--|---------------|--------------------|
| <b>CA6.04</b> | Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.  | <p>Observed the entry and exit points of Zoho facilities to ascertain whether entry/exit points were manned 24x7 by the Security personnel restricting access to authorized individuals.</p> <p>Inspected for sample dates the security guard register for aspects such as 'date', 'shift details', 'time-in and time-out details', and 'signature details' to ascertain whether entry/exit points were manned 24x7 by the Security personnel restricting access to authorized individuals</p>   | 3.9.1         | No Exception Noted |
| <b>CA6.05</b> | Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities and recorded. | <p>Inspected and observed for sample dates the visitor-vendor register for aspects such as 'date', 'visitor/vendor name', 'time-in and time-out details' to ascertain whether entry and exit details of the vendors / visitors to Zoho were recorded through VMS/visitor register.</p> <p>Inspected and observed for sample dates the visitor-vendor register for aspects such as 'Vendor/Visitor name', 'date', and 'electronic device declaration details' to ascertain whether laptops of the vendors/visitors were declared at the entrance of the Zoho facilities and recorded.</p> | 3.9.1         | No Exception Noted |

| #             | Control Activity  | Tests Performed  | CUEC/C<br>SOC | Results of Tests   |
|---------------|---|--|---------------|--------------------|
| <b>CA6.06</b> | Proximity card-based access control system is installed at the entry / exit points within the facility. In addition, access to the Zoho Server room, NOC room, Switch room, Zorro Workspace and asset storage room is restricted using proximity card-based access control system and PIN based authentication. | Inspected Zoho facilities for aspects such as 'installation of proximity card-based access control system', 'PIN based authentication' and 'location of installation' to ascertain whether proximity card based access control system was installed at the entry / exit points within the facility and also whether access to the Zoho Server room, NOC room, Switch room, Zorro Workspace and asset storage room was restricted using proximity card-based access control system and PIN based authentication | 3.9.1         | No Exception Noted |
| <b>CA6.07</b> | Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.  | <p>Observed the Zoho premises and server rooms for aspects such as 'Installation of CCTV cameras' and 'installation points' to ascertain whether Zoho premises and server rooms were monitored through Closed-Circuit Television (CCTV) cameras.</p> <p>Inspected the CCTV footage for sample dates for aspects such as 'Location' and 'recordings' to ascertain whether CCTV recordings were retained for a minimum of 60 days.</p>   | 3.9.1         | No Exception 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.

| #      | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|---|---|---------------|--------------------|
| CA7.01 | Environmental safeguards are installed in Zoho facilities comprising of the following:<br><ul style="list-style-type: none"> <li>• Cooling Systems</li> <li>• UPS with Battery and diesel generator back-up</li> <li>• Smoke detectors</li> <li>• Water sprinklers</li> <li>• Fire resistant floors</li> <li>• Fire extinguisher</li> </ul> | Observed the Zoho facility for aspects such as ‘cooling facilities’, ‘UPS with battery and diesel generator’, ‘smoke detectors’, ‘water sprinklers’, ‘fire extinguisher’ and ‘fire-resistant floors’ to ascertain whether environmental safeguards were installed in Zoho facilities comprising the following:<br><ul style="list-style-type: none"> <li>• Cooling Systems</li> <li>• UPS with Battery and diesel generator back-up</li> <li>• Smoke detectors</li> <li>• Water sprinklers</li> <li>• Fire resistant floors</li> <li>• Fire extinguisher</li> </ul> | 3.9.1         | No Exception Noted |
| CA7.02 | Planned Preventive Maintenance (PPM) is performed on quarterly basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.  | Inspected for sample quarters the preventive maintenance report for aspects such as ‘name of equipment’, ‘date of maintenance report’ and ‘performed by’ to ascertain whether planned preventive maintenance (PPM) was performed on a quarterly basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.   | 3.9.1         | No Exception Noted |



| #      | Control Activity  | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|---|--|---------------|--------------------|
| CA7.03 | Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.    | Inspected the mock fire drill report for aspects such as 'Conducted on', 'location', 'Observations of mock fire drill' and 'closure details of mock fire drill' to ascertain whether mock Fire drills were conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster          | 3.9.1         | No Exception Noted |
| CA7.04 | Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis. | Inspected Business Continuity & Disaster Recovery Plan document for aspects such as 'name of the document', 'Contents', 'Prepared by' and 'reviewed and approved by' to ascertain whether Zoho had defined Business Continuity Plan and Disaster Recovery procedures which was reviewed and approved by the Compliance Leadership team on an annual basis. | None          | No Exception Noted |

| #      | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|--|--|---------------|--------------------|
| CA7.05 | <p>Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On an annual basis, the Zorro team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness and also to perform DC maintenance operations, if required. This is done using the ZAC tool with the approval of the Zorro Manager.</p> | <p>Inspected Business Continuity Plan document for aspects such as 'name of the Policy', 'version no', 'contents of policy', 'preparer by', 'reviewed by' and 'approved by' and 'approved on' to ascertain whether Zoho had a Disaster Recovery Data Center (DR DC) to ensure the business continuity.</p> <p>Inspected the annual DR Testing report and status from ZAC tool for aspects such as 'disaster recovery testing details', 'test results', 'approval details' and 'DC' to ascertain whether on a periodic basis, the Zorro team switched the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness and also to perform DC maintenance operations, if required and whether this was done using the ZAC tool with the approval of the Zorro Manager.</p> | None          | No Exception Noted |

**4.3.1.4 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.

| #      | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|---|---|---------------|--------------------|
| CA8.01 | Upon a new associate joining, an induction training is conducted by the Training Team and HR Team to make the associate aware of the information security practices and various policies of Zoho. The attendance for the training is captured in Zoho people. | <p>Inspected for sample newly joined associates, the training attendance register in Zoho People for aspects such as ‘employee name’, ‘date of attendance (issued time)’, ‘date of joining’ to ascertain whether upon a new associate joining, an induction training was conducted by the Training Team and HR Team to make the associate aware of the information security practices and various policies of Zoho and whether the attendance for the training was captured in Zoho people.</p> <p>Inspected for the induction deck for aspects such as ‘name of deck’ and ‘contents’ to ascertain whether feedback was collected upon completion of training by the HR Team.</p> | None          | No Exception Noted |

| #             | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|---------------|---|---|---------------|--------------------|
| <b>CA8.02</b> | Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions and approved by the Senior Manager-HR on an annual basis.   | Inspected the Policy Description Manual for the aspects such as 'Name of the document', 'details of the policy', 'version no.', 'number of jobs defined', 'roles and responsibilities' 'prepared by', 'prepared on', 'approved by' and 'approved on' to ascertain whether Zoho HR Team had defined job descriptions specifying the responsibilities for key job positions and approved by the Senior Manager-HR on an annual basis. | None          | No Exception Noted |
| <b>CA8.03</b> | Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis. | Inspected the Human Resources Security Policy for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved date' to ascertain whether the procedures for background verification of Zoho associates was defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.               | None          | No Exception Noted |

| #             | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests  |
|---------------|--|--|---------------|---|
| <b>CA8.04</b> | Upon new associates joining Zoho, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated. | <p>Inspected for sample newly joined associates the Background Check Reports for aspects such as 'associate name', 'BGC performed by' and 'BGC result' to ascertain whether upon new associates joining Zoho, a Background Check (BGC) was performed by the third party service providers and also whether a BGC report was provided to Zoho on completion of the background check and in case of a negative result, the employee was terminated.</p> <p>Inspected the Background check report for sample newly joined associated and noted that there were no instances of negative result in the background check during the period of examination, hence DHS LLP was not able to test the aspect of control related to negative result.</p> | 3.9.2         | <p>No Exception Noted</p> <p>The operating effectiveness of employee terminations due to negative background verification results could not be tested as there was no related activity during the examination period.</p> |
| <b>CA8.05</b> | Upon joining Zoho, the associates are required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.   | Inspected for the sample newly joined associates the documents signed by associates for aspects such as 'employee ID', 'Full name', 'date of joining', and 'date of signing the document' to ascertain whether upon joining Zoho, the associates were required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.   | None          | <p>Exceptions Noted.</p> <p>Refer Section 4.4 Exception #3</p>  |

| #             | Control Activity  | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|---------------|---|---|---------------|--------------------|
| <b>CA8.06</b> | Zoho has a defined Code of Ethics document that is reviewed and approved by the Manager - HR on an annual basis and it is made available on Intranet to the associates. The Code defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. | Inspected Code of Ethics document for aspects such as 'policy name', 'contents of the document', 'prepared by', 'approved by', 'approved on', 'reviewed by' and 'availability on intranet' to ascertain whether Zoho had a defined Code of Ethics document that was reviewed and approved by the Manager - HR on an annual basis and it was made available on Intranet to the associates and also whether the Code defined the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. | None          | No Exception Noted |
| <b>CA8.07</b> | Zoho has a Human Resource Security policy, which is defined by the Assistant Manager - HR Operations and approved by the Senior Manager - HR on an annual basis. The policy is made available to the Zoho associates through Intranet (Zoho People).  | Inspected the Human Resource Security Policy and the Zoho intranet website for aspects such as 'policy name', 'Scope', 'Prepared by', 'Approved by/on' and 'availability of policy on Intranet' to ascertain whether Zoho had a Human Resource Security policy, which was defined by the Assistant Manager - HR Operations and approved by the Senior Manager - HR on an annual basis and also whether the policy was made available to the Zoho associates through Intranet (Zoho People).   | None          | No Exception Noted |

| #             | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|---------------|--|---|---------------|--------------------|
| <b>CA8.08</b> | Zoho has a defined organizational structure establishing the key areas of authority and responsibility, lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis. | Inspected the Organizational chart and the email communication for aspects such as 'name of the document', 'contents of the organizational chart', 'roles and responsibilities' 'document prepared by', 'prepared on', 'approved by' and 'approved on' to ascertain whether Zoho had a defined organizational structure establishing the key areas of authority and responsibility, lines of reporting and defined roles which was reviewed and approved by Senior Manager-HR on an annual basis. | None          | No Exception Noted |

**4.3.1.5 Incident Management**

**Control Objective:** Controls provide reasonable assurance that incident tickets are recorded, analyzed and tracked to closure

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.

| #      | Control Activity  | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|---|--|---------------|--------------------|
| CA9.01 | Zoho has defined an Incident Management Policy, which is prepared by Manager in Incident Management team and approved by the Information Security Manager. The policy is reviewed on an annual basis and version history is maintained within the document. | Inspected Incident Management policy for aspects such as 'name of policy', 'version number', 'revision date', 'contents of policy', 'prepared by', 'approved by' and 'approved on' to ascertain whether Zoho had defined an Incident Management Policy, which was prepared by Manager in Incident Management team, approved by the Information Security Manager and whether the policy was reviewed by leadership staff on an annual basis and version history was maintained within the document. | None          | No Exception Noted |



| #      | Control Activity  | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|--------|---|--|---------------|--------------------|
| CA9.02 | Based on the inputs received via service desk, the incident management team coordinates with relevant stakeholders to analyse the potential impact of the security incident raised in Creator application. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. | Inspected for sample security incidents the security incident ticket workflow details from Creator application for aspects such as 'incident ID', 'Incident Title', 'Description of the incident', 'RCA available', 'Raised By', 'Related to', 'Incident Cause', 'Incident Category' and 'Incident start time' and 'Status' to ascertain whether based on the inputs received via service desk, the incident management team coordinated with relevant stakeholders to analyse the potential impact of the security incident raised in Creator application and whether the relevant product team preformed root cause analysis (RCA) and updated the security incident in the Zoho creator tool. | 3.8.3         | No Exception Noted |

| #      | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|--------|--|---|---------------|--------------------|
| CA9.03 | <p>Based on the alert triggered by the availability monitoring tools, an automated entry of an event is created in the Zoho creator tool and a downtime post is made on Zoho Connect to notify the stakeholders. The relevant product team performs RCA and the action points are identified for implementation. The incident ticket is updated appropriately and tracked for closure.</p> | <p>Inspected for sample alerts the Creator form requests for aspects such as 'incident ID', 'customer affected', 'Services impacted', 'Incident Ticket updated by' and 'RCA available' to ascertain whether based on the alert triggered by the availability monitoring tools, an automated entry of an event was created in the Zoho creator tool and a downtime post was made on Zoho Connect to notify the stakeholders and whether the relevant product team performed RCA and the action points were identified for implementation and also whether the incident ticket was updated.</p> | None          | No Exception Noted |
|        |  | <p>Inspected the alerts configuration for aspects such as 'type', 'priority', 'alert triggered to' to ascertain whether based on the alert triggered by the availability monitoring tools, an automated entry of an event was created in the Zoho creator tool and a downtime post was made on Zoho Connect to notify the stakeholders and whether the relevant product team performed RCA and the action points were identified for implementation and also whether the incident ticket was updated.</p>   |               |                    |

| #             | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|---------------|--|--|---------------|--------------------|
| <b>CA9.04</b> | 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 'name of report', 'report uploaded by', 'date of report upload', 'Incident - review comments by', 'incident - downtime and description details' 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 also whether the report included the categories of incidents, downtime details (in case of availability incident) and the incident description. | None          | No Exception Noted |

[Space left blank intentionally]

**4.3.1.6 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.

| #       | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|---------|--|--|---------------|--------------------|
| CA10.01 | The NOC team uses an in-house tool (DeviceExpert) to backup network device configurations on a daily basis (incremental backup) and also on a weekly basis (full backup). In case of a backup failure, an automated email is triggered, and remediation action is taken. | Inspected for sample days/weeks and the Network Configuration Manager Schedule and alert configuration for aspects such as 'datacenter', 'frequency of backup', 'devices backed up', 'sample date/week', 'type of backup', 'failure alert sent to' and 'remedial action' to ascertain whether the NOC team used an in-house tool (Device Expert) to backup network device configurations on a daily (incremental backup) and weekly (full backup) and whether in case of a backup failure, an automated email was triggered, and remediation action was taken by NOC team. | None          | No Exception Noted |

| #       | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests   |
|---------|--|---|---------------|--------------------|
| CA10.02 | The Zorro team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Zorro team and appropriate corrective action is taken. | Inspected backup configuration in ZAC tool, deployment configuration for aspects such as 'datacenter', 'server', 'frequency of backup', 'backup retention period', 'notification alert to' and 'backup encryption' to ascertain whether the Zorro team had configured the ZAC tool for daily incremental and weekly full backups of the database servers and whether in case of a backup failure, an automated email is sent to the Zorro team and corrective action was taken. | None          | No Exception Noted |
|         |  | Inspected for sample dates/weeks the backup status and the backup configuration for aspects such as 'backup retention period', 'type of backup' and 'backup available' to ascertain whether backups were retained for a period of 3 months.   |               |                    |
| CA10.03 | Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Zorro team through Zoho Creator tool, who handles the backup restoration.   | Inspected for sample backup restoration requests the request ticket for aspects such as 'backup restoration request ID', 'service type', 'database backup type', 'Creation date and time', 'cluster IP' to ascertain whether backup restoration requests were received from the customers to the respective Product Support Team and that the Product Support Team routed the request to Zorro team through Zoho Creator tool, who handled the backup restoration.              | 3.8.2         | No Exception Noted |

| #       | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|---------|--|--|---------------|--------------------|
| CA10.04 | IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR. | Inspected and observed Mirroring Dashboard for aspects such as 'Name of DC', 'Replication time', 'Availability of cluster dashboard' and 'Cluster replication' to ascertain whether IDCs were set up with redundant database clusters to ensure mirroring of customer data and also whether the customer data was mirrored in a separate geographic location to ensure BCP/DR. | None          | No Exception Noted |
| CA10.05 | The failed hard disk drives are degaussed prior to disposal / replacement.   | Inspected for sample hard disk failures the disposal register and email communication for aspects such as 'email sent by', 'email sent to', 'email sent on', 'subject of email', 'contents of email', 'disposal details' and 'Label details' to ascertain whether the failed hard disk drives were degaussed prior to disposal / replacement.                                  | None          | No Exception Noted |

[Space left blank intentionally]

### 4.3.1.7 Third Party Management

**Control Objective: Controls provide reasonable assurance that the sub processors, and third party vendors in relation to hosting of servers are monitored by Zoho.**

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.

| #       | Control Activity   | Tests Performed   | CUEC/<br>CSOC | Results of Tests    |
|---------|--|---|---------------|---------------------|
| CA11.01 | On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centres and are reviewed by the Zoho Compliance team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action. | Inspected the Data center co-location provider certification/report review email for the aspects such as 'attestation report details', 'observations noted', 'Action taken', 'Report evaluated by' and 'Report evaluated on' to ascertain whether on an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports were obtained for co-location data centers and were reviewed by the Zoho Compliance team and whether in case there were any non-compliances noted in the report, the compliance team followed up with the co-location service provider for further action. | 3.9.1         | No Exception Noted. |
| CA11.02 | Risk assessment is performed annually by Zoho Privacy Team to assess the risk of sub processors identified by them and identify suitable risk treatment plan on an annual basis.   | Inspected for sample sub-processors the Risk Assessment performed for aspects such as 'name of vendor', 'service description' and 'applicable services' and 'Risk assessment details' to ascertain whether Risk assessment was performed annually by Zoho Privacy Team to assess the risk of sub processors identified by them and identify suitable risk treatment plan on an annual basis.  |               |                     |

| #              | Control Activity   | Tests Performed  | CUEC/<br>CSOC | Results of Tests   |
|----------------|--|--|---------------|--------------------|
| <b>CA11.03</b> | A contract is defined, documented and approved between Zoho and sub processors/third party vendors for services in relation to hosting of servers. The contract includes the scope of services to be provided and confidentiality clauses. | Inspected for sample third parties the agreement document signed between Zoho and third party vendor for aspects such as 'scope', 'confidentiality clause', 'validity', 'type of service', 'agreement signed by' and 'agreement signed on' to ascertain whether a contract was defined, documented and approved between Zoho and sub processors/third party vendors for services in relation to hosting of servers and whether the contract included the scope of services to be provided and confidentiality clauses. | 3.9.1         | No Exception Noted |

[Space left blank intentionally]



#### 4.4 Management Response to Exceptions

The Audit exceptions presented in the Section 4 of this report were reviewed and discussed on 27/02/2023, during a dedicated Closing Meeting attended by the Management.

The Management Responses to the exceptions noted is as under:

##### Exception 1

| Description of Exception  | Control Objective and Activity description  | Management Response to Exception  |
|---|---|---|
| <p>We noted the password parameter configured in Domain (AD) and IAM tool is not line with Zoho’s password policy.</p> <p>Domain:<br/>Maximum Password Age<br/>Lockout Bad count</p> <p>IAM:<br/>Maximum Password Age</p> | <p>CO 4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated</p> <p>CA4.01: Security settings for account lockout, password minimum length and password history are configured for authentication into Domain (AD), IAM (for Zoho accounts), IAN (for Zodoor and IDC) and also for IDC infrastructure. Users are required to use two-factor authentication to connect to the IDC infrastructure from IAN network.</p> | <p>We agree with the exception noted.</p> <p>The password age for AD and IAM was not configured in line with policy as there was a sync issue between Mac workstation and AD due to which the password parameter was modified on a temporary basis. We have initiated the rectification activity for the same.</p> <p>Considering MFA is enforced for entire organization and VPN authentication is performed through MFA, the risk is reduced.</p> |

**Exception 2**

| Description of Exception   | Control Objective and Activity description   | Management Response to Exception   |
|--|--|--|
| <p>For 2 out of 25 samples, we noted that access for the IDC landing machine was not revoked in a timely manner as per the Access control procedure.</p> | <p>CO 4: Controls provide reasonable assurance that logical access to Zoho systems is restricted to authorized users and access is authenticated</p> <p>CA4.11: Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro Team based on the IDC access revocation process on a timely manner.</p> | <p>We agree with the exception noted.</p> <p>The access to the two user ids was restricted only to the authorized members of the Infrastructure team and Zoho performed a periodic user access review by the designated personnel in every team and no discrepancies were identified. The password to these two user ids is controlled and changed on a periodical basis.</p> <p>The direct access to the IDC machines is governed by our access control policies. Zoho has controls over the users who have left the organization where the access revocation happens automatically on the employee exit. The auto sync between IDC landing access (IAN) and Zoho People (HR system) is in place and if an account of a Zoho employee is disabled in Zoho people, the user cannot login to the Zoho Portal and also to the IDC landing machine (IAN).</p> <p>Based on the above measures in place in Zoho, the risk is reduced.</p> |

**Exception 3**

| Description of Exception  | Control Objective and Activity description   | Management Response to Exception   |
|---|--|--|
| We noted for 1 out of 35 samples that the NDA and other documents was signed after 353 days of joining. | <p>CO8: Controls provide reasonable assurance that policies and procedures for hiring and separation of the associates are adhered to.</p> <p>CA8.05: Upon joining Zoho, the associates are required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.</p> | <p>We agree with the exceptions noted.</p> <p>The NDA was signed during the onboarding as part of the process but was misplaced. The document was re-signed and updated in the file.</p> |

# **Deloitte Haskins & Sells LLP**

This material has been prepared by Deloitte Haskins & Sells LLP (“DHSLLP”), on a specific request from you and contains proprietary and confidential information. This material may contain information sourced from publicly available information or other third-party sources. DHSLLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. The information contained in this material is intended solely for you. Any disclosure copy or further distribution of this material or the contents thereof is strictly prohibited.

Nothing in this material creates any contractual relationship between DHSLLP and you. Any mutually binding legal obligations or rights may only be created between you and DHSLLP upon execution of a legally binding contract. By using this material and any information contained in it, the user accepts this entire notice and terms of use.

©2023 Deloitte Haskins & Sells LLP.

Document Reference No.: RA-TPA-31036472-2022-23-R105