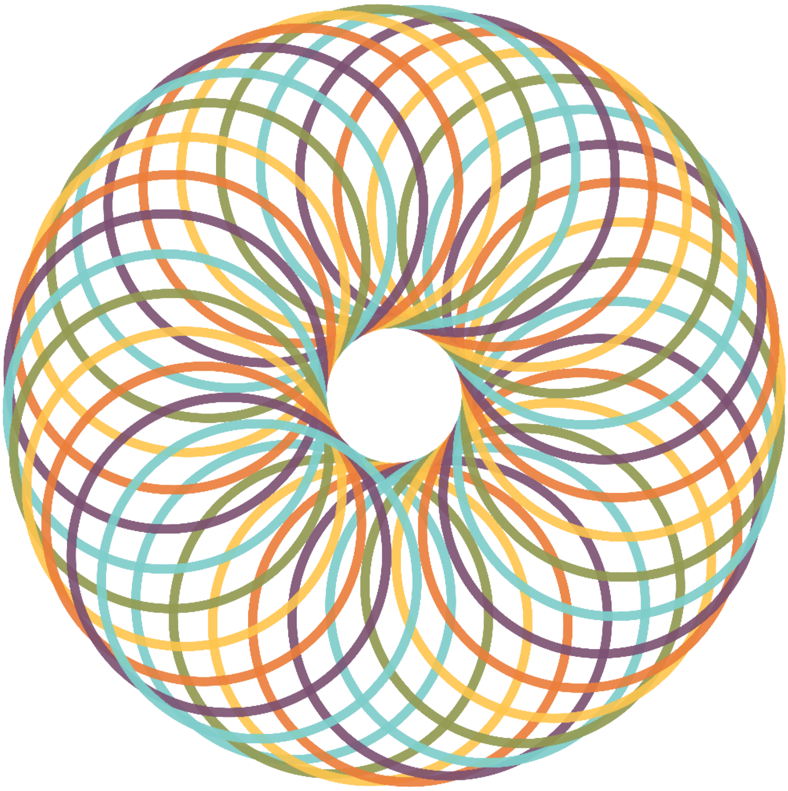
NOTICE

You and your company have obtained access to this report dated December 21, 2024, on services related to Application development, Production Support and the related General Information Technology Controls hosted in datacenters located in USA for the services performed by Deloitte Haskins & Sells LLP (“DHSLLP”) as agreed with Zoho Corportion Private Limited (herein referred to as "Zoho" or “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 any one including Recipient who may obtain this Report.

DHSLLP, 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 (SOC 2 Type 2) on the Description of system of Zoho related to Application Development, Production Support and the related General Information Technology Controls hosted in datacenter located in USA for the services provided to customers relevant to Security, Availability, Confidentiality, Processing Integrity and Privacy and Suitability of the Design and Operating Effectiveness of controls for the period from December 01, 2023 through September 30, 2024

This report is intended solely for the information and use of Zoho Corporation Private Limited, its 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 Auditor’s Report

Deloitte
Haskins & Sells LLP

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

Tel: +91 44 66885000

Section 1. Independent Service Auditor's Report

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

To the Management of Zoho Corporation Private Limited

Scope

We have examined the description of the system of Management of Zoho Corporation Private Limited (the "Service Organization" or "Company" or "Zoho") related to Application development, Production Support and the related General Information Technology Controls hosted in datacenters located in USA for the services provided to customers ("User entities" or "User Organizations" or "Clients"), from Zoho locations ("Facilities") located at Chennai, Tenkasi and Renigunta in India and Austin in United States of America included in Section 3 "Management of Zoho's Description of Its System" throughout the period from December 01, 2023 through September 30, 2024 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period December 01, 2023 through September 30, 2024, to provide reasonable assurance that Zoho's service commitments and system requirements would be 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 in AICPA Trust Services Criteria.

Zoho uses Sabey Data Center Properties LLC, Databank Holdings Limited for Datacenter Co-Location Services in USA ("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 service 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 extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization’s Responsibilities

Management of 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 would be achieved. Management of Zoho has provided the accompanying assertion in Section 2 titled “Management of Zoho’s Assertion” (the “Assertion”) about the Description and the suitability of design and operating effectiveness of controls stated therein. Management of 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 Auditor’s 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 (AICPA). Those standards require that we plan and perform the 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 Zoho’s service commitments and system requirements would be 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 service organization’s service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the Description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that Zoho 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.

Service Auditor's Independence and Quality Control

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

Inherent Limitations

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of 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 tested, and the nature, timing, and results of those tests are listed in Section 4, "Management of Zoho's Description of Its Relevant Criteria and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results."

Opinion

In our opinion, in all material respects,

a. The Description presents Zoho's system for the Application Development, Production Support and the related General Information Technology Controls that was designed and implemented throughout the period December 01, 2023 to September 30, 2024 in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period December 01, 2023 to September 30, 2024 to provide reasonable assurance that Zoho's service commitments and systems requirements would be achieved based on the applicable trust services criteria, if its 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, 2023 to September 30, 2024, to provide reasonable assurance that Zoho's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organizations and user entities applied the complementary 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 Management of Zoho, user entities of Zoho's system related to Application Development, Production Support and the General Information Technology Controls during some or all of the period December 01, 2023 to September 30, 2024, 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 Zoho.
- How Zoho’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 Zoho to achieve Zoho’s commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use Zoho's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of Zoho’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. 029935

December 21, 2024

SECTION - 2

Management of Zoho’s Assertion

Section 2. Management of Zoho's Assertion

Management of Zoho Corporation Private Limited's Assertion

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

The signed Management assertion has been provided by Management of Zoho Corporation Private Limited via letter dated December 21, 2024. The extract of the letter is as under:

We have prepared the description of the system of Management of Zoho Corporation Private Limited (the "Service Organization" or "Company" or "Zoho") related to Application development, Production Support and the related General Information Technology Controls hosted in datacenters located in USA for the services provided to customer ("User entities" or "User Organizations" or "Clients"), from Zoho locations ("Facilities") located at Chennai, Tenkasi and Renigunta in India and Austin in United States of America included in Section 3 "Management of Zoho's Description of Its System" throughout the period from December 01, 2023 through September 30, 2024 (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 in AICPA Description Criteria ("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, in AICPA Trust Services Criteria.

Zoho uses Sabey Data Center Properties LLC, Databank Holdings Limited for Datacenter Co-Location Services in USA ("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 does not extend to controls of the subservice organizations.

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. The Description does not extend to controls of the user entities.

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, 2023 to September 30, 2024 in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period December 01, 2023 to September 30, 2024, 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 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, 2023 to September 30, 2024 to provide reasonable assurance that Zoho's service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organizations and user entities applied the complementary 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: December 21, 2024

SECTION - 3
Management of Zoho’s Description of its System

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

3.1 Zoho Business Overview

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

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

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

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

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

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

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

System Overview

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

Zoho has established an internal controls framework that reflects:

- The overall control environment within the organization and its various processes
- The Risk Assessment procedure
- 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.

3.2 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 Customer Support team. The team coordinates with Product teams to resolve reported issues.

c. Server Operations and NOC team

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

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

d. Sysadmin team

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

e. Compliance team

The Compliance team is responsible for 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:

Product Name	Product Category	Product Description	Product Scale	Division
Zoho CRM	Sales and Marketing	Zoho CRM is a cloud-based CRM system that helps manage and streamline sales, marketing, and customer support activities, all in one single platform.	High	Zoho
Zoho SalesIQ	Sales and Marketing	Zoho SalesIQ offers marketing, sales, and support teams digital customer engagement tools to communicate with site visitors at every stage of the customer lifecycle.	High	Zoho
Zoho Forms	Sales and Marketing	Zoho Forms is an online no-code platform to build forms for lead generation, customer engagement and other business needs.	Medium	Zoho
Zoho Bigin	Sales and Marketing	Zoho Bigin is a pipeline management and CRM solution for small business.	Medium	Zoho
Zoho Bookings	Sales and Marketing	Zoho Bookings is an online appointment scheduling software that syncs calendars while letting customers self-schedule and pay for appointments.	Low	Zoho
Zoho CRM Plus	Sales and Marketing	Zoho CRM Plus is a unified customer experience platform that helps deliver an exceptional experience to every customer, across all stages of their lifecycle, and helps convert them into brand advocates.	High	Zoho
Zoho Campaigns	Sales and Marketing	Zoho Campaigns helps customers meet their email marketing needs by helping with responsive design creation, message customization, delivery of	High	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
		emails to inboxes, and triggering of automated workflows.		
Zoho Backstage	Marketing	Zoho Backstage is an event management software that empowers event organizers to plan and run conferences, meetups, and product launches with greater efficiency and impact.	Low	Zoho
Zoho Social	Marketing	Zoho Social allows users to schedule unlimited social media posts, monitor what performance, and create custom-reports to analyze further.	Medium	Zoho
Zoho Survey	Marketing	Zoho Survey allows users to easily create surveys, reach audiences across devices, and view results graphically and in real-time.	Medium	Zoho
Zoho Commerce	Marketing	Zoho Commerce contains all the tools needed to build a website, accept orders, track inventory, process payments, manage shipping, market the brand, and analyze data.	Low	Zoho
Zoho Meeting and Zoho Webinar	Marketing	Zoho Meeting is a secure online meeting platform and webinar solution that helps people find new ways to collaborate and efficiently work remotely. Zoho Webinar provides a secure platform for managing and webcasting online webinars.	Medium	Zoho
Zoho Marketplace	Marketing	Zoho Marketplace provides online extensions across 40+ categories, allowing users to connect third-party business	Low	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
		tools with the Zoho products they already use.		
Zoho Marketing Plus	Marketing	Zoho Marketing Plus unifies all marketing activities onto one platform. It helps engage audiences across multiple channels, helps increase marketing spend ROI, and optimizes team productivity.	High	Zoho
Zoho Sites	Marketing	Zoho Sites helps users build professional websites quickly.	Medium	Zoho
Zoho Pagesense	Marketing	Zoho Pagesene helps optimize web pages for better engagement and conversion.	Medium	Zoho
Zoho Marketing Automation	Marketing	Zoho Marketing Automation is an all-in-one marketing automation software that helps successfully manage marketing activities across multiple channels.	Low	Zoho
Zoho Assist	Help Desk	Zoho Assist is a tool to troubleshoot customer issues remotely for quick resolutions.	Low	Zoho
Zoho Desk	Help Desk	Zoho Desk is a ticket management software that helps support customers across multiple channels from one central tool.	High	Zoho
Zoho Lens	Help Desk	Zoho Lens helps train, troubleshoot, and collaborate with AR tech.	Low	Zoho
Zoho Books	Finance	Zoho Books is an online accounting software that manages your finances, keeps users GST compliant, automates business workflows, and helps users	High	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
		collaborate across departments.		
Zoho Invoice	Finance	Zoho Invoice is an online invoicing software that helps craft professional invoices, send payment reminders, keep track of expenses, log work hours, and get paid faster	Medium	Zoho
Zoho Expense	Finance	Zoho Expense turns receipts into expense reports for quick approval.	Medium	Zoho
Zoho Inventory	Finance	Zoho Inventory is an inventory management software to manage orders, track inventory, handle GST billing, oversee warehouses and run all inventory operations.	Medium	Zoho
Zoho Billing	Finance	Zoho Billing helps automate recurring billing, manage subscriptions, send professional GST-compliant invoices, and get timely payments.	Medium	Zoho
Zoho Checkout	Finance	Zoho Checkout is an online tool that helps quickly build custom, branded payment pages.	Medium	Zoho
Zoho Payroll	Finance	Zoho Payroll helps process an organization's payroll quickly and pay employees in a timely manner.	Low	Zoho
Zoho People	People and Culture	Zoho People is a HR management system for managing employees and their hiring, onboarding, attendance, schedules, and appraisals	Low	Zoho
Zoho Recruit	People and Culture	Zoho Recruit is a cloud based applicant tracking system	Medium	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
		built to provide diverse, end-to-end hiring solutions for staffing agencies, corporate HRs and temporary workforce.		
Zoho Shifts	People and Culture	Zoho Shifts is a dedicated shift scheduling tool to draft work schedules, track team hours, and communicate with employees across devices.	Low	Zoho
Zoho Connect	People and Culture	Zoho Connect is a private social networking system for team discussions and sharing resources.	High	Zoho
Zoho Creator	Customer Solutions	Zoho Creator is a low-code platform to turn unique business processes into custom applications.	High	Zoho
Zoho Vault	Information Technology(IT)	Zoho Vault is a secure password manager that safely manages passwords and auto-fills them across websites and applications.	Medium	Zoho
Zoho Catalyst	Information Technology(IT)	Zoho Catalyst is a scalable serverless platform that allows developers to build and deploy world-class solutions without managing servers.	Medium	Zoho
Zoho Workerly	People and Culture	Zoho Workerly is an employee scheduling software that enables agencies to manage their client and temp database, schedule jobs based on client requirements, generate timesheets, and send out invoices, all from a single interface.	Low	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
Zoho Contracts	Information Technology(IT)	Zoho Contracts is a comprehensive contract life cycle management software.	Low	Zoho
Zoho Flow	Information Technology(IT)	Zoho Flow is an online tool to visually build integrations between apps, and automate business workflows.	Low	Zoho
ManageEngine Site24x7	Application Monitoring	Site24x7 is a cloud infrastructure monitoring service that helps monitor the uptime and performance of websites, online applications, servers, mobile websites, and custom APIs.	High	ManageEngine
Zoho Office Integrator	Customer Solution	Zoho Office Integrator is a built-in document editor for web apps.	Low	Zoho
Zoho Gadgets	Customer Solution	Zoho Gadgets acts as a single point of management for third-party integrations, helps avoid duplicate features, and enables adherence to the best integration practices across all Zoho products.	Low	Zoho
Zoho Sigma	Customer Solution	Zoho Sigma is an extension development platform where developers can build and host extensions for various Zoho applications.	Low	Zoho
Zoho Analytics	Business Intelligence (BI) & Analytics	Zoho Analytics is a BI and analytics platform that helps users get insights into every aspect of their business.	High	Zoho
Zoho Dataprep	Business Intelligence (BI) & Analytics	Zoho DataPrep is an augmented self-service data preparation and pipeline service to connect, explore, transform, and enrich data for analytics, machine	Medium	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
		learning, migration, and data warehousing.		
Zoho Notebook	Email & Office	Zoho Notebook is a digital notebook that allows users to capture, organize, and collaborate on their notes, documents, and projects.	Low	Zoho
Zoho ToDo	Email & Office	Zoho ToDo is a task management tool designed to help individuals and teams stay organized by helping manage tasks, deadlines, and workflows.	Low	Zoho
ZeptoMail	Email & Office	ZeptoMail is a secure and reliable transactional email sending service that ensures timely delivery of important emails such as password reset, OTPs, welcome emails and so on.	Medium	Zoho
Zoho Writer	Email & Office	Zoho Writer is a word processor tool available across devices that allows users to create documents in a clean interface and collaborate with teammates in real-time.	High	Zoho
Zoho Calendar	Email & Office	Zoho Calendar is a cloud-based online calendar application that helps users with scheduling, syncing, and sharing of calendars.	Low	Zoho
Zoho Mail	Email & Office	Zoho Mail is a secure, encrypted, privacy-guaranteed, and ad-free email hosting service for businesses.	High	Zoho
Zoho Show	Email & Office	Zoho Show is an online presentation software that allows users to design professional slides,	Medium	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
		collaborate with teammates, and deliver visually engaging presentations		
Zoho Learn	Email & Office	Zoho Learn is an online learning management platform to create, manage, and share organizational knowledge, curate training programs, and analyze training performance.	Low	Zoho
Zoho Sheet	Email & Office	Zoho Sheet is a cloud-based spreadsheet tool that lets users to create, edit, and share data with teammates in real-time.	High	Zoho
Zoho Sprints	Project Management	Zoho Sprints is a cloud-based Agile project management application for scrum teams.	Low	Zoho
Zoho Projects and BugTracker	Project Management	Zoho Projects is a cloud-based project management software that helps users plan projects, track work efficiently, and collaborate with teammates. Zoho Bugtracker is an automatic tool for tracking and managing bugs.	High	Zoho
Zoho Workdrive	Collaboration	Zoho WorkDrive is a secure cloud storage and online file sharing platform that lets users store, share, and collaborate on documents across devices.	High	Zoho
Zoho Cliq	Collaboration	Zoho Cliq is a secure and private team chat platform that lets user stay connected with their workplace.	High	Zoho
Zoho Voice	Collaboration	Zoho Voice is a cloud-based VOIP and telephony service for businesses.	Medium	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
Zoho Sign	Collaboration	Zoho Sign is an online tool to create, digitally sign, and manage documents easily and securely.	Low	Zoho
Zoho Workplace	Email & Office	Zoho Workplace is an enterprise productivity and collaboration suite that brings together multiple Zoho products into one unified platform.	Medium	Zoho
Zoho One and Directory	Email & Office	Zoho One is an online all-in-one business management software that offers solutions for user management, project management, organization, sales, marketing, and accounting, with centralized administration and provisioning. Zoho Directory is a platform that secures identity and access with single sign-on, multi-factor authentication, & access management.	High	Zoho
Zoho Graphikos	Email & Office	Zoho Graphikos is a suite of online services (Zoho Show, Nila, Vani, and Whiteboard) and mobile/desktop/TV apps which are used to create, render and deliver graphical objects.	High	Zoho
Zoho TeamInbox	Email & Office	Zoho TeamInbox is a shared inbox tool that allows users to create common shared inboxes for their teams, and allows users to collaborate, organize, and automate conversations in a single place workspace.	Low	Zoho

Product Name	Product Category	Product Description	Product Scale	Division
Zoho LandingPage	Marketing	Zoho LandingPage is a user-friendly, no-code solution that helps users create responsive landing pages.	Medium	Zoho
Zoho Thrive	Marketing	Zoho Thrive is a unified platform to build and run affiliate and loyalty programs. It helps create brand awareness, increase engagement rates, and build stronger customer relationships.	Low	Zoho
Zoho Apptics went live in June '24	Information Technology(IT)	Zoho Apptics is an end-to-end product analytics solution used by developers, marketers, and product owners to optimize and enhance their products.	Medium	Zoho
Zoho Tables went live in March '24	Email & Office	Zoho Tables is a work management software that helps plan and track work efficiently, organize and visualize data, collaborate contextually, and streamline workflows.	Medium	Zoho
Zoho RPA went live in May '24	Robotic Process Automation	Zoho RPA is a robotic process workflow automation tool that can be used to automate manual, repetitive and rule-based tasks.	Medium	Zoho
Ulaa Browser	Enterprise Browser	Ulaa is a web browser that respects user privacy, protects data, and enhances online work productivity.	Medium	Zoho
ManageEngine ServiceDesk Plus(Cloud)	Enterprise and IT Management	ManageEngine ServiceDesk Plus Cloud is an online comprehensive helpdesk and asset management software that provides helpdesk agents and IT managers an integrated console to	High	ManageEngine

Product Name	Product Category	Product Description	Product Scale	Division
		monitor and maintain the assets and IT requests generated by users in the organization.		
ManageEngine Identity360	Identity Governance and Administration	ManageEngine Identity360 empowers organizations with powerful IAM capabilities to manage and secure identities.	Low	ManageEngine
ManageEngine Log360 Cloud	Security Information Event Management and User Entity Behavior Analysis	ManageEngine Log360 Cloud is a cloud-based SIEM solution that helps protect organizations from cyberattacks using security analytics, threat detection, and compliance management.	High	ManageEngine
ManageEngine Remote Access Plus Cloud	Endpoint Management	Remote Access Plus Cloud is a remote access software for enterprises that helps system administrators and IT help desk technicians troubleshoot remote computers from a central location.	Medium	ManageEngine
ManageEngine Remote Access Plus Cloud	Endpoint Management	Patch Manager Plus Cloud is an all-round patching solution, offering automated patch deployment for Windows, macOS, and Linux endpoints.	Medium	ManageEngine
ManageEngine Endpoint Central Cloud	Endpoint Management	Endpoint Central Cloud is a unified endpoint management (UEM) cloud solution that helps manage servers, laptops, desktops, smartphones, and tablets from a central location.	High	ManageEngine
Qntrl	Workflow Automation	Qntrl is a workflow orchestration platform to design, automate, and	Medium	Qntrl

Product Name	Product Category	Product Description	Product Scale	Division
		analyze all business processes.		
Zakya	Point of Sale (POS) Solution	Zakya is a cloud-based POS software for retail businesses in India, which helps efficiently manage inventory, sales, vendors, payments, and e-commerce.	Medium	Zakya
TrainerCentral	Training	TrainerCentral is a no-code platform that helps design, market, and manage an online training business.	Medium	TrainerCentral
ChARMHealth	Healthcare IT	ChARMHealth is a cloud-based EHR, practice management, and medical billing solution that helps healthcare organizations function efficiently.	Medium	MedicalMine
ManageEngine CloudDNS	DNS and DHCP management	ManageEngine CloudDNS is a DNS Management tool that optimizes domain performance and real-time monitoring.	Medium	ManageEngine

3.3 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
Availability: 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 Terms of Service / Master Service Agreement. 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. Zoho undertakes to acknowledge and resolve Service Defects reported by the user entities as per the agreed timelines.	CA58: Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho. CA76: Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team. CA112: IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days. CA113: Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness. CA134: Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.
Privacy: Zoho ensures to maintain security, confidentiality, processing integrity and privacy of Client's/User Entities' data as committed in the Privacy Policy. 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.	CA61: Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis. CA135: Members of the privacy staff verify that the entity has legal grounds to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, on a periodic basis, the privacy team verify that the entity has requested and received explicit written consent from the data subjects, when such consent is required. CA148: The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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

Principal Commitments and Requirements	Related Controls
	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. CA103: Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application. CA105: Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis. CA151: The use of personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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. CA153: The Data Subject Access Request policy of Zoho is defined by the Privacy team and is reviewed and approved annually by the Director of Compliance. The policy document defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. CA140: Management Review Meeting is performed for Privacy team Zoho on an annual basis 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. CA155: Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines the purpose and use of the collection of personal information, including detailed use, ability to

Principal Commitments and Requirements	Related Controls
	optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information. CA157: The privacy team establishes a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements. This document is reviewed and approved annually by the Director of Compliance. The document defines the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.
Security: 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. 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.	CA02: Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates. CA08: For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action. CA07: For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining. CA09: For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People. CA14: For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining. CA15: For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date. CA21: Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance. CA20: Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry. CA26: Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.

Principal Commitments and Requirements	Related Controls
	CA27: Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days. CA39: Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified. CA54: Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used. CA85: Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure. CA93: Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified. CA130: Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.
Processing Integrity: Zoho is committed to process the data pertaining to the services offered to the user entity completely, accurately and in a timely manner in accordance with system specifications to meet the entity's objectives.	CA76: Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team. CA68: Product description and terms of use for Zoho Cloud products is published in company's website. CA103: Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
Confidentiality: Zoho is responsible for maintaining non-disclosure agreement with the parties that would address the confidentiality of Customer's information in connection with the provision of the services by Zoho to its Customers.	CA09: For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People. CA07: For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining. CA147: The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.

3.4 Boundaries of the System

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

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

   - Corporate website refers to Zoho's corporate websites - www.zoho.com which is publicly accessible via the internet.
   - International Datacenter (IDC) infrastructure refers to servers, databases and network devices hosted in datacenters located in USA. Only the servers and products hosted through the USA data centers is covered in the scope of this report. The datacenters in USA are hosted through colocation providers. The physical and environmental controls in the data centers are managed by the outsourced service providers.
   - Production environment refers to servers within the IDC infrastructure used to support the production instances of products.
   - IDC Access network along with Zero Trust security is used to restrict logical access to the IDC infrastructure from Zoho Development centers.
   - 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 Server Operations team, NOC Team Members and Sysadmin teams.
   - 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.
   - The infrastructure of Zoho includes database and servers pertaining to the in-scope applications. The firewalls and Intrusion Prevention System ('IPS') which are configured in the perimeter firewall and Vulnerability assessment and penetration testing is performed by Zoho. The in-scope applications are primarily supported by operating system (Unix) and database (SQL)

b. Software - 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. The criteria 'processing integrity' pertaining to the in-scope applications is covered through the relevant IT controls that are responsible for the processing of transactions completely, accurately and on a timely basis. Product functionality, including automated controls configured to process clients' business transactions completely and accurately do not form part of the assessment scope of this report.

c. 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 include the Admin Team, Legal team, Server Operations (Server Operations

Team) Team, Network Operations Centre (NOC) team, physical security, system administration, and HR Team.

d. 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.

e. Data – The Backup of Zoho's IDC servers data taken via ZAC tool and stored in Zoho Datacenters for SaaS products. Basis the request from customer restoration of data is performed by the Zoho Server Operations team.

3.5 Control Environment Elements

3.5.1 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
    - Security and Privacy Awareness Training

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.

3.5.2 Commitment to Competence

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

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

3.5.3 Management’s Philosophy and Operating Style

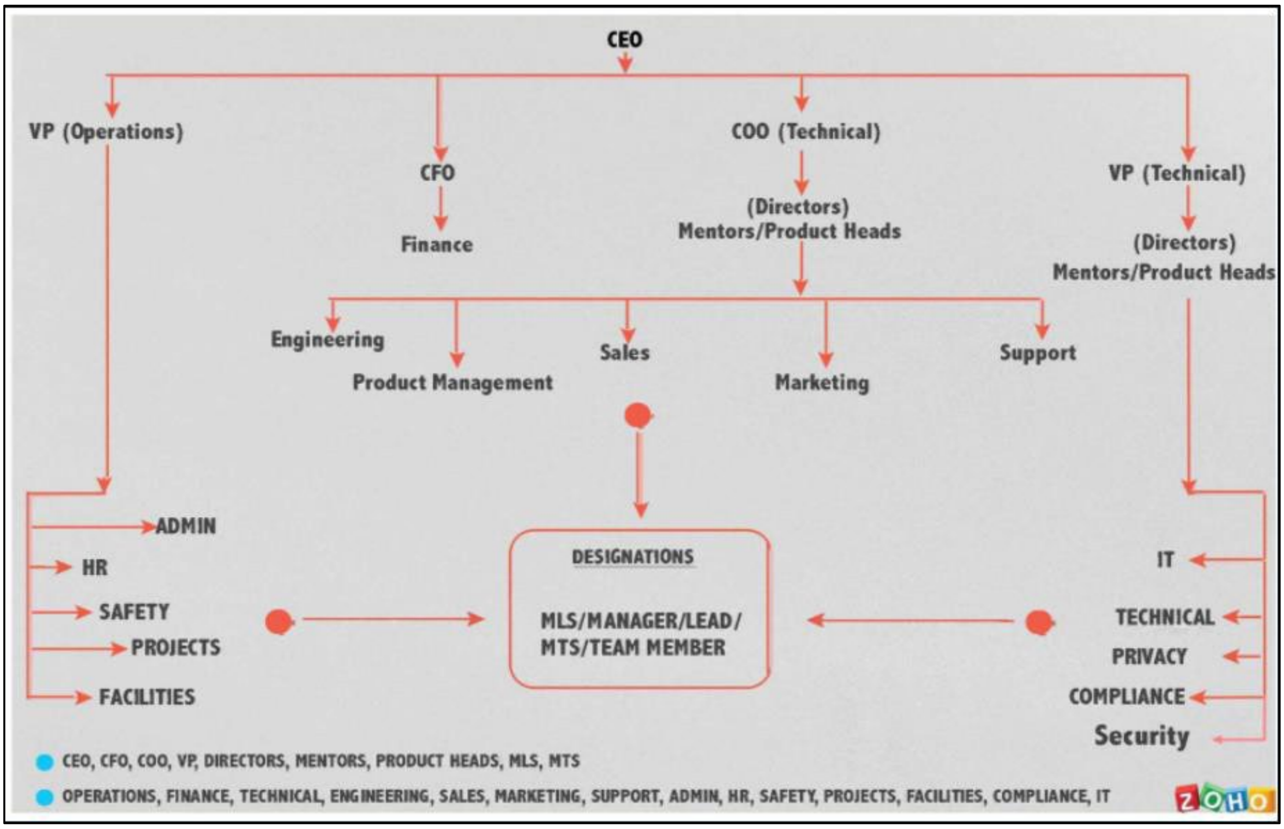
Zoho Management’s philosophy and operating style encompass a broad range of characteristics including Management’s approach to taking and monitoring business risks, and Management’s attitudes toward information processing, accounting functions, and personnel. Specific control activities that Zoho has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

3.5.4 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.



3.5.5 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.

3.5.6 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 - 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.

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

Role	Responsibility and Authority
	- 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. - To monitor compliance with this the applicable data protection laws, and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. - To provide advice were requested as regards the data protection impact assessment and monitor its performance - To cooperate with the supervisory/data protection regulatory authorities - To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation of certain types of processing of personally identifiable information(as maybe required by the laws) and to consult, where appropriate, with regard to any other matter related to it.
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.

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

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

3.5.7 Human Resource Policies and Practices

Zoho has defined policies and procedures on the intranet portal consisting of 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.

3.6 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.

3.7 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 associates during the induction program.

3.8 Monitoring

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

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

3.9 Process and controls

Human Resource

HR policies and processes:

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

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

Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.

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

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

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

Hiring and Termination Process:

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

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

For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People. For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn. For associates joining Zoho, the HR team enters the joining date in Zoho people.

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

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

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

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

For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.

Physical and Environmental Security:

Physical Access Management:

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

Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.

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

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

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

The access to Server Operations Team and NOC room is restricted to Server Operations Team and NOC team members.

For revocation of access to Server Operations Team and NOC room, the request is raised in Zoho SDP. Admin team revokes physical access to Server Operations Team and NOC room for the associate. For associates leaving from Zoho, the physical access to Server Operations Team and NOC room is revoked on the associate's last working date.

Access to Server Operations Team and NOC room of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any).

Access to Facilities of Zoho (at Chennai, Tenkasi and Renigunta.) is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)

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

Environmental Security:

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

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

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

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

- Cooling system
- UPS
- DG
- Fire suppression system

System Administration:

Endpoint Security:

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

Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.

Zoho uses Manage Engine Mobile Device Management (MDM solution developed by Zoho) to manage the endpoints and enabling remote data wipe.

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

Workstations of Zoho are blocked from disabling CrowdStrike.

Workstations of Zoho uses encryption software to encrypt the disk.

Local Admin Rights is restricted for Zoho workstations.

Access to removable device is restricted for Zoho workstations.

Server Security:

Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.

For newly onboarded corporate servers and network device the hardening checklist is maintained by the respective team.

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

Corporate servers of Zoho are blocked from mounting removable storage media device.

Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.

Authentication and Asset Management:

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

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

Passman tool is inhouse developed password management application of Zoho. For creation of access to corporate server of Zoho, the request is raised by the user (in SDP tool). System administration team creates access to passman for the associate based on the approval provided by System Administration Manager.

For revocation of access to corporate jump server of Linux based corporate server of Zoho, the request is raised in Zoho SDP. System administration team revokes access to jump server for the associate. For associates leaving from Zoho, the access to jump server is revoked on the associate's last working date.

Access to passman is reviewed by the System administration team on an annual basis. The review of the access to passman is recorded in RACI (Responsible, Accountable, Consulted, and Informed) sheet. Corrective action is performed by System administration team for discrepancies identified (if any).

Access to corporate jump server is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).

For associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho is revoked based on the integration with Zoho People.

Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.

System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.

Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option. IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any)

Compliance:

Compliance and Risk Management:

Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.

Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis.

The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.

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

The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.

Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.

Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.

Business Continuity Management:

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

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

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

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

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

Product Specific Processes:

Risk assessment for the products of Zoho on information security and privacy is performed an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.

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

Product description and terms of use for Zoho Cloud products is published in company's website.

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

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

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

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

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

Network Operations:

Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.

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

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

For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.

Access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is reviewed by the Network Operations team on an Annual basis. Corrective action is performed by Network Operations team for discrepancies identified (if any).

Administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is restricted to NOC engineers.

Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.

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

Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.

Business continuity test is performed for NOC room on an annual basis by Network Operations team. All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.

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

Network Operations team changes network device configuration based on approval provided by Network Operations Manager.

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

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

MAC Binding is implemented for workstation connecting from NOC room to IDC network.

Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.

Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.

Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server.

The Network time protocol server fetch time from authorized time sync source. Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.

Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool. The network traffic from malicious source are blocked by the third party tool.

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

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

Server Operations:

Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.

IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.

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

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

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

For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People. Administrative access to Server Operation tools (ZAC and Server Operations Passman) of Zoho is restricted to Server Operations Team.

Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.

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

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

Server Operations team has implemented load balancers for IDC servers.

IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.

IDC servers of Zoho are restricted from accessing internet.

IDC servers of Zoho are blocked from mounting removable device.

Zoho Server Operations team maintains an asset registry of the IDC Servers.

Zoho uses asset discovery tool to identify and track the servers added in IDC network. Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.

Security:

Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used.

For creation of access to Key management service tool of Zoho, the request is raised in Email. EAR (Encryption at rest) team lead creates access to KMS tool for the associate based on the approval provided by EAR team manager.

For associates leaving Zoho, the access to Key management service tool is revoked based on the integration with Zoho People.

For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.

For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.

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

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

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

The attachments of email sent to Zoho domain are scanned for malware content. The emails are quarantined if anomalies identified.

The logs for just in time access are recorded and stored in Zero trust application.

Server Operations has defined list of sensitive commands executions in IDC servers of Zoho. The list of sensitive commands are reviewed and approved by Server Operations Manager on an annual basis.

Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.

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

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

Customer Support:

Customer Support process document of Zoho is defined by the Zoho customer support team. The document is reviewed and approved by Director of customer support team on an annual basis. The document defines the support process for Zoho products.

Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team.

Legal:

Master service agreement is signed between Zoho and third party vendor. Any changes to the contracts are agreed by Zoho and the third party vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses. Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.

Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis.

Privacy:

Policy and Notice:

The privacy policy of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The policy outlines the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.

Procedure for data subject correction request in Zoho is defined by privacy team. The policy document is reviewed and approved by Director of IT on an annual basis.

The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.

The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following:

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.

Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following:

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

Procedure to determine if explicit consent is required is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The policy defines the procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent and procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.

<u>Collection:</u>

Privacy team maintains inventory of data collected from the data subjects. The inventory is reviewed on an annual basis by Privacy team to ensure the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.

The policy for choice and consent is defined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following:

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 definition of sensitive personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The use of personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following:

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.

Procedure for personal information retention is defined as part of privacy policy by the legal team. The policy document is reviewed and approved by the General Counsel on an annual basis. The policy covers the following:

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.

The Data Subject Access Request policy of Zoho is defined by the Privacy team and is reviewed and approved annually by the Director of Compliance. The policy document 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 privacy team establishes a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements. This document is reviewed and approved annually by the Director of Compliance. The document defines the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.

Disclosure:

Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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.

Zoho provides data subjects with 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.

For new/changes made to consent process, the business unit personnel obtains approval from Director of Compliance (DOC) before implementing the change. 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.

For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects. Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.

Incident Management and Monitoring:

Privacy team reviews the complaints related to privacy raised to Zoho against unfair or unlawful practices. Members of the privacy staff verify that the entity has legal grounds to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, on a periodic basis, the privacy team verify that the entity has requested and received explicit written consent from the data subjects, when such consent is required.

On an annual basis, Director of Compliance (DOC) reviews cases relating to request raised by data subjects for disagreements over the accuracy of personal data and validate the appropriate justifications provided thereof.

On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof. Privacy team maintains list of sub processors and third party vendors in Zoho.

Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.

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

Procedure to determine PIA requirement is defined by Privacy team. The procedure document is reviewed and approved by Director of Compliance on an annual basis.

Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.

3.10 Trust Services Criteria and Description of Related Controls

3.10.1 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
CA01	Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.
CA02	Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.
CA03	Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.
CA04	Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information,

Control Activity Number	Control Activities
	legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.
CA05	Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.
CA06	Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.
CA07	For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA08	For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA55	Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.
CA57	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA59	Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA77	Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.
CA104	Disciplinary complaints (if any) are raised to Zoho's HR team for appropriate action as per Zoho Disciplinary action policy.

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
CA30	Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.
CA31	Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.
CA33	Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.

Control Number	Activity	Control Activities
CA55		Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.
CA56		Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.
CA57		Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA59		Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA60		Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.
CA61		Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.
CA77		Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.
CA104		Disciplinary complaints (if any) are raised to Zoho's HR team for appropriate action as per Zoho Disciplinary action policy.

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

Control Number	Activity	Control Activities
CA01		Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.
CA03		Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.
CA06		Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.
CA30		Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.

Control Number	Activity	Control Activities
CA31		Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.
CA33		Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.
CA55		Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.
CA57		Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA59		Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA101		Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.
CA104		Disciplinary complaints (if any) are raised to Zoho’s HR team for appropriate action as per Zoho Disciplinary action policy.
CA145		The privacy policy of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The policy outlines the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.
CA148		The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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.

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
CA02	Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.
CA03	Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.
CA04	Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.
CA05	Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.
CA07	For associates joining Zoho, Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA08	For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA09	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA10	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA18	For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.

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

Control Number	Activity	Control Activities
CA03		Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.
CA07		For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA18		For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.
CA56		Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.
CA104		Disciplinary complaints (if any) are raised to Zoho's HR team for appropriate action as per Zoho Disciplinary action policy.

3.10.2 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 Number	Activity	Control Activities
CA01		Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.
CA02		Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.
CA06		Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.
CA08		For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA11		For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.
CA12		For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.
CA13		For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for

Control Number	Activity	Control Activities
		the new card based on the automatic email triggered from Zoho People on the date of request.
CA18		For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.
CA34		Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.
CA44		Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA98		Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA99		Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.
CA106		Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.
CA107		For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.
CA108		For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.
CA109		For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.
CA114		For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.
CA115		For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.
CA118		For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.
CA119		For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.
CA124		IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA127		Zoho Server Operations team maintains an asset registry of the IDC Servers.
CA128		Zoho uses asset discovery tool to identify and track the servers added in IDC network.

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
CA03	Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.
CA04	Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.
CA05	Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.
CA07	For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA09	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA10	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA47	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA110	The logs for just in time access are recorded and stored in Zero trust application.

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

Control Number	Activity	Control Activities
CA04		Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.
CA05		Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.
CA47		Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52		Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA62		Master service agreement is signed between Zoho and third party vendor. Any changes to the contracts are agreed by Zoho and the third party vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA70		Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.
CA75		Customer Support process document of Zoho is defined by the Zoho customer support team. The document is reviewed and approved by Director of customer support team on an annual basis. The document defines the support process for Zoho products.
CA76		Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team.
CA102		Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA103		Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA104		Disciplinary complaints (if any) are raised to Zoho's HR team for appropriate action as per Zoho Disciplinary action policy.
CA154		Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following: 1. readily accessible and made available to the data subject. 2. Provided in a timely manner to the data subjects

Control Number	Activity	Control Activities
		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

3.10.3 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 Number	Activity	Control Activities
CA04		Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.
CA07		For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA08		For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA09		For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA10		For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA47		Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52		Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA55		Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.
CA56		Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.

Control Number	Activity	Control Activities
CA57		Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA59		Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA60		Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.
CA61		Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.
CA77		Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.
CA141		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.

CC3.2: 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 Number	Activity	Control Activities
CA38		System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.
CA56		Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.
CA58		Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA89		Business continuity test is performed for NOC room on an annual basis by Network Operations team.
CA101		Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.

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
CA34	Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.
CA60	Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.
CA61	Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.
CA62	Master service agreement is signed between Zoho and third party vendor. Any changes to the contracts are agreed by Zoho and the third party vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA79	Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.
CA99	Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.
CA102	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA127	Zoho Server Operations team maintains an asset registry of the IDC Servers.

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
CA34	Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.
CA44	Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA69	Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.
CA72	Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.
CA73	Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the

Control Number	Activity	Control Activities
		changes are deployed in production environment/publishing in website with blocking issue.
CA79		Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.
CA98		Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA109		For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.
CA121		Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA123		Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.
CA124		IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA129		Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.
CA131		Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.

3.10.4 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 Number	Activity	Control Activities
CA44		Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA47		Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52		Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA55		Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.
CA56		Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security

Control Number	Activity	Control Activities
		Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.
CA60		Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.
CA61		Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.
CA62		Master service agreement is signed between Zoho and third party vendor. Any changes to the contracts are agreed by Zoho and the third party vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA82		Access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is reviewed by the Network Operations team on an Annual basis. Corrective action is performed by Network Operations team for discrepancies identified (if any)
CA98		Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA101		Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.
CA102		Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA103		Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA106		Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.
CA112		IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA124		IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA133		Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.
CA145		The privacy policy of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The policy outlines the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.
CA148		The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 1. Notification of a mechanism to opt-out of the collection and use of their personal

Control Number	Activity	Control Activities
		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.

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 Number	Activity	Control Activities
CA59		Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA97		Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.
CA141		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.

3.10.5 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 Number	Activity	Control Activities
CA06		Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.
CA09		For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA10		For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA33		Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.
CA35		For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team.

Control Number	Activity	Control Activities
CA54		Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used.
CA55		Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.
CA56		Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.
CA57		Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA58		Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA59		Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA69		Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.
CA71		Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.
CA72		Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.
CA73		Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.
CA77		Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.
CA78		Servers onboarded in IDC network are hardened using standard image by server operations team.
CA79		Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.

Control Number	Activity	Control Activities
CA86		Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA88		Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA89		Business continuity test is performed for NOC room on an annual basis by Network Operations team.
CA90		All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.
CA93		Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.
CA96		Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.
CA99		Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.
CA101		Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.
CA116		Administrative access to Jump Server of Zoho is restricted to Server Operations team.
CA120		Administrative access to Server Operation tools (ZAC and Server Operations Passman) of Zoho is restricted to Server Operations Team.
CA122		Server Operations team has implemented load balancers for IDC servers.
CA125		IDC servers of Zoho are restricted from accessing internet.
CA127		Zoho Server Operations team maintains an asset registry of the IDC Servers.
CA128		Zoho uses asset discovery tool to identify and track the servers added in IDC network.
CA133		Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.
CA145		The privacy policy of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The policy outlines the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.
CA148		The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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.

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

Control Number	Activity	Control Activities
CA11		For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.
CA12		For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.
CA13		For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.
CA14		For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining
CA15		For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date
CA16		For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.
CA17		For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.
CA30		Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.
CA31		Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.
CA32		Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.
CA35		For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team.
CA36		The attachments of email sent to Zoho domain are scanned for malware content. The emails are quarantined if anomalies identified.
CA40		Workstations of Zoho are blocked from disabling CrowdStrike.
CA41		Workstations of Zoho uses encryption software to encrypt the disk.
CA45		For creation of access to corporate server of Zoho, the request is raised by the user. System administration team creates access to passman for the associate based on the approval provided by System Administration Manager.
CA46		For associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho is revoked based on the integration with Zoho People.
CA48		For revocation of access to corporate jump server of Linux based corporate server of Zoho, the request is raised in Zoho SDP. System administration team revokes access to jump server for the associate. For associates leaving from Zoho, the access to jump server is revoked on the associate's last working date.

Control Number	Activity	Control Activities
CA49		Access to passman is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).
CA50		Access to corporate jump server is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).
CA51		Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.
CA53		Local Admin Rights and access to removable device is restricted for Zoho workstations.
CA64		Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option.
CA65		For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.
CA66		For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.
CA67		IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any).
CA68		Product description and terms of use for Zoho Cloud products is published in company's website.
CA72		Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.
CA78		Servers onboarded in IDC network are hardened using standard image by server operations team.
CA80		For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.
CA81		For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.
CA82		Access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is reviewed by the Network Operations team on an Annual basis. Corrective action is performed by Network Operations team for discrepancies identified (if any)
CA83		Administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is restricted to NOC engineers.
CA84		Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.
CA87		Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.

Control Number	Activity	Control Activities
CA91		For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA92		For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA94		For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA95		MAC Binding is implemented for workstation connecting from NOC room to IDC network.
CA107		For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.
CA108		For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.
CA109		For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.
CA110		The logs for just in time access are recorded and stored in Zero trust application.
CA111		Data copy restriction is imposed for IDC servers of Zoho.
CA112		IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA114		For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.
CA115		For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.
CA117		Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.
CA118		For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.
CA119		For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.
CA121		Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA123		Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload.

Control Number	Activity	Control Activities
		Malware check validation for application code relating to file upload is validated using Hacksaw tool.
CA126		IDC servers of Zoho are blocked from mounting removable device.
CA143		For creation of access to Key management service tool of Zoho, the request is raised via Email. EAR team lead creates access to KMS tool for the associate based on the approval provided by EAR team manager.
CA144		For associates leaving Zoho, the access to Key management service tool is revoked based on the integration with Zoho People.

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 Number	Activity	Control Activities
CA01		Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.
CA05		Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.
CA07		For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA08		For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA19		Physical Security policy of Zoho is defined by Admin team. The policy document is reviewed and approved by Head of safety and security on an annual basis. The policy document defines the physical access restrictions for Zoho associates.
CA23		The access to Server Operations Team and NOC room is restricted to Server Operations Team and NOC team members.
CA24		For revocation of access to Server Operations Team and NOC room, the request is raised in Zoho SDP. Admin team revokes physical access to Server Operations Team and NOC room for the associate. For associates leaving from Zoho, the physical access to Server Operations Team and NOC room is revoked on the associate's last working date.
CA33		Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.
CA60		Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.
CA61		Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.

Control Number	Activity	Control Activities
CA69		Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.
CA70		Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.
CA75		Customer Support process document of Zoho is defined by the Zoho customer support team. The document is reviewed and approved by Director of customer support team on an annual basis. The document defines the support process for Zoho products.
CA97		Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.
CA100		Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.
CA106		Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.
CA129		Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.
CA131		Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.
CA147		The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.
CA154		Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following: 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.

3.10.6 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 Number	Activity	Control Activities
CA01		Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.
CA11		For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.
CA12		For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.
CA13		For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.
CA14		For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining
CA15		For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date
CA16		For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.
CA17		For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.
CA18		For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.
CA32		Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.
CA33		Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.
CA34		Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.
CA37		Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.
CA43		Corporate servers of Zoho are blocked from mounting removable storage media device.
CA44		Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA45		For creation of access to corporate server of Zoho, the request is raised by the user. System administration team creates access to passman for the associate based on the approval provided by System Administration Manager.

Control Number	Activity	Control Activities
CA46		For associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho is revoked based on the integration with Zoho People.
CA48		For revocation of access to corporate jump server of Linux based corporate server of Zoho, the request is raised in Zoho SDP. System administration team revokes access to jump server for the associate. For associates leaving from Zoho, the access to jump server is revoked on the associate's last working date.
CA49		Access to passman is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).
CA50		Access to corporate jump server is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).
CA51		Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.
CA53		Local Admin Rights and access to removable device is restricted for Zoho workstations.
CA54		Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used.
CA64		Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option.
CA65		For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.
CA66		For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.
CA67		IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any).
CA77		Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.
CA79		Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.
CA80		For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.
CA81		For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.
CA82		Access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is reviewed by the Network

Control Number	Activity	Control Activities
		Operations team on an Annual basis. Corrective action is performed by Network Operations team for discrepancies identified (if any)
CA83		Administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is restricted to NOC engineers.
CA84		Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.
CA87		Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.
CA90		All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.
CA91		For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA92		For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA93		Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.
CA94		For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA95		MAC Binding is implemented for workstation connecting from NOC room to IDC network.
CA98		Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA107		For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.
CA108		For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.
CA109		For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.
CA114		For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.
CA115		For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.
CA116		Administrative access to Jump Server of Zoho is restricted to Server Operations team.
CA117		Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.

Control Number	Activity	Control Activities
CA118		For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.
CA119		For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.
CA120		Administrative access to Server Operation tools (ZAC and Server Operations Passman) of Zoho is restricted to Server Operations Team.
CA121		Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA124		IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA127		Zoho Server Operations team maintains an asset registry of the IDC Servers.
CA128		Zoho uses asset discovery tool to identify and track the servers added in IDC network.
CA131		Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.
CA132		Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.
CA143		For creation of access to Key management service tool of Zoho, the request is raised via Email. EAR team lead creates access to KMS tool for the associate based on the approval provided by EAR team manager.
CA144		For associates leaving Zoho, the access to Key management service tool is revoked based on the integration with Zoho People.

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 Number	Activity	Control Activities
CA14		For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining
CA15		For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date
CA16		For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.
CA17		For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.
CA18		For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.

Control Number	Activity	Control Activities
CA32		Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.
CA37		Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.
CA43		Corporate servers of Zoho are blocked from mounting removable storage media device.
CA45		For creation of access to corporate server of Zoho, the request is raised by the user. System administration team creates access to passman for the associate based on the approval provided by System Administration Manager.
CA46		For associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho is revoked based on the integration with Zoho People.
CA48		For revocation of access to corporate jump server of Linux based corporate server of Zoho, the request is raised in Zoho SDP. System administration team revokes access to jump server for the associate. For associates leaving from Zoho, the access to jump server is revoked on the associate's last working date.
CA49		Access to passman is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).
CA50		Access to corporate jump server is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).
CA51		Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.
CA53		Local Admin Rights and access to removable device is restricted for Zoho workstations.
CA54		Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used.
CA64		Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option.
CA65		For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.
CA66		For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.
CA67		IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any).
CA77		Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.
CA79		Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.
CA80		For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho

Control Number	Activity	Control Activities
		SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.
CA81		For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.
CA82		Access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is reviewed by the Network Operations team on an Annual basis. Corrective action is performed by Network Operations team for discrepancies identified (if any)
CA83		Administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is restricted to NOC engineers.
CA84		Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.
CA87		Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.
CA90		All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.
CA91		For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA92		For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA93		Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.
CA94		For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA95		MAC Binding is implemented for workstation connecting from NOC room to IDC network.
CA107		For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.
CA108		For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.
CA109		For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.
CA114		For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.
CA115		For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.

Control Activity Number	Control Activities
CA116	Administrative access to Jump Server of Zoho is restricted to Server Operations team.
CA117	Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.
CA118	For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.
CA119	For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.
CA120	Administrative access to Server Operation tools (ZAC and Server Operations Passman) of Zoho is restricted to Server Operations Team.
CA121	Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA143	For creation of access to Key management service tool of Zoho, the request is raised via Email. EAR team lead creates access to KMS tool for the associate based on the approval provided by EAR team manager.
CA144	For associates leaving Zoho, the access to Key management service tool is revoked based on the integration with Zoho People.

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
CA32	Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.
CA37	Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.
CA43	Corporate servers of Zoho are blocked from mounting removable storage media device.
CA45	For creation of access to corporate server of Zoho, the request is raised by the user. System administration team creates access to passman for the associate based on the approval provided by System Administration Manager.
CA46	For associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho is revoked based on the integration with Zoho People.
CA48	For revocation of access to corporate jump server of Linux based corporate server of Zoho, the request is raised in Zoho SDP. System administration team revokes access to jump server for the associate. For associates leaving from Zoho, the access to jump server is revoked on the associate's last working date.
CA51	Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.

Control Activity Number	Control Activities
CA53	Local Admin Rights and access to removable device is restricted for Zoho workstations.
CA54	Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used.
CA64	Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option.
CA65	For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.
CA66	For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.
CA67	IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any).
CA74	Log of activities performed by users in Zoho Cloud products are stored using Zoho logs application.
CA79	Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.
CA80	For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.
CA81	For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.
CA83	Administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is restricted to NOC engineers.
CA84	Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.
CA87	Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.
CA90	All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.
CA91	For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA92	For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA93	Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.

Control Activity Number	Control Activities
CA94	For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA95	MAC Binding is implemented for workstation connecting from NOC room to IDC network.
CA110	The logs for just in time access are recorded and stored in Zero trust application.
CA114	For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.
CA115	For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.
CA116	Administrative access to Jump Server of Zoho is restricted to Server Operations team.
CA117	Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.
CA120	Administrative access to Server Operation tools (ZAC and Server Operations Passman) of Zoho is restricted to Server Operations Team.

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
CA11	For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.
CA12	For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.
CA13	For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.
CA19	Physical Security policy of Zoho is defined by Admin team. The policy document is reviewed and approved by Head of safety and security on an annual basis. The policy document defines the physical access restrictions for Zoho associates.
CA20	Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.
CA21	Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance.
CA22	Access to Facilities of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)
CA23	The access to Server Operations Team and NOC room is restricted to Server Operations Team and NOC team members.

Control Number	Activity	Control Activities
CA24		For revocation of access to Server Operations Team and NOC room, the request is raised in Zoho SDP. Admin team revokes physical access to Server Operations Team and NOC room for the associate. For associates leaving from Zoho, the physical access to Server Operations Team and NOC room is revoked on the associate's last working date.
CA25		Access to Server Operations Team and NOC room of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)
CA26		Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.
CA27		Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.
CA28		Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis: -Cooling system -UPS -DG - Fire suppression system
CA29		Mock fire drill is conducted by Admin team of Zoho on an annual basis.
CA106		Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.

.

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 Number	Activity	Control Activities
CA20		Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.
CA26		Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.
CA27		Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.
CA28		Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system

Control Number	Activity	Control Activities
CA101		Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.
CA110		The logs for just in time access are recorded and stored in Zero trust application.
CA129		Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.

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

Control Number	Activity	Control Activities
CA30		Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.
CA31		Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.
CA32		Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.
CA35		For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team.
CA36		The attachments of email sent to Zoho domain are scanned for malware content. The emails are quarantined if anomalies identified.
CA37		Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.
CA39		Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA40		Workstations of Zoho are blocked from disabling CrowdStrike.
CA41		Workstations of Zoho uses encryption software to encrypt the disk.
CA42		Corporate servers of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA43		Corporate servers of Zoho are blocked from mounting removable storage media device.
CA78		Servers onboarded in IDC network are hardened using standard image by server operations team.
CA85		Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure.
CA86		Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA88		Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA96		Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.

Control Number	Activity	Control Activities
CA97		Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.
CA100		Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.
CA111		Data copy restriction is imposed for IDC servers of Zoho.
CA112		IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA123		Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.
CA125		IDC servers of Zoho are restricted from accessing internet.
CA126		IDC servers of Zoho are blocked from mounting removable device.
CA130		Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.

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 Number	Activity	Control Activities
CA30		Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.
CA31		Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.
CA35		For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team.
CA36		The attachments of email sent to Zoho domain are scanned for malware content. The emails are quarantined if anomalies identified.
CA39		Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA40		Workstations of Zoho are blocked from disabling CrowdStrike.
CA41		Workstations of Zoho uses encryption software to encrypt the disk.
CA42		Corporate servers of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA78		Servers onboarded in IDC network are hardened using standard image by server operations team.
CA86		Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA88		Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full

Control Number	Activity	Control Activities
		Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA96		Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.
CA97		Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.
CA99		Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.
CA100		Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.
CA111		Data copy restriction is imposed for IDC servers of Zoho.
CA112		IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA113		Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.
CA121		Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA122		Server Operations team has implemented load balancers for IDC servers.
CA123		Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.
CA125		IDC servers of Zoho are restricted from accessing internet.
CA126		IDC servers of Zoho are blocked from mounting removable device.
CA128		Zoho uses asset discovery tool to identify and track the servers added in IDC network.
CA131		Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.
CA132		Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.
CA133		Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.
CA134		Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.

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 Number	Activity	Control Activities
CA34		Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.
CA127		Zoho Server Operations team maintains an asset registry of the IDC Servers.

3.10.7 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
CA30	Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.
CA31	Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.
CA35	For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team.
CA36	The attachments of email sent to Zoho domain are scanned for malware content. The emails are quarantined if anomalies identified.
CA37	Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.
CA39	Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA40	Workstations of Zoho are blocked from disabling CrowdStrike.
CA41	Workstations of Zoho uses encryption software to encrypt the disk.
CA42	Corporate servers of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA43	Corporate servers of Zoho are blocked from mounting removable storage media device.
CA51	Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.
CA53	Local Admin Rights and access to removable device is restricted for Zoho workstations.
CA60	Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.
CA61	Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.
CA74	Log of activities performed by users in Zoho Cloud products are stored using Zoho logs application.
CA84	Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.
CA85	Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure.
CA86	Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA87	Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.
CA88	Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full

Control Activity Number	Control Activities
	Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA90	All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.
CA91	For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA92	For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA93	Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.
CA94	For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA95	MAC Binding is implemented for workstation connecting from NOC room to IDC network.
CA96	Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.
CA99	Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.
CA100	Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.
CA110	The logs for just in time access are recorded and stored in Zero trust application.
CA111	Data copy restriction is imposed for IDC servers of Zoho.
CA112	IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA117	Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.
CA121	Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA122	Server Operations team has implemented load balancers for IDC servers.
CA123	Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.
CA125	IDC servers of Zoho are restricted from accessing internet.
CA126	IDC servers of Zoho are blocked from mounting removable device.
CA128	Zoho uses asset discovery tool to identify and track the servers added in IDC network.
CA129	Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.

Control Activity Number	Control Activities
CA130	Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.
CA131	Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.
CA133	Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.

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
CA37	Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.
CA38	System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.
CA57	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA58	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA89	Business continuity test is performed for NOC room on an annual basis by Network Operations team.
CA96	Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.
CA97	Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.
CA113	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.
CA122	Server Operations team has implemented load balancers for IDC servers.
CA134	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.

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
CA22	Access to facilities of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)
CA25	Access to Server Operations Team and NOC room of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)
CA38	System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.
CA39	Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA40	Workstations of Zoho are blocked from disabling CrowdStrike.
CA42	Corporate servers of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA47	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA58	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA65	For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.
CA66	For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.
CA85	Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure.
CA86	Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA87	Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.
CA91	For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.
CA92	For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.
CA93	Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.

Control Activity Number	Control Activities
CA94	For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.
CA95	MAC Binding is implemented for workstation connecting from NOC room to IDC network.
CA106	Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.
CA113	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.
CA121	Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.
CA123	Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.
CA130	Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.

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
CA47	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA101	Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.

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

Control Activity Number	Control Activities
CA47	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA52	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA100	Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.

Control Activity Number	Control Activities
CA159	Privacy team reviews the complaints related to privacy raised to Zoho against unfair or unlawful practices.

3.10.8 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
CA71	Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.
CA72	Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.
CA73	Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.

3.10.9 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
CA56	Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.
CA57	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA59	Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.

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

Control Activity Number	Control Activities
CA20	Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.
CA21	Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance.
CA62	Master service agreement is signed between Zoho and third party vendor. Any changes to the contracts are agreed by Zoho and the third party vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA102	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.

3.10.10 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
CA07	For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.
CA09	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA152	Procedure for personal information retention is defined as part of privacy policy by the legal team. The policy document is reviewed and approved by the General Counsel on an annual basis. The policy covers the following: 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
CA147	The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.
CA152	Procedure for personal information retention is defined as part of privacy policy by the legal team. The policy document is reviewed and approved by the General Counsel on an annual basis. The policy covers the following: 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.

3.10.11 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
CA34	Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.
CA44	Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA47	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.
CA58	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA86	Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.
CA89	Business continuity test is performed for NOC room on an annual basis by Network Operations team.
CA97	Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.
CA98	Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA100	Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.

Control Activity Number	Control Activities
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA113	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.
CA122	Server Operations team has implemented load balancers for IDC servers.
CA124	IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.
CA129	Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.
CA134	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.

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
CA27	Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.
CA28	Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system
CA29	Mock fire drill is conducted by Admin team of Zoho on an annual basis.
CA38	System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.
CA75	Customer Support process document of Zoho is defined by the Zoho customer support team. The document is reviewed and approved by Director of customer support team on an annual basis. The document defines the support process for Zoho products.
CA76	Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team.
CA88	Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA96	Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.

Control Activity Number	Control Activities
CA112	IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA132	Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.
CA133	Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.
CA134	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.

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

Control Activity Number	Control Activities
CA28	Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment are serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system
CA38	System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.
CA58	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.
CA88	Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.
CA89	Business continuity test is performed for NOC room on an annual basis by Network Operations team.
CA113	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.
CA132	Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.

3.10.12 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
CA09	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA10	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA68	Product description and terms of use for Zoho Cloud products is published in company's website.
CA70	Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.
CA75	Customer Support process document of Zoho is defined by the Zoho customer support team. The document is reviewed and approved by Director of customer support team on an annual basis. The document defines the support process for Zoho products.
CA76	Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team.
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA139	Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA147	The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.

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
CA39	Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA42	Corporate servers of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.
CA64	Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option.

Control Activity Number	Control Activities
CA68	Product description and terms of use for Zoho Cloud products is published in company's website.
CA70	Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.
CA74	Log of activities performed by users in Zoho Cloud products are stored using Zoho logs application.
CA123	Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.

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
CA69	Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.
CA71	Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.
CA72	Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.
CA73	Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.
CA76	Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team.

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
CA112	IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.
CA134	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.

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
CA41	Workstations of Zoho uses encryption software to encrypt the disk.
CA133	Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.
CA134	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.
CA132	Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.

3.10.13 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
CA57	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA148	The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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.

Control Activity Number	Control Activities
CA154	Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following: 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
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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.

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
CA142	For new/changes made to consent process, the business unit personnel obtains approval from Director of Compliance (DOC) before implementing the change.
CA149	The policy for choice and consent is defined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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
CA150	The definition of sensitive personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel.
CA156	Procedure to determine if explicit consent is required is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The policy defines the procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent and procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA157	The privacy team establishes a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements. This document is reviewed and approved annually by the Director of Compliance. The document defines the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.
CA135	Members of the privacy staff verify that the entity has legal grounds to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, on a periodic basis, the privacy team verify that the entity has requested and received explicit written consent from the data subjects, when such consent is required.

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
CA63	Zoho provides data subjects with 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.
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.
CA139	Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA148	The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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.

Control Activity Number	Control Activities
CA150	The definition of sensitive personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel.
CA158	Procedure to determine PIA requirement is defined by Privacy team. The procedure document is reviewed and approved by Director of Compliance on an annual basis.
CA159	Privacy team reviews the complaints related to privacy raised to Zoho against unfair or unlawful practices.
CA135	Members of the privacy staff verify that the entity has legal grounds to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, on a periodic basis, the privacy team verify that the entity has requested and received explicit written consent from the data subjects, when such consent is required.

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
CA63	Zoho provides data subjects with 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.
CA142	For new/changes made to consent process, the business unit personnel obtains approval from Director of Compliance (DOC) before implementing the change.
CA149	The policy for choice and consent is defined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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.
CA154	Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following: 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

Control Activity Number	Control Activities
	5. Documents the changes to privacy practices that were communicated to data subjects.
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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
CA156	Procedure to determine if explicit consent is required is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The policy defines the procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent and procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA157	The privacy team establishes a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements. This document is reviewed and approved annually by the Director of Compliance. The document defines the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.

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
CA59	Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.
CA61	Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.
CA129	Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.
CA151	The use of personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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.
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines the purpose and use of the collection of personal information, including

Control Activity Number	Control Activities
	detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.

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

Control Activity Number	Control Activities
CA137	Privacy team maintains inventory of data collected from the data subjects. The inventory is reviewed on an annual basis by Privacy team to ensure the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA152	Procedure for personal information retention is defined as part of privacy policy by the legal team. The policy document is reviewed and approved by the General Counsel on an annual basis. The policy covers the following: 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.

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

Control Activity Number	Control Activity
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA146	Procedure for data subject correction request in Zoho is defined by privacy team. The policy document is reviewed and approved by Director of IT on an annual basis.
CA147	The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.

Control Activity Number	Control Activity
CA159	Privacy team reviews the complaints related to privacy raised to Zoho against 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
CA09	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.
CA10	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA105	Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis.
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA145	The privacy policy of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The policy outlines the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.
CA148	The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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.

Control Activity Number	Control Activities
	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.
CA149	The policy for choice and consent is defined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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.
CA150	The definition of sensitive personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel.
CA153	The Data Subject Access Request policy of Zoho is defined by the Privacy team and is reviewed and approved annually by the Director of Compliance. The policy document defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information.
CA154	Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following: 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
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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.
CA135	Members of the privacy staff verify that the entity has legal grounds to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, on a periodic basis, the privacy team verify that the entity has requested and received explicit written consent from the data subjects, when such consent is required.
CA136	On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.

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
CA08	For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.
CA136	On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.
CA139	Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA146	Procedure for data subject correction request in Zoho is defined by privacy team. The policy document is reviewed and approved by Director of IT on an annual basis.
CA151	The use of personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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.
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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
CA156	Procedure to determine if explicit consent is required is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The policy defines the procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent and procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA157	The privacy team establishes a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements. This document is reviewed and approved annually by the Director of Compliance. The

Control Activity Number	Control Activities
	document defines the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.
CA160	On an annual basis, Director of Compliance (DOC) reviews cases relating to request raised by data subjects for disagreements over the accuracy of personal data and validate the appropriate justifications provided thereof.

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
CA63	Zoho provides data subjects with 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.
CA105	Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis.
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.
CA139	Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA141	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.
CA142	For new/changes made to consent process, the business unit personnel obtains approval from Director of Compliance (DOC) before implementing the change.
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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
CA158	Procedure to determine PIA requirement is defined by Privacy team. The procedure document is reviewed and approved by Director of Compliance on an annual basis.

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
CA102	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the

Control Activity Number	Control Activities
	co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA105	Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis.

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
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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.

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
CA101	Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.
CA102	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.

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
CA102	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.
CA136	On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.

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
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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.

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
CA105	Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis.
CA136	On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.
CA153	The Data Subject Access Request policy of Zoho is defined by the Privacy team and is reviewed and approved annually by the Director of Compliance. The policy document defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information.

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
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.
CA139	Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA141	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.
CA146	Procedure for data subject correction request in Zoho is defined by privacy team. The policy document is reviewed and approved by Director of IT on an annual basis.
CA151	The use of personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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.
CA152	Procedure for personal information retention is defined as part of privacy policy by the legal team. The policy document is reviewed and approved by the General Counsel on an annual basis. The policy covers the following: 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.
CA160	On an annual basis, Director of Compliance (DOC) reviews cases relating to request raised by data subjects for disagreements over the accuracy of personal data and validate the appropriate justifications provided thereof.

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
CA136	On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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.
CA142	For new/changes made to consent process, the business unit personnel obtains approval from Director of Compliance (DOC) before implementing the change.
CA153	The Data Subject Access Request policy of Zoho is defined by the Privacy team and is reviewed and approved annually by the Director of Compliance. The policy document defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information.
CA159	Privacy team reviews the complaints related to privacy raised to Zoho against unfair or unlawful practices.
CA160	On an annual basis, Director of Compliance (DOC) reviews cases relating to request raised by data subjects for disagreements over the accuracy of personal data and validate the appropriate justifications provided thereof.

3.11 Complementary User Entity Controls ('CUECs')

The controls at Zoho relating to the Application development, Production Support and the related General Information Technology 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 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:

3.11.1 User entities are responsible for providing and managing the access of with their associates having access to Zoho products including access provisioning, de-provisioning, periodical access review and restriction of administrative access. (CA14, CA15, CA32 and CA67)
3.11.2 User entities are responsible for requesting and approving the Master Service Agreement ('MSA') and the approval for implementation of application (CA103)
3.11.3 User entities are responsible for respective the documents made available through the corporate website (CA68 and CA147)
3.11.4 User entities are responsible for raising any backup restoration request to Zoho. (CA132)
3.11.5 User entities are responsible for communicating any security or privacy incidents to Zoho on a timely basis. (CA52 and CA159)
3.11.6 User entities are responsible for reviewing the privacy policy and accepting to the privacy notice of Zoho. (CA63, CA145 and CA155)
3.11.7 User entities are responsible for reviewing and approving the changes related to the configurations and processes within the applications (CA72)

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 4.3.1

3.12 Vendor v/s Subservice Organization (SSO) Analysis

Zoho utilizes subservice organizations to support complete, accurate and timely processing of client transactions which are identified in table 1 below. Zoho management assesses the risks associated with these subservice organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner. These include, but are not limited to, the review of third-party service 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 Information Technology 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 Information Technology Controls to be achieved solely by Zoho. Therefore, each user entity's internal control 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 - Databank Holdings Limited	Datacenter Co-Location Services

Subservice organizations are responsible for defining and implementing CSOCs provided in sub-section 3.12.

3.12.1 Subservice organizations are responsible for supporting the physical security and environmental safeguard controls for the datacenter. (CA12, CA13, CA20, CA21, CA22, CA26, CA27, CA28 and CA29)

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 (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 Limited - HVAC Space air Pvt ltd - Ardelisys Technologies Private Limited - SVE Energy Private Limited	Environmental equipment maintenance
- G4S Secure Solutions India Private Limited	Physical Security Agency for Security Personnel
- KPMG Assurance and Consulting Services LLP - Matrix Business Services India Private Limited	Background Verification Services
- Amazon Web Services, Inc.	Content Delivery Network
- Easy Post: Simpler Postage Inc.	Shipping Services
- Google translate: Google LLC	Translation Service
- Litmus Software Inc.	Email Marketing Service
- Kaleyra US Inc. - Telnyx LLC	SMS Service
- Tata Communications Limited	Dialing Service

SECTION - 4
Management of Zoho’s Description of Its Relevant Criteria and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results.

Section 4. Management of Zoho's Description of Its Relevant Criteria and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results.

4.1 Description of testing procedures performed

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

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

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

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

4.2 Testing of tools supporting control activities

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

4.3 Reliability of information produced by the Service Organization

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

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

4.4 Reporting on results of testing

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

(Space left intentionally blank)

4.4.1 Test Procedure Performed by Service Auditors

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

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA01	Hiring and separation policy of Zoho is defined by HR team. The policy document is reviewed and approved by Deputy Manager HR on an annual basis. The policy document defines the onboarding and offboarding process for Zoho associates.	CC1.1 CC1.3 CC2.1 CC5.3 CC6.1	Inspected Hiring and Separation policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether hiring and separation policy of Zoho was defined by HR team and the policy document was reviewed and approved by Deputy Manager HR on an annual basis and whether the policy document defined the onboarding and offboarding process for Zoho associates.	None	None	No Exceptions Noted.
CA02	Background Verification Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the background verification process for Zoho associates.	CC1.1 CC1.4 CC2.1	Inspected Background Verification policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Background Verification Policy of Zoho was defined by HR team and the policy document was reviewed and approved by the Deputy Manager HR on an annual basis and whether the policy document defined the background verification process for Zoho associates.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA03	Code of ethics document of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.	CC1.1 CC1.3 CC1.4 CC1.5 CC2.2	Inspected code of ethics document of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'contents' to ascertain whether code of ethics document of Zoho was defined by HR team and the policy document was reviewed and approved by the Deputy Manager HR on an annual basis and whether the policy document defined the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection of Zoho associates.	None	None	No Exceptions Noted.
CA04	Whistle Blower Policy of Zoho is defined by HR team. The policy document is reviewed and approved by the Deputy Manager HR on an annual basis. The policy document defines the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously. It also specifies the action to be taken in case of any violation for Zoho associates.	CC1.1 CC1.4 CC2.2 CC2.3 CC3.1	Inspected Whistle Blower Policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Whistle Blower Policy of Zoho was defined by HR team and the policy document was reviewed and approved by the Deputy Manager HR on an annual basis and whether the policy document defined the guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance through Zoho Connect anonymously; also whether it also specified the action to be taken in case of any violation for Zoho associates.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA05	Job Description of Zoho is defined by Senior Manager TA and HR operations. The policy document is reviewed and approved by the Associate Director TA and HR operations on an annual basis. The policy document defines the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.	CC1.1 CC1.4 CC2.2 CC2.3 CC5.3	Inspected Job Description of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Job Description of Zoho was defined by Senior Manager TA and HR operations and the policy document was reviewed and approved by the Associate Director TA and HR operations on an annual basis and whether the policy document defined the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection.	None	None	No Exceptions Noted.
CA06	Organization chart is defined by HR team. The policy document is reviewed and approved by Senior Manager HR on an annual basis. The organization chart defines the departments and internal structure of Zoho.	CC1.1 CC1.3 CC2.1 CC5.1	Inspected Organization chart of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether Organization chart was defined by HR team and the policy document was reviewed and approved by Senior Manager HR on an annual basis and whether the organization chart defined the departments and internal structure of Zoho.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA07	For associates joining Zoho, Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy are signed by the associate before date of joining.	CC1.1 CC1.4 CC1.5 CC2.2 CC3.1 CC5.3 C1.1	Inspected for sample new joiners the Non Disclosure Agreement for aspects such as 'associate's date of joining', 'Signatory', 'date of signature' and 'content' to ascertain whether Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy were signed by the associate before date of joining.	None	None	No Exceptions Noted.
CA08	For associates joining Zoho, background verification is initiated by HR team within 2 days from date of joining. Third party vendor performs background verification and provides the report. For negative background verification results, HR team performs follow-up action.	CC1.1 CC1.4 CC2.1 CC3.1 CC5.3 P5.2	Inspected for sample new joiners the background verification report for aspects such as ‘associate ID’, ‘associate name’, 'associate's date of joining', 'date of BGV initiation', 'date of BGV completion', 'BGV result' to ascertain whether background verification was initiated by HR team within 2 days from date of joining and whether third party vendor performed background verification and provides the report; also ascertained whether for negative background verification results, HR team performed follow-up action.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA09	For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People.	CC1.4 CC2.2 CC3.1 CC5.1 C1.1 PI1.1 P5.1	Inspected for sample new joiners the Induction Training records in Zoho People for aspects such as 'associate's date of joining', 'date of training completion', ‘attendance status’, 'training completion status' and 'content of induction training material' to ascertain whether induction training was completed by the associate on the date of joining and the induction training covered the information security and privacy commitments of Zoho and also whether the attendance for completion of induction training is captured in Zoho People.	None	None	Exception Noted. Refer Exception #1
CA10	For active associates of Zoho, annual refresher training is completed by the associate. The annual refresher training covers the information security and privacy commitments of Zoho. The attendance for completion of annual refresher training is captured in Zoho Learn.	CC1.4 CC2.2 CC3.1 CC5.1 PI1.1 P5.1	Inspected for sample active associates the annual refresher training records in Zoho Learn for aspects such as ‘Associate ID’, ‘Associate name’, 'date of training completion', 'training completion status' and 'content of induction training material' to ascertain whether annual refresher training was completed by the associate and the annual refresher training covers the information security and privacy commitments of Zoho and whether the attendance for completion of annual refresher training was captured in Zoho Learn.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA11	For associates joining Zoho, the HR team enters the joining date in Zoho people. Admin team creates physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.	CC2.1 CC5.2 CC6.1 CC6.4	Inspected for sample new joiners the physical access creation log and email relating to access creation for aspects such as ‘Associate ID’, ‘Associate name’, 'associate's date of joining', 'access creation email sent on', 'access creation email sent from', 'access creation email sent to', 'access created on', 'access created by' and 'email configuration' to ascertain whether the HR team enters the joining date in Zoho people and whether the admin team created physical access for the associate based on the automatic email triggered from Zoho People after the associate's date of joining.	None	None	No Exceptions Noted.
CA12	For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.	CC2.1 CC5.2 CC6.1 CC6.4	Inspected for sample leavers the physical access revocation log and email relating to access revocation for aspects such as ‘Associate ID’, ‘Associate name’, 'associate's last working date', 'access revocation email sent on', 'access revocation email sent from', 'access revocation email sent to', ' access revoked on', 'access revoked by' and 'email configuration' to ascertain whether the HR team enters the last working date in Zoho people and whether admin team revoked physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date.	None	3.12.1	Exception Noted. Refer Exception #2

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA13	For associate losing physical access card, the associate raise request in Zoho People. Admin team revokes physical access for the lost card and creates physical access for the new card based on the automatic email triggered from Zoho People on the date of request.	CC2.1 CC5.2 CC6.1 CC6.4	Inspected for sample access card lost cases the physical access logs and ticket from Zoho People for aspects such as 'associate's access card lost date', 'access recreation email sent on', 'access recreation email sent from', 'access recreation email sent to', 'old access revoked on', 'new access created on', 'access recreated by', 'access revoked by' and 'email configuration' to ascertain whether the associate raise request in Zoho People and whether admin team revoked physical access for the lost card and created physical access for the new card based on the automatic email triggered from Zoho People on the date of request.	None	3.12.1	No exceptions noted.
CA14	For associates joining Zoho, the HR team creates the IAM account in Zoho people for the associate on their date of joining.	CC5.2 CC6.1 CC6.2	Inspected for sample joiners the IAM account creation log for aspects such as 'associate's date of joining', 'access created on' and 'access created by' to ascertain whether the HR team created the IAM account in Zoho people for the associate on their date of joining.	3.11.1	None	No Exceptions Noted.
CA15	For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date.	CC5.2 CC6.1 CC6.2	Inspected for sample leavers the IAM account revocation LOG for aspects such as ‘Associate ID’, ‘Associate name’, ‘Associate's last working date' 'Access revoked on' 'Access revoked by' 'Email sent by' 'to ascertain whether the HR team revoked the IAM account in Zoho people for the associate on their last working date.	3.11.1	None	Exception Noted. Refer Exception #3

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA16	For associates joining Zoho, the HR team notifies the sysadmin team for domain account creation. An automated SDP ticket is created and closed by the sysadmin team upon creation of the domain ID.	CC5.2 CC6.1 CC6.2	Inspected the SDP integration and for sample new joiners the domain account creation log and email relating to domain account creation for aspects such as 'Associate's date of joining ' 'Access created on' 'Access created by' 'Email sent by' 'Email sent to' 'Email sent on' to ascertain whether the HR team notified the sysadmin team for domain account creation and whether an automated SDP ticket was created and closed by the sysadmin team upon creation of the domain ID.	None	None	No Exceptions Noted.
CA17	For associates leaving Zoho, the HR team notifies the sysadmin team for domain account revocation. An automated SDP ticket is created and closed by the sysadmin team upon deletion of the domain ID.	CC5.2 CC6.1 CC6.2	Inspected for sample leavers the domain account revocation log and ticket relating to domain account revocation for aspects such as ‘Access name’, ‘Associate ID’, 'Associate's last working date' 'Access revoked on' 'Access revoked by', ‘Ticket ID', Email sent by' 'Email sent to' 'Email sent on' to ascertain whether the HR team notified the sysadmin team for domain account revocation and also whether an automated SDP ticket was created and closed by the sysadmin team upon deletion of the domain ID.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA18	For associates leaving Zoho, the sysadmin team reclaims assets of the associate on or before last working date.	CC1.4 CC1.5 CC2.1 CC6.1 CC6.2	Inspected for sample leavers the asset reclaim records for aspects such as ‘Associate name’, ‘Associate ID’, ‘Last working date’, ‘Reclaimed by’ and ‘Date of asset reclaim’ to ascertain whether for associates leaving Zoho, the sysadmin team reclaimed assets of the associate on or before last working date.	None	None	No Exceptions Noted.
CA19	Physical Security policy of Zoho is defined by Admin team. The policy document is reviewed and approved by Head of safety and security on an annual basis. The policy document defines the physical access restrictions for Zoho associates.	CC5.3 CC6.4	Inspected the physical security policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether physical Security policy of Zoho was defined by Admin team and the policy document was reviewed and approved by Head of safety and security on an annual basis and whether the policy document defined the physical access restrictions for Zoho associates.	None	None	No Exceptions Noted.
CA20	Visitor and vendors entering Zoho are recorded in visitor management system. The escort details are recorded as part of the registry.	CC6.4 CC6.5 CC9.2	Inspected for sample dates the visitor and vendor registry from visitor management system for aspects such as ‘vendor and visitor details’, ‘date’, ‘review sign’, ‘Escort details’ and ‘location’ to ascertain whether visitor and vendors entering Zoho are recorded in visitor management system and the escort details were recorded as part of the registry.	None	3.12.1	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA21	Entry and Exit points of Zoho Facilities is manned by security guards. Security guard registry is maintained by the admin team to track attendance.	CC6.4 CC9.2	Inspected for sample dates the security guard registry for aspects such as entry and exit points of Zoho Facilities was manned by security guards and security guard registry was maintained by the admin team to track attendance.	None	3.12.1	No Exceptions Noted.
CA22	Access to Facilities of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)	CC6.4 CC7.3	Inspected the physical access review records to Zoho Facilities for aspects such as 'Reviewer', 'Date of review', 'List used as part of the review' and 'Corrective action performed' to ascertain whether access to Facilities of Zoho was reviewed by the Admin team on an annual basis. Inspected the user access review report to Zoho Facilities and noted that there were no instance of discrepancies identified during Zoho Facilities access review during the examination period. Further obtained email confirmation from Admin head stating that there were no instance of discrepancies identified during Zoho Facilities access review during the examination period. Therefore, DHS LLP could not test the operating effectiveness of corrective action performed for discrepancies identified during Zoho Facilities access review during the examination period.	None	3.12.1	No Exception Noted. The operating effectiveness of corrective action performed for discrepancies identified during Zoho Facilities access review could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA23	The access to Server Operations Team and NOC room is restricted to Server Operations Team and NOC team members.	CC5.3 CC6.4	Inspected the user access listing of Server Operations Team and NOC room for aspects such as ‘User list’ and ‘Team name’ to ascertain whether the access to Server Operations Team and NOC room was restricted to Server Operations Team and NOC team members.	None	None	No Exceptions Noted.
CA24	For revocation of access to Server Operations Team and NOC room, the request is raised in Zoho SDP. Admin team revokes physical access to Server Operations Team and NOC room for the associate. For associates leaving from Zoho, the physical access to Server Operations Team and NOC room is revoked on the associate’s last working date.	CC5.3 CC6.4	Inspected for sample access revocation requests from SDP to Server Operations Team and NOC room for aspects for aspects such as 'Associate's last working date', 'Ticket number', 'Date of ticket raising', 'Date of ticket closure', 'Access revoked by' and 'Access revoked on' to ascertain whether request was raised in Zoho SDP and whether admin team revoked physical access to Server Operations Team and NOC room for the associate; also whether for associates leaving from Zoho, the physical access to Server Operations Team and NOC room was revoked on the associate's last working date.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA25	Access to Server Operations Team and NOC room of Zoho is reviewed by the Admin team on an annual basis. Corrective action is performed by Admin team for discrepancies identified (if any)	CC6.4 CC7.3	Inspected the physical access review details to Zoho Facilities for aspects such as 'Reviewer' 'Date of review', 'List used as part of the review' and 'Corrective action performed' to ascertain whether Access to Server Operations Team and NOC room of Zoho was reviewed by the Admin team on an annual basis. Inspected the user access review report to Server Operations Team and NOC room and we noted that there were no instances of discrepancies identified during Server Operations Team and NOC room access review during the examination period. Further, obtained email confirmation from Admin Head, stating that, that there were no instances of discrepancies identified during Server Operations Team and NOC room access review during the examination period. Therefore, DHS LLP could not test the operating effectiveness of corrective action performed for discrepancies identified during Server Operations Team and NOC room access review during the examination period	None	None	No Exceptions Noted. The operating effectiveness of corrective action performed for discrepancies identified during Server Operations Team and NOC room access review could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA26	Access to Facilities, Server Operations Team and NOC room of Zoho is restricted by proximity card system. In addition, Server Operations Team and NOC room are protected with PIN based access.	CC6.4 CC6.5	Inspected the Zoho Facilities Server Operations Team and NOC room of Zoho for aspects such as 'Location', 'PIN based access system status' and 'Proximity card system status' to ascertain whether access to facilities, Datacenter, Server Operations Team and NOC room of Zoho was restricted by proximity card system and whether in addition, Server Operations Team and NOC room were protected with PIN based access.	None	3.12.1	No Exceptions Noted.
CA27	Facilities, Server Operations Team and NOC room of Zoho is monitored by CCTV. The CCTV recordings are retained for a period of 60 days.	CC6.4 CC6.5 A1.2	Inspected the Zoho Facilities, Server Operations Team and NOC room of Zoho for aspects such as 'Location', 'Availability of CCTV' and 'CCTV retention period' to ascertain whether Facilities, Server Operations Team and NOC room of Zoho was monitored by CCTV and whether the CCTV recordings are retained for a period of 60 days.	None	3.12.1	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA28	Facilities, Datacenter, Server Operations Team and NOC room of Zoho are installed with the following environmental safeguards. The equipment is serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system	A1.2 A1.3 CC6.4 CC6.5	Inspected the Planned Preventive Maintenance reports of Zoho facilities for aspect such as 'Date of service', 'Location' 'Service report output' to ascertain whether Facilities, Datacenter, Server Operations Team and NOC room of Zoho were installed with the following environmental safeguards and also whether the equipment was serviced on a periodic basis: - Cooling system - UPS - DG - Fire suppression system	None	3.12.1	No Exception Noted.
CA29	Mock fire drill is conducted by Admin team of Zoho on an annual basis.	A1.2 CC6.4	Inspected the annual mock fire drill report of Zoho facilities for aspects such as 'Date of drill' 'Drill participants ' 'Drill outcome' to ascertain whether mock fire drill was conducted by Admin team of Zoho on an annual basis.	None	3.12.1	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA30	Hardening guidelines for onboarding corporate servers and build servers of Zoho is defined by System administration team. The guidelines document is reviewed and approved by System administration Manager on an annual basis.	CC1.2 CC1.3 CC5.2 CC6.6 CC6.7 CC7.1	Inspected Hardening guidelines of corporate servers for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether hardening guidelines for onboarding corporate servers and build servers of Zoho was defined by System administration team and whether the guidelines document was reviewed and approved by System administration Manager on an annual basis.	None	None	No Exceptions Noted.
CA31	Hardening guidelines for onboarding workstation of Zoho is defined by System Administration team. The guidelines document is reviewed and approved by System Administration Manager on an annual basis.	CC1.2 CC1.3 CC5.2 CC6.6 CC6.7 CC7.1	Inspected Hardening guidelines of workstation for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether hardening guidelines for onboarding workstation of Zoho was defined by System Administration team and whether the guidelines document was reviewed and approved by System Administration Manager on an annual basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA32	Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.6	Inspected Zoho password policy and password configuration of Active directory, Zoho Directory and IAM for aspects such as 'Password configuration', 'Account lockout configuration' and 'Password guidelines as per policy' to ascertain whether security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account were defined as per Zoho password policy.	3.11.1	None	Exception Noted. Refer Exception #4
CA33	Mobile device management policy of Zoho is defined by System Administration team. The policy document is reviewed and approved by System Administration Manager on an annual basis. The policy document defines the mobile device handling process for Zoho associates.	CC1.2 CC1.3 CC5.1 CC5.3 CC6.1	Inspected Mobile device management policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether mobile device management policy of Zoho was defined by System Administration team and whether the policy document was reviewed and approved by System Administration Manager on an annual basis and also whether the policy document defined the mobile device handling process for Zoho associates.	None	None	No Exceptions Noted.
CA34	Zoho System Administration team maintains an asset registry of the workstations, corporate servers and build servers.	CC2.1 CC3.3 CC3.4 CC6.1 CC6.8 A1.1	Inspected the asset registry for aspects such as 'Type of asset', ‘Asset assigned to’ and 'Parameters' to ascertain whether Zoho System Administration team maintained an asset registry of the workstations, corporate servers and build servers.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA35	For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team.	CC5.1 CC5.2 CC6.6 CC6.7 CC7.1	Inspected for sample newly onboarded devices the hardening checklist for aspects such as 'Date of onboarded', 'Hardening performed on', 'Hardening checks' to ascertain whether for newly onboarded corporate servers and network device the hardening checklist was maintained by the respective team.	None	None	Exception Noted. Refer Exception #5
CA36	The attachments of email sent to Zoho domain are scanned for malware content. The emails are quarantined if anomalies identified.	CC5.2 CC6.6 CC6.7 CC7.1	Inspected email security configuration for aspects such as 'Domain', ‘Quarantine configuration’ and 'Malware scan configuration' to ascertain whether the attachments of email sent to Zoho domain were scanned for malware content and whether the emails were quarantined if anomalies identified.	None	None	No Exceptions Noted.
CA37	Zoho uses manage engine mobile device management to manage the endpoints and enabling remote data wipe.	CC6.1 CC6.2 CC6.3 CC6.6 CC7.1 CC7.2	Inspected manage engine mobile device management console for aspects such as 'Type of devices monitored' and 'Remote wipe configuration'; further inspected for sample workstations the MDM configuration for aspects such as ‘Hostname’ and ‘MDM Status’ to ascertain whether Zoho used manage engine mobile device management to manage the endpoints and enabled remote data wipe.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA38	System administration team performed business continuity test for Corporate servers of Zoho on an annual basis.	CC3.2 CC7.2 CC7.3 A1.2 A1.3	Inspected business continuity test report of corporate server for aspects such as 'Scope', 'Date of business continuity test' and 'Test outcome' to ascertain whether system administration team performed business continuity test for Corporate servers of Zoho on an annual basis.	None	None	No Exceptions Noted.
CA39	Workstations of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.	CC6.6 CC6.7 CC7.1 CC7.3 PI1.2	Inspected for sample workstations the CrowdStrike EDR console for aspects such as 'Host name', 'Type of OS', 'Location' and 'Status of EDR' to ascertain whether workstations of Zoho were installed with CrowdStrike EDR. Further inspected for sample EDR alerts the service desk plus ticket for aspects such as 'Ticket ID', 'Opened on', 'Closed on' and 'Corrective action performed' to ascertain whether system administration team performed follow-up action for anomalies identified.	None	None	No Exceptions Noted.
CA40	Workstations of Zoho are blocked from disabling CrowdStrike.	CC5.2 CC6.6 CC6.7 CC7.1 CC7.3	Inspected for sample workstations the CrowdStrike EDR console for aspects such as 'Host name', 'Type of OS', 'Location' and 'Status of EDR Disabling Block' to ascertain whether workstations of Zoho were blocked from disabling CrowdStrike.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA41	Workstations of Zoho uses encryption software to encrypt the disk.	CC5.2 CC6.6 CC6.7 CC7.1 PI1.5	Inspected for sample workstations the disk encryption configuration for aspects such as 'Host name', 'Type of OS', 'Location' and 'Status of disk encryption' to ascertain whether workstations of Zoho used encryption software to encrypt the disk.	None	None	No Exceptions Noted.
CA42	Corporate servers of Zoho are installed with CrowdStrike EDR. System administration team performs follow-up action for anomalies identified.	CC6.6 CC6.7 CC7.1 CC7.3 PI1.2	Inspected for sample corporate servers the CrowdStrike EDR console for aspects such as 'Host name', 'Type of OS', 'Location' and 'Status of EDR' to ascertain whether corporate servers of Zoho were installed with CrowdStrike EDR. Further inspected for sample EDR alerts the service desk plus ticket for aspects such as 'Ticket ID', 'Opened on', 'Closed on' and 'Corrective action performed' to ascertain whether system administration team performed follow-up action for anomalies identified.	None	None	No Exceptions Noted.
CA43	Corporate servers of Zoho are blocked from mounting removable storage media device.	CC6.1 CC6.2 CC6.3 CC6.6 CC7.1	Inspected for sample corporate servers the Disk mounting configuration for aspects such as 'Host name' and 'Disk mounting status' to ascertain whether corporate servers of Zoho were blocked from mounting removable storage media device.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA44	Corporate servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.	CC2.1 CC3.4 CC4.1 CC6.1 A1.1	Inspected for sample corporate servers the time sync configuration for aspects such as 'Host name', 'time sync configuration' and 'Time sync source' to ascertain whether Corporate servers of Zoho were connected to Network time protocol server and whether the Network time protocol server fetch time from authorized time sync source.	None	None	No Exceptions Noted.
CA45	For creation of access to corporate server of Zoho, the request is raised by the user. System administration team creates access to passman for the associate based on the approval provided by System Administration Manager.	CC5.2 CC6.1 CC6.2 CC6.3	Inspected for sample access creation to corporate server of Zoho the approval records for aspects such as 'Associate date of joining', 'Associate name', 'Date of access creation', 'Approved by', 'Approved on' and 'Access created by' to ascertain whether for creation of access to corporate server of Zoho, the request is raised by the user and whether system administration team had created access to passman for the associate based on the approval provided by System Administration Manager.	None	None	No Exceptions Noted.
CA46	For associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho is revoked based on the integration with Zoho People.	CC5.2 CC6.1 CC6.2 CC6.3	Inspected the passman tool and Zoho people integration for aspects such as 'Tool name' and 'Integration with Zoho people' to ascertain whether for associates leaving Zoho, the access to passman tool to access password of windows based corporate server of Zoho was revoked based on the integration with Zoho People.	None	None	No Exception Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA47	Zoho Cloud products are monitored for downtime using Site 24x7 tool. Anomalies (if any) are tracked to closure by incident management team.	CC2.2 CC2.3 CC3.1 CC4.1 CC7.3 CC7.4 CC7.5 A1.1	Inspected for sample products the site 24x7 dashboard for aspects such as 'Product name', 'DC Name' and 'Monitoring status'; Further inspected for sample incidents the 'Incident ID', 'Date of incident opening' and 'Date of incident closing', 'Incident closed by' to ascertain whether Zoho cloud products were monitored for downtime using Site 24x7 tool and whether anomalies (if any) were tracked to closure by incident management team.	None	None	No Exceptions Noted.
CA48	For revocation of access to corporate jump server of Linux based corporate server of Zoho, the request is raised in Zoho SDP. System administration team revokes access to jump server for the associate. For associates leaving from Zoho, the access to jump server is revoked on the associate's last working date.	CC5.2 CC6.1 CC6.2 CC6.3	Inspected the user list, tickets and logs for access revocation to Linux based corporate server of Zoho and we noted that there were no instances of access revocation during the examination period. Further, obtained email confirmation from System Admin Head, stating that, that there were no instances of access revocation to Linux based corporate server of Zoho during the examination period. Therefore, DHS LLP could not test the operating effectiveness of access revocation to Linux based corporate server of Zoho during the examination period	None	None	The operating effectiveness of the control activity could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA49	Access to passman is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).	CC5.2 CC6.1 CC6.2	Inspected the RACI Sheet and email communication relating to review of access to passman for aspects such as 'Date of review', 'Reviewed by' and 'Corrective action performed to ascertain whether access to passman was reviewed by the System administration team on an annual basis and whether corrective action was performed by System administration team for discrepancies identified (if any).	None	None	No Exceptions Noted.
CA50	Access to corporate jump server is reviewed by the System administration team on an annual basis. Corrective action is performed by System administration team for discrepancies identified (if any).	CC5.2 CC6.1 CC6.2	Inspected the RACI Sheet and email communication relating to review of access to corporate jump server for aspects such as 'Date of review', 'Reviewed by' and 'Corrective action performed to ascertain whether access to corporate jump server was reviewed by the System administration team on an annual basis and whether corrective action was performed by System administration team for discrepancies identified (if any).	None	None	No Exceptions Noted.
CA51	Security setting for authentication to Zoho Corporate VPN is managed by Active Directory.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1	Inspected authentication configuration of VPN application for aspects such as 'Tool name' and 'Integration' to ascertain whether security setting for authentication to Zoho Corporate VPN was managed by Active Directory.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA52	Incidents raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.	CC2.2 CC2.3 CC3.1 CC4.1 CC7.3 CC7.4 CC7.5	Inspected for sample incidents, the ticket from creator tool for aspects such as ‘Incident ID’, ‘Incident Title’, ‘Description of the incident’, ‘RCA available’, ‘Raised By’ ‘Incident Cause’, ‘Incident Category’ and ‘Incident start time’ and ‘Status’ to ascertain whether incidents raised from customer were raised as ticket in Zoho Desk Portal which was assigned to the Zoho incident management team for resolution and whether the relevant product team performed root cause analysis (RCA) and updates the incident in the Zoho creator tool.	3.11.5	None	No Exceptions Noted.
CA53	Local Admin Rights and access to removable device is restricted for Zoho workstations.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1	Inspected for sample workstations the local admin rights and removable device restriction configuration for aspects such as 'Host name', 'Type of OS', 'Location' and 'Status of local admin rights' to ascertain whether local Admin Rights was restricted for Zoho workstations.	None	None	Exception Noted. Refer Exception #6
CA54	Key Management Service policy of Zoho is defined by Encryption at Rest team. The policy document is reviewed and approved by Security team manager on an annual basis. The policy document defines the use of encryption and methods used.	CC5.1 CC6.1 CC6.2 CC6.3	Inspected Key management service policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether key management service policy of Zoho was defined by Encryption at Rest team and whether the policy document was reviewed and approved by Security team manager on an annual basis and whether the policy document defined the use of encryption and methods used.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA55	Internal audit policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Director of compliance on an annual basis. The policy document defines the roles, responsibilities and key activities of the internal audit function of Zoho.	CC1.1 CC1.2 CC1.3 CC3.1 CC4.1 CC5.1	Inspected Internal audit policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether internal audit policy of Zoho was defined by Information security compliance Manager and whether the policy document was reviewed and approved by Director of compliance on an annual basis and whether the policy document defined the roles, responsibilities and key activities of the internal audit function of Zoho.	None	None	No Exceptions Noted.
CA56	Risk management policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Information Security Compliance Manager on an annual basis. The policy document defines the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.	CC1.2 CC1.5 CC3.1 CC3.2 CC4.1 CC5.1 CC9.1	Inspected Risk management policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether risk management policy of Zoho was defined by Information security compliance Manager and whether the policy document was reviewed and approved by Information Security Compliance Manager on an annual basis and whether the policy document defined the process for operational, strategic and IT risks related to the infrastructure and services provided by Zoho.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA57	Information Security Management System policy of Zoho is defined by Information security compliance Manager. The policy document is reviewed and approved by Chief Information Security Officer on an annual basis. The policy document defines the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.	CC1.1 CC1.2 CC1.3 CC3.1 CC5.1 CC7.2 CC9.1 P1.1	Inspected Information Security Management System policy for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether Information Security Management System policy of Zoho was defined by Information security compliance Manager and whether the policy document was reviewed and approved by Chief Information Security Officer on an annual basis and whether the policy document defined the measures to minimize risk, ensure business continuity, and meet regulatory compliance of Zoho.	None	None	No Exceptions Noted.
CA58	Business continuity plan of Zoho is defined by Information security compliance Manager. The plan document is reviewed and approved by BCP Head on an annual basis. The plan document outlines how a business will continue to operate during an unplanned disruption in Zoho.	CC3.2 CC5.1 CC7.2 CC7.3 A1.1 A1.3	Inspected Business continuity plan of Zoho for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether business continuity plan of Zoho was defined by Information security compliance Manager and whether the plan document was reviewed and approved by BCP Head on an annual basis and whether the plan document outlines how a business would continue to operate during an unplanned disruption in Zoho.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA59	Management Review Meeting is performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment.	CC1.1 CC1.2 CC1.3 CC3.1 CC4.2 CC5.1 CC9.1 P4.1	Inspected management review minutes of meeting and presentation for aspects such as 'Scope', 'Audit period', 'Meeting participants', 'Date of meeting' and 'Action items' to ascertain whether Management Review Meeting was performed for the support functions of Zoho on an annual basis to discuss the key findings noted in the internal audit, incorporate management functions and also to reviewed the risk assessment.	None	None	No Exceptions Noted.
CA60	Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis. Risk assessment for the support functions of Zoho is performed on an annual basis and updated in risk registry. The risk registry is reviewed by manager of support function on an annual basis.	CC1.2 CC3.1 CC3.3 CC4.1 CC5.3 CC7.1	Inspected for sample support functions the risk registry for aspects such as 'Scope', 'Date of risk assessment', 'Risk summary', 'Reviewed by' and 'Reviewed on' to ascertain whether risk assessment for the support functions of Zoho was performed on an annual basis and updated in risk registry and whether the risk registry was reviewed by manager of support function on an annual basis.	None	None	No Exceptions Noted.
CA61	Risk assessment for the products of Zoho on information security and privacy is performed on an annual basis and updated in risk registry. The risk registry is reviewed by product managers on an annual basis.	CC1.2 CC3.1 CC3.3 CC4.1 CC5.3 CC7.1 P4.1	Inspected for sample products the risk registry for aspects such as 'Scope', 'Date of risk assessment', 'Risk summary', 'Reviewed by', Types of risk assessment’ and 'Reviewed on' to ascertain whether risk assessment for the products of Zoho on information security and privacy was performed on an annual basis and updated in risk registry and whether the risk registry was reviewed by product managers on an annual basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA62	Master service agreement is signed between Zoho and third party vendor. Any changes to the contracts are agreed by Zoho and the third party vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	CC2.3 CC3.3 CC4.1 CC9.2	Inspected for sample vendors the master service agreement for aspects such as 'Vendor name', 'Scope of service', 'Signatory details', 'availability of confidentiality and related clauses' and 'Tenure' to ascertain whether master service agreement was signed between Zoho and third party vendor and whether any changes to the contracts were agreed by Zoho and the third party vendor and whether the contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	None	None	No Exception Noted.
CA63	Zoho provides data subjects with 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.	P3.1 P3.2 P6.1	Inspected the signup page of Zoho for aspects such as ‘Signup form’ and ‘Availability of consent option’ to ascertain whether Zoho provided data subjects with user interface (UI) screens that had a click button that captured and records a data subject’s consent before the data subject submits the information.	3.11.6	None	No Exceptions Noted.
CA64	Cloud Products of Zoho are authenticated using identity and access management portal. Users can also authenticate using third party single sign on option.	CC5.2 CC6.1 CC6.2 CC6.3 PI1.2	Inspected for sample cloud products the authentication page for aspects such as 'Product name', 'Datacenter' and 'Authentication option' to ascertain whether cloud products of Zoho were authenticated using identity and access management portal and whether the users can also authenticate using third party single sign on option.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA65	For creation of access to admin panel of Cloud Products of Zoho, the request is raised in Zoho IAN. Server Operations Team creates access to Zodoor account for the associate based on the approval provided by Associates' Manager.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.3	Inspected for sample Zodoor account access creation from Zoho IAN for aspects such as 'Associate name', 'Joining date', 'Access approved on', 'Access created on' and 'Request ID in IAN' to ascertain whether for creation of access to admin panel of Cloud Products of Zoho, the request was raised in Zoho IAN and whether Server Operations Team created access to Zodoor account for the associate based on the approval provided by Associates' Manager.	None	None	No Exceptions Noted.
CA66	For associates leaving Zoho, the Zodoor account is revoked based on the integration with Zoho People.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.3	Inspected the Zero Trust and Zoho people integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the Zodoor account was revoked based on the integration with Zoho People.	None	None	No Exceptions Noted.
CA67	IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any)	CC5.2 CC6.1 CC6.2 CC6.3	Inspected the IAM role review report for aspects such as 'Content of report', 'Date of review', 'Reviewed on', 'Approval details' and 'Corrective action taken' to ascertain whether IAM roles access to Zoho associates were reviewed on an annual basis and whether the extension of IAM roles were based on approval provided by the associate and associate's manager and whether corrective action was performed by IAM team for discrepancies identified (if any)	3.11.1	None	Exception Noted. Refer Exception #7

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA68	Product description and terms of use for Zoho Cloud products is published in company's website.	CC5.2 PI1.1 PI1.2	Inspected for sample products the product description page and terms of use page for aspects such as 'Product name', 'Product description page URL' and 'Product terms of use page URL' to ascertain whether product description and terms of use for Zoho Cloud products was published in company's website.	3.11.3	None	No Exception Noted.
CA69	Software development life cycle document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the change testing and deployment process for the product.	CC3.4 CC5.1 CC5.3 PI1.3	Inspected for sample products the software development life cycle document for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether software development life cycle document of Zoho Cloud products was defined by the product team and whether the document was reviewed and approved by Product manager on an annual basis and whether the document defined the change testing and deployment process for the product.	None	None	No Exceptions Noted.
CA70	Support process document of Zoho Cloud products is defined by the product team. The document is reviewed and approved by Product manager on an annual basis. The document defines the support process and data flow of the product.	CC2.3 CC5.3 PI1.1 PI1.2	Inspected for sample products the support process document for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether Support process document of Zoho Cloud products was defined by the product team and whether the document was reviewed and approved by Product manager on an annual basis and whether the document defined the support process and data flow of the product.	None	None	No Exception Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA71	Zoho Cloud products maintain dedicated development and test environment in local Zoho. The local Zoho environment is segregated from production environment of Zoho Cloud products.	CC5.1 CC8.1 PI1.3	Inspected for sample cloud products the production and local page for aspects such as 'Product name', 'Product page URL' and 'Local page URL' to ascertain whether Zoho Cloud products maintained dedicated development and test environment in local Zoho and whether the local Zoho environment was segregated from production environment of Zoho Cloud products.	None	None	No Exception Noted.
CA72	Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website.	CC3.4 CC5.1 CC5.2 CC8.1 PI1.3	Inspected for sample changes made to Cloud/On-Prem product the deployment logs for aspects such as 'Build URL', 'Date of local deployment', 'Date of production deployment'; Further inspected for sample changes made to Cloud product the testcases and testing signoff record for aspects such as 'Tested by', 'Tested on' and 'Testcases' to ascertain whether changes made to Cloud products were deployed using inhouse SD tool to production and local environment and whether the build generated were tested in local Zoho and signoff was provided by product manager before deployment in production environment/publishing in website.	3.11.7	None	Exception Noted. Refer Exception #8

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA73	Changes made to Cloud products are reviewed for code vulnerabilities using inhouse Hacksaw tool. Exceptional approval is provided by the product manager if the changes are deployed in production environment/publishing in website with blocking issue.	CC3.4 CC5.1 CC8.1 PI1.3	Inspected for sample changes made to Cloud product the hacksaw report and exceptional approval records for aspects such as 'Build URL', 'Number of blocking issue', 'Exceptional approval provided by' and 'Exceptional approval provided on' to ascertain whether changes made to Cloud products were reviewed for code vulnerabilities using inhouse Hacksaw tool and whether exceptional approval was provided by the product manager if the changes were deployed in production environment/publishing in website with blocking issue.	None	None	No Exceptions Noted.
CA74	Log of activities performed by users in Zoho Cloud products are stored using Zoho logs application.	CC6.3 CC7.1 PI1.2	Inspected for sample cloud products the Zoho logs application page for aspects such as 'Product name', 'Datacenter ID', 'Type of logs' and 'Retention of logs' to ascertain whether log of activities performed by users in Zoho Cloud products were stored using Zoho logs application.	None	None	No Exceptions Noted.
CA75	Customer Support process document of Zoho is defined by the Zoho customer support team. The document is reviewed and approved by Director of customer support team on an annual basis. The document defines the support process for Zoho products.	CC2.3 CC5.3 A1.2 PI1.1	Inspected customer support process document for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether customer support process document of Zoho was defined by the Zoho customer support team and whether the document was reviewed and approved by Director of customer support team on an annual basis and whether the document defined the support process for Zoho products.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA76	Customer support tickets raised by customer over email/chat/phone are automatically raised as ticket in Zoho desk application. The support tickets are resolved within agreed SLA with customer by Zoho Technical Support team.	CC2.3 A1.2 PI1.1 PI1.3	Inspected for sample support tickets the SDP ticket for aspects such as 'Ticket ID', 'Ticket opened on', 'Ticket closed on', 'Resolution provided' and 'Status' to ascertain whether customer support tickets raised by customer over email/chat/phone were automatically raised as ticket in Zoho desk application and whether the support tickets were resolved within agreed SLA with customer by Zoho Technical Support team.	None	None	No Exceptions Noted.
CA77	Network Operations policy and procedure of Zoho is defined by the NOC team. The document is reviewed and approved by NOC manager on an annual basis. The document defines the network operations of Zoho.	CC1.1 CC1.2 CC3.1 CC5.1 CC6.1 CC6.2	Inspected Network Operations policy and procedure for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether network operations policy and procedure of Zoho was defined by the NOC team and whether the document was reviewed and approved by NOC manager on an annual basis and whether the document defined the network operations of Zoho.	None	None	No Exceptions Noted.
CA78	Servers onboarded in IDC network are hardened using standard image by server operations team.	CC5.1 CC5.2 CC6.6 CC6.7	Inspected for sample newly onboarded servers the hardening log for aspects such as ‘Hostname’, ‘Date of onboarding’, ‘Date of hardening’ and ‘Type of OS’ to ascertain whether servers onboarded in IDC network were hardened using standard image by server operations team.	None	None	Exceptions Noted. Refer Exception #9

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA79	Network diagram of Zoho is defined by the Network operations team. The network diagram is reviewed and approved by Network operations team on an annual basis. The network diagram defines the components and connections within Zoho network.	CC3.3 CC3.4 CC5.1 CC6.1 CC6.2 CC6.3	Inspected network diagram for aspects such as 'Scope', 'Content of network diagram', 'Reviewed by' and 'Date of review' to ascertain whether network diagram of Zoho was defined by the Network operations team and whether the network diagram was reviewed and approved by network operations team on an annual basis and whether the network diagram defined the components and connections within Zoho network.	None	None	No Exceptions Noted.
CA80	For creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network operations team creates access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.	CC5.2 CC6.1 CC6.2 CC6.3	Inspected for sample access creation to network operations tools the SDP ticket for aspects such as 'Associate joining date', 'Ticket ID', 'Approved by', 'Approved on', 'Access created by', 'Access created to' and 'Access created on' to ascertain whether for creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request was raised in Zoho SDP and whether network operations team created access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA81	For revocation of access to a Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request is raised in Zoho SDP. Network Operations team revokes access to Network Operations tools for the associate. For associates leaving from Zoho, the access to Network Operations tools is revoked on the associate's last working date.	CC5.2 CC6.1 CC6.2 CC6.3	Inspected for sample access revocation to network operations tools the SDP ticket for aspects such as 'Associate last working date', 'Ticket ID', 'Approved by', 'Approved on', 'Access revoked by', 'Access revoked to' and 'Access revoked on' to ascertain whether for creation of access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman), the request was raised in Zoho SDP and whether network operations team created access to Network Operations tools for the associate based on the approval provided by Network Operations Manager.	None	None	No Exceptions Noted.
CA82	Access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is reviewed by the Network Operations team on an Annual basis. Corrective action is performed by Network Operations team for discrepancies identified (if any)	CC4.1 CC5.2 CC6.1 CC6.2	Inspected NOC Tool (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) user Access review report for aspects such as 'Scope of review', 'Reviewed by', 'Reviewed on' and 'Corrective action performed' to ascertain whether access to Network Operation tools (Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho was reviewed by the Network Operations team on an Annual basis and whether corrective action was performed by Network Operations team for discrepancies identified (if any)	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA83	Administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho is restricted to NOC engineers.	CC5.2 CC6.1 CC6.2 CC6.3	Inspected user listing of Network operation tools for aspects such as 'user details', 'Team as per HR' and 'Type of access' to ascertain whether administrative access to Network Operation tools (NOCMON, Network Configuration Manager, Event Log Analyzer and Network Operations Passman) of Zoho was restricted to NOC engineers.	None	None	No Exceptions Noted.
CA84	Security setting for password configurations and account lockout configuration of Firewall are defined as per Zoho password policy.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1	Inspected for sample network devices the password configuration and Zoho password policy for aspects such as 'Host name', 'Password configuration', 'Account lockout configuration' and 'Password guidelines as per policy' to ascertain whether security setting for password configurations and account lockout configuration of Firewall were defined as per Zoho password policy.	None	None	No Exceptions Noted.
CA85	Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure.	CC6.6 CC7.1 CC7.3	Inspected the penetration testing report for aspects such as 'Scope', 'Scan result' and 'closure action performed' to ascertain whether penetration testing was performed for External IP of Zoho on an annual basis and whether vulnerabilities identified if any were tracked to closure.	None	None	Exception Noted. Refer Exception #10

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA86	Firewall, Router and Managed Switches are monitored for downtime and process utilization using NOCMON tool. Network Operations team performs follow-up action for anomalies identified.	CC5.1 CC6.6 CC6.7 CC7.1 CC7.3 A1.1	Inspected for sample network devices the monitoring configuration for aspects such as 'Hostname', 'Parameters monitored' and 'monitoring tool'; Further inspected for sample NOCMON alerts the tickets for aspects such as 'Ticket ID', 'Date of incident opening', 'Date of incident closing', 'Closure action performed' to ascertain whether Firewall, Router and Managed Switches were monitored for downtime and process utilization using NOCMON tool and whether Network Operations team performed follow-up action for anomalies identified.	None	None	No Exception Noted.
CA87	Log of activities performed by users in Firewall, Router and Managed Switches are stored using Zoho logs application. The access to view logs is restricted to authorized personnel from Network Operations team.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1 CC7.3	Inspected for sample network devices the log monitoring configuration for aspects such as 'Hostname' and 'log forwarding status'; Further inspected Zoho logs application for aspects such 'Type of logs monitored' and 'Access list' to ascertain whether log of activities performed by users in Firewall, Router and Managed Switches were stored using Zoho logs application and whether the access to view logs was restricted to authorized personnel from Network Operations team.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA88	Backup of Network device configurations (Firewall, Router and Managed Switches) are performed using Network Configuration Manager tool on a daily basis (Full Backup). In case of a backup failure, an automated email is triggered and remediation action is taken by Network Operations team.	CC5.1 CC6.6 CC6.7 CC7.1 A1.2 A1.3	Inspected for sample network devices the backup configuration for aspects such as 'Hostname', 'Type of backup' and 'backup frequency'; Further inspected for sample dates the backup logs for aspects such as 'Backup status' and 'Corrective action performed' to ascertain whether backup of Network device configurations (Firewall, Router and Managed Switches) were performed using Network Configuration Manager tool on a daily basis (Full Backup) and whether in case of a backup failure, an automated email was triggered and remediation action was taken by Network Operations team.	None	None	No Exceptions Noted.
CA89	Business continuity test is performed for NOC room on an annual basis by Network Operations team.	CC3.2 CC5.1 CC7.2 A1.1 A1.3	Inspected business continuity test report for aspects such as 'Scope', 'Date of test' and 'Test Outcome' to ascertain whether business continuity test was performed for NOC room on an annual basis by Network Operations team.	None	None	No Exceptions Noted.
CA90	All rules of Zoho wide area network is blocked by default at Firewall by Network Operations team.	CC5.1 CC6.1 CC6.2 CC6.3 CC7.1	Inspected for sample firewall the firewall rules for aspects such as 'Hostname' and 'Default deny all rule' to ascertain whether all rules of Zoho wide area network was blocked by default at Firewall by Network Operations team.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA91	For addition/modification for firewall ruleset, the request is raised in Zoho SDP. Network Operations team adds/modifies firewall ruleset for request based on the approval provided by Network Operations Manager.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1 CC7.3	Inspected for sample firewall ruleset changes the SDP ticket for aspects such as 'Ticket ID', 'Date of ticket opening', 'Date of ticket closing', 'Approved by', 'Approved on' to ascertain whether for addition/modification for firewall ruleset, the request was raised in Zoho SDP and whether Network Operations team added/modified firewall ruleset for request based on the approval provided by Network Operations Manager.	None	None	No Exceptions Noted.
CA92	For changes to network device configuration, the request is raised in Zoho SDP. Network Operations team changes network device configuration based on approval provided by Network Operations Manager.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1 CC7.3	Inspected for sample network device configuration changes the SDP ticket for aspects such as 'Ticket ID', 'Date of ticket opening', 'Date of ticket closing', 'Approved by', 'Approved on' to ascertain whether for changes to network device configuration, the request was raised in Zoho SDP and whether network Operations team changed network device configuration based on approval provided by Network Operations Manager.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA93	Rules of Zoho wide area network and local area network is reviewed by Network Operations team on a half yearly basis. Network Operations team performs follow-up action for anomalies identified.	CC5.1 CC6.1 CC6.2 CC6.3 CC7.1 CC7.3	Inspected for sample half year the firewall rule review ticket for aspects such as 'Ticket ID', 'Scope', 'Date of review' and 'Reviewed by' to ascertain whether rules of Zoho wide area network and local area network was reviewed by Network Operations team on a half yearly basis. Inspected the firewall rule review ticket and we noted that there were no instances of anomalies noted from the rule review during the examination period. Further, obtained email confirmation from Network Operations Head, stating that, that there were no instances of anomalies noted from the rule review during the examination period. Therefore, DHS LLP could not test the operating effectiveness of follow-up action for anomalies identified from rule review during the examination period	None	None	No Exceptions Noted. The operating effectiveness of corrective action performed for anomalies identified from rule review could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA94	For setup/modification to segregated VLAN, the request is raised in Zoho SDP. Network Operations team creates/modifies segregated VLAN for the request based on the approval provided by Network Operations Manager.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1 CC7.3	Inspected for sample VLAN setup/modification request the SDP ticket for aspects such as 'Ticket ID', 'Date of ticket opening', 'Date of ticket closing', 'Approved by', 'Approved on' to ascertain whether for setup/modification to segregated VLAN, the request was raised in Zoho SDP and whether Network Operations team created/modified segregated VLAN for the request based on the approval provided by Network Operations Manager.	None	None	No Exceptions Noted.
CA95	MAC Binding is implemented for workstation connecting from NOC room to IDC network.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1 CC7.3	Inspected for sample workstations connecting to IDC the MAC binding configuration for aspects such as 'Host name' and 'MAC Binding configuration' to ascertain whether MAC Binding was implemented for workstation connecting from NOC room to IDC network.	None	None	No Exceptions Noted.
CA96	Communication between primary and secondary datacenter are by ethernet over MACsec security. Standby IPsec tunnel is established to ensure redundancy of connectivity.	CC5.1 CC6.6 CC6.7 CC7.1 CC7.2 A1.2	Inspected the tunneling configuration for aspects such as 'Datacenter ID', 'Authentication protocol' and 'Availability of standby IPsec tunnel' to ascertain whether Communication between primary and secondary datacenter were by ethernet over MACsec security and whether standby IPsec tunnel was established to ensure redundancy of connectivity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA97	Zoho IDC network and corporate network are supported by primary and standby ISP Link to ensure redundancy of internet connectivity.	CC4.2 CC5.3 CC6.6 CC6.7 CC7.2 A1.1	Inspected the ISP link configuration for aspects such as 'Datacenter ID' and 'Availability of redundant ISP' to ascertain whether Zoho IDC network and corporate network were supported by primary and standby ISP Link to ensure redundancy of internet connectivity.	None	None	No Exceptions Noted.
CA98	Firewall, Router and Managed Switches of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.	CC2.1 CC3.4 CC4.1 CC6.1 A1.1	Inspected for sample network device time sync configuration for aspects such as 'Host name', 'Time sync configuration' and 'Time sync source' to ascertain whether Firewall, Router and Managed Switches of Zoho were connected to Network time protocol server and whether the network time protocol server fetch time from authorized time sync source.	None	None	No Exceptions Noted.
CA99	Zoho Network Operations team maintains an asset registry of the Firewalls, Routers and Managed Switches.	CC2.1 CC3.3 CC5.1 CC6.7 CC7.1	Inspected the asset inventory for aspects such as 'Type of asset', 'Asset owner' and 'Criticality' to ascertain whether Zoho Network Operations team maintained an asset registry of the Firewalls, Routers and Managed Switches.	None	None	No Exceptions Noted.
CA100	Ingress traffic to IDC network of Zoho is scanned for Distributed Denial of Service attack by DDoS Monitoring tool.	CC5.3 CC6.6 CC6.7 CC7.1 CC7.5 A1.1	Inspected the DDoS Monitoring configuration for aspects such as 'Datacenter ID', 'Ingress source' and 'Implementation of DDoS monitoring' to ascertain whether Ingress traffic to IDC network of Zoho was scanned for Distributed Denial of Service attack by DDoS Monitoring tool.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA101	Network Operations team reviews the third party reports of co location datacenter on an annual basis. Follow-up action is performed by compliance team for exceptions identified.	CC1.3 CC3.2 CC4.1 CC5.1 CC6.5 CC7.4 P6.4	Inspected reports relating to review of third party report for aspects such as 'Datacenter ID', 'Vendor name', 'Exceptions identified', 'Relevance to Zoho' and 'Follow-up action performed' to ascertain whether Network Operations team reviewed the third party reports of co location datacenter on an annual basis and whether follow-up action was performed by compliance team for exceptions identified.	None	None	No Exceptions Noted.
CA102	Master service agreement is signed between Zoho and co location datacenter hosting service vendor. Any changes to the contracts are agreed by Zoho and the co location datacenter hosting service vendor. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	CC2.3 CC3.3 CC4.1 CC9.2 P6.2 P6.4 P6.5	Inspected the master service agreement with co-location vendors for aspects such as 'Datacenter ID', 'Vendor name', 'Signatory details', 'Scope', 'Availability of confidentiality and related clause' and 'Tenure' to ascertain whether master service agreement was signed between Zoho and co location datacenter hosting service vendor and whether any changes to the contracts were agreed by Zoho and the co location datacenter hosting service vendor and whether the contract included the scope of services to be provided, confidentiality and other related commitments / clauses.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA103	Zoho enters into Master Service Agreement (MSA) with customer based on request raised. The agreement covers scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.	CC2.3 CC3.3 CC4.1 CC9.2 A1.1 C1.1 PI1.1 P6.4 P6.5	Inspected for sample MSA request from customer the agreement and ticket for aspects such as 'Request ID', 'Date of request opening', 'Date of request closing', 'Signatory', 'availability of confidentiality and related clauses' and 'Tenure' to ascertain whether Zoho entered into Master Service Agreement (MSA) with customer based on request raised and whether the agreement covered scope, definition of services and confidentiality requirements relating to hosting and support services of Zoho application.	3.11.2	None	No Exceptions Noted.
CA104	Disciplinary complaints (if any) are raised to Zoho's HR team for appropriate action as per Zoho Disciplinary action policy.	CC1.1 CC1.2 CC1.3 CC1.5 CC2.3	Inspected the disciplinary complaints tracker and noted that there were no instance of disciplinary complaints raised during the examination period. Further obtained email confirmation from HR head stating that there were no instance of disciplinary complaints during the examination period. Therefore, DHS LLP could not test the operating effectiveness of follow up action performed for disciplinary complaints raised during the examination period.	None	None	The operating effectiveness of the control activity could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA105	Zoho legal team records the data disclosure request raised to Zoho. When required, consent of data subject is obtained before processing the request. Privacy team reviews the data disclosure request status on an annual basis.	P5.1 P6.1 P6.2 P6.7	Inspected for sample Disclosure request the ticket for aspects such as 'Request ID', 'Date of request opening', 'Date of request closing', 'consent from customer', 'type of request' and 'type of data shared' to ascertain whether Zoho legal team recorded the data disclosure request raised to Zoho and whether when required, consent of data subject was obtained before processing the request and whether privacy team reviewed the data disclosure request status on an annual basis.	None	None	No Exceptions Noted.
CA106	Server Operations policy and procedure of Zoho is defined by the Server Operations team. The document is reviewed and approved by Server Operations manager on an annual basis. The document defines the server operations of Zoho including procedures for degaussing the disks.	CC2.1 CC4.1 CC5.3 CC6.4 CC7.3	Inspected Server Operations policy and procedure document for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether server operations policy and procedure of Zoho was defined by the Server Operations team and whether the document was reviewed and approved by Server Operations manager on an annual basis and whether the document defined the server operations of Zoho including procedures for degaussing the disks.	None	None	No Exceptions Noted.
CA107	For associates joining Zoho, the Zero Trust account is created based on the integration with Zoho People.	CC2.1 CC5.2 CC6.1 CC6.2	Inspected the Zero Trust and Zoho people integration aspects such as 'Tool name' and 'Integration' to ascertain whether for associates joining Zoho, the Zero Trust account was created based on the integration with Zoho People.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA108	For associates leaving Zoho, the Zero Trust account is revoked based on the integration with Zoho People.	CC2.1 CC5.2 CC6.1 CC6.2	Inspected the Zero Trust and Zoho people integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the Zero Trust account was revoked based on the integration with Zoho People.	None	None	No Exceptions Noted.
CA109	For creation of access to Zero Trust policy, the request is raised in Zero trust application by the associate. SPM team creates access to the associate based on the report from hardening agent installed at the associate's endpoint.	CC2.1 CC3.4 CC5.2 CC6.1 CC6.2	Inspected for sample zero trust policy access creation the ticket for aspects such as 'Policy name', 'Approved by', 'Approved on', 'Access created by', 'Access created on' and 'Hardening agent version' to ascertain whether for creation of access to Zero Trust policy, the request was raised in Zero trust application by the associate and whether SPM team created access to the associate based on the report from hardening agent installed at the associate's endpoint.	None	None	No Exceptions Noted.
CA110	The logs for just in time access are recorded and stored in Zero trust application.	CC2.2 CC5.2 CC6.3 CC6.5 CC7.1	Inspected the logs from Zero trust for aspects such as 'Date of log' and 'parameters recorded' to ascertain whether the logs for just in time access were recorded and stored in Zero trust application.	None	None	No Exceptions Noted.
CA111	Data copy restriction is imposed for IDC servers of Zoho.	CC5.2 CC6.6 CC6.7 CC7.1	Inspected for sample IDC servers the security configuration for aspects such as 'Host name' and 'Data copy restriction' to ascertain whether data copy restriction was imposed for IDC servers of Zoho.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA112	IDC servers of Zoho are monitored for execution of sensitive commands using HI agent installed in the server. The logs are centrally stored in Zoho logs application for a period of 30 days.	CC4.1 CC5.2 CC6.6 CC6.7 CC7.1 PI1.4 A1.2	Inspected for sample IDC servers the monitoring agent for aspects such as 'Host name' and 'Status of HI Agent' to ascertain whether IDC servers of Zoho were monitored for execution of sensitive commands using HI agent installed in the server. Further inspected the Zoho logs application for aspects such as 'Datacenter ID', 'Type of log' and 'Log retention period' to ascertain whether the logs were centrally stored in Zoho logs application for a period of 30 days.	None	None	No Exceptions Noted.
CA113	Server operations team on an annual basis switches service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.	CC6.7 CC7.2 CC7.3 A1.1 A1.3	Inspected the Disaster recovery readiness report for aspects such as 'Datacenter ID', 'Date of test' and 'Test outcome' to ascertain whether server operations team on an annual basis switched service from main datacenter to disaster recovery datacenter to ensure Disaster Recovery (DR) readiness.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA114	For creation of access to Jump server, the request is raised in Zoho SDP. Server Operations team creates access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.	CC2.1 CC5.2 CC6.1 CC6.2 CC6.3	Inspected for sample access creation to jump server the SDP ticket for aspects such as 'Ticket ID', 'Associate name', 'Associate date of joining', 'Approved by', 'Approved on', 'Access created by' and 'Access created on' to ascertain whether for creation of access to Jump server, the request was raised in Zoho SDP and whether server operations team created access to jump server and IDC server account for the associate based on the approval provided by Server Operations Manager from puppet tool.	None	None	No Exceptions Noted.
CA115	For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date.	CC2.1 CC5.2 CC6.1 CC6.2 CC6.3	Inspected for sample access revocation to jump server the SDP ticket for aspects such as 'Ticket ID', 'Associate name', 'Associate last working date', 'Access revoked by' and 'Access revoked on' to ascertain whether for revocation of access to jump server, the request was raised in Zoho SDP and whether server operations team revoked access to Jump server and IDC server account for the associate and whether for associates leaving from Zoho, the access to Jump server and IDC server account was revoked on the associate's last working date.	None	None	Exception Noted. Refer Exception #11
CA116	Administrative access to Jump Server of Zoho is restricted to Server Operations team.	CC5.1 CC6.1 CC6.2 CC6.3	Inspected the user access list of jump server for aspects such as 'User listing' and 'Team name' to ascertain whether administrative access to Jump Server of Zoho was restricted to Server Operations team.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA117	Security setting for password configurations and account lockout configuration of jump server are generated in Zoho Passman tool based on the configuration defined in Zoho password policy.	CC5.2 CC6.1 CC6.2 CC6.3 CC7.1	Inspected Zoho password policy and password setting of jump server for aspects such as 'Password guidelines', 'Password settings' and 'Account lockout settings' to ascertain whether security setting for password configurations and account lockout configuration of jump server were generated in Zoho Passman tool based on the configuration defined in Zoho password policy.	None	None	No Exceptions Noted.
CA118	For creation of access to Server Operation tools (ZAC and Server Operations Passman), the request is raised in Zoho SDP. Server Operations team creates access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.	CC2.1 CC5.2 CC6.1 CC6.2	Inspected for sample access creation to server operation tools the SDP ticket for aspects such as 'Associate joining date', 'Ticket ID', 'Approved by', 'Approved on', 'Access created by', 'Access created to' and 'Access created on' to ascertain whether for creation of access to Server Operation tools (ZAC and Server Operations Passman), the request was raised in Zoho SDP and whether server operations team created access to Server Operations tools for the associate based on the approval provided by Server Operations Manager.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA119	For associates leaving Zoho, the access to Server Operations Passman tool is revoked based on the integration with IAM. For associates leaving Zoho, the access to ZAC is revoked based on the integration with Zoho People.	CC2.1 CC5.2 CC6.1 CC6.2	Inspected the passman tool and IAM integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the access to Server Operations Passman tool was revoked based on the integration with IAM. Further inspected the ZAC tool and Zoho people integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the access to ZAC was revoked based on the integration with Zoho People.	None	None	No Exceptions Noted.
CA120	Administrative access to Server Operation tools (ZAC and Server Operations Passman) of Zoho is restricted to Server Operations Team.	CC5.1 CC6.1 CC6.2 CC6.3	Inspected the user access list of server operations tools for aspects such as 'User listing' and 'Team name' to ascertain whether administrative access to server operation tools (ZAC and Server Operations Passman) of Zoho was restricted to Server Operations Team.	None	None	No Exceptions Noted.
CA121	Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.	CC3.4 CC5.2 CC6.1 CC6.2 CC6.7 CC7.1 CC7.3	Inspected for sample IDC patches the ticket for aspects such as 'Patch ID', 'Tested by', 'Tested on', 'Approved by', 'Approved on' and 'Deployed on' to ascertain whether operating system of IDC servers were patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager.	None	None	Exception Noted. Refer Exception #12

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA122	Server Operations team has implemented load balancers for IDC servers.	CC5.1 CC6.7 CC7.1 CC7.2 A1.1	Inspected for sample IDC servers the load balancing configuration for aspects such as 'Host name' and 'Integration with load balancer' to ascertain whether server operations team had implemented load balancers for IDC servers.	None	None	No Exceptions Noted.
CA123	Files uploaded to Zoho applications are scanned for malware content before storing data in IDC network. Anomalies identified if any are blocked from upload. Malware check validation for application code relating to file upload is validated using Hacksaw tool.	CC3.4 CC5.2 CC6.6 CC6.7 CC7.1 CC7.3 PI1.2	Inspected the malware monitoring configuration for aspects such as 'Malware database', 'Scan scope' and 'follow-up action configuration' to ascertain whether files uploaded to Zoho applications were scanned for malware content before storing data in IDC network and whether anomalies identified if any were blocked from upload. Further inspected the hacksaw tool for aspects such as 'Hacksaw validation rule' and 'file upload check' to ascertain whether malware check validation for application code relating to file upload was validated using Hacksaw tool.	None	None	No Exceptions Noted.
CA124	IDC servers of Zoho are connected to Network time protocol server. The Network time protocol server fetch time from authorized time sync source.	CC2.1 CC3.4 CC4.1 CC6.1 A1.1	Inspected for sample IDC servers the time sync configuration for aspects such as 'Host name', 'time sync configuration' and 'Time sync source' to ascertain whether IDC servers of Zoho are connected to Network time protocol server and whether the Network time protocol server fetch time from authorized time sync source.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA125	IDC servers of Zoho are restricted from accessing internet.	CC5.1 CC6.6 CC6.7 CC7.1	Inspected for sample IDC servers the ping configuration for aspects such as 'Host name' and 'Internet access block' to ascertain whether IDC servers of Zoho were restricted from accessing internet.	None	None	No Exceptions Noted.
CA126	IDC servers of Zoho are blocked from mounting removable device.	CC5.2 CC6.6 CC6.7 CC7.1	Inspected for sample IDC servers the mount configuration for aspects such as 'Host name' and 'removable device block' to ascertain whether IDC servers of Zoho were blocked from mounting removable device.	None	None	No Exceptions Noted.
CA127	Zoho Server Operations team maintains an asset registry of the IDC Servers.	CC2.1 CC3.3 CC5.1 CC6.1 CC6.8	Inspected the asset inventory for aspects such as 'Type of asset' and 'Parameters' to ascertain whether Zoho server operations team maintained an asset registry of the IDC Servers.	None	None	No Exceptions Noted.
CA128	Zoho uses asset discovery tool to identify and track the servers added in IDC network.	CC2.1 CC5.1 CC6.1 CC6.7 CC7.1	Inspected the ZAC tool configuration for aspects such as 'Scan source' and 'Datacenter ID' to ascertain whether Zoho used asset discovery tool to identify and track the servers added in IDC network.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA129	Server operations team maintain an asset disposal registry at Zoho Datacenter. The assets are degaussed and disposed based on the approval provided by Server operations manager.	CC3.4 CC5.3 CC6.5 CC7.1 A1.1 P4.1	Inspected for sample assets disposed the approval records and asset disposal registry for aspects such as 'Asset ID', 'Disposed on', 'Approved by', 'Approved on' and 'Parameters in registry' to ascertain whether server operations team maintained an asset disposal registry at Zoho Datacenter and whether the assets were degaussed and disposed based on the approval provided by Server operations manager.	None	None	No Exceptions Noted.
CA130	Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure.	CC6.6 CC7.1 CC7.3	Inspected for sample weeks the vulnerability assessment report for aspects such as 'Scope', 'Scan result' and 'follow-up performed' to ascertain whether vulnerability assessment was performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis and whether vulnerabilities identified if any were notified to relevant team for closure.	None	None	Exception Noted.. Refer Exception #13
CA131	Hardening guidelines for onboarding IDC Servers of Zoho is defined by Server Operations team. The guidelines document is reviewed and approved by Server Operations Manager on an annual basis.	CC3.4 CC5.3 CC6.1 CC6.7 CC7.1	Inspected Hardening guidelines of IDC servers for aspects such as 'Document name', 'Reviewed by', 'Approved by', 'Date of review' and 'Content of document' to ascertain whether hardening guidelines for onboarding IDC Servers of Zoho was defined by server operations team and whether the guidelines document was reviewed and approved by Server Operations Manager on an annual basis.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA132	Restoration of backup of IDC servers are performed using ZAC tool based on request from customer.	CC6.1 CC6.7 A1.2 A1.3 PI1.5	Inspected for sample backup restoration request the restoration tickets for aspects such as ‘Ticket ID’, ‘Date of request’, ‘Date of closure’ and ‘Restoration status’ to ascertain whether restoration of backup of IDC servers were performed using ZAC tool based on request from customer.	3.11.4	None	No Exceptions Noted.
CA133	Backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) are configured using ZAC tool by Server Operations team.	CC4.1 CC5.1 CC6.7 CC7.1 A1.2 PI1.5	Inspected for sample IDC servers the backup configuration for aspects such as 'Host name', 'Type of backup' and 'Backup frequency' to ascertain whether backup of IDC servers on a daily basis (incremental backup) and weekly basis (full backup) were configured using ZAC tool by Server Operations team.	None	None	No Exception Noted.
CA134	Data stored in IDC network are set up with redundant database clusters to ensure mirroring of customer data.	CC6.7 CC7.2 A1.1 A1.2 PI1.4 PI1.5	Inspected for sample IDC servers the cluster configuration for aspects such as 'Host name' and 'implementation of redundant cluster' to ascertain whether data stored in IDC network were set up with redundant database clusters to ensure mirroring of customer data.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA135	Members of the privacy staff verify that the entity has legal grounds to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, on a periodic basis, the privacy team verify that the entity has requested and received explicit written consent from the data subjects, when such consent is required.	P2.1 P3.1 P5.1	Inspected the privacy minutes of meeting and master activity registry for aspects such as 'Reviewed by', 'Reviewed on' and 'Content of review' to ascertain whether members of the privacy staff verified that the entity had legal grounds to collect data from the data subjects and that such legal grounds were documented prior to collection and whether additionally, on a periodic basis, the privacy team verified that the entity had requested and received explicit written consent from the data subjects, when such consent was required.	None	None	No Exceptions Noted.
CA136	On an annual basis, Director of Compliance (DOC) reviews cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.	P5.1 P5.2 P6.5 P6.7 P8.1	Inspected the SDP tickets and privacy minutes of meeting for aspects such as 'Ticket ID', 'Request denial reason', 'Reviewed by' and 'Reviewed on' to ascertain whether on an annual basis, Director of Compliance (DOC) reviewed cases relating to denial of data subject requests and validate the appropriate justifications provided thereof.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA137	Privacy team maintains inventory of data collected from the data subjects. The inventory is reviewed on an annual basis by Privacy team to ensure 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 privacy minutes of meeting and master activity registry for aspects such as ‘Reviewed by’, ‘Reviewed on’ and ‘Content of review’ to ascertain whether privacy team maintained inventory of data collected from the data subjects and whether the inventory was reviewed on an annual basis by Privacy team to ensure the documentation was kept current and included the location of the data, a description of the data, and identified data owners.	None	None	No Exceptions Noted.
CA138	Changes made to Cloud products are reviewed for PIA requirement by Data Privacy Coordinators. For changes that require PIA the change is assessed for privacy implications by Privacy team.	P3.1 P5.1 P6.1 P6.3 P6.6 P7.1	Inspected for sample changes made to cloud products the privacy impact assessment report for aspects such as 'Build URL', 'PIA requirement status', ‘PIA requirement reviewed by’, 'Date of build deployment', 'Date of PIA' and 'PIA Output' to ascertain whether changes made to Cloud products were reviewed for PIA requirement by Data Privacy Coordinators and whether for changes that required PIA the change was assessed for privacy implications by Privacy team.	None	None	No Exception Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA139	Data Privacy Coordinators are designated for each product team of Zoho. An annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators. The attendance for completion of annual refresher training is captured in Zoho Learn.	P3.1 P5.2 P6.1 P7.1 PI1.1	Inspected for sample data privacy coordinators the training completion records for aspects such as 'Associate name' and 'Training completion date' to ascertain whether Data Privacy Coordinators are designated for each product team of Zoho and whether an annual refresher training covering the PIA as part of change application management process is provided for the Data Privacy Coordinators and whether the attendance for completion of annual refresher training is captured in Zoho Learn.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA140	Management Review Meeting is performed for Privacy team Zoho on an annual basis 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 privacy minutes of meeting and master activity registry for aspects such as 'Reviewed by', 'Reviewed on' and 'Content of review' to ascertain whether Management Review Meeting was performed for Privacy team Zoho on an annual basis 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 whether for any new personal information that is collected, systems and processes were updated to provide notice to the data subjects. Inspected privacy minutes of meeting and we noted that there were no instances of new personal information collected during the examination period. Further, obtained email confirmation from Privacy Head, stating that, that there were no instances of new personal information collected during the examination period. Therefore, DHS LLP could not test the operating effectiveness providing notice for new personal information collected during the examination period.	None	None	No Exceptions Noted. The operating effectiveness of providing notice for new personal information collected could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA141	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 P6.1 P7.1	Inspected the privacy team organization chart for aspects such as 'Roles and responsibilities' and 'Reporting lines' to ascertain whether Zoho had constituted a Privacy Team which was responsible for implementing and maintaining the data privacy program at Zoho and whether privacy team report to the Director of Compliance who in-turn reported to the Vice President.	None	None	No Exceptions Noted.
CA142	For new/changes made to consent process, the business unit personnel obtains approval from Director of Compliance (DOC) before implementing the change.	P2.1 P3.2 P6.1 P8.1	Inspected the privacy minutes of meeting and we noted that there were no instances of new/changes made to consent process during the examination period. Further, obtained email confirmation from Privacy Head, stating that, that there were no instances of new/changes made to consent process during the examination period. Therefore, DHS LLP could not test the operating effectiveness of the control activity during the examination period	None	None	The operating effectiveness of the control activity could not be tested as there was no related activity during the examination period.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA143	For creation of access to Key management service tool of Zoho, the request is raised via Email. EAR team lead creates access to KMS tool for the associate based on the approval provided by EAR team manager.	CC5.2 CC6.1 CC6.2	Inspected for sample user creation to key management service tool the approval records for aspects such as 'Associate name', 'Associate date of joining', 'Approved by', 'Approved on', 'Access created on' and 'Access raised on' to ascertain whether for creation of access to Key management service tool of Zoho, the request was raised via Email and whether EAR team lead creates access to KMS tool for the associate based on the approval provided by EAR team manager.	None	None	No Exceptions Noted.
CA144	For associates leaving Zoho, the access to Key management service tool is revoked based on the integration with Zoho People.	CC5.2 CC6.1 CC6.2	Inspected the key management service tool and Zoho people integration for aspects such as 'Tool name' and 'Integration' to ascertain whether for associates leaving Zoho, the access to Key management service tool was revoked based on the integration with Zoho People.	None	None	No Exceptions Noted.
CA145	The privacy policy of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The policy outlines the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.	CC1.3 CC4.1 CC5.1 P5.1	Inspected privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether the privacy policy of Zoho was defined by the Legal team and was reviewed and approved annually by the General Counsel and whether the policy outlined the limitations on the collection and processing of information, as well as provisions regarding notice, usage, and disclosure.	3.11.6	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA146	Procedure for data subject correction request in Zoho is defined by privacy team. The policy document is reviewed and approved by Director of IT on an annual basis.	P4.3 P5.2 P7.1	Inspected Data Deletion and Rectification Process of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether procedure for data subject correction request in Zoho was defined by privacy team and whether the policy document was reviewed and approved by Director of IT on an annual basis.	None	None	No Exceptions Noted.
CA147	The policy for the retention and disposal of client information upon the discontinuation of Zoho services is defined by the Legal team and is reviewed and approved annually by the General Counsel. This policy is published on the corporate website.	CC5.3 C1.2 PI1.1 P4.3	Inspected privacy policy of Zoho and Zoho website for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision', 'Availability of policy in website' and 'content' to ascertain whether the policy for the retention and disposal of client information upon the discontinuation of Zoho services was defined by the Legal team and was reviewed and approved annually by the General Counsel and whether this policy was published on the corporate website	3.11.3	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA148	The privacy notice of Zoho is defined by the Legal team and is reviewed and approved annually by the General Counsel. The notice outlines the following: 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.	CC1.3 CC4.1 CC5.1 P1.1 P3.1 P5.1	Inspected privacy policy of Zoho for aspects such as ‘preparer’, ‘reviewer’, ‘approver’, ‘change history’, ‘date of revision’ and ‘content’ to ascertain whether the privacy notice of Zoho was defined by the Legal team and was reviewed and approved annually by the General Counsel and whether the notice satisfied the criteria specified in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA149	The policy for choice and consent is defined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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 P3.2 P5.1	Inspected privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether the policy for choice and consent was defined as part of the privacy policy by the Legal team and was reviewed and approved annually by the General Counsel and whether the policy satisfied the criteria specified in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA150	The definition of sensitive personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel.	P2.1 P3.1 P5.1	Inspected privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether the definition of sensitive personal information was outlined as part of the privacy policy by the Legal team and was reviewed and approved annually by the General Counsel.	None	None	No Exceptions Noted.
CA151	The use of personal information is outlined as part of the privacy policy by the Legal team and is reviewed and approved annually by the General Counsel. The policy covers the following: 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	Inspected privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether the use of personal information was outlined as part of the privacy policy by the Legal team and was reviewed and approved annually by the General Counsel and whether the policy satisfied the criteria specified in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA152	Procedure for personal information retention is defined as part of privacy policy by the legal team. The policy document is reviewed and approved by the General Counsel on an annual basis. The policy covers the following: 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 of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether procedure for personal information retention was defined as part of privacy policy by the legal team and whether the policy document was reviewed and approved by the General Counsel on an annual basis and whether the policy satisfied the criteria specified in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA153	The Data Subject Access Request policy of Zoho is defined by the Privacy team and is reviewed and approved annually by the Director of Compliance. The policy document defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information.	P5.1 P6.7 P8.1	Inspected subject access request policy and procedure for aspects such as ‘preparer’, ‘reviewer’, ‘approver’, ‘change history’, ‘date of revision’ and ‘content’ to ascertain whether the Data Subject Access Request policy of Zoho was defined by the Privacy team and was reviewed and approved annually by the Director of Compliance and whether the policy document defined authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA154	Privacy practice to data subject of the system is defined as part of privacy notice of Zoho defined by legal team. The notice is reviewed and approved by General Counsel on an annual basis. The notice document defines the following: 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 P3.2 P5.1	Inspected privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether privacy practice to data subject of the system was defined as part of privacy notice of Zoho defined by legal team and whether the notice was reviewed and approved by General Counsel on an annual basis and whether the notice satisfied the criteria specified in the control activity.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA155	Procedure for data subject related communication to internal and external users is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The procedure defines 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.	P1.1 P3.2 P4.1 P5.1 P5.2 P6.1 P6.2 P6.6	Inspected privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether procedure for data subject related communication to internal and external users was defined as part of privacy policy by legal team and whether the policy document was reviewed and approved by Director of Compliance on an annual basis and whether the procedure defined 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.	3.11.6	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA156	Procedure to determine if explicit consent is required is defined as part of privacy policy by legal team. The policy document is reviewed and approved by Director of Compliance on an annual basis. The policy defines the procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent and 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 privacy policy of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether procedure to determine if explicit consent was required was defined as part of privacy policy by legal team and whether the policy document was reviewed and approved by Director of Compliance on an annual basis and whether the policy defined the procedures to assess the nature of the information collected to determine whether personal information received required an explicit consent and procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.	None	None	No Exceptions Noted.
CA157	The privacy team establishes a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements. This document is reviewed and approved annually by the Director of Compliance. The document defines the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.	P2.1 P3.2 P5.2	Inspected consent guidelines and consent seeking process of Zoho for aspects such as 'preparer', 'reviewer', 'approver', 'change history', 'date of revision' and 'content' to ascertain whether the privacy team established a process to identify and review applicable privacy laws and regulations, as well as to determine consent requirements and whether this document was reviewed and approved annually by the Director of Compliance and also whether the document defined the procedure to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data.	None	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA158	Procedure to determine PIA requirement is defined by Privacy team. The procedure document is reviewed and approved by Director of Compliance on an annual basis.	P3.1 P6.1	Inspected data privacy protection impact assessment policy and procedure of Zoho for aspects such as ‘preparer’, ‘reviewer’, ‘approver’, ‘change history’, ‘date of revision’ and ‘content’ to ascertain whether procedure to determine PIA requirement was defined by Privacy team and whether the procedure document was reviewed and approved by Director of Compliance on an annual basis.	None	None	No Exceptions Noted.
CA159	Privacy team reviews the complaints related to privacy raised to Zoho against unfair or unlawful practices.	CC7.5 P3.1 P4.3 P8.1	Inspected for sample privacy related complaints the tickets for aspects such as ‘Ticket ID’, ‘Ticket opened on’, ‘Ticket closed on’, ‘Closed by’ and ‘Closure action’ to ascertain whether privacy team reviewed the complaints related to privacy raised to Zoho against unfair or unlawful practices.	3.11.5	None	No Exceptions Noted.

#	Control Activity	Trust Services Criteria	Tests Performed	CUECs	CSOCs	Results of Tests
CA160	On an annual basis, Director of Compliance (DOC) reviews cases relating to request raised by data subjects for disagreements over the accuracy of personal data and validate the appropriate justifications provided thereof.	P5.2 P7.1 P8.1	Inspected the SDP tickets of Zoho and we noted that there were no instances of request raised by data subjects for disagreements over the accuracy of personal data during the examination period. Further, obtained email confirmation from Privacy Head, stating that, that there were no instances of request raised by data subjects for disagreements over the accuracy of personal data during the examination period. Therefore, DHS LLP could not test the operating effectiveness of the control activity during the examination period	None	None	The operating effectiveness of the control activity could not be tested as there was no related activity during the examination period.

4.5 Management Responses to Exceptions

The Audit exceptions presented in the Section 4 of this report were reviewed and discussed on December 12, 2024 during a dedicated Closing Meeting attended by the Zoho Compliance Team. The Management Responses to the exceptions noted is as under:

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 1	We noted that there is no induction training completion record maintained for 3 out of 25 sample associates.	CA09: For associates joining Zoho, induction training is completed by the associate on the date of joining. The induction training covers the information security and privacy commitments of Zoho. The attendance for completion of induction training is captured in Zoho People. Trust Service Criteria: CC1.4, CC2.2, CC3.1, CC5.1, C1.1, PI1.1 and P5.1.	We agree with the exception noted. The same has been actioned upon with appropriate escalation to our senior management after the completion of examination period. Also, we noted that there were no security violations by these 3 employees. In addition to this, management will periodically monitors the completion status of induction training as part of the onboarding process to identify the employees who have not completed. Going forward, the same shall be rigorously monitored by the human resource team to ensure there are very minimal defaults.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 2	We noted that there was a delay in physical access revocation for 3 out of 25 sample associates ranging from 7 to 12 days.	CA12: For associates leaving Zoho, the HR team enters the last working date in Zoho people. Admin team revokes physical access for the associate based on the automatic email triggered from Zoho People on the associate's last working date. Trust Service Criteria: CC2.1, CC5.2, CC6.1 and CC6.4.	We agree with the exception noted. There was a delay in revocation of access for 3 sample associates. However, upon inspection of the physical access logs, the access cards were not used after the last working date and the logical access to the domain and IAM accounts were revoked on the last working date of the associate. In addition to this, there were no security incidents noted due to these associates. Going forward, the management shall implement measures to revoke physical access to facility as part of the exit clearance process.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 3	We noted that the IAM accounts access was revoked after last working date for 7 of 25 sample associates with a delay ranging from 2 to 34 days	CA15: For associates leaving Zoho, the HR team revokes the IAM account in Zoho people for the associate on their last working date. Trust Service Criteria: CC5.2, CC6.1 and CC6.2.	We agree with the exception noted. There was a delay in revocation of access for 7 sample associates. However, upon inspection of the IAM access logs, the associates did not login after the last working date. Hence, no customer data was accessed by the associates after their last working date. In addition to this, there were no security incidents noted due to these associates. Going forward, the management shall implement measures to revoke IAM access as part of the exit clearance process.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 4	We noted that the password history configuration for IAM and ZD, password expiry configuration for AD and account lockout configuration of Zero Trust, IAM and ZD were configured but were not in line with Zoho's password policy.	CA32: Security setting for password configurations and account lockout configuration of Active Directory, Zoho Directory, Zero Trust and IAM account are defined as per Zoho password policy. Trust Service Criteria: CC5.2, CC6.1, CC6.2, CC6.3 and CC6.6.	We agree with the exception noted. The password configurations mentioned are not in line with the policy. We have initiated the rectification activity for the same. However, to access customer data in IDC network the user has to utilize password from the passman tool. The password in passman tool adheres to Zoho password policy during the examination period.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 5	We noted that for 5 sample corporate servers that went live during the examination period, there was no formal documentation maintained to assess the severity of the failed parameters while hardening the server. Further we noted that there were no records maintained for hardening the network devices onboarded during the examination period.	CA35: For newly onboarded corporate server and network device the hardening checklist is maintained by the respective team. Trust Service Criteria: CC5.1, CC5.2, CC6.6, CC6.7 and CC7.1.	We agree with the exception noted. No formal documentation was maintained to assess the severity of the failed parameters while hardening the corporate server. We analyzed the parameters which were not complied with and assessed the impact as low and further implemented the servers in production. Moving forward, the management will document formal response for the failed parameters identified from the hardening check. Also, there were no formal record maintained for hardening the network devices onboarded during the examination period. Further for external facing network devices, the management performs vulnerability assessment on a periodic basis. Also, there are no security incidents identified because of hardening misconfigurations during the examination period. Moving forward, the management will document formal hardening checklist for newly onboarded network devices.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 6	We noted that for 5 out for 25 sample workstations the local admin rights and USB access were not restricted	CA53: Local Admin Rights and access to removable device is restricted for Zoho workstations. Trust Service Criteria: CC5.2, CC6.1, CC6.2, CC6.3 and CC7.1.	We agree with the exception noted. The 5 sample workstations were provided with local admin rights and USB access. However, the associate’s assigned with those workstations were from customer support and development team who did not have access to the IDC servers and underlying customer data. Additionally, those identified workstations were installed with CrowdStrike EDR solution to actively monitor and scan for malware and the file contents within the removable media. Further, the management is reviewing the list of local admin users and USB access to non restricted users and will take corrective actions by Q3 2025.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 7	We noted that Zoho associates' IAM access/role review was not performed during the examination period.	CA67: IAM roles access to Zoho associates are reviewed on an annual basis. The extension of IAM roles are based on approval provided by the associate and associate's manager. Corrective action is performed by IAM team for discrepancies identified (if any) Trust Service Criteria: CC5.2, CC6.1, CC6.2 and CC6.3.	We agree with the exception noted. The management is developing a new tool for the review of IAM roles because of which there is a delay in the review process. However, the IAM roles are created and assigned based on the approval from managers and the access to IAM accounts are revoked on the associate's last working date. The previous IAM role access review was completed in June 2023. Further, there were no security incidents identified due to inappropriate IAM roles assigned to Zoho associates. The management has started the IAM role review activity and will complete by Q1 2025.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 8	We noted that for 2 out of 25 sample builds selected, there were no records of testing document maintained.	CA72: Changes made to Cloud products are deployed using inhouse SD tool to production and local environment. The build generated are tested in local Zoho and signoff is provided by product manager before deployment in production environment/publishing in website. Trust Service Criteria: CC3.4, CC5.1, CC5.2, CC8.1 and PI1.3.	We agree with the exception noted. There were no formal documentation maintained for testcases validated as part of the QA process for the identified 2 sample build. However, QA signoff was obtained before pushing build to production. Further, there were no incidents noted from pushing the 2 changes to production. Going forward, the management will formally document the testcases validated as part of the QA process.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 9	We noted that there were no logs maintained for onboarding 2 Unix servers out of 25 sample servers with standard image.	CA78: Servers onboarded in IDC network are hardened using standard image by server operations team. Trust Service Criteria: CC5.1, CC5.2, CC6.6 and CC6.7.	We agree on the exception noted. The hardening logs were not available for 2 Unix servers out of 25 sample IDC servers onboarded. However, the servers are onboarded using standard images and upon verifying the hardening configurations after the examination period, we noted that all the hardening checks were properly implemented. Further the management has implemented tool to monitor the hardening compliance status from September 2024.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 10	We noted that there was no formal documentation maintained for corrective action performed for all vulnerabilities identified from the PT reports pertaining to 10 out of 25 sample products.	CA85: Penetration testing is performed for External IP of Zoho on an annual basis. Vulnerabilities identified if any are tracked to closure. Trust Service Criteria: CC6.6, CC7.1 and CC7.3.	We agree with the exception noted. The PT report template used for the 10 sample reports did not capture the individual closure status of the vulnerabilities identified. Further, vulnerability scans were performed on a regular basis at a weekly frequency. However, the management has updated the template from Q3 2024 and the PT reports will capture the closure status of the vulnerabilities identified.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 11	We noted that there was a delay in access revocation to jump servers for 2 out of 25 sample associates ranging from 12 to 43 days.	CA115: For revocation of access to Jump server, the request is raised in Zoho SDP. Server Operations team revokes access to Jump server and IDC server account for the associate. For associates leaving from Zoho, the access to Jump server and IDC server account is revoked on the associate's last working date. Trust Service Criteria: CC2.1, CC5.2, CC6.1, CC6.2 and CC6.3.	We agree with the exception noted. There was a delay in revocation of access for 2 sample associates. However, the zero trust accounts were disabled on a timely manner. Further, upon inspection of the access logs, it was noted that the associates did not login after the last working date to the jump servers. In addition to this, there were no security incidents noted due to these associates. Going forward, the management shall implement measures to revoke jump servers access as part of the exit clearance process.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 12	We noted that 5 out of 25 sample servers run on Unix version whose support life ended in June 2024.	CA121: Operating System of IDC servers are patched on a periodic basis by Server Operations team after testing patches in test environment and based on the approval provided by Server operations manager. Trust Service Criteria: CC3.4, CC5.2, CC6.1, CC6.2, CC6.7, CC7.1 and CC7.3.	We agree with the exception noted. The management was in process of selecting the EOL support vendor because of which there was no end of life support for the period July 2024 till September 2024. However, the management performs vulnerability assessment and penetration testing on a periodic basis to identify the vulnerabilities and perform corrective action. Further, the management has purchased end of life support from November 2024. The servers will be migrated to a vendor supported OS by Q3 2025.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity and Impacted by Exception	Management Response to Exception
Exception 13	We noted that the vulnerability assessment for external IP of product was performed with a delay for 7 out of 25 samples selected.	CA130: Vulnerability assessment is performed for External IP of Zoho using Rapid7/Tenable tool on a weekly basis. Vulnerabilities identified if any are notified to relevant team for closure. Trust Service Criteria: CC6.6, CC7.1 and CC7.3.	We agree with the exception noted. The vulnerability assessment was performed on a weekly basis. However, there was a delay of few days in performing vulnerability scan for the 7 samples selected. However, the management performed scans in the upcoming weeks and no issues were identified. Moving forward, the management shall track the status of vulnerability assessment and ensure timely completion.

Deloitte
Haskins & Sells LLP

Document Reference No.: RA-TPA-31094494-2024-25-R77