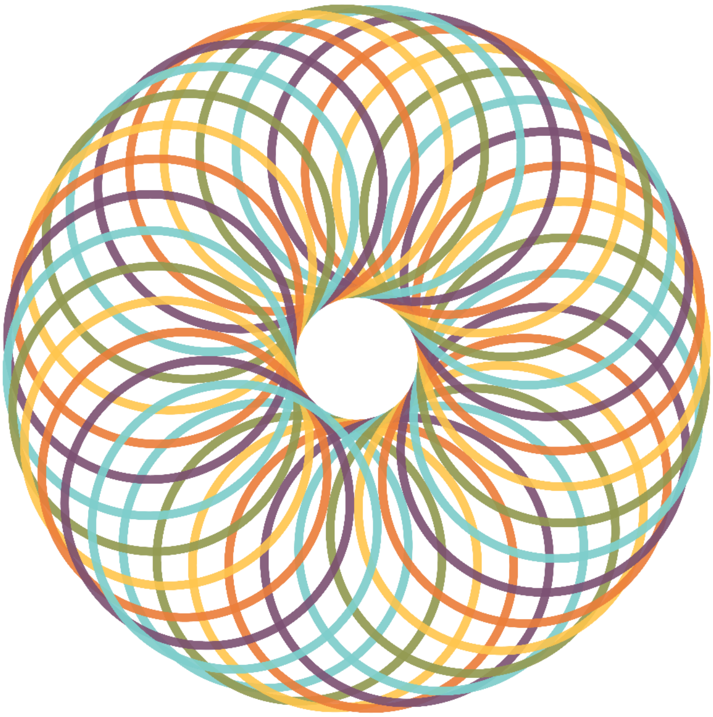
Deloitte
Haskins & Sells LLP

ZOHO



You and your company have obtained access to this report dated 25th February, 2022 on the Application Development, Production Support and the related General IT Controls services performed by Deloitte Haskins & Sells LLP ("DHS LLP") as agreed with Zoho Corporation Private Limited (herein referred to as "Client") ("Report), by accepting the terms of the Click Through Access Agreement that was attached to this Report and acknowledging that your company ("Recipient") is a prospect customer of the Client/ or as per contractual agreement with the client eligible to receive this report.

The terms of the Access Agreement include, among other things, an agreement by you and your company not to further disclose, distribute, quote, or reference this Report and an agreement to release and indemnify DHSLLP for certain claims. By reading this Report, you agree that you and your company have agreed to the terms of such Access Agreement. If you are not the Recipient and you have not accessed this Report by agreeing to the terms of such Access Agreement then you are prohibited from having access to this Report and you must permanently delete if from your and your company's computer and network systems.

This Report is intended only to be used by the Client solely for its internal purposes. DHSLLP and its subcontractors and their respective personnel shall have no liability, duties, responsibilities or other obligations to anyone including Recipient who may obtain this Report.

DHS LLP, its subcontractors and their respective personnel do not have any obligation to advise or consult with any entity regarding their use of this Report. Any use of this Report by a party other than Client is at such party's sole and exclusive risk. This Report is not to be further disclosed, distributed, quoted, or referenced to any third party or included or incorporated by reference in any other document.

SOC 2 Type 2 Examination

Zoho Corporation Private Limited ('Zoho')

Report on the description of system of Zoho related to Application Development, Production Support and the related General Information Technology Controls relevant to Security, Availability, Confidentiality, Processing Integrity and Privacy Trust Service Criteria and Suitability of the Design and Operating Effectiveness of controls for the period from December 01, 2020 through November 30, 2021

This report is intended solely for the information and use of Zoho Corporation Private Limited, user entities and other specified parties 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

Deloitte
Haskins & Sells LLP

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

Tel: +91 44 66885000

Section 1. Independent Service 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

To the Management of Zoho Corporation Private Limited

Scope

We have examined the attached description of the system of Zoho Corporation Private Limited (the "Service Organization" or "Company" or "Zoho") related to Application Development, Production Support and the related General Information Technology ('IT') Controls for the services provided to customers ("User entities" or the "User Organizations"), from Zoho offshore development centers located at Chennai, Tenkasi and Renigunta in India and Austin and Pleasanton in United States of America throughout the period December 01, 2020 to November 30, 2021 (the "description") based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 01, 2020 to November 30, 2021, to provide reasonable assurance that Zoho's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Zoho, to achieve Zoho's service commitments and system requirements based on the applicable trust services criteria. The description presents Zoho's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Zoho's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Zoho is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Zoho's service commitments and system requirements were achieved. Zoho has provided the accompanying assertion titled "Assertion of Zoho Management" (the "assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Zoho is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

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

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

- Obtaining an understanding of the system and the Zoho's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the Description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Description of 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.

Emphasis of Matter

The Service Organization identified a security incident during the assessment period, which, along with corresponding actions to remediate the issue / incident, is described in sub-section 3.6 of Section 3 of this report.

A zero-day vulnerability and a critical vulnerability was identified in the ManageEngine AD Self Service Plus (on-premise product) and ManageEngine ServiceDesk Plus (on-premise product) respectively. The vulnerability was due to an authentication bypass vulnerability that could enable remote code execution in the impacted systems. This was notified by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA).

Zoho has taken remedial actions as mentioned in Section 3 to fix the vulnerabilities identified and prevent similar incidents.

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 presents Zoho's system for the Application Development, Production Support and the related General IT Controls that was designed and implemented throughout the period December 01, 2020 to November 30, 2021 in accordance with description criteria.

b. The controls stated in the description were suitably designed throughout the period December 01, 2020 to November 30, 2021 to provide reasonable assurance that Zoho's service commitments and systems requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period and the subservice organizations and user entities applied the complementary controls assumed in the design of Zoho's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period December 01, 2020 to November 30, 2021, to provide reasonable assurance that Zoho's service commitments and system requirements were achieved based on the applicable trust services criteria, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Zoho's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Zoho, user entities of the system of Zoho during some or all of the period December 01, 2020 to November 30, 2021, business partners of Zoho subject to risks arising from interactions with Zoho's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following :

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

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

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

S. Ravi Veeraraghavan
Partner
M. No. 29935

February 25, 2022

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 February 25, 2022. The extract of the letter is as under:

We have prepared the description of the system in Section 3 of Zoho Corporation Private Limited (the "Service Organization" or "Zoho") throughout the period December 01, 2020 to November 30, 2021 (the "period") related to Application Development, Production Support and the related General IT Controls for the services, provided to customers ("User entities" or the "User Organizations"), from Zoho offshore development centers located at Chennai, Tenkasi and Renigunta in India and Austin and Pleasanton in United States of America throughout the period December 01, 2020 to November 30, 2021 (the "description") based on criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Zoho's system, particularly information about system controls that Zoho has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Zoho, to achieve Zoho's service commitments and system requirements based on the applicable trust services criteria. The description presents Zoho's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Zoho's controls.

Description Criteria

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

a. The description presents Zoho’s system that was designed and implemented throughout the period December 01, 2020 to November 30, 2021 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period December 01, 2020 to November 30, 2021, to provide reasonable assurance that Zoho’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and if user entities applied the complementary controls assumed in the design of Zoho’s controls throughout that period.

c. The controls stated in the description operated effectively throughout the period December 01, 2020 to November 30, 2021 to provide reasonable assurance that Zoho’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of Zoho’s controls operated effectively throughout that period.

For Zoho Corporation Private Limited

Sd/-

Name: N Jai Anand
Title: Chief Financial Officer
Date: February 25, 2022

SECTION - 3
System Description provided by Service Organization

Section 3. System Description provided by Service Organization

3.1 Zoho Business Overview

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

Zoho's primary facilities are based 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)
- Europe – Amsterdam, Dublin (www.zoho.eu)
- India – Mumbai, Chennai (www.zoho.in)
- Australia – Sydney, Melbourne (www.zoho.com.au)

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

- Zoho - offers a comprehensive suite of online business, productivity & collaboration applications to assist user entities manage their business processes and information.
- ManageEngine - offers enterprise IT management software for service management, operations management, Active Directory and security needs.
- 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 transform business' disparate activities into a more connected and agile organization. Zoho includes more than 40 enterprise-level online applications including Mail, CRM, Writer, Workdrive, Cliq, Books to grow sales, market business, accounting, communicate with teammates and customers, and much more. This plan includes web, mobile, and installed versions of Zoho's applications, as well as browser extensions and other useful extras. Zoho includes a powerful 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 a proactive 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 is vital to analyze bandwidth usage patterns and track bandwidth utilization of non-business-critical applications. Bandwidth monitoring software provides the flexibility of choosing what you want to see, which will help you stay on top of your network bandwidth needs.
- **Server and Application Management:** Comprehensive application management software that gives deep performance insight into complex, dynamic environments. It lets you reduce troubleshooting time and improve performance of your business-critical 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. It's a modern take on desktop management that can be scaled as per organizational needs.
- **Mobile Device Management:** A comprehensive 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 Services

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. Zoho has developed the following products across divisions:

The below products are internally classified as Large, Medium and Small based on the scale of usage and complexity of the product. Zoho has developed the following products across divisions:

(i) Division - Zoho Cloud Services

Division	Small	Medium	Large
Sales and Marketing apps	• Zoho Sales Inbox • Zoho Bookings	• Zoho Forms • Zoho Bigin	• Zoho CRM • Zoho SalesIQ • Zoho Campaigns • Zoho CRM Plus
Marketing	• Zoho Backstage • Zoho Commerce • Zoho Marketplace • Zoho Spotlight • Zoho Marketing Automation • Zoho Domains	• Zoho Social • Zoho Forms • Zoho Survey • Zoho Sites • Zoho Pagesense • Zoho Meeting	• Zoho Campaigns • Zoho Marketing Plus
Help Desk	• Zoho Assist • Zoho Lens	• Zia Skills Platform	• Zoho Desk
Finance	• Zoho Payroll • Zoho GSP(GST)	• Zoho Invoice • Zoho Expense • Zoho Inventory	• Zoho Books

Division	Small	Medium	Large
		• Zoho Subscriptions • Zoho Checkout	
People and Culture	• Zoho Workerly • Trainer Central • Zoho Shifts	• Zoho Recruit • Zoho BackTowork	• Zoho People • Zoho Connect
IT	• Zoho Flow • Zoho Assist • Zoho BugTracker • Zoho Contracts • Zoho Lens • Zoho SmartURL	• Zoho Vault • Zoho Catalyst	• Zoho Creator • Zoho Site24x7
Custom Solution	• Zoho Flow • Zoho Office Integrator • Zoho Sigma • Zoho Gadgets	• Zoho TransMail	• Zoho Creator
BI & Analytics	-	• Zoho Dataprep	• Zoho Analytics
Email and Office	• Zoho Calendar • Zoho Task • Zoho Notebook • Zoho Bookings • Zoho TeamInbox • Zoho Learn	• Zoho Show • Zoho TransMail	• Zoho Mail • Zoho Writer • Zoho Sheet • Zoho Graphikos
Project Management	• Zoho Sprints	-	• Zoho Projects
Collaboration	• Zoho Sign	• Zoho Meeting • Trainer Central • Zoho Voice	• Zoho WorkDrive • Zoho Cliq • Zoho Connect
Others	• Zoho Maps	vTouch	• ZohoOne Engineering

(ii) Division - ManageEngine [Cloud Services & On-premises products]

Division	Small	Medium	Large
Enterprise and IT service management		-	• Zoho ServiceDesk Plus • Service Desk Plus On-Premises
Customer service management		• Zoho SupportCenter Plus	-
IT asset management		• Zoho AssetExplorer	-
Active Directory management		• ADManager Plus • ADSelfService Plus	-

Division	Small	Medium	Large
		● Exchange Reporter Plus ● RecoveryManager Plus	
Identity governance and administration	● Identity Manager Plus	● O365 Manager Plus	● AD360
Privileged access management	● Access Manager Plus	● Key Manager Plus ● Password Manager Pro ● PAM360	-
Security information event management and user entity behavior analytics	● SharePoint Manager Plus ● M365 Security Plus ● DataSecurity Plus ● FileAnalysis	● EventLog Analyzer ● Firewall Analyzer ● ADAudit Plus ● Cloud Security Plus	● Log360 – Cloud and On-Premise
Endpoint management	-	● OS Deployer ● Remote Access Plus – Cloud and On-Premise ● Patch Manager Plus – Cloud and On-Premise ● Patch Connect Plus	● Desktop Central ● Mobile Device Manager Plus ● Desktop Central Cloud
Endpoint security	● Browser Security Plus ● Application Control Plus ● Vulnerability Manager Plus ● Device Control Plus	-	-
Network performance monitoring	-	● NetFlow Analyzer ● Network Configuration Manager ● OpUtils	● OpManager Plus ● OpManager
Application performance monitoring	-	-	● Applications Manager ● Site24x7 ● Site24x7 APM Insight
IT incident management	● AlarmsOne	● Site24x7 StatusIQ	-
IT analytics	-	● Analytics Plus ● Site24x7 CloudSpend	-
Others	-	● ManageEngine Solutions	-

(iii) Site24x7

Small	Medium	Large
-	● Site24x7 StatusIQ ● Site24x7 CloudSpend	● Site24x7 ● Site24x7 APM Insight

(iv) Qntrl

Small	Medium	Large
-	● Qntrl	-

(v) TrainerCentral

Small	Medium	Large
-	● TrainerCentral	-

(vi) Zakya

Small	Medium	Large
● Zakya	-	-

(vii) MedicalMine

Small	Medium	Large
-	● CharmHealth	-

3.2 The Principal Service Commitments and System Requirements

Zoho makes service commitments to its User Entities and has established system requirements as part of its service delivery. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria.

Zoho is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Zoho's service commitments and system requirements are achieved.

Service commitments to User Entities are documented and communicated in Master Service agreement and Terms of Service or any other agreements as agreed by Zoho and User Entities.

Principal Commitments and Requirements	Related Controls
Zoho ensures the availability of their product services, Zoho's policy for scheduling of downtime for maintenance and the remedies available to User Entities/Subscribers in the event of Zoho's failure to meet the service availability commitment as per the agreed timelines in the Master Service Agreement.	CA-49: Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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. CA-63: Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications. CA-70: The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability,

Principal Commitments and Requirements	Related Controls
	storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers. CA-71: The Zorro team uses an in-house tool called ‘Site24x7’ to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location based on which the action is taken accordingly. CA-72: Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP. CA-90: 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.
Zoho undertakes to acknowledge and resolve Service Defects reported by the user entities as per the agreed timelines.	CA-61: The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis. CA-62: Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers. CA-63: Based on the request from customers, Zoho enters into a Master Service Agreements (‘MSA’) with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.
Zoho ensures to maintain security, confidentiality, integrity and privacy of Client’s/User Entities’ data as committed in the Privacy Policy.	CA-07: On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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. CA-09: A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses. CA-10: Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and

Principal Commitments and Requirements	Related Controls
	responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis. CA-12: 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. CA-13: Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis. CA-18: On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis. CA-27: On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any. CA-63: Based on the request from customers, Zoho enters into a Master Service Agreements (‘MSA’) with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications. CA-68: 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. CA-81: Client data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho facility.
Zoho ensures to obtain consent from the data subjects, process only those data as required, respond to the requests from the data subject and follow the disclosure requirements specified in the privacy policy.	CA-13: Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed on an annual basis. CA-98: The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity’s policies for conformity to the requirement.

Principal Commitments and Requirements	Related Controls
	CA-106: On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity's privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations. CA-109: The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance. CA-111: Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.
Zoho shall provide training to its associates covering the aspects such as the security, confidentiality and availability and Zoho shall perform appropriate background checks for its associates in accordance with its Background Verification policies.	CA-03: Upon a new associate joining, an induction training is conducted by the Training Team and HR Team to make the associates aware of the information security practices and various policies of Zoho. The attendance for the training is captured in Zoho people. CA05: 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. CA-06: Upon new associates joining, 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. CA-08: 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 is responsible for developing, implementing and maintaining a comprehensive written Information Security Policy and Risk Management Program that includes administrative, technical and physical safeguards that are appropriate to the security, confidentiality, availability, processing integrity and	CA-10: Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis. CA-11: 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

Principal Commitments and Requirements	Related Controls
privacy of the information handled by Zoho.	related to information security are made available to associates through the intranet portal. CA-12: 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. CA-13: Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis. CA-18: On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis. CA-19: Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting. CA-27: On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity. CA-36: 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. CA-38: Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days. CA-39: 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

Principal Commitments and Requirements	Related Controls
	CA-79: Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.
Zoho will execute the Business Continuity and Disaster recovery plan as specified in the relevant individual agreement to periodically test, review and demonstrate the business continuity and disaster recovery plan to, and ensure it is fully operational.	CA-26: Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis. CA-49: Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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.
Zoho shall establish a mechanism to prevent unauthorized access to its systems by the means of logical and physical security and also employ appropriate encryption mechanism for the data stored in their servers.	CA-23: Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis. CA-29: 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 all the logical access of the associate. CA-54: 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. CA-57: 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 is taken. CA-34: 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. CA-35: Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals. CA-37: 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

Principal Commitments and Requirements	Related Controls
	storage room is restricted to authorized personnel using proximity card-based access control system and PIN based authentication. CA-38: Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days. CA-115: Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails. CA-116: Zoho Cloud products use TLS encryption for data that are transferred through public networks.

3.3 Boundaries of the System

The boundaries of the system for the purposes of this report includes the following details:

- Services – The services provided by Zoho to its User entities for the Application Development, Production Support and the related General IT Controls relevant to applicable Trust Service criteria. The services pertaining to Zoho Cloud services, ManageEngine, TrainerCentral, Zakya, Qntrl, Site24x7 and MedicalMine is covered as part of the scope.

- Infrastructure – Zoho Corporate Office and offshore development centers located in
  a. Chennai, India
  b. Tenkasi, India
  c. Renigunta, India
  d. Austin, USA
  e. Pleasanton, USA

  - Corporate website refers to Zoho's corporate websites - www.zoho.com, www.zoho.au, www.zoho.eu and www.zoho.in which is publicly accessible via the internet.
  - International Datacenter (IDC) infrastructure refers to servers, databases and network devices available within the IDCs.
  - Production environment refers to servers within the IDC infrastructure used to support the production instances of products.
  - IDC Access Network or IAN Network refers to the IDC Access Network that is used for highly restricted logical access from Zoho Development center to the IDC Infrastructure.
  - Network Operations Centre or NOC refers to a physically segregated and access controlled work area located in Zoho Development Centers occupied by members from the Zorro, NOC Team Members and Sysadmin teams.
  - IAN work area refers to the physically segregated areas within the Zoho Development Centers containing desktops. Logical access to the servers is provided through an isolated & dedicated network and is highly secured and monitored. The accessing machines are securely hardened so that no data can be copied or transferred from the data center. Physical Access to the data centers is protected with Biometric and PIN. No visitors are allowed inside the dedicated cages

of Zoho in the data centers. Only a very restricted number of associates have the access to the servers to carry out emergencies.

- Zoho server rooms refer to servers, databases and network devices available within Zoho's Development Centers used to support non-production environments of products.
- Local Zoho Environment refers to servers and databases supporting development and test instances of products hosted within Zoho server rooms.

- Software - Zoho has a standard software list for internal use which is approved by the Information Technology Service (ITS) Team. All the Zoho workstations are installed with the standard software; additional software other than those from the approved list are installed based on the approval from the respective managers.

- People – Zoho has dedicated teams and personnel involved in the operation and use of the system. These are Executive Management, Operations, Technical and Leadership staff, and Support personnel. The Executive Management at Zoho is responsible for establishment of organization policies, overseeing organization activities and achieving business objectives. Operations Management and staff are responsible for client implementation and day-to-day client support. Additionally, they monitor and manage inbound and outbound data flows and related processes. The support personnel includes the Admin Team, Legal team, Zorro Team, Network Operations Centre (NOC) team, physical security, system administration, and HR Team.

- Policies and Procedures – Zoho's Management has developed and communicated policies and procedures across functions including Application Development and Maintenance, Information Security, Data Privacy, Human Resource, Logical Security, Network Security, Infrastructure Change Management, Physical and Environmental Security, Backup and Restoration, and Incident Management to its associates through the intranet. These policies and procedures are reviewed and approved by Zoho's Management on an annual basis and primarily used internally to guide Zoho associates to support the day-to-day operations. The roles and responsibilities of the team members are defined in the policy and procedure document.

3.4 Control Environment Elements

3.4.1 Communication and Enforcement of 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. Zoho’s continuous education programs enhance the relevance and effectiveness of learning. 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.

Code of Conduct and Ethics

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

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

3.4.2 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, 2022.

3.4.3 Management’s Philosophy and Operating Style

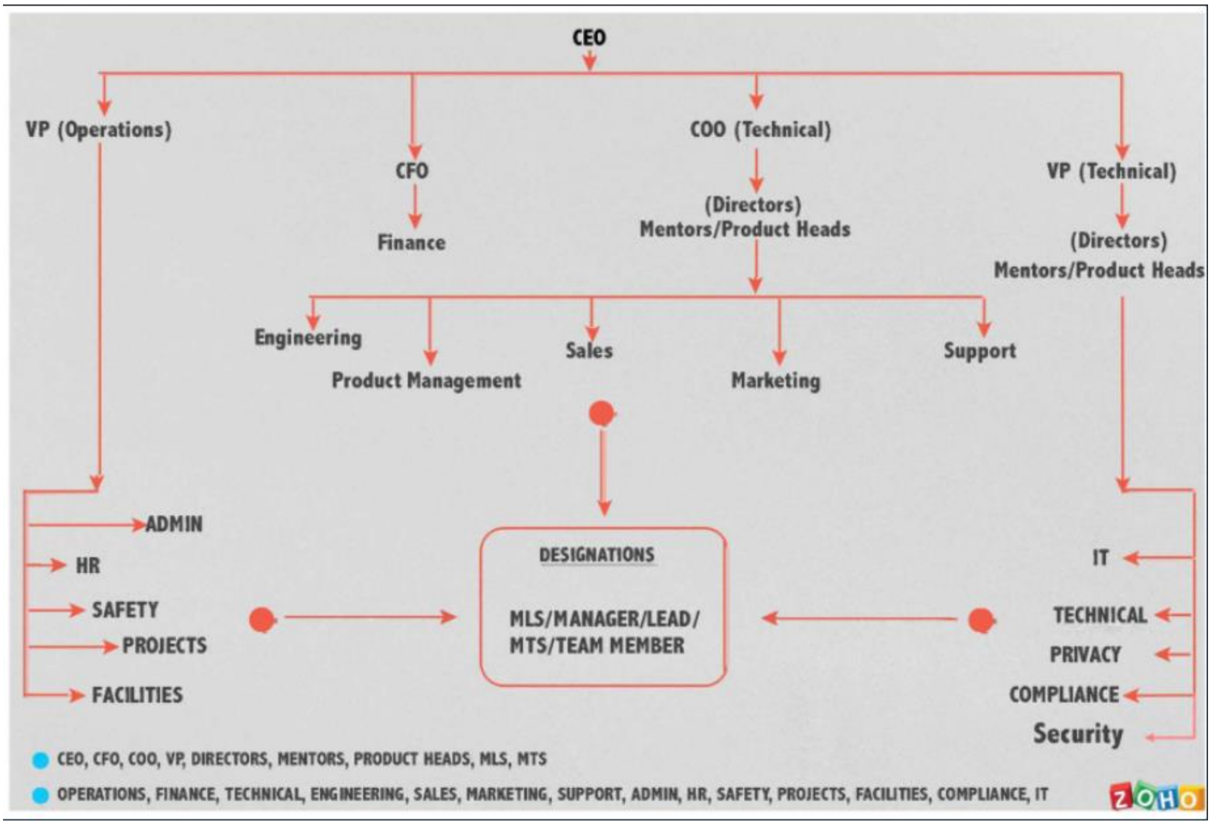
Zoho Management’s philosophy and operating style encompass a broad range of characteristics including Management’s approach to taking and monitoring business risks, and Management’s attitudes toward information processing, accounting functions, and personnel. Specific control activities that Zoho has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

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

3.4.4 Organization Structure

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

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



3.4.5 Board of Directors

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.

3.4.6 Assignment of Authority and Responsibility

Following are the roles and responsibilities of personnel within Zoho:

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

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

Role	Responsibility and Authority
	• Ensure integrity, quality, safety, optimal cost, schedule, performance, reliability, accuracy and maintainability of products and services in order to satisfy customer requirements • Ensure that the personnel comply with applicable standards, regulations, specifications, and documented procedures • Provide the corrective actions
Product Data Protection Officer (P-DPO)	• Heads & oversees the privacy implementation in their respective products/business units. • Maintains the Data inventory (Information Asset Register) for their respective product/business unit. • Reviews the documents pertaining to the common privacy practices, IAR in their respective teams. • Provides oversight and guidance to the PIMs in privacy related tasks, implementations in their respective products/business unit. • Co-ordinates with the Privacy Steering Committee on various activities related to privacy and compliance within their product/business unit. • Heads, authorizes and reviews the RCA of privacy incidents • Serves as the first point of contact in case of any privacy incidents or escalations • Must be or report to the Head of the Business Function/Product
Member-Compliance Audit	• Establish and execute compliance monitoring programs around information technology. Participate in internal security assessments, internal audits, customer audits, compliance certifications (external audit), and customer security questionnaire responses. • Assists in creating policies and procedures to help reduce risk , meet regulatory requirements and best business practices. • Performs Information security assessments and prepares findings and remediation reports. • Assists in updating and maintain policies, standards and procedures documents. • Evaluate security controls to ensure effectiveness and compliance, including managing the security control remediation efforts. • Coordinate with various teams in the organization regarding standards, regulations. • Coordinate with teams for Information Security awareness training. • Mapping and analyzing the adherence level with the applicable standards. • Performs other job-related duties as assigned.
Data Protection Officer (DPO)	• To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the data privacy regulations.

Role	Responsibility and Authority
	• To monitor compliance with this the applicable data protection laws, and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; • To provide advice where requested as regards the data protection impact assessment and monitor its performance • To cooperate with the supervisory/data protection regulatory authorities • To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation of certain types of processing of personally identifiable information (as maybe required by the laws) and to consult, where appropriate, with regard to any other matter related to it.
Privacy Implementation Member (PIM)	• Implements or assist in implementing the privacy controls and features • Provides reports of the consistency to the P-DPO on request. • Consults with the Privacy Team and/or Legal team on new activities or processes. • Conducts the Risk Assessment (DPIA) for their team's activities processes and products/features. • Co-operate during Privacy incidents by finding the root cause and works to fix it on priority. • Conduct privacy awareness trainings and exercises during team member on-boarding and periodically. • Ought to report directly to the P-DPO • Provide suggestions to the P-DPO on how to address privacy risks in a better way, proactively.
Lead - Privacy Operations & Management	• Establish and maintain the Privacy Program, which addresses the personal data management of both customers and employees • Aids the ISH in defining the Information Privacy Policy of the organization • Serve as the internal point of contact for the organisation's information privacy initiatives • Co-ordinate with the Services and Operations teams to operationalize the program across all the applicable business units • Facilitate Privacy Risk & Impact assessments as per the scope defined in the DPIA policy • Initiate, facilitate and promote activities to foster information privacy awareness within the organization • Perform ongoing monitoring of the compliance with the organisation's policies related to information privacy • Work with the Legal team on negotiation of contracts with customers, vendors and other third parties.

Role	Responsibility and Authority
	• Review the organisation's policies pertaining to the Information Privacy Program • Work with the Incident Management team during incident analysis and investigations that have effect on the privacy of the applicable parties • Provide consultation to business personnel on methods to mitigate the risks identified • Conduct trainings to internal auditors on PIMS • Work with the Compliance team during internal and external audits to assess and review the implementation of the privacy controls and the maturity. • Review third party's privacy posture during vendor on-boarding especially when the third party processes personal data on behalf of the organization or it's products • Convert stakeholders' requirements into action plans for the organization, based on the applicable laws and lead the compliance program that follows.
Data Privacy Analyst	• Work as part of the Privacy team and assist in the administration, management, of the Zoho's Privacy Program and related projects, such as the EU GDPR compliance program • Assist the DPO & the Privacy Lead in the handling and coordination of daily firm-wide data privacy exceptions, including but not limited to, response, investigation, logging, reporting and coordination; • Assist in the management and coordination of other on-going compliance, and projects. • Continuously assess Zoho's operations to develop policies, processes, and procedures related to Zoho's privacy practices and programs. • Remain well-informed and support the team members with questions related to Information Privacy Concepts. • Work closely with internal stakeholders, such as legal teams and other corporate functions to analyze and respond to privacy related issues, in co-operation with the Privacy Lead. • Work with internal stakeholders to implement and to maintain privacy best practices, such as conducting Data Protection Impact Assessments. • Assist Information Security team in responding to customer related surveys and questionnaires regarding the Zoho's compliance initiatives. • Evaluate vendor's privacy stature during vendor on-boarding process, especially if the vendor processes personal data on behalf of the organization or its products.
Director of IT (DOIT)	• Reviews and approves procedures pertaining to handling some of the privacy and security compliance related processes.

Role	Responsibility and Authority
	• Advises on ways to achieve intended outcomes with respect to addressing risks in processing data. • Enables / spearheads some operations to improve the overall working of the GRC program and serves as an important person in the privacy steering committee.
Central Security Team	• Accountable for the overall Information Security and Cloud security Program • Initiate, facilitate and promote activities related to security awareness in the organization • Conduct Security Risk & Impact assessments for any new product, technology and architecture component. • Assist and guide the product security engineers on secure coding standards and security assessments guidelines within the product scope • Responsible for identifying and building security tools and frameworks to assist the development and operations teams • Evaluate evolving new technologies in the context of information security and provide guidance on secure adoption to the product teams • Closely work with the Incident management team during incident analysis and investigations.

3.4.7 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.

3.5 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.

3.6 Information and 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.

3.6.1 A brief description of the cyber security incident of Zoho ManageEngine products:

Zoho had been made aware of zero-day vulnerability in ManageEngine AD Self Service Plus (on-premise) and critical vulnerability in ManageEngine ServiceDesk Plus (on-premise) during the assessment period, which was rated as critical by the Common Vulnerability Scoring System (CVSS).

ManageEngine AD Self Service Plus (on-premise):

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) on September 3, 2021 notified the threat of active exploitation of the newly found vulnerability.

The root cause of the vulnerability was due to an authentication bypass vulnerability affecting representational state transfer (REST) application programming interface (API) URLs that could enable remote code execution.

An incident was raised immediately by Zoho with the Product and the Security teams and the vulnerability was investigated and rectified by the respective teams. A patch update was released on September 07, 2021 to fix this vulnerability. The same was communicated to all the customer and a public announcement was made regarding the same in their website.

The product is an on-premise product and the data resides in the client environment. Zoho actively persuaded the clients to update the patches to prevent an attack.

ManageEngine ServiceDesk Plus (on-premise):

Based on the vulnerability identified in ManageEngine AD Self Service Plus, Zoho performed internal review and had identified a similar vulnerability due to unauthenticated remote code execution (RCE) in the product ManageEngine ServiceDesk Plus (on-premise) in September 2021. A patch update was provided on September 11th, 2021 for all its customers to fix the issue in the product. However, since the active exploitations were detected in November 2021, the same was highlighted as a critical vulnerability by the Federal Bureau of Investigation (FBI), United States Coast Guard Cyber Command (CGCYBER), and the Cybersecurity and Infrastructure Security Agency (CISA) on December 02, 2021.

The same was communicated to all the customer and a public announcement was made regarding the same in their website, urging the customers to update the versions. The product is an on-premise product and the data resides in the client environment. Zoho actively persuaded the clients to update the patches to prevent the attack.

Measures taken by Zoho post the Zero-Day Vulnerabilities:

Zoho had conducted investigation once it had been made aware of zero-day vulnerabilities on its ManageEngine on-premise products.

The following measures were taken immediately as part of incident response:

a. Release of patch update to rectify the vulnerability
b. Notification to external and internal stakeholders
c. Complete review of authentication mechanism
d. Internal security testing and source code review

Additionally, long term service improvement plans were identified to strengthen the WAF layer and to undergo third-party penetration testing.

Impact due to the Zero-day Vulnerability:

The zero-day vulnerability in Zoho ManageEngine AD Self Service Plus (on-premise product) had an impact on the below control activity, as it pertains to the penetration testing. The existing process of the penetration testing was unable to detect since it was zero-day vulnerability and the testing was enhanced post the identification of this vulnerability.

CA-57: 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 is taken.

The above affected products are on-premise and the data resides with the user entities and hence the impact analysis on the data exploitation / breach is the responsibility of the respective user entities who had been using the impacted product / version.

3.7 Monitoring

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

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

Process and controls

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 portals.

Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.

Zoho has a defined procedure for the Internal audits and is closely monitored by the Director of Compliance (DOC). The Compliance team conducts an internal assessment of services delivered to the user entities on a half-yearly basis and the internal audit program plan for the same is approved by the Information Security Compliance Manager and the Top Management (Vice president).

On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.

A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses. The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.

Risk Management and Compliance

On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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. Zoho also monitors the service levels and commitments of the vendors on a periodical basis.

The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.

On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.

Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

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). 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.

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.

Whistle Blower mechanism is defined as part of Code of Ethics document and it provides guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc., through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation. In case of any non-compliance with the policies, disciplinary action is taken inline with policy.

Further, there are defined procedures for periodic performance appraisals including the review and assessment of professional development activities.

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.

Upon new associates joining, 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.

Further, 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. 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.

Physical 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 colour 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.

A 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.

Logical Security

Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities. It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.

Access 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.

For newly joined associates, 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.

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 all the logical access of the associate.

For tools such as Wiki, MI, SDP, ZAC and Password Manager Pro (managed by Zorro team) a request for new access and request for access revocation is sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team. The access to the tools are granted / revoked by the Zorro Manager.

Logical access to the tools (managed by NOC team) used for performing NOC’s daily operations are granted by Senior NOC member based on approval by NOC manager and revoked on a timely manner based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member.

Zoho ensures that the client data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho facility.

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

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. Further, the access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM 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 products 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.

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.

Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.

Network Security

Zoho has a network diagram detailing the network devices such as firewalls and switches and is maintained by the NOC Manager. Further, access to the network devices are restricted to designated members to prevent unauthorized access.

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.

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.

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.

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 is taken.

Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.

Network Monitoring:

The network monitoring is performed by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto generated and sent to the NOC SDP Portal for performing necessary actions.

The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.

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

Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.

Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis. Further, the monitoring of AV console is performed on a real time basis by the IT Team.

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

Encryption:

Zoho follows the encryption methods as communication to the customers. Zoho employs the following methods of encryption.

- Encryption of data in transit
- Encryption of data at rest
- The hard-disks used by Zoho are encrypted (Full Disk Encryption 'FDE')
- Application-level encryption.

Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.

Zoho Cloud products use TLS encryption for data that are transferred through public networks.

Change Management

Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis. Support documents including the system flow diagrams and other design documents for the products are maintained and 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.

Product descriptions help documents and terms of usage / service are defined and are made available for to the customers via corporate website.

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 respective Product Teams on an annual basis.

Based on the change request raised by the respective product team, the changes are carried out in the Development environment and tested in the QA environment, which is separate from the Production environment.

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 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.

On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.

Infrastructure Changes:

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.

Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. 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 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.

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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.

Incident Handling

Zoho has defined an Incident Management System Policy, which is prepared by Incident Management team and approved by the Information Security Manager. The policy is reviewed by leadership staff 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 preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.

The alerts are triggered by the monitoring tools and once an alert is triggered 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, where necessary. The relevant product team performs RCA and the action points are identified for implementation. The incident ticket is updated.

A 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.

Customer Service Handling

The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.

Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.

Data Backup and Restoration

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 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 in relation to the cloud-based services within the agreed SLA.

Availability

The Zorro team has defined a Zoho Data Center Operations document defining the procedures relating to day-to-day operations of Zorro including procedures for degaussing the disks. The document is prepared by the Zorro team and approved by the Director of Network and IT Infrastructure. The documented is reviewed and approved by the Director on an annual basis.

The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.

Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.

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 Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.

Asset Management

Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.

Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.

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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.

Data Privacy

Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis. Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.

The Zoho compliance team conducts internal audit of Zoho's information security and privacy controls on a half-yearly basis. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

The entity provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.

On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy, security and confidentiality commitments and system requirements that are consistent with those of the entity commitments for privacy and security.

Collection and Use:

The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity’s privacy practices). The notice is:
1) readily accessible and made available to the data subject.
2) Provided in a timely manner to the data subjects
3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity.
4) informs data subjects of a change to a previously communicated privacy notice
5) Documents the changes to privacy practices that were communicated to data subjects.

Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by
1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information.
2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution.
3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.

On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects. The Director of Compliance (DOC) reviews its policies to ensure the definition of "sensitive" personal information is properly delineated and communicated to personnel.

Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.

The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.

The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.

Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.

The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information.

Choice and Consent

Zoho's Privacy Policy includes the below policy around Choice and Consent:
1) Consent is obtained before the personal information is processed or handled.
2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences.
3) When authorization is required (explicit consent), the authorization is obtained in writing.
4) Implicit consent has clear actions on how a data subject opts out.
5) Action by a data subject to constitute valid consent.
6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.

The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.

The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity's policies for conformity to the requirement.

Privacy practices – Retention and Disclosure:

The Director of Compliance and the General Counsel reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:
1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information
2) Policies regarding retention, sharing, disclosure, and disposal of their personal information

3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information
4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.

On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in
1) Conformity with the purposes identified in the entity's privacy notice.
2) Conformity with the consent received from the data subject.
3) Compliance with applicable laws and regulations."

The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:
1) The system processes in place to delete information in accordance with specific retention requirements.
2) Deletion of backup information in accordance with a defined schedule.
3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention.
4) Annually reviews information marked for retention.
An annual review of the organization's data inventory is performed to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.

When consent is required, business unit personnel implement a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).

The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.

Further, on an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.

Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.

Breach

A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.

Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices.

A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by the Security and Compliance team upon which incidents flagged as privacy issues are resolved.

Business Continuity

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

Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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.

Environmental Safeguards

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.

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

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.

3.8 Trust Service Criteria and Description of Related Controls

3.8.1 Common criteria related to Control Environment

CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control Activity Number	Control Activities
CA-01	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.
CA-03	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.
CA-05	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.
CA-06	Upon new associates joining, 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.
CA-08	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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also

Control Activity Number	Control Activities
	defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-20	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.
CA-59	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.
CA-65	Whistle Blower mechanism is defined as part of Code of Ethics document and it provides guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation. In case of any non-compliance with the policies, disciplinary action is taken in line with policy.
CA-112	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Activity Number	Control Activities
CA-01	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.
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

Control Activity Number	Control Activities
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-112	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Activity Number	Control Activities
CA-01	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.
CA-02	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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-13	Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

Control Activity Number	Control Activities
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-112	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Activity Number	Control Activities
CA-02	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.
CA-03	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.
CA-05	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.
CA-06	Upon new associates joining, 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.
CA-08	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.
CA-14	Support documents including the system flow diagrams and other design documents for the products are maintained and are made available to the respective team members of Zoho.
CA-20	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.
CA-30	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).
CA-59	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.
CA-100	The entity provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Activity Number	Control Activities
CA-01	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.
CA-02	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.
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-20	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.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-59	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.
CA-112	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.
CA-113	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.

3.8.2 Common criteria related to Communication and Information:

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Activity Number	Control Activities
CA-01	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.
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-08	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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control Activity Number	Control Activities
CA-02	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.
CA-03	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.
CA-06	Upon new associates joining, 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.
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-08	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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-12	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.
CA-14	Support documents including the system flow diagrams and other design documents for the products are maintained and are made available to the respective team members of Zoho.
CA-15	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-30	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).

Control Activity Number	Control Activities
CA-42	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.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-65	Whistle Blower mechanism is defined as part of Code of Ethics document and it provides guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation. In case of any non-compliance with the policies, disciplinary action is taken inline with policy.
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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.
CA-91	A 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.
CA-100	The entity provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.

CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control Activity Number	Control Activities
CA-09	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by

Control Activity Number	Control Activities
	Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-12	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.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.
CA-62	Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA-63	Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-65	Whistle Blower mechanism is defined as part of Code of Ethics document and it provides guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation. In case of any non-compliance with the policies, disciplinary action is taken inline with policy.
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are

Control Activity Number	Control Activities
	taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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.
CA-91	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.
CA-92	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is: 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.

3.8.3 Common criteria related to Risk Assessment:

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control Activity Number	Control Activities
CA-04	Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-12	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.

Control Activity Number	Control Activities
CA-15	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-65	Whistle Blower mechanism is defined as part of Code of Ethics document and it provides guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation. In case of any non-compliance with the policies, disciplinary action is taken inline with policy.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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.
CA-91	A 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.

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.

Control Activity Number	Control Activities
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-12	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.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-57	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 is taken.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control Activity Number	Control Activities
CA-09	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-12	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.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.
CA-57	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 is taken.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-88	Zoho has defined an Incident Management Policy, which is prepared by Incident Management team and approved by the Information Security Manager. The policy is

Control Activity Number	Control Activities
	reviewed by leadership staff on an annual basis and version history is maintained within the document.

CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Activity Number	Control Activities
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-12	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.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.
CA-51	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.
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.
CA-53	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.
CA-54	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.
CA-55	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.
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.

Control Activity Number	Control Activities
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.
CA-82	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 respective Product Teams on an annual basis.
CA-84	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.
CA-85	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.
CA-86	On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.

3.8.4 Common criteria related to Monitoring Activities:

CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control Activity Number	Control Activities
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-09	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-13	Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.

Control Activity Number	Control Activities
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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.
CA-91	A 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.

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Activity Number	Control Activities
CA-04	Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

Control Activity Number	Control Activities
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-57	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 is taken.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-91	A 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.
CA-112	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

3.8.5 Common criteria relating to Control Activities

CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is

Control Activity Number	Control Activities
	prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-13	Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-49	Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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.
CA-57	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 is taken.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.

Control Activity Number	Control Activities
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.
CA-80	Changes are carried out in the Development environment and tested in the QA environment, which is separate from the Production environment.
CA-82	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 respective Product Teams on an annual basis.
CA-84	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.

CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-14	Support documents including the system flow diagrams and other design documents for the products are maintained and are made available to the respective team members of Zoho.
CA-15	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.
CA-16	Product descriptions, help documents and terms of usage / service are defined and are made available for to the customers via corporate website.
CA-21	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.
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-28	For newly joined associates, 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.

Control Activity Number	Control Activities
CA-29	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 all the logical access of the associate.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-56	Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-68	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.
CA-69	Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-84	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.
CA-85	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.
CA-86	On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.

CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA-13	Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The

Control Activity Number	Control Activities
	Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-25	Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-30	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).
CA-34	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.
CA-42	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.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.
CA-66	The Zorro team has defined a Zoho Data Center Operations document defining the procedures relating to day-to-day operations of Zorro including procedures for degaussing the disks. The document is prepared by the Zorro team and approved by the Director of Network and IT Infrastructure. The documented is reviewed and approved by the Director on an annual basis.
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.
CA-82	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 respective Product Teams on an annual basis.
CA-88	Zoho has defined an Incident Management Policy, which is prepared by Incident Management team and approved by the Information Security Manager. The policy

Control Activity Number	Control Activities
	is reviewed by leadership staff on an annual basis and version history is maintained within the document.
CA-92	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is: 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.

3.8.6 Common criteria related to Logical and Physical Access Controls

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-21	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.
CA-28	For newly joined associates, 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.
CA-29	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 all the logical access of the associate.
CA-43	Logical access to the tools (managed by NOC team) used for performing NOC's daily operations are granted by Senior NOC member based on approval by NOC manager and revoked on a timely manner based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member.
CA-44	For tools such as Wiki, MI, SDP, ZAC and Password Manager Pro (managed by Zorro team) a request for new access and request for access revocation is sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team. The access to the tools are granted / revoked by the Zorro Manager.
CA-45	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 designated members to prevent unauthorized access.

Control Activity Number	Control Activities
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.
CA-54	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.
CA-56	Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-67	Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.
CA-68	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.
CA-69	Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner.
CA-76	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 in relation to the cloud-based services within the agreed SLA.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.
CA-87	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 half-yearly basis. Corrective actions, if any, are taken on a timely manner.
CA-115	Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.
CA-116	Zoho Cloud products use TLS encryption for data that are transferred through public networks.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is

Control Activity Number	Control Activities
	prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-12	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.
CA-21	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.
CA-28	For newly joined associates, 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.
CA-29	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 all the logical access of the associate.
CA-43	Logical access to the tools (managed by NOC team) used for performing NOC's daily operations are granted by Senior NOC member based on approval by NOC manager and revoked on a timely manner based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member.
CA-44	For tools such as Wiki, MI, SDP, ZAC and Password Manager Pro (managed by Zorro team) a request for new access and request for access revocation is sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team. The access to the tools are granted / revoked by the Zorro Manager.
CA-56	Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-67	Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.
CA-68	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.
CA-69	Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner.
CA-87	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 half-yearly basis. Corrective actions, if any, are taken on a timely manner.
CA-115	Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.
CA-116	Zoho Cloud products use TLS encryption for data that are transferred through public networks.

CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-12	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.
CA-21	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.
CA-43	Logical access to the tools (managed by NOC team) used for performing NOC's daily operations are granted by Senior NOC member based on approval by NOC manager and revoked on a timely manner based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member.
CA-44	For tools such as Wiki, MI, SDP, ZAC and Password Manager Pro (managed by Zorro team) a request for new access and request for access revocation is sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team. The access to the tools are granted / revoked by the Zorro Manager.
CA-56	Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.
CA-67	Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.
CA-68	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.
CA-69	Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner.
CA-87	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 half-yearly basis. Corrective actions, if any, are taken on a timely manner.

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control Activity Number	Control Activities
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-31	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.
CA-32	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.
CA-33	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.
CA-34	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.
CA-35	Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.
CA-36	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.
CA-37	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.
CA-38	Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.
CA-39	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
CA-40	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.
CA-41	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.

.

CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Control Activity Number	Control Activities
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-12	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.
CA-36	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.
CA-37	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.
CA-38	Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.
CA-87	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 half-yearly basis. Corrective actions, if any, are taken on a timely manner.

CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Activity Number	Control Activities
CA-21	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.
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-56	Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.
CA-57	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.

Control Activity Number	Control Activities
	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 is taken.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-67	Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.

CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control Activity Number	Control Activities
CA-44	For tools such as Wiki, MI, SDP, ZAC and Password Manager Pro (managed by Zorro team) a request for new access and request for access revocation is sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team. The access to the tools are granted / revoked by the Zorro Manager.
CA-45	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 designated members to prevent unauthorized access.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-67	Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.
CA-68	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.
CA-69	Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.

Control Activity Number	Control Activities
CA-75	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 corrective action is taken.
CA-76	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 in relation to the cloud-based services within the agreed SLA.
CA-77	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.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control Activity Number	Control Activities
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-24	Monitoring of AV console is performed on a real time basis by the IT Team.
CA-45	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 designated members to prevent unauthorized access.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.
CA-53	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.
CA-57	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 is taken.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.

Control Activity Number	Control Activities
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.

3.8.7 Common criteria related to System Operations

CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control Activity Number	Control Activities
CA-15	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-24	Monitoring of AV console is performed on a real time basis by the IT Team.
CA-45	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 designated members to prevent unauthorized access.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-51	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.
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.
CA-53	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.
CA-55	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.

Control Activity Number	Control Activities
CA-57	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 is taken.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.
CA-84	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.
CA-85	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.
CA-86	On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.

Control Activity Number	Control Activities
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.

Control Activity Number	Control Activities
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-49	Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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.
CA-57	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 is taken.
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called ‘Site24x7’ to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.
CA-77	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.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.

CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Activity Number	Control Activities
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.

Control Activity Number	Control Activities
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA-24	Monitoring of AV console is performed on a real time basis by the IT Team.
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-57	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 is taken.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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.

Control Activity Number	Control Activities
CA-91	A 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.

CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-57	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 is taken.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are

Control Activity Number	Control Activities
	taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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.
CA-91	A 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.

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Activity Number	Control Activities
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.
CA-90	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

Control Activity Number	Control Activities
	Connect to notify the stakeholders. The relevant product team performs RCA and the action points are identified for implementation. The incident ticket is updated.
CA-91	A 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.

3.8.8 Common criteria related to Change Management

CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Activity Number	Control Activities
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.
CA-51	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.
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.
CA-53	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.
CA-54	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.
CA-55	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.
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.
CA-80	Changes are carried out in the Development environment and tested in the QA environment, which is separate from the Production environment.
CA-81	Client data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho facility.
CA-82	Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and

Control Activity Number	Control Activities
	implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.
CA-84	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.
CA-85	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.
CA-86	On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.

3.8.9 Common criteria related to Risk Mitigation

CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control Activity Number	Control Activities
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.
CA-12	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.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.

CC9.2 The entity assesses and manages risks associated with vendors and business partners.

Control Activity Number	Control Activities
CA-09	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA-12	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.
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.

3.8.10 Additional controls for Confidentiality:

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

Control Activity Number	Control Activities
CA-03	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.
CA-08	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.
CA-09	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA-25	Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.
CA-76	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 in relation to the cloud-based services within the agreed SLA.
CA-78	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 /

Control Activity Number	Control Activities
	replacement. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.
CA-107	The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies: 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.

C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Control Activity Number	Control Activity
CA-25	Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.
CA-107	The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies: 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.

3.8.11 Additional controls for Availability:

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Control Activity Number	Control Activities
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.

Control Activity Number	Control Activities
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.
CA-47	The NOC team uses an in-house tool (DeviceExpert) to backup network device configurations on a daily (incremental backup) and weekly (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team.
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA-49	Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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.
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.
CA-57	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 is taken.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-77	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.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

Control Activity Number	Control Activities
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.
CA-34	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.
CA-38	Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.
CA-40	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.
CA-39	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
CA-41	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.
CA-47	The NOC team uses an in-house tool (DeviceExpert) to backup network device configurations on a daily (incremental backup) and weekly (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team.
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-75	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 corrective action is taken.
CA-76	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 in relation to the cloud-based services within the agreed SLA.
CA-77	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.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Control Activity Number	Control Activities
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.
CA-75	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 corrective action is taken.
CA-76	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 in relation to the cloud-based services within the agreed SLA.
CA-77	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.

3.8.12 Additional criteria for Processing Integrity:

PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

Control Activity Number	Control Activities
CA-16	Product descriptions, help documents and terms of usage / service are defined and are made available for to the customers via corporate website.
CA-25	Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.
CA-62	Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA-63	Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.

Control Activity Number	Control Activities
CA-16	Product descriptions, help documents and terms of usage / service are defined and are made available for to the customers via corporate website.
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs.

Control Activity Number	Control Activities
	Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.
CA-81	Client data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho facility.
CA-84	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.
CA-85	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.
CA-86	On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.

Control Activity Number	Control Activities
CA-14	Support documents including the system flow diagrams and other design documents for the products are maintained and are made available to the respective team members of Zoho.
CA-15	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.
CA-55	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.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.
CA-62	Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.

Control Activity Number	Control Activities
CA-80	Changes are carried out in the Development environment and tested in the QA environment, which is separate from the Production environment.
CA-82	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 respective Product Teams on an annual basis.

PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.

Control Activity Number	Control Activities
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.
CA-71	The Zorro team uses an in-house tool called 'Site24x7' to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA-90	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.

PI1.5: The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.

Control Activity Number	Control Activities
CA-75	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 corrective action is taken.
CA-76	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 in relation to the cloud-based services within the agreed SLA.
CA-77	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.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.

Control Activity Number	Control Activities
CA-115	Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.

3.8.13 Additional controls for Privacy:

Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-92	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is: 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-94	The Director of Compliance and the General Counsel reviews the privacy notice and documents his / her approval that the notice includes the following disclosures: 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information 4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.

Privacy Criteria Related to Choice and Consent

P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

Control Activity Number	Control Activities
CA-96	Zoho's Privacy Policy includes the below policy around Choice and Consent: 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.
CA-97	The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA-98	The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity's policies for conformity to the requirement.
CA-99	On an annual basis, the Director of Compliance (DOC) reviews its policies to ensure the definition of "sensitive" personal information is properly delineated and communicated to personnel.
CA-100	The entity provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.
CA-101	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.
CA-110	When consent is required, business unit personnel implement a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).

Privacy Criteria Related to Collection

P3.1: Personal information is collected consistent with the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-94	The Director of Compliance and the General Counsel reviews the privacy notice and documents his / her approval that the notice includes the following disclosures: 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information 4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.
CA-101	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.
CA-102	Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices.
CA-103	Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.
CA-104	Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.

P3.2: For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.

Control Activity Number	Control Activities
CA-97	The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA-105	The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information.
CA-110	When consent is required, business unit personnel implement a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).

Privacy Criteria Related to Use, Retention, and Disposal

P4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.
CA-103	Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.
CA-105	The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information.
CA-106	On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity's privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.

P4.2: The entity retains personal information consistent with the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or

Control Activity Number	Control Activities
	inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-107	The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies: 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.
CA-108	An annual review of the organization's data inventory is performed to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.

P4.3: The entity securely disposes of personal information to meet the entity's objectives related to privacy.

Control Activity Number	Control Activity
CA-22	The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.
CA-25	Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-102	Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices.

Privacy Criteria Related to Access

P5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-13	Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis.
CA-73	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA-92	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is: 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.
CA-96	Zoho's Privacy Policy includes the below policy around Choice and Consent: 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.

Control Activity Number	Control Activities
CA-109	The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.
CA-111	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.

P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-22	The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.
CA-73	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.
CA-97	The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA-106	On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity's privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.

Privacy Criteria Related to Disclosure and Notification

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.
CA-104	Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.
CA-110	When consent is required, business unit personnel implement a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).
CA-111	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.
CA-114	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by the Security and Compliance team upon which incidents flagged as privacy issues are resolved.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-111	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.
CA-113	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

Control Activity Number	Control Activity
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-114	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by the Security and Compliance team upon which incidents flagged as privacy issues are resolved.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

Control Activity Number	Control Activity
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-113	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-73	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.

Control Activity Number	Control Activities
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-113	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.
CA-114	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by the Security and Compliance team upon which incidents flagged as privacy issues are resolved.

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

Control Activity Number	Control Activity
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.
CA-114	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by the Security and Compliance team upon which incidents flagged as privacy issues are resolved.

P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-73	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.

Control Activity Number	Control Activities
CA-109	The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.
CA-111	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.
CA-113	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.

Privacy Criteria Related to Quality

P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.

Control Activity Number	Control Activities
CA-22	The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-106	On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity's privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.
CA-107	The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies: 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.

Privacy Criteria Related to Monitoring and Enforcement

P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identify deficiencies are made or taken in a timely manner.

Control Activity Number	Control Activities
CA-73	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA-102	Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices.
CA-106	On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity's privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.
CA-109	The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.
CA-110	When consent is required, business unit personnel implement a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).
CA-111	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.

3.9 Complementary User Entity Controls

The controls at Zoho relating to the Application development, Production Support and the related General IT Controls relevant to the applicable trust service criteria, cover only a portion of the overall internal control structure of User entities. The trust services criteria cannot be achieved without taking into consideration operating effectiveness of controls at the Zoho's User entities. Therefore, User entities' internal control structure must be evaluated in conjunction with Zoho's control policies and procedures, and the results of testing summarized in section 4 of this report.

This section highlights those internal control structure responsibilities that Zoho believes should be present at user entities, and which Zoho have 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 Entities Controls ('CUECs') mentioned below or similar procedures are in place and operating effectively.

The CUECs mentioned below are as explained and provided by Zoho's management. 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 applicable trust services criteria of User entities.

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

3.9.1 User entities are responsible for providing and managing the access shared with their associates on Zoho products (CA-21)

3.9.2 User entity is responsible for requesting and approving the Master Service Agreement ('MSA') and the approval for implementation of application on Cloud environment (CA-63)

3.9.3 User entities are responsible for utilising the documents made available through the corporate website (CA-16)

3.9.4 User entities are responsible for raising any backup restoration request to Zoho. (CA-76)

3.9.5 User entities are responsible for communicating any security or privacy incidents to Zoho on a timely basis. (CA-89, CA-102)

3.9.6 User entities are responsible for reviewing the privacy policy and accepting to the privacy notice of Zoho. (CA-92, CA-95, CA-105).

These CUECs relate to the specific control activities. However, for the ease of reference and enhanced readability, wherever possible, we have provided the cross reference for these CUECs against the control activities in the subsection 4.3.

3.10 Complementary Subservice Organization Controls

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 auditor 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 applicable trust services criteria process covers only a portion of overall internal control for each user entity of Zoho. It is not feasible for the criteria 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
- Sabey Data Center Properties LLC - Zayo Group, LLC Colocation Services ("zColo") - Interxion HeadQuarters B.V. - Equinix (EMEA) B.V.,	Co-Location Services of IDC Servers

Name of Subservice Organization	Nature of Services Provided
- CtrlS Datacenters Limited - Equinix Asia Pacific Pte. Ltd.	
- KPMG - Matrix Business Services India Private Limited - Hire Right LLC	Background Verification Services

Subservice organizations are responsible for defining and implementing CSOCs provided in sub-section 3.10.

3.10.1 Subservice organizations are responsible for the scope of services covering the co-location services for International Data Centers (IDC) including the physical security and environmental security in the co-location data centers. (CA-07, CA-31, CA-32, CA-33, CA-35, CA-36, CA-37, CA-38, CA-39, CA-40 and CA-41)

3.10.2 Subservice organization is responsible for performing the background verification of Zoho associates, based on request from Zoho HR Teams. (CA-06)

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 entity’s internal control over financial reporting (that is, achievement of the criteria 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 criteria in section 4 of this report. However, the activities performed by these vendors are not required to meet the assertions specified in the criteria, and as a result, no additional procedures are required to be evaluated related to the activities of these vendors.

Name of Vendor	Description of Services Provided
- Powerica - HVAC - Ardelisys Technologies Private Limited - SVE Energy Private Limited - Pinnacle System	Environmental equipment maintenance
G4S Secure Solutions India Private Limited	Physical Security Agency for Security Personnel

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, as referred in section 3.7. 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:

- Communication and Enforcement of Integrity and Ethical Values
- Commitment to Competence
- Management Philosophy and Operating Style
- Organizational Structure
- Board of Directors
- Assignment of Authority and Responsibility
- Human Resources Policies and Procedures
- Corporate Internal Audit Function
- Risk Assessment
- Information and Communication
- Monitoring

Our procedures included testing those relevant elements of the control environment that we considered necessary to provide reasonable assurance that the related criteria 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 documents and records. The control environment was considered in determining the nature, timing, and extent of the tests of operating effectiveness of controls.

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. Observation and inspection procedures were performed as it relates to manually prepared reports, queries, and listings to assess the accuracy and completeness (reliability) of the information used in our testing of the 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 01, 2020 to November 30, 2021. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions during some or all of the period of December 01, 2020 to November 30, 2021, 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
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 01, 2020 to November 30, 2021.

It is user organization’s responsibility to evaluate this information in relation to internal controls in place at user organization to assess the total system of internal controls. If it is concluded that the user organization 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 Security, Availability, Confidentiality, Processing Integrity and Privacy Trust Services Criteria

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	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-01	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.	CC1.1 CC1.2 CC1.3 CC1.5 CC2.1	Inspected the Organizational chart and the email communication for aspects such as 'name of the document', 'contents of the organizational chart', '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	None	No Exceptions Noted.
CA-02	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.	CC1.3 CC1.4 CC1.5 CC2.2	Inspected the Policy Description Manual for the aspects such as 'Name of the document', 'details of the policy', 'version no.', 'number of jobs defined', '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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-03	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.	CC1.1 CC1.4 CC2.2 C1.1	Inspected the attendance register in Zoho People for sample newly joined associates for aspects such as 'employee name', 'date of attendance (issued time)', 'date of joining' and 'contents of induction deck' 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.	None	None	No Exceptions Noted.
CA-04	Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.	CC3.1 CC4.2	Inspected the RACI Matrix on aspects such as such as 'preparer', 'version no.', 'reviewer', 'approver' and 'version history' to ascertain whether Zoho had constituted a Privacy Team which was responsible for implementing and maintaining the data privacy program at Zoho. Inspected the Employee Tree Structure within Zoho People application on aspects such as 'organization structure', 'employee name', 'role name' and 'reporting details' to ascertain whether privacy team reported to the Director of Compliance who in-turn reported to the Vice President.	None	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-05	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.	CC1.1 CC1.4	Inspected the Human Resources Process Description Manual document 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	None	No Exceptions Noted.
CA-06	Upon new associates joining, 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.	CC1.1 CC1.4 CC2.2	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, 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.	None	Refer 3.10.2	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-07	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers 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.	CC1.2 CC1.5 CC2.1 CC2.2 CC3.1 CC3.2 CC4.1 CC6.4 CC6.5 P6.4	Inspected the Data center co-location provider certification/report review email for the aspect 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.	None	Refer 3.10.1	No Exceptions Noted.
CA-08	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.	CC1.1 CC1.4 CC2.1 CC2.2 C1.1	Inspected for the sample newly joined employees 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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-09	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	CC2.3 CC3.3 CC4.1 CC9.2 C1.1	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 third parties for services in relation to hosting of servers and any changes to the contracts were agreed by Zoho and also whether the contract included the scope of services to be provided, confidentiality and other related commitments/clauses.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-10	Zoho has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Security Compliance Manager on an annual basis.	CC1.1 CC1.2 CC1.3 CC1.5 CC2.1 CC2.2 CC2.3 CC3.1 CC4.1 CC5.1 CC5.2 CC5.3 CC6.1 CC6.2 CC6.3 CC7.4 CC9.1	Inspected Integrated Information Security and Privacy Manual document for aspects such as 'name of the policy', 'contents of policy', '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 Information Security & Privacy Manual" which specified the information security and privacy requirements and also defined the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team) and whether it was prepared by Compliance / Privacy Team and approved by the management team and was reviewed by Information Security Compliance Manager on an annual basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-11	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.	CC1.1 CC1.2 CC1.3 CC1.5 CC2.1 CC2.2 CC2.3 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC5.1 CC5.3	Inspected the information security policy in Zoho portal for the aspects such as 'name of document', 'contents of policy' and 'policy available at' to ascertain whether Zoho's management committee was responsible for defining, implementing, and monitoring policies and procedures related to Information security, on an annual basis and whether policies and procedures related to information security were made available to associates through the intranet portal.	None	None	No Exceptions Noted.
CA-12	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.	CC2.2 CC2.3 CC3.1 CC3.2 CC3.3 CC3.4 CC6.2 CC6.3 CC6.4 CC6.5 CC9.1 CC9.2	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.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-13	Zoho has defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by General Counsel and is reviewed by Senior Corporate Counsel on an annual basis.	CC1.3 CC4.1 CC5.1 CC5.3 P5.1	Inspected Privacy Policy document for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'preparer', 'reviewer', 'approver' and 'date of approval' to ascertain whether Zoho had defined organisation wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure and whether the Policy was prepared by Legal Team, approved by General Counsel and was reviewed by Senior Corporate Counsel on an annual basis.	None	None	No Exceptions Noted.
CA-14	Support documents including the system flow diagrams and other design documents for the products are maintained and are made available to the respective team members of Zoho.	CC1.4 CC2.2 CC5.2 PI1.3	Inspected the supporting documents for the sample products for aspects such as 'Product details', 'Category' and 'availability' to ascertain whether support documents including the system flow diagrams and other design documents for the products were maintained and also whether they were made available to the respective team members of Zoho.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-15	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.	CC2.2 CC3.1 CC5.2 CC7.1 PI1.3	Inspected the availability of coding practices document for sample products for aspects such as 'availability of coding practice', 'Description of Secure coding practices' to ascertain whether secure coding practices were defined and communicated to the respective personnel as part of the Zoho's SDLC process.	None	None	No Exceptions Noted.
CA-16	Product descriptions, help documents and terms of usage / service are defined and are made available for to the customers via corporate website.	CC5.2 PI1.1 PI1.2	Inspected the corporate website for sample products for aspects such as 'Product name', 'website - URL where the document is hosted' and 'contents' to ascertain whether product descriptions, help documents and terms of usage / service were defined and were made available for to the customers through corporate website.	Refer 3.9.3	None	No Exceptions Noted.
CA-17	Zoho has defined an Internal audit process manual which is prepared by Compliance Team and approved by the Director of Compliance (DOC) on an annual basis.	CC1.3 CC1.5 CC2.1 CC2.2 CC4.1 CC5.1 CC9.1	Inspected Internal Audit Process Description Manual document for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved on' to ascertain whether Zoho had defined an Internal audit process manual and was approved by the Director of Compliance (DOC) on an annual basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-18	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.	CC1.2 CC1.3 CC2.1 CC2.2 CC3.2 CC3.3 CC4.1 CC4.2 CC5.1 CC5.3 CC9.1	Inspected for a sample half-year the Internal Audit Report for aspects such as 'audit period', 'agenda', 'scope', 'audit risk count' and 'department / teams' to ascertain whether on a half-yearly basis, the Zoho compliance team conducted internal audit of Zoho's information security and privacy controls. Inspected ISMS Management review meeting for aspects such as 'meeting date', 'auditors', 'remediation action', 'MoM prepared by' and 'approved by' for sample half-year to ascertain whether findings from the internal audit were presented to the management and remediation action was taken on a timely basis.	None	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-19	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.	CC1.2 CC1.3 CC1.5 CC2.1 CC2.2 CC2.3 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.3 CC7.3 CC9.1 CC9.2 A1.1	Inspected for sample half-year the Management review Meeting document for aspects such as ‘meeting name’, ‘period’, ‘summary of internal and external audit reports’, ‘conducted by’, ‘members present’ and ‘non-conformances with implementation status’ to ascertain whether Management Review Meeting was held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment and summary of non-conformances along with implementation status was discussed as part of the meeting.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-20	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.	CC1.1 CC1.4 CC1.5	Inspected Code of Ethics document for aspects such as 'policy name', 'contents of the document', 'prepared by', 'approved by', 'approved on' and 'availability of document in the 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	None	No Exceptions Noted.
CA-21	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.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.6	Inspected the password configuration in Domain Controller, IAM, IAN and IDC infrastructure for aspects such as 'Password Configuration and Complexity', 'Session Configuration', and 'authorization upon every logon' and '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.	Refer 3.9.1	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-22	The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.	P4.3 P5.2 P7.1	Inspected the privacy policy for the aspects such as 'policy name', 'contents of policy', last updated by/on', 'approved by/on' to ascertain whether the Privacy Team had defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. Noted that there were no instances of cases that involved disagreements over the accuracy and completeness of personal information in Zoho during the audit period of examination, hence DHS LLP was not able to opine on the said control activity.	None	None	No exceptions noted. DHS LLP could not test the operating effectiveness of review of disagreements as there was no related activity during the assessment period.
CA-23	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.	CC4.1 CC5.1 CC5.2 CC6.6 CC6.8 CC7.1 CC7.2 CC7.3	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 on a periodical basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-24	Monitoring of AV console is performed on a real time basis by the IT Team.	CC6.8 CC7.1 CC7.3	Inspected AV console dashboard for aspects such as ‘tool name’, ‘type of monitoring’ and ‘device status’ to ascertain whether monitoring of AV console was performed on a real time basis by the IT Team.	None	None	No Exceptions Noted.
CA-25	Zoho has defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which is hosted in the corporate website as part of Zoho policies available to end users.	CC5.3 C1.1 C1.2 P4.3 PI1.1	Inspected Privacy Policy document hosted in Zoho corporate website for aspects such as ‘policy name’, ‘contents of policy’ and 'availability of policy' to ascertain whether Zoho had defined and documented policies for retention and disposal of client information upon discontinuation of Zoho services, which was hosted in the corporate website as part of Zoho policies available to end users.	None	None	No Exceptions Noted.
CA-26	Zoho has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.	CC3.2 CC7.2 CC7.3 CC7.4 A1.2 A1.3	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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-27	On an annual and continuous basis, Zoho performs organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.	CC1.2 CC2.1 CC3.1 CC4.2 CC5.1 CC5.3 CC7.2 CC9.1 CC9.2	Inspected Information Technology (IT) Risk Assessment report for aspects such as 'ISO Assessment performed on', 'Location', 'Criteria', 'Domains' 'Validity' and 'Corrective action' to ascertain whether on an annual and continuous basis, Zoho performed organisation wide Information Technology Risk Assessment as part of the ISO standards (27001 27017 27018 and 27701) and also whether the ISO standards identified the processes, and related information assets that were critical for Zoho to ensure information security and privacy standards were adhered across the entity .	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-28	For newly joined associates, 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.	CC5.2 CC6.1 CC6.2	Inspected for sample new joiners the Zoho IT Incident Request ticket for aspects such as 'associate name', 'date of joining', '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, the HR team created an account in ZohoPeople (Control Panel) and once the account was created, AD account was auto created by the system. 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 and the same was assigned and actioned upon by the SysAdmin team.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-29	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 all the logical access of the associate.	CC5.2 CC6.1 CC6.2	Inspected 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 notified the SysAdmin / Zorro team who disabled all the logical access of the associate.	None	None	No Exceptions Noted.
CA-30	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).	CC1.4 CC2.2 CC5.3	Inspected the HR Policy document 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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-31	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.	CC6.4	Inspected for sample new associates / trainees / contractors, the Zoho HRMS application for aspects such as 'Employee ID', 'associate name', 'date of joining', 'HRMS details updated by', 'HRMS details updated on' and 'physical access granted by/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. 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.	None	Refer 3.10.1	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-32	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.	CC6.4	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.	None	Refer 3.10.1	No Exceptions Noted.
CA-33	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.	CC6.4	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', '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.	None	Refer 3.10.1	No Exceptions Noted. The operating effectiveness of physical access revocation for absconders could not be tested as there was no related activity during the examination period,

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-34	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.	CC5.3 CC6.4 A1.2	Inspected the physical security policy for the aspects such as 'policy name', 'version no', 'contents of policy' 'prepared by', 'reviewed by/on' to ascertain whether Zoho had defined and documented Physical Security Policy which was reviewed and approved by the Head of Safety and Security on an annual basis and whether it included the physical access restrictions to the NOC / Zorro processing area.	None	None	No Exceptions Noted.
CA-35	Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.	CC6.4	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. 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.	None	Refer 3.10.1	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-36	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.	CC6.4 CC6.5	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. Inspected and observed for sample dates the visitor-vendor register for aspects such as '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.	None	Refer 3.10.1	Exception Noted. Refer Exception #1 below.
CA-37	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.	CC6.4 CC6.5	Observed 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.	None	Refer 3.10.1	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-38	Zoho premises and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.	CC6.4 CC6.5 A1.2	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. 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.	None	Refer 3.10.1	No Exceptions Noted.
CA-39	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	CC6.4 A1.2	Observed the Zoho facility for aspects such as 'cooling facilities', 'UPS with battery and diesel generator', 'smoke detectors', 'water sprinklers' and 'fire-resistant floors' to ascertain whether environmental safeguards were installed in Zoho facilities.	None	Refer 3.10.1	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-40	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.	CC6.4 A1.2	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.	None	Refer 3.10.1	Exception Noted. Refer Exception #2 below.
CA-41	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.	CC6.4 A1.2	Inspected the mock fire drill report for aspects such as 'Conducted on', '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.	None	Refer 3.10.1	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-42	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.	CC2.2 CC5.3	Inspected Network Operation Center- Policy and Process for aspects such as 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved on' to ascertain whether the policies and procedures covering the logical access and operations of NOC were 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. Inspected Zoho NOC intranet site for aspects such as 'policy name' and 'availability of policy' to ascertain whether this policy was hosted on NOC's intranet site with access available to the designated team members.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-43	Logical access to the tools (managed by NOC team) used for performing NOC's daily operations are granted by Senior NOC member based on approval by NOC manager and revoked on a timely manner based on the approval of the NOC Manager in the Zoho Creator tool where the request is raised by the Senior NOC Member.	CC6.1 CC6.2 CC6.3	Inspected sample access requests for aspects such as 'ID', 'Added time', 'Name', 'Access required to tool' 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 member in the Zoho Creator tool where the request was raised by the Senior NOC Member. Inspected sample access revocation for aspects such as 'ID', 'Name', 'Access to tool', 'request date', '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.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-44	For tools such as Wiki, MI, SDP, ZAC and Password Manager Pro (managed by Zorro team) a request for new access and request for access revocation is sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team. The access to the tools are granted / revoked by the Zorro Manager.	CC6.1 CC6.2 CC6.3 CC6.7	Inspected the service request ticket for sample access creation requests for aspects such as ‘request ID’, ‘requestor name’, ‘requestor email ID', 'status’ to ascertain whether for internal tools like Wiki, ZAC and Password Manager Pro, a request (for new access) was sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team and whether the access to the tools were granted by the Zorro Manager. Inspected the service request ticket for sample access revocation requests for aspects such as ‘request ID’, ‘requestor name’, ‘requestor email ID', 'status’ to ascertain whether for internal tools like Wiki, ZAC and Password Manager Pro, a request (for access revocation) was sent by the Senior NOC Member or by the individual Zorro team member to the Zorro team and whether the access to the tools were granted by the Zorro Manager.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-45	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 designated members to prevent unauthorized access.	CC6.1 CC6.7 CC6.8 CC7.1	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. Inspected the access listing of users having access to network devices for aspects such as ‘user’, ‘role’ and ‘rationale for access’ to ascertain whether access to the network devices were restricted to designated members to prevent unauthorized access.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-46	Based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices are auto-generated and sent to the NOC SDP Portal.	CC3.2 CC3.3 CC4.1 CC4.2 CC5.1 CC5.2 CC6.6 CC6.7 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5 A1.1	Inspected the monitoring dashboard, alert configuration for aspects such as 'dashboard contents', 'type of alerts triggered', 'datacenter', 'notification sent to', 'event information captured' to ascertain whether based on the network monitoring by the NOC team through MI, EventLog Analyzer and SOC tools, alerts for changes to network configurations and alerts / errors relating to network devices were auto-generated and sent to the NOC SDP Portal.	None	None	No Exceptions Noted
CA-47	The NOC team uses an in-house tool (DeviceExpert) to backup network device configurations on a daily (incremental backup) and weekly (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team.	A1.1 A1.2	Inspected Network Configuration Manager Schedule and alert configuration for aspects such as 'datacenter', 'frequency of backup', 'devices backed up', '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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-48	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.	CC3.3 CC5.1 CC5.2 CC6.6 CC6.7 CC6.8 CC7.1 CC7.2 CC7.3 CC7.5 A1.1	Inspected network alert auto mitigation settings and dashboard for aspects such as ‘datacenter', 'name of the DDOS monitoring application', 'alerts captured' and 'network summary' to ascertain whether Zoho had implemented measures to monitor the network in order to detect any attacks from the external network.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-49	Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic 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.	CC5.1 CC7.2 A1.1	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. Inspected the annual DR Testing report 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.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-50	Zoho maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the NOC Manager or SysAdmin or Zorro team.	CC3.3 CC3.4 CC6.1 CC6.8 CC8.1 A1.1	Inspected the assets register for aspects such as 'Location', 'asset details captured', 'responsibility' to ascertain whether Zoho maintained an asset register for its IT Assets. Inspected the approval for sample tickets for aspects such as ‘request ID’, 'asset type', ‘requestor type’, ‘description’, ‘approver email’ and ‘approval status’ to ascertain whether in case of any additions, replacements or removal of IT Assets including the workstations, network devices, storage etc., a ticket was raised and was approved by the NOC Manager or SysAdmin or Zorro team.	None	None	No Exceptions Noted.
CA-51	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.	CC3.4 CC7.1 CC8.1	Inspected for sample patches the tickets for aspects such as ‘patch ticket ID’, ‘requestor name’, ‘patch tested by- local environment’ 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	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-52	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). Managers / L3 of the Sysadmin team or Zorro team approve / deny the requests based on the provided inputs. Upon approval, the request is routed to NOC SDP Portal for processing by NOC team.	CC3.4 CC6.8 CC7.1 CC8.1 PI1.2 PI1.3	Inspected the change tickets for sample VLAN changes 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 whether Managers / L3 of the Sysadmin team or Zorro team approved / denied the requests based on the provided inputs and whether upon approval, the request was routed to NOC SDP Portal for processing by NOC team.	None	None	No Exceptions Noted
CA-53	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.	CC3.4 CC6.8 CC7.1 CC8.1	Inspected for sample firewall rule changes, the firewall rule change tickets for aspects such as 'request ID', 'Datacenter', 'requested by', 'request raised to', 'approved by', 'completion notes', 'firewall change logs' 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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-54	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.	CC3.4 CC6.1 CC8.1	Inspected for a sample half-year the request ticket raised for firewall rule review 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	None	No Exceptions Noted.
CA-55	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.	CC3.4 CC7.1 CC8.1 PI1.3	Inspected for sample change requests the change request ticket raised for aspects such as ‘subject’, ’change’, ‘Backup plan available’, ‘tested by’, ‘approved by’, ‘servers and sites impacted’, ’availability of completion notes’, ’implementer’ and ‘close date’ to ascertain whether 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	None	No Exceptions noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-56	Access to Corporate VPN is authenticated with Zoho users' AD account by the Zoho Sysadmin team.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.6	Inspected the integration settings between VPN and AD for aspects such as 'if AD is configured', 'number of authentication layers' and 'remote gateway used' to ascertain whether access to corporate VPN was authenticated with Zoho users' AD account by the Zoho Sysadmin team.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-57	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 is taken.	CC3.2 CC3.3 CC4.2 CC5.1 CC6.6 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 A1.1	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. Inspected for sample products the penetration testing report for aspects such as 'risk category', 'scope', 'test cases handled', 'date performed', '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.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-58	The Zoho Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.	CC1.2 CC1.5 CC2.2 CC3.1 CC3.2 CC3.3 CC4.1 CC5.1 CC5.3 CC6.7 CC9.1 CC9.2 A1.1 A1.2	Inspected Risk Management Policy document for aspects such as 'policy name', 'contents of policy' and 'prepared by', 'approved by', and 'version no.' to ascertain whether the Zoho Compliance team had developed a Risk Management Policy that covers the operational, strategic and IT risks related to the Zoho infrastructure and services provided by Zoho and whether the Risk Management Policy was reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.	None	None	No Exceptions Noted.
CA-59	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.	CC1.1 CC1.4 CC1.5	Inspected MID (CAR - Carrier Achievement Policy) and CAR Process flow for aspects such as 'policy name', 'version', 'performance appraisal procedures defined', 'prepared by', 'approved by' and 'approved date' to ascertain whether Zoho had defined procedures for periodic performance appraisals and review and assessment of professional development activities.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-60	Access to external storage devices and internet are disabled on IDC workstations to prevent data loss.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.6 CC6.7 CC6.8 CC7.1 CC7.2	Inspected the configuration in IDC workstation 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	None	No Exceptions Noted.
CA-61	The Zoho Customer Success Team has a defined and documented Process Description Manual for Product Support which is approved by the Director of Customer Service on an annual basis.	CC2.3 CC5.3 CC6.3 PI1.1 PI1.2 PI1.3	Inspected Process Description Manual- Customer Success team for aspects such as 'name of the policy', 'contents of the policy', 'version no.', 'prepared by', 'approved by' and 'approved on' to ascertain whether the Zoho Customer Success Team had a defined and documented Process Description Manual for Product Support which was approved by the Director of Customer Service on an annual basis.	None	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-62	Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.	CC2.3 PI1.1 PI1.3	Inspected for sample requests the automated email containing Query ticket for aspects such as 'query ticket no.', 'query received via', 'description', 'ticket raised by', 'ticket raised on', 'assigned to', 'assigned by', 'assigned on' and 'SLA details' to ascertain whether based on the support requested by the customer via email / phone / chat, an automated ticket was generated in the Zoho Desk Portal and assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.	None	None	No Exceptions Noted
CA-63	Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.	CC2.3 PI1.1	Inspected for sample customers the MSA signed between Zoho and the customer for aspects such as 'name of customer', 'type of service', 'agreement signed by' and 'agreement signed on' to ascertain whether Zoho entered into a Master Service Agreements ('MSA') with customers for hosting Zoho Cloud applications on Cloud and the agreement covered the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Cloud Applications.	Refer 3.9.2	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-64	The General Counsel - Legal of Zoho is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.	CC1.2 CC1.3 CC2.2 CC2.3 CC3.1 CC3.3 CC3.4	Inspected the Responsibility Matrix, Privacy Policy and contracts for sample agreements for aspects such as 'responsibility', 'name of policy', 'contents of policy', 'contracts entered' 'contents of contract' to ascertain whether the General Counsel - Legal of Zoho was responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.	None	None	No Exceptions Noted.
CA-65	Whistle Blower mechanism is defined as part of Code of Ethics document and it provides guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc., through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation. In case of any non-compliance with the policies, disciplinary action is taken in line with policy.	CC1.1 CC2.2 CC2.3 CC3.1	Inspected Code of Ethics policy for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'prepared by', 'approved by', 'approved on' and 'Disciplinary action in case of code violation' to ascertain whether Whistle Blower mechanism was defined as part of Code of Ethics document and it provided guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc., through Zoho Connect anonymously and whether it also specified the action to be taken in case of any violation and whether in case of any non-compliance with the policies, disciplinary action was taken in line with policy.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-66	The Zorro team has defined a Zoho Data Center Operations document defining the procedures relating to day-to-day operations of Zorro including procedures for degaussing the disks. The document is prepared by the Zorro team and approved by the Director of Network and IT Infrastructure. The documented is reviewed and approved by the Director on an annual basis.	CC5.3	Inspected Zorro Operations document for aspects such as ‘name of the policy’, ‘contents of policy’, ‘version no.’, ‘prepared by’, ‘approved by’, and ‘approved on’ to ascertain whether the Zorro team had defined a Zoho Data Center Operations document defining the procedures relating to day-to-day operations of Zorro including procedures for degaussing the disks and also whether the document was prepared by the Zorro team and approved by the Director of Network and IT Infrastructure and was reviewed and approved by the Director on an annual basis.	None	None	No Exception Noted.
CA-67	Access to Site24x7 for Zorro TM is managed through common login credentials maintained in the in-house developed Zoho Wiki Tool.	CC6.1 CC6.2 CC6.3 CC6.6 CC6.7	Inspected the Zoho wiki page for aspects such as 'URL', 'Datacenter', 'Contents of the page', 'Tool access provision' to ascertain whether access to Site24x7 was managed through common login credentials maintained in the in-house developed Zoho wiki tool.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-68	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.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.7	Inspected for sample access creation the tickets 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’, 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	None	No Exceptions Noted.
CA-69	Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.7	Inspected the 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 TM based on the IDC access revocation process on a timely manner.	None	None	Exception Noted. Refer Exception #3 below.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-70	The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers.	CC4.2 CC5.1 CC5.2 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5 A1.1 PI1.3 PI1.4	Inspected the MI tool for aspects such as 'Datacenter', 'Dashboard URL', 'Services Monitored' to ascertain whether Zorro team monitored the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. Inspected the alerts on sample dates for aspects such as 'Date', 'Datacenter', 'Type of error' and 'Status' to ascertain whether in case an error was detected in the MI tool, action was taken by the Zorro engineers.	None	None	Exception Noted. Refer Exception #4 below.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-71	The Zorro team uses an in-house tool called ‘Site24x7’ to monitor the availability of Zoho's services from different geographical locations across the globe. Automated email alerts to the respective application teams and Zorro TMs are triggered when the services are unavailable from the monitored location and action is taken accordingly.	CC4.2 CC5.1 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5 A1.1 A1.2 PI1.4	Inspected the 24x7 site dashboard and configuration for aspects such as 'name of the tool', 'locations', 'alert segregation' and 'contents in alert groups' to ascertain whether Zorro team used an in-house tool called ‘Site24x7’ to monitor the availability of Zoho's services from different geographical locations across the globe. Inspected for sample alerts the alert requests raised for aspects such as ‘incident ID’, ‘customer affected’, ‘Services impacted’, ‘Closed by’ and ‘RCA available’ to ascertain whether automated email alerts to the respective application teams and Zorro TMs were triggered when the services were unavailable from the monitored location and action was taken accordingly.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-72	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.	CC3.2 CC3.3 CC4.1 CC5.1 CC6.7 CC6.8 CC7.1 CC7.2 CC7.4 CC7.5 A1.1 PI1.4	Inspected the network dashboards for aspects such as 'Name of the DC', 'ISP of the DC', 'ISP of the peer DC' to ascertain whether Zoho ensured availability of data centers through redundant networks in the data centers and whether redundancy of internet connectivity was also ensured via utilization of separate ISP.	None	None	No Exceptions Noted.
CA-73	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.	P5.1 P5.2 P6.5 P6.7 P8.1	Inspected the email communication from Zoho and noted that there were no instances of cases of data subjects whose access request has been denied in Zoho during the period of examination, hence DHS LLP was not able to test the control.	None	None	DHS LLP could not test the operating effectiveness of this control activity as there was no related activity during the assessment period.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-74	Zorro team has defined OS Hardening Guidelines to ensure that the Operating Systems (workstations and servers) are hardened. The guidelines are prepared by the Zorro team and approved by Manager - Zorro on an annual basis.	CC3.1 CC3.4 CC5.1 CC6.6 CC6.7 CC7.1 CC7.2 CC8.1	Inspected Zorro OS Hardening Procedure for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved on' to ascertain whether Zorro team had defined OS Hardening Guidelines (workstations and servers) to ensure that the Operating Systems were hardened and whether the guidelines were prepared by the Zorro team and approved by Manager - Zorro on an annual basis.	None	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-75	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 corrective action is taken.	CC6.7 A1.2 A1.3 PI1.5	Inspected backup configuration, 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. 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.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-76	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 in relation to the cloud-based services within the agreed SLA.	CC6.1 CC6.7 C1.1 A1.2 A1.3 PI1.5	Inspected for sample backup restoration requests the request ticket for aspects such as ‘backup restoration request ID’, ‘service type’, ‘database backup type’, ‘backup date and time’, ‘cluster IP’, ‘approved by’ 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 in relation to the cloud-based services within the agreed SLA.	Refer 3.9.4	None	No Exceptions Noted
CA-77	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.	CC6.7 CC7.2 A1.1 A1.2 A1.3 PI1.5	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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-78	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. For SSD and NVMe storage devices, a Crypto-Erase tool is used to securely remove data prior to disposal.	CC6.1 CC6.5 CC7.2 CC7.3 C1.1 C1.2 PI1.5 P4.3	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 storage devices were disposed securely using secure disposal methods by the Zorro team and whether the failed hard disk drives (HDD) were degaussed prior to disposal / replacement and also whether for SSDs and NVMe storage devices, a Crypto-Erase tool was used to securely remove data prior to disposal.	None	None	No Exceptions Noted.
CA-79	Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes. The policy is reviewed and approved on an annual basis.	CC2.2 CC2.3 CC3.4 CC5.3 CC8.1 PI1.3	Inspected Change Management policy for aspects such as 'name of policy', 'contents of policy', 'prepared by', 'approved by' and 'approved on' to ascertain whether Zoho has defined policies and procedures for change management as part of Change Management Policy pertaining to infrastructure and product changes and also noted that policy was reviewed and approved on an annual basis.	None	None	No Exceptions noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-80	Changes are carried out in the Development environment and tested in the QA environment, which is separate from the Production environment.	CC5.1 CC8.1 PI1.3	Inspected for sample products for aspects such as 'Development environment paths/URL's', 'QA environment paths/URL's' and 'Production environment paths/URL's' to ascertain whether changes were carried out in the Development environment and tested in the QA environment, which was separate from the Production environment.	None	None	No Exceptions Noted.
CA-81	Client data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho facility.	CC8.1 PI1.2	Inspected the VPN configuration for DC and the hosting of production and pre-production servers to ascertain whether client data can be accessed from DC only through IAN VPN or the dedicated IAN servers in the Zoho facility.	None	None	No Exceptions Noted
CA-82	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 respective Product Teams on an annual basis.	CC3.4 CC5.1 CC5.3 CC8.1 PI1.3	Inspected Development Life Cycle document for aspects such as 'name of policy' 'version no.', prepared by', 'approved by, and 'approved on' to ascertain whether Zoho had defined 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 respective product Teams on annual basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-83	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed by Privacy Lead on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.	CC7.3 CC7.4 CC7.5 P6.1 P6.3 P6.4 P6.5 P6.6 P6.7	Inspected Privacy Incidents and Breach Response Procedure document for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'date of approval' to ascertain whether comprehensive incident identification and breach response procedure was documented by Privacy team; approved by the Director of Compliance; reviewed by Privacy lead on an annual basis and provided examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constituted a breach. Inspected the announcement details in Zoho Connect portal for aspects such as 'announcement name', 'contents of announcement- procedure name' and 'uploaded by' to ascertain whether the procedure was communicated to personnel who handled personal information.	None	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-84	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.	CC3.4 CC5.1 CC5.2 CC7.1 CC8.1 PI1.2	Inspected for sample builds the Code Review details for aspects such as 'Reviewed by', 'details of the URL's/Paths of codes', 'repository' and 'review date' to ascertain whether the code created by the development team was maintained in a centralised repository by the Configuration Management (CM) team and the code developed by the Developers was pushed into the CM tool, which was an in-house tool used by the CM team.	None	None	No Exceptions Noted
CA-85	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.	CC3.4 CC5.2 CC7.1 CC8.1 PI1.2	Inspected for sample builds the build workflow details for aspects such as 'configuration check completed by', 'configuration team approval details', 'details of the URL's/Paths', 'QA tested by' 'and 'QA tested on' to ascertain whether the Developed code was tested systematically 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 on the build in the local (Testing) Environment.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-86	On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment.	CC3.4 CC5.2 CC7.1 CC8.1 PI1.2	Inspected for sample builds the automated E-mail and build workflow details for aspects such as 'build name', 'date of hacksaw report', 'generated by', 'details of the URL's/Paths' , 'contents of QA report- result', '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, the Security team generated the QA report and performed security tests on the build and also whether 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.	None	None	Exception Noted. Refer Exception #5 below.
CA-87	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 half-yearly basis. Corrective actions, if any, are taken on a timely manner.	CC6.1 CC6.2 CC6.3 CC6.5	Inspected for a sample half-year 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 half-yearly basis and corrective actions, if any, were taken on a timely manner.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-88	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 by leadership staff on an annual basis and version history is maintained within the document.	CC2.2 CC2.3 CC3.1 CC3.2 CC3.3 CC4.1 CC4.2 CC5.3 CC7.3 CC7.5	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 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	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-89	Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant product team preforms root cause analysis (RCA) and updates the security incident in the Zoho creator tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.	CC2.2 CC2.3 CC3.1 CC4.1 CC7.3 CC7.4 CC7.5	Inspected for sample security incidents the security incident ticket workflow details for aspects such as 'incident ID', 'Description of the incident', 'RCA available', 'Impacted Services, 'incident start time', 'incident type' and 'submitted via' to ascertain whether based on the inputs received via email/chat/phone, the incident management team coordinated with relevant stakeholders to analyze the potential impact of the security incident and also to ascertain whether the relevant product team performed root cause analysis (RCA) and updated the security incident in the Zoho creator tool and whether corrective actions were taken on a timely basis and preventive measures were deployed to prevent future incidents.	Refer 3.9.5	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-90	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.	CC2.2 CC2.3 CC3.1 CC4.1 CC7.3 CC7.4 CC7.5 PI1.4	Inspected for sample alerts the Creator form requests for aspects such as 'incident ID', 'customer affected', 'Services impacted', 'Closed 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.	None	None	No Exceptions Noted.
CA-91	A 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.	CC2.2 CC2.3 CC3.1 CC4.1 CC4.2 CC7.3 CC7.4 CC7.5	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	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-92	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is: 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.	CC2.3 CC5.3 P1.1 P5.1	Inspected for sample data collection points the evidence of providing privacy notice for aspects such as 'privacy policy- check box', 'privacy policy - agreement option', 'account signup page details' and 'website URL' and inspected Privacy Policy hosted in Zoho corporate website for aspects such as 'contents of the policy- notification of changes' and 'date last updated' to ascertain whether the entity provided notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes were made to the entity's privacy practices) and also whether the notice satisfied the criteria specified in the control activity.	Refer 3.9.6	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-93	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.	P1.1 P4.2 P4.3 P5.1 P5.2 P7.1 P8.1	Inspected the MOM of the privacy review meeting for aspects such as , 'contents of MOM', 'Date of review meeting', 'prepared by', 'approved by', 'date of approval' and 'Details of sharing the MOM' to ascertain whether on an annual basis, the Director of Compliance and privacy staff met to discuss the new types of personal information that was collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items and for any new personal information that was collected, systems and processes were updated to provide notice to the data subjects.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-94	The Director of Compliance and the General Counsel reviews the privacy notice and documents his / her approval that the notice includes the following disclosures: 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information 4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.	P1.1 P3.1	Inspected the Privacy Policy and Review details for aspects such as 'policy name', 'contents of policy', 'version no.', 'prepared by', 'reviewed by', 'approved by', 'date of approval' to ascertain whether the Director of Compliance and the General Counsel reviewed the privacy notice and documented his / her approval that the notice included the disclosures as specified in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-95	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. Also, if any changes are made the same is notified in the respective products websites.	P1.1 P3.2 P4.1 P5.1 P5.2 P6.1	Inspected the Zoho connect portal/ website for aspects such as 'sent by', 'sent to', 'sent on', 'subject', and 'contents of email communication- announcement of Privacy Policy', to ascertain whether the entity communicated to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information and also, if any changes were made the same was notified in the respective products websites.	Refer 3.9.6	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-96	Zoho's Privacy Policy includes the below policy around Choice and Consent: 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.	P2.1 P5.1	Inspected Privacy Policy document for aspects such as 'name of the policy', 'contents of policy', version no.', 'preparer', 'reviewer', 'approver' and 'date of approval' to ascertain whether Privacy Policy contained information about choice and consent options included the aspects mentioned in the control activity. Inspected for sample activities from the Master activity register for aspects such as 'type of activity', 'mode of receiving the consent' and 'consent seeking process' to ascertain whether Zoho's choice and consent options included the aspects mentioned in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-97	The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.	P2.1 P3.2 P5.2	Inspected revision history of Master Activity register for aspects such as ‘reviewed by’, ‘version details’, ‘approved by’ and ‘date of approval’ to ascertain whether the privacy team had established procedures to assess the nature of the information collected to determine whether personal information received required an explicit consent. Inspected for sample activities/products from Master activity register for aspects such as ‘type of activity’, ‘mode of receiving the consent’ and ‘consent seeking process’ to ascertain whether the privacy team had also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-98	The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity's policies for conformity to the requirement.	P2.1	Inspected Privacy Review Checklist document for aspects such as 'contents', 'version details', 'review details', 'reviewed by', 'approved by' and 'date of approval' to ascertain whether the privacy staff reviewed relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possessed other legal ground to process the data and whether they also reviewed and updated the entity's policies for conformity to the requirement.	None	None	No Exceptions Noted.
CA-99	On an annual basis, the Director of Compliance (DOC) reviews its policies to ensure the definition of "sensitive" personal information is properly delineated and communicated to personnel.	P2.1	Inspected the Information Classification Policy for Personal and Special Category of Data document for aspects such as, 'Prepared by', 'Contents of the document', 'version details', 'date of review' and 'Reviewed by' to ascertain whether on an annual basis, the Director of Compliance (DOC) reviewed its policies to ensure the definition of "sensitive" personal information was properly delineated and communicated to personnel.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-100	The entity provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.	CC1.4 CC2.2 P2.1	Inspected Privacy Awareness Training session viewers report for aspects such as ‘associate name’, ‘viewed date and time’ and also inspected and observed the Privacy Awareness Training deck for aspects such as ‘name of the deck’, ‘presented by’ and ‘contents of deck’ to ascertain whether the entity provided updated privacy training and awareness to personnel that included defining what constitutes personal information and what personal information was considered sensitive.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-101	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.	P2.1 P3.1	Inspected Privacy Policy document, Privacy Notice and Privacy Review Meeting for aspects such as ‘policy name’, ‘contents of policy’, ‘version no.’, ‘privacy notice to data subjects’ ‘Privacy regulations review’ and ‘contents of the meeting’ to ascertain whether members of the privacy staff verified that the entity has legal ground to collect data from the data subjects and that such legal grounds were documented prior to Collection. Inspected the sample review performed for activities/products from Master activity register for aspects such as ‘type of activity’, ‘mode of receiving the consent’ and ‘consenting seeking process’ to ascertain whether members of the privacy staff verify, on a test basis, that the entity had requested and received explicit written consent from the data subjects, when such consent was required.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-102	Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices.	P3.1 P4.3 P8.1	Inspected the tickets for sample privacy incident for aspects such as ‘incident title’, ‘incident type’, ‘incident start date’, ‘notification details’, ‘mitigation details’, ‘whether PIA was conducted’, and ‘incident end date’ to ascertain whether privacy related complaints were investigated on as-needed basis to identify whether there were incidents of unfair or unlawful practices.	Refer 3.9.5	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-103	Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.	P3.1 P4.1	Inspected Privacy Policy document and Master Activity register for aspects such as ‘name of the policy’, ‘contents of policy’, version no.’, ‘preparer’, ‘reviewer’, ‘approver’, ‘date of approval’, and ‘nature of information collected’ to ascertain whether members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-104	Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.	P3.1 P6.1	Inspected the Privacy Impact Assessment Report document for sample changes in the manual tracker for aspects such as 'description of request', 'change request - document name', 'approved by', 'date of approval', 'residual risk and mitigation measures' to ascertain whether Privacy Impact Assessment (PIA) was conducted for system changes to assess for privacy implications. Inspected the Privacy Awareness Training deck for aspects such as 'training name', 'contents of deck', 'associate name', 'associate ID' and 'completion date and time' to ascertain whether personnel who were authorized to make system changes were trained to perform PIA.	None	None	Exception Noted. Refer Exception #6 below.
CA-105	The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information.	P3.2 P4.1	Inspected the "Zoho's customer creation account sign-up webpages" and other sample customer facing portals for aspects such as 'URL name', 'consent details', 'Location specific details' and 'privacy policy link' to ascertain whether the entity's application(s) provided for user interface (UI) screens that had a click button that captured and recorded a data subject's consent before the data subject submitted the information.	Refer 3.9.6	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-106	On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.	P4.1 P5.2 P7.1 P8.1	Inspected Privacy Policy document and Privacy review meeting for aspects such as ‘name of the policy’, ‘contents of policy’, version no.’, ‘reviewed by’ and ‘privacy review meeting content’ to ascertain whether on an annual basis the entity reviewed privacy policies and procedures to ensure that personal information was used for 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.	None	None	No Exceptions Noted

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-107	The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies: 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.	C1.1 C1.2 P4.2 P7.1	Inspected Privacy Policy and Data Retention document for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'preparer', 'reviewer', 'approver' and 'date of approval' to ascertain whether the entity had documented its personal information retention policies and procedures, which were reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations and also whether the policy contained the contents specified in the control activity	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-108	An annual review of the organization's data inventory is performed to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.	P4.2	Inspected the Master activity register and Revision History of Master activity Register for aspects such as 'field name', 'source of data', 'reason for collection', 'access and storage details', 'retention details', 'reviewed by', 'version details', 'approved by' and 'date of approval' to ascertain whether an annual review of the organization's data inventory was performed to verify that the documentation was kept current and included the location of the data, description of the data, and identified data owners.	None	None	No Exceptions Noted.
CA-109	The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.	P5.1 P6.7 P8.1	Inspected Subject Access Request Policy for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'date of approval' to ascertain whether the Director of Compliance (DOC) established a 'Subject Access Request Policy' that defined authentication of data subjects into system and how the entity personnel were to respond to requests by data subjects to access their information and also to ascertain that the policy was reviewed and approved on an annual basis by the Director of Compliance (DOC).	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-110	When consent is required, business unit personnel implement a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).	P2.1 P3.2 P6.1 P8.1	Inspected the Consent Guidelines & Consent seeking process document for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'date of approval' to ascertain whether when consent was required, business unit personnel implemented a process for obtaining explicit consent and updates to the consent process were reviewed and approved by the Director of Compliance (DOC).	None	None	No Exceptions Noted.
CA-111	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. The privacy staff reviews the disclosure requests and their status as part of the annual privacy review meeting.	P5.1 P6.1 P6.2 P6.7 P8.1	Observed and inspected for the sample disclosure requests recorded and maintained by the Zoho Legal team for aspects such as 'Request type', 'Date of Request', 'Request details' and 'Request closed by' to ascertain whether requests for disclosure were recorded by business unit personnel, (including the date received and specific details regarding the request) and compared to pre-approved types of disclosures before processing and also when required, consent of the data subject was obtained prior to processing and the rejections were recorded in a repository.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-112	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.	CC1.1 CC1.2 CC1.3 CC1.5 CC4.2	Observed the minutes of the sample meetings held for aspects such as 'Date of meeting', 'Participants of meeting', 'Agenda / minutes of meeting' to ascertain whether management established an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-113	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.	CC1.5 P6.2 P6.4 P6.5 P6.7	Inspected the review for service specific sub processors for aspects such as ‘entity name’, ‘purpose’, ‘location of processing’ and ‘applicable services’ to ascertain whether on an annual basis, the privacy staff obtained a list of paid vendors or other third parties and identified those that process personal information. Inspected for sample vendors the contract documents for aspects such as ‘vendor name’, ‘contents of contract’, ‘approved by’ and ‘approved on’ to ascertain whether the privacy staff also reviewed the contracts with those vendors or other third parties to determine whether the contracts contained privacy and security commitments and system requirements that were consistent with those of the entity commitments for privacy and security.	None	None	No Exceptions Noted.

#	Control Activity	Trust Service Criteria mapping	Tests Performed	CUECs	CSOCs	Results of Tests
CA-114	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by the Security and Compliance team upon which incidents flagged as privacy issues are resolved.	P6.1 P6.3 P6.5 P6.6	Observed the ticket and communication for sample incidents for aspects such as ‘incident ID’, ‘incident title’, ‘incident type’, ‘incident start date’, ‘notification details’, ‘RCA details’ and ‘incident end date’ to ascertain whether message was sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process and whether RCA was prepared by the Security and Compliance team upon which incidents flagged as privacy issues were resolved.	None	None	No Exceptions Noted.
CA-115	Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.	CC6.1 CC6.2 PI1.5	Inspected the encryption agent of sample products for aspects such as 'type of encryption', 'if encryption is enabled' and ‘use of full disk encryption’ to ascertain whether Zoho Key Management service team Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products and whether Zoho used encryption for its emails.	None	None	No Exceptions Noted.
CA-116	Zoho Cloud products use TLS encryption for data that are transferred through public networks.	CC6.1 CC6.2	Inspected the certificate for aspects such as ‘issued to’, ‘if TLS encryption is available’, ‘signature hash algorithm used’ and ‘validity period’ to ascertain whether Zoho Cloud products used TLS encryption for data that were transferred through public networks.	None	None	No Exceptions Noted.

4.3.2 Management Responses to Exceptions

The Audit exceptions presented in the Section 4 of this report were reviewed and discussed on February 11, 2022, during a dedicated Closing Meeting attended by the Zoho Compliance Team.

The Management Responses to the exceptions noted is as under:

Exception 1

Control Activity and Criteria Impacted by Exception	Description of Testing Exception	Management Response to Exception
CA-36 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. **Criteria:** CC6.4 and CC6.5	For the location Austin in USA, the visitor register was not available for review during the audit period.	We agree with the exception noted. Work from home was enforced to all the employees due to the pandemic situation and no visitors entered/visited the US office premises during this audit period. In addition to that, Zoho office in US Austin has been relocated within the same state and during this relocation the visitor register was misplaced. Instead of physical register, web application-based visitor management system will be implemented by Q2 of 2022.

Exception 2

Control Activity and Criteria Impacted by Exception	Description of Testing Exception	Management Response to Exception
CA-40 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. **Criteria:** CC6.4 and A1.2	For locations Austin and Pleasanton in USA, Preventive Maintenance reports for UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators were not available for review.	We agree with the exception noted. Since March 4, 2020, Zoho's USA offices have been closed due to the pandemic and the employees work from home during the period. Therefore, Zoho has not performed a formal preventive maintenance over the equipment in the front offices in USA. Further, we will have quarterly PPM for all systems put into place from first quarter of 2022.

Exception 3

Control Activity and Criteria Impacted by Exception	Description of Testing Exception	Management Response to Exception
CA-69 Access revocation in IDC Landing Access Machine and IDC server for Zorro associates are done by the designated Zorro TM based on the IDC access revocation process on a timely manner. **Criteria:** CC5.2, CC6.1, CC6.2, CC6.3 and CC6.7	The user access in the IDC Landing Access Machine / server was not revoked on a timely basis for the users having access to the servers.	We agree with the exception noted. The direct access to the datacenter machines are 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) Further, the access to the accounts are restricted only to the authorized members of the team and Zoho performs a periodic user access review by the designated personnel in every team. The password to these accounts are controlled and changed on a periodical basis. Based on the above measures in place in Zoho, we determine the risk to be mitigated. In addition, we are also bringing in a timed access policy where the user needs to raise access request and access is granted only for the specified duration. This process has been implemented for the product teams in EU datacenter in 2021 and will be rolled out in phased manner for all our other datacenters.

Exception 4

Control Activity and Criteria Impacted by Exception	Description of Testing Exception	Management Response to Exception
CA-70 The Zorro team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the MI tool, action is taken by the Zorro Engineers. **Criteria:** CC4.2, CC5.1, CC5.2, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, A1.1, PI1.3 and PI1.4	For 1 out of 15 sample errors detected in MI tool, the evidence for corrective action taken by Zorro engineers was not available for review.	We agree with the exception noted. Due to COVID19 pandemic, we were not able to fix the issue as the issue needs to be fixed in person by an engineer. Our engineer will be rectifying the issue during the physical visit scheduled in Q1 of 2022. Further, going forward Zoho shall ensure that a DC engineer in Europe is based out permanently for carrying out the DC operations to avoid such events in the future.

Exception 5

Control Activity and Criteria Impacted by Exception	Description of Testing Exception	Management Response to Exception
CA-86 On completion of the quality checks by the Quality Assurance team, a 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 and then the code is deployed in the production environment. **Criteria:** CC3.4, CC5.2, CC7.1, CC8.1 and PI1.2	For 5 out of 35 samples, the signoffs and documentation in relation to the approvals by Quality Assurance team were not formally documented and retained by Zoho.	We agree with the exception noted. Zoho has adequate checks in various levels such as static code analyser, automated and manual functional testing included as part of the QA process. The quality assurance has been performed for the changes however, Zoho shall retain the explicit documentation for the changes to ensure that the signoffs are captured prior to the deployment. In addition, the changes made to the system follow the approval process (post the QA clearance) by the CM/SD team prior to implementation is available. The sample changes as identified in the exception were monitored post implementation for any impact in the production system by the respective product teams and no impact has been observed.

Exception 6

Control Activity and Criteria Impacted by Exception	Description of Testing Exception	Management Response to Exception
CA-104 Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA. **Criteria:** P3.1 and P6.1	We noted that the documentation on the requirement of privacy impact assessment was not captured or documented in the change ticketing tool for sample changes as part of the change request form.	We agree with the exception noted. Based on the change management policy, for the changes that are determined to have an implication on the privacy, Zoho performs Privacy Impact Assessment (PIA). Wherever it is determined as necessary, the product teams raise a request for performing the PIA through emails and the same is maintained in a manual tracker. Going forward, we will bring in a process to capture the need to carry out a PIA or not in the respective system change forms / tickets.

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.

Document Reference No.: RA-TPA-31015640-2021-22-R77