KPMG Assurance and Consulting Services LLP
First Floor, Block A,
02 Godrej Business District,
Pirojshanagar, Vikhroli – West,
Mumbai – 400 079, India
Telephone: +91 (22) 6808 6000

Yotta Data Services Private Limited
5th Floor, Scorpio Building,
Hiranandani Gardens, Powai,
Maharashtra,
Mumbai – 400076

Date: 4 March 2025

Attention: Rupali Kale, Head – Governance, Risk and Compliance.

KPMG Assurance and Consulting Services LLP (hereinafter referred to as "KPMG", "We", "Our") have completed SOC 2 Type 2 examination for Yotta Data Services Private Limited (hereinafter referred to as "Yotta", "service organization", "you") as outlined in our Engagement Letter dated 10 October 2024. This report to you represents our final report for SOC 2 Type 2 examination.

The data included in this report was obtained from you, on or before 7 February 2025. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 7 February 2025. The attached report is the electronic version of our signed deliverable, which has been issued to you in the hard copy format.

This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions. While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not independently verified the correctness or authenticity of the same.

This report is intended solely for the information and use of the management of Yotta, its user entities and the independent auditors of user entities (collectively referred to as authorized parties) and is not intended to be, and should not be, used by anyone other than these authorized parties. If this report is received by anyone other than authorized parties, the recipient is placed on notice that the attached SOC 2 Type 2 report has been prepared solely for authorized parties for their internal use and this report and its contents shall not be shared with or disclosed to anyone by the recipient without the express written consent of Yotta and KPMG. KPMG shall have no liability and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report. We have been engaged by Yotta for the Services and to the fullest extent permitted by law, we will not accept responsibility or liability to any other party in respect of our Services or the report. We thus disclaim all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such other party arising out of or in connection with the report or any part thereof. By reading our report the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.

Please contact me at sr@kpmg.com if you have any questions or comments. We look forward to providing services to your company.

Yours sincerely

Sundar Ramaswamy
Partner
KPMG Assurance and Consulting Services LLP

KPMG Assurance and Consulting Services LLP, an Indian limited liability partnership and a member firm of KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee

KPMG (Registered) (a partnership firm with Registration No. BA-62445) converted into KPMG Assurance and Consulting Services LLP (a Limited Liability Partnership with LLP Registration No. AAT-0367), with effect from July 23, 2020

Registered Office:
2nd Floor, Block T2 (B Wing)
Lodha Excelus, Apollo Mills
Compound, N M Joshi Marg,
Mahalaxmi, Mumbai-400 011.

YOTTA DATA SERVICES PRIVATE LIMITED

SYSTEM AND ORGANIZATION CONTROLS (SOC) 2 TYPE 2 REPORT

Report on description of System, Suitability of Design of Controls and Operating Effectiveness relevant to Trust Service Criteria - Security, Confidentiality, Availability and Privacy related to Colocation services and supporting General Operating Environment from the delivery centres located at Noida, Panvel, Airoli and Gift City, India

For the period 1 January 2024 to 31 December 2024.

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

KPMG Assurance and Consulting Services LLP
First Floor, Block A,
02 Godrej Business District,
Pirojshanagar, Vikhroli – West,
Mumbai – 400 079, India
Telephone: +91 (22) 6808 6000

To,
The Board of Directors,
Yotta Data Services Private Limited

Scope

We have been engaged to report on Yotta Data Services Private Limited's (hereinafter referred to as "Yotta" or "service organization") description in section 3 of its system for providing Colocation services and supporting General Operating Environment to user entities from the delivery centres located in Noida, Panvel, Airoli and Gift City, India throughout the period 1 January 2024, to 31 December 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 (AICPA, Description Criteria), (description criteria) and on the design and operation of controls stated in the description to provide reasonable assurance that Yotta's' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (applicable trust services criteria).

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

Service Organization's Responsibilities

Yotta is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services category or categories and stating the related controls in the description; identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and designing, implementing, and operating controls that are suitably designed and operating effectively to provide reasonable assurance that its service commitments and system requirements were achieved.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the design and operation of controls related to the service commitments and system requirements stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented in accordance with the description criteria and the controls are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

An assurance engagement to report on the description and the design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not presented in accordance with the description criteria and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to obtain reasonable assurance that the service commitments and system requirements stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description.

KPMG Assurance and Consulting Services LLP, an Indian limited liability partnership and a member firm of KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee

KPMG (Registered) (a partnership firm with Registration No. BA-62445) converted into KPMG Assurance and Consulting Services LLP (a Limited Liability Partnership with LLP Registration No. AAT-0367), with effect from July 23, 2020

Registered Office:
2nd Floor, Block T2 (B Wing)
Lodha Excelus, Apollo Mills
Compound, N M Joshi Marg,
Mahalaxmi, Mumbai-400 011.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Service Auditor's Independence and Quality Management

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Management 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Limitations of Controls at a Service Organization

The description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that individual user entity may consider important in its own environment. Also, because of their nature, service organization 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 of any evaluation of the suitability of design or operating effectiveness of controls to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects,

a) the description presents Yotta's system for providing Colocation services that was designed and implemented throughout the period 1 January 2024 to 31 December 2024 in accordance with the description criteria;
b) the controls stated in the description were suitably designed throughout the period 1 January 2024 to 31 December 2024 to provide reasonable assurance that Yotta'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 user entities applied the complementary controls assumed in the design of Yotta's controls throughout that period; and
c) the controls, which were those necessary to provide reasonable assurance that Yotta's service commitments and system requirements were achieved based on the applicable trust services criteria, operated effectively throughout the period from 1 January 2024 to 31 December 2024, if complementary user entity controls assumed in the design of Yotta's controls operated effectively throughout that period.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in section 4.

Intended Users and Purpose

This report and the description of tests of controls in section 4 are intended only for Yotta, user entities who have used Yotta's system for providing Colocation services and their auditors, who have sufficient knowledge and understanding of the following:

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

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

KPMG Assurance and Consulting Services LLP

Date: 7 February 2025

SECTION 2

STATEMENT BY SERVICE ORGANIZATION

STATEMENT BY THE SERVICE ORGANIZATION

We have prepared the accompanying description of Yotta Data Services Private Limited (hereinafter referred to as "Yotta" or "service organization") in section 3 for providing Colocation service and supporting General Operating Environment to user entities from the delivery centres located in Noida, Panvel, Airoli and Gift City, India throughout the period 1 January 2024 to 31 December 2024 (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 (AICPA, Description Criteria) ("description criteria"). The description is intended to provide report users with information about the Yotta's system that may be useful when assessing the risks arising from interactions with Yotta's system, particularly information about system controls that Yotta 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, 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 (AICPA, Trust Services Criteria).

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

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

a) the description presents Yotta's system for providing Colocation services that was designed and implemented throughout the period 1 January 2024 to 31 December 2024 in accordance with the description criteria.

b) the controls stated in the description were suitably designed throughout the period 1 January 2024 to 31 December 2024 to provide reasonable assurance that Yotta'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 user entities applied the complementary controls assumed in the design of Yotta's controls throughout that period.

c) the controls stated in the description operated effectively throughout the period 1 January 2024 to 31 December 2024 to provide reasonable assurance that Yotta's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Yotta's controls, operated effectively throughout that period.

SECTION 3

YOTTA'S DESCRIPTION OF THE SYSTEM

Scope of the Report

The scope of this report includes description of Yotta Data Services Private Limited (herein after referred to as "Yotta" or "service organization") system supporting the Colocation services provided to user entities from the delivery centres at Noida, Panvel, Airoli and Gift City, India, for the period 1 January 2024 to 31 December 2024, based on the criteria for a description of service organization's system in DC section 200, 2018 Description Criteria for a Description of Service Organization's System (AICPA, Description Criteria), (description criteria) and suitability of the design and operating effectiveness of controls stated in the description for the period 1 January 2024 to 31 December 2024, to provide reasonable assurance that Yotta's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (applicable trust services criteria).

The description indicates that certain applicable trust services criteria stated in the description can be achieved only if complementary user entity controls assumed in the design of Yotta's controls are suitably designed and operating effectively, along with related controls at Yotta. The description does not extend to controls of the user entities.

The scope of this report includes the following four centres of Yotta

- D1: Yotta Data Centre Park - Plot no. 7, Sector Knowledge Park V, Greater Noida Dist. Gautam Buddha Nagar 201 306, Uttar Pradesh, India.
- NM1: Yotta Data Centre Park - Panvel Hiranandani Fortune City. Survey No. 30, MH SH 76, Panvel, Navi Mumbai, Maharashtra 410206.
- TB2: Yotta Data Services Private Limited Data Centre - Unit 204, C wing, 2nd floor, Reliable Tech Park Gut no. 31, Village- Airoli, Navi Mumbai, 400708, Maharashtra, India.
- G1: Yotta Data Centre, Gift City- 12th Floor, Signature Building, Gujarat International Finance Tec-City, Gandhinagar, Gujarat 382355, India[1].

The scope of the report does not include any other services or facilities of Yotta other than those mentioned above.

The report has been prepared to cover multiple user entities of Yotta. Any user entity having unique control requirements is outside the scope of this report.

Overview of Yotta

Yotta provides hosting (IaaS) and co-location services to user entities and complements the same with a comprehensive suite of managed and professional services, allowing user entities to construct modular solutions that are suitable to meet their specific requirements. Yotta has focused on building their managed services for their enterprise user entities with a capability to manage and support critical Information Technology (IT) infrastructure.

Yotta offers private cloud services that deliver secure, reliable, and scalable cloud environment through an IaaS model, optimizing costs and providing enhanced control. Hosted in Yotta's Uptime Institute-certified Tier IV data centre, the solution endeavours to provide a seamless cloud experience for deployments. With a robust 15-layer security framework safeguarding access to the racks, Yotta combines the cost-efficiency of public cloud solutions with the exclusivity and control of a private cloud environment. In addition to cloud services, Yotta provides data centre network and connectivity riding on high capacity, performance, and reliable networks.

Yotta has a robust Information Security Management System (ISMS) and has achieved International Organization for Standardization (ISO) 27001- 2022 and Payment Card Industry Data Security Standard (PCI DSS) certification. The key services provided are as under:

Colocation: Yotta provides data centre infrastructure for user entities to host and manage their systems based on the services opted by them.

[1] Yotta datacenter located in Gift city, Gujarat is operational from April 2024.

System Overview

Yotta operates in a well-defined and structured system to provide Colocation services to its user entities. This system consists of multiple components such as policies and procedures, governance structure, support functions and applications. The policies and procedures provide guidance to users regarding the processes to be followed for providing services to user entities and assist in their consistent implementation. The governance structure establishes a framework for operating within the defined system and assists in demonstrating management commitment for adherence to policies. Yotta has implemented processes for information systems, including physical access, environmental security, Human Resources (HR) security, Information Security (IS), security administration, and network security to provide services to its user entities. Multiple applications are used by Yotta to support the service delivery.

Internal control framework consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. Yotta has established an internal controls framework that reflects the five components as described below:

- **Control Environment:** The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal controls across the organization. Yotta's management has established the tone at the top regarding the importance of internal controls including expected standards of conduct. Management reinforces expectations at various levels of the organization. The control environment comprises of the integrity and ethical values of the organization; the parameters enabling the management to carry out its governance oversight responsibilities; the organization structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal controls.

- **Risk Assessment:** Yotta faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks for the achievement of objectives. Risks pertaining to the achievement of these objectives across the entity are considered relative to the established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is establishment of objectives, which are linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal controls ineffective.

- **Control Activities:** Control activities are the actions established through policies and procedures that help implement management's directives to mitigate the risks pertaining to the achievement of objectives. Control activities are performed at multiple levels within Yotta, at various stages within user entity services, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

- **Information and Communication:** Information is necessary for Yotta to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal controls. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.

- **Monitoring Activities:** Ongoing evaluations, separate evaluations, or some combination of the two are used to demonstrate whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Ongoing evaluations, built into user entity services as well as internal processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, vary in frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies and management; deficiencies are communicated to the management as appropriate.

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

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Yotta's security, availability, confidentiality, and privacy commitments are comprehensively documented and communicated in its contracts with user entities. Changes to these commitments are agreed upon and signed off by Yotta and user entities. These commitments outline Yotta's responsibilities, including implementing and monitoring robust security measures, ensuring service uptime and availability, and maintaining confidentiality of user entities' information. Yotta's employees are held to strict standards to safeguard sensitive data, delivering reliable and secure services while upholding the trust of its user entities. These commitments are taken into account by Yotta while establishing the operational and system requirements for user entities' operations. These requirements are defined in contracts with its user entities.

Yotta designs its processes and procedures related to Colocation services to meet its objectives. These objectives are based on the service commitments agreed between Yotta and its user entities, and applicable laws and regulations that govern the provision of the said services.

Yotta has adopted ISO 27001:2022 to establish a management framework for ISMS. Yotta has also adopted PCI DSS standard. Information Security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and network are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation.

COMPONENTS OF THE SYSTEM FOR PROVIDING SERVICES

Yotta has defined processes and teams for information systems, network communication, change management, incident management, logical access, backup and recovery, physical access, and Human Resources (HR) to support the services.

Yotta uses the following components to provide services:

- Infrastructure: Yotta has designed its physical and IT infrastructure to incorporate elements of security, availability, confidentiality, and privacy.
- Software: The applications are managed by Yotta for service delivery to user entities.
- People: Yotta is responsible for management and supervision of employees involved in providing services delivered to user entities.
- Procedures: Procedures are established by the management of Yotta to provide guidance to the employees regarding the process followed for providing services to user entities.

Infrastructure

Yotta has data centres based out of its Noida, Airoli, Panvel and Gift City centres. Yotta operates and manages multi-tenant colocation infrastructure. Yotta has a dedicated floor space with security measures for user entities to maintain their rack space. Dedicated rack space is maintained for each user entity offering sufficient capacity to host servers managed by the user entities. A Disaster Recovery (DR) site is available for user entities who have opted for backup plan for recovery of operations in the event of a failure at the primary site.

Yotta has implemented physical security controls such as access control system, close circuit television (CCTV) and cameras installed in restricted areas including server and utility hall to safeguard infrastructure from unauthorized access. Security guards are stationed at each entry and exit gate to verify the authorization of visitors and vehicles entering the data centre. Environmental controls such as heat and smoke detectors, Uninterruptible Power Supply (UPS), chillers and fire suppression system, are implemented within data centre facility to address the threats posed by environmental hazards. Water sprinklers and fire extinguishers are also installed within the facilities to protect the facilities from fire.

Firewall is configured at the perimeter of the network to prevent it from external threats. It consists of different modules such as Unified Threat Management (UTM) and advanced threat protection. Email access is provided to employees through Microsoft Office 365 for internal and external communication.

Crowdstrike antivirus is installed on workstations and servers to prevent them from the threat of viruses, trojans, and malware. Yotta uses Netskope application for Data Leakage Prevention (DLP) and is configured on endpoints to prevent leakage of confidential information. Additionally, access to Universal Serial Bus (USB) drives is restricted at employee workstations through DLP. Exception approval from CISO is required in case of requirment to activate USB port on endpoint devices.

Software

Key applications used by Yotta are managed by the software team and is used by Yotta to support services delivered to user entities or to support Yotta's general operating environment. Please refer to table below for the list of key applications for which applicable General IT Control (GITC) have been covered, as relevant.

Sr. No.	Application Name	Description
1	Salesforce (SFDC)	SFDC is used by employees to save user entity details and Know Your Client (KYC), sales order creations and approvals to create sales order
2	Tussom	Application used to raise incident ticket, change ticket and service requests. It is also used for maintaining the Yotta assets
3	Sectona- Privilege Access Management (PAM) tool	Application used to access critical Servers
4	CISCO ISE	Application used to grant access to network devices authenticated via PAM.

Sr. No.	Application Name	Description
5	Netskope	Application used for detecting data leakage from the endpoint devices. Additionally, application is also used for real-time visibility, threat protection, and data security for websites, and private applications.
6	Zabbix	Application used to monitor capacity and performance of network components.
7	IBMQradar	Security Incident and Event Monitoring (SIEM) Application used to capture and monitor activity logs of all network components and servers.
8	Commvault	Application used to perform backup of servers managed by Yotta.

The other internal applications used by Yotta for supporting day to day processes are listed below. GITCs for these applications are not covered in the scope of this report.

Sr. No.	Application Name	Description
1	ATHENA	Application maintained by Yotta where all the policy documents are uploaded
2	DarwinBox	Unified platform that manages the entire employee lifecycle, from recruitment and onboarding to performance management and offboarding. Further, application is used to communicate changes to organization structures, announcement and key achievements.
3	Milestone	Application used to capture CCTV footage at Mumbai location
4	Genetics	Application used to capture CCTV footage at Noida and Gift City. It is also used for physical access management
5	OneYotta	User Entity portal on which reports are uploaded for their review
6	Visitor Management System (VMS)	Application used to manage and record visitor access
7	Manage Engine	Application used maintaining endpoint devices including hardening of end-point devices and endpoint device status (active / inactive).
8	CanIphish	Application used to conduct and track simulated phishing.
9	Qualys	Application used to perform internal vulnerability assessment.

Policy and Procedures

The management of Yotta have established policies and procedures which enables its employees to understand and implement the defined processes for providing the services to its user entities. Yotta has implemented ISMS inline with the ISO 27001:2022 standard. Yotta undergoes annual ISO 27001:2022 and PCI-DSS certification. The alignment to ISMS framework helps Yotta in implementing and monitoring information security based on leading practices across multiple domains and thereby assist in safeguarding its assets, network, systems, and personnel. Organization's policies and procedures are available on ATHENA for employees to refer on an on-going basis.

Yotta's management has developed and communicated policies and procedures across functions including information security, HR, logical security, network security, infrastructure management, physical and environmental security, backup and restoration, change management and incident management to its employees. The roles and responsibilities of the team members are defined in the policy and procedure documents.

These policies and procedures are reviewed and approved by Yotta's management annually and primarily used internally to guide the Yotta's employees to support the day-to-day operations.

People

The senior management at Yotta is responsible for establishment of organization policies, overseeing of organization activities and achieving business objectives. Yotta has extablished various teams which are responsible for day-to-day operations and is supported by the Governance, Risk and Compliance (GRC) team, Corporate IT team, IS team, HR and Admin team. The IT team manages, monitors and supports the service organization's information application resources and maintenance. The IS team manages the service organization's security commitments pertaining to the flow of information in and outside the service organization. The HR team is responsible for employees, third party personnel, and third-party vendors, providing services, for their background check and granting physical access. The Admin team is responsible for physical security and maintenance of the facilities.

CONTROL ENVIRONMENT

Commitment to Integrity and Ethical Values

Code of Conduct

Yotta is committed to ethics and integrity and believes in the conduct of affairs in a fair and transparent manner by adopting highest standards of professionalism, integrity, honesty and ethical behavior, and adherence to laws across the organization. Yotta has documented code of business conduct and ethical standards applicable to employees, vendors, and contractors as part of Code of Business Conduct policy which is approved by the Head GRC and CISO on an annual basis. The objective of these policies is to define guidelines on behavior of employees and contractors at work place. These are communicated to employees and are made available on the Company's intranet. The employee upon joining required to sign the Code of Conduct (CoC) document. Every Yotta employee is expected to abide by these policies and when in doubt seek suitable clarifications. It is important that any employee misconduct is promptly dealt with in an appropriate manner.

Organization Structure

The organization structure of Yotta provides the framework within which activities for achieving objectives are planned, executed, and monitored. The organization structure covering the teams / functions is depicted below:

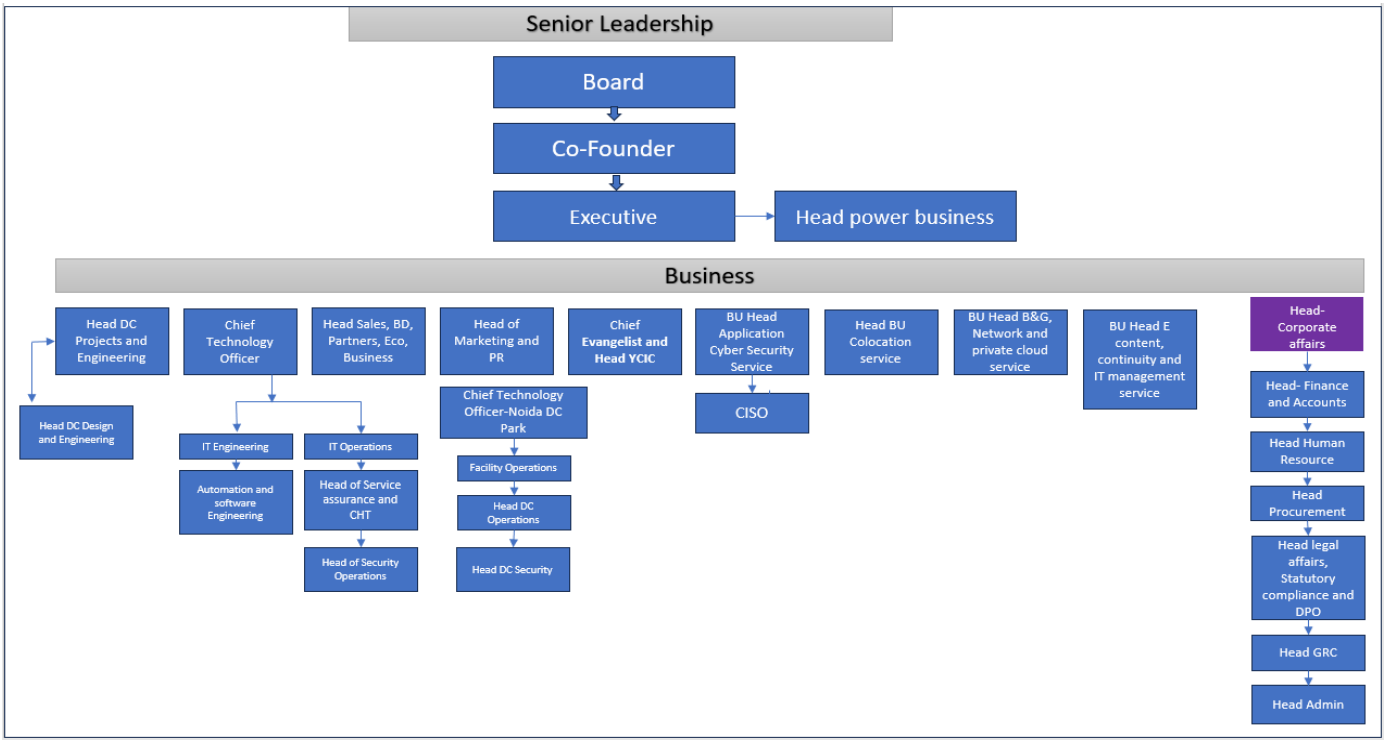

Figure 1: Organization Structure

Yotta's organization structure provides the overall framework for planning, directing, controlling, and monitoring business operations. Employees and business functions are separated into departments according to operational responsibilities. The structure also provides defined job responsibilities and lines of authority for reporting and communication.

Oversight by the Management

Yotta operations are monitored closely by Yotta's management. On a periodic basis, a Management Review Meeting (MRM) is conducted including department heads to assess the objectives set in previous meets, review actions taken on findings and set new objectives. The objectives are communicated within each department by the department heads.

Board of Directors

The Board of Directors (BoD) establish the tone at the top regarding the importance of internal controls including expected standards of conduct. Management reinforces expectations at various levels of the organization. The control environment

comprises of the integrity and ethical values of the organization; the parameters enabling the BoD to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals.

Support Functions

Yotta has various support functions that support the service delivery to user entities and manage the overall environment.

Support Functions	Responsibility

Human Resources team	***HR Operations team***
	
	The HR team is responsible for overseeing whether processes run smoothly that help govern employment conditions at Yotta.
	
	Following are the primary responsibilities of the HR Operations team:
	
	• Introduces and updates HR checklist.
	• Conduct background verification for new hires to confirm validity of criminal, education and employment records as confirmed candidates
	• Manage and comply with the HR policies and procedures like:
	  ○ On-boarding Formalities
	  ○ Employee Movements
	  ○ Reporting
	  ○ Employee Exit Process
	
	Talent Acquisition team
	
	Following are the primary responsibilities of the Talent Acquistion team:
	
	• Assist in hiring of candidates on receipt of requests
	• Document and update the Job Descriptions (JDs) and the summary criteria prepared / approved by the hiring manager, and initiate sourcing the candidates through various job portals, social networking sites, internal references
	• Conduct aptitude / technical test of candidates
	• Schedule interview rounds for candidates
	• Review the JDs for positions in the organization at least once a year and send a summary of such reviews to the management at the end of the year
	• Conduct induction and periodic training for employees

Corporate IT team	The Corporate IT team manages identity and access provisioning and deprovisioning within the Active Directory (AD) during employee onboarding and offboarding. The team oversees the lifecycle management of assets including Yotta-issued devices and personal employee assets to impose compliance with endpoint hardening policies. The team also performs endpoint management encompassing device health, performance, and implementation of system-wide security measures to protect corporate data.
Network team	The Network team is responsible for the management and security of network components ensuring alignment with Yotta's cybersecurity framework. Their responsibilities include configuring access control for network devices and ensuring compliance with network hardening policy. The team continuously monitors the health and performance of network components, addressing any issues and oversees resolution on network related incidents.

Support Functions	Responsibility
CISO – Information Security team	The Information Security (IS) team is responsible for maintaining overall information security posture within Yotta. Information Security team is headed by CISO. Roles and responsibility of the IS team is: • Documenting and updating IS policy and supporting procedures on an annual basis or in case of any major changes • Conducting Vulnerability Assessment (VA) and Penetration Testing (PT) • Monitoring IS incidents • Monitoring DLP incidents • Implementing and monitoring dark web and public URL protection • Managing policy exceptions • Monitoring phishing simulation • Responding to due-diligence requests received from user entities
Service Management team	The team is responsible for managing incident and change tickets within the Tussom application. They monitor SLA adherence during incident tickets closure and addresses any breaches in the management meeting. The change manager attends weekly CAB meetings to review and discuss planned, pre-approved and emergency changes.
Management Information System (MIS) team	The MIS team is responsible for tracking identified vulnerabilities on a Quarterly basis.
Storage and Backup team (Backup operations team)	The Backup team is responsible for executing backup operations for Yotta's internal servers and user entity servers in alignment with defined schedules and subscription plans chosen by user entity. In addition to scheduled backups, the team performs backups upon request from the respective operations teams. The Storage team manages tape storage workflows, including transferring Yotta's internal tape backups to the designated storage vault within the data centres. For user entity subscribed to physical tape storage services, the team oversees the secure transport of tapes to secondary offsite locations as per service agreements.
Capacity Management – IT Engineering and Security team	The team is responsible for monitoring CPU utilization, space utilization, RAM, server uptime and critical URL monitoring for Yotta managed infrastructure.
Data Centre (DC) security team	The team is responsible for managing access to the data centre, including visitor access, performing thorough verification of visitor credentials at all critical entry points within the facility. They operate a dedicated CCTV monitoring room, where they oversee 24/7 surveillance of the building to maintain security and operational integrity.
DC Operations team	The team is responsible for conducting preventive maintenance of the data centre, enabling optimal performance of critical infrastructure components. They also oversee vendor-conducted maintenance activities, to help ensure they are carried out effectively and in accordance with scheduled timelines.
Customer Happiness Team (CHT)	The team is responsible for maintaining communication with user entities including cases of any issues faced.
Governance Risk and Compliance (GRC) team	The GRC team is responsible for overseeing the overall compliance across all towers. The GRC team performs annual internal audit based on findings captured in the risk register. The identified gaps are escalated to the respective tower heads and the remediation points are discussed along with targeted date of closure. Additionally, the Head of GRC conducts an annual review of the security policy to help ensure compliance.

RISK ASSESSMENT

Risk Management Framework and Internal Audit

The Risk Management function at Yotta operates as an independent entity responsible for establishing the Risk Management framework, formulating related policies, and overseeing the management of risks approved by the Head GRC and CISO on an annual basis. This function helps implement a consistent and structured approach to identifying and mitigating potential threats.

A comprehensive risk register is maintained to document regulatory, operational and technical risks identified across various verticals. Each risk is classified and assigned a risk score based on a scoring matrix outlined in the policy document. The risk score is calculated by multiplying the likelihood rating and impact rating each ranging from one (very low) to five (very high). The risk apetite is depicted using Red, Amber, Yellow and green colour.

Risk evaluation criteria and expected mitigation time is as follows:

Risk score	Risk category	Indicator	Mitigation time
17 to 25	Critical	Red	6 months
10 to 16	High	Amber	12 months
6 to 9	Medium	Yellow	18 months
3 to 5	Low	Green	No action
1 to 2	Very Low	Green	No action

For high-scoring risks, treatment plans are developed collaboratively by the GRC team and the relevant operational units. These plans specify risk treatment strategies and controls aimed at effectively mitigating high-impact risks. Target closure dates for each risk are recorded in the risk register. In cases of delays in risk resolution, the operational teams engage with the GRC team to address the underlying issues.

Risk treatment includes developing plans to reduce the risk to an acceptable level. The decision to accept the residual risk after mitigation is the responsibility of the risk owner or the compliance team.The GRC team conducts an annual internal audit covering all operational verticals, including compliance with legal requirements. Audit findings and observations are documented and shared with the respective operational heads, who are assigned target dates to resolve critical issues. The operations teams implement the recommended mitigation measures within the specified timelines and submit closure reports to the GRC team.

Periodic management review meetings are held to evaluate identified risks, vulnerabilities, and audit findings. These meetings facilitate discussions with leadership on risk status, reinforce accountability, and drive the implementation of necessary actions to strengthen the organization’s overall risk posture.

MONITORING ACTIVITIES

Vulnerability Scanning and Monitoring:

Yotta has a documented Vulnerability Assessment policy and is reviewed and approved by the CISO on an annual basis .The Yotta Host Cyber Security team conducts internal vulnerability assessments on a weekly and quarterly basis for Yotta-owned servers, infrastructure, and network devices. These assessments are performed using the Qualys application, with an agent installed on each system component that initiates scanning commands every four hours. The Qualys application operates based on an OEM-configured ruleset, which can be modified or updated by Yotta based on requirements. The vendor does not have direct access to the Qualys application; all configurations are managed by the Host Cyber Security team, with vendor support as needed. Vulnerabilities are categorized on the scale from 1 to 5, where:

Risk categoty	Risk description
5 – Critical	Risks that pose a significant threat to the organization's objectives and require immediate action to prevent or mitigate potential damage.
4 – High	Risks that pose a considerable impact to the organization's objectives and require timely action to prevent or mitigate potential damage.
3 – Medium	Risks that pose a moderate impact to the organization's objectives and require periodic review and monitoring.
2 & 1 – Low and Informational	Risks that pose a minor or negligible impact to the organization's objectives and can be ignored or monitored through daily monitoring processes.

The Qualys application compiles scan results from configured system agents and generates a comprehensive vulnerability report. The Management Information System (MIS) team downloads the report from the Qualys application and shares with the relevant Operations teams for analysis and remediation. Those vulnerablities which are critical in nature and impact servers that are critical to user entity services are addressed immediately. Critical, high, and medium vulnerabilities are also recorded in the risk register maintained by the respective operations team.

In case of identified vulnerabilities cannot remediated, exception approval is obtained from Yotta management and vulnerability along with the approval is documented as part of the risk register. Futher manual vulnerability scan is triggered as needed. A weekly review meeting with senior management is perfromed to discuss active vulnerabilities and any required actions.

Penetration Testing:

EsecForte, a third-party vendor, conducts an annual Penetration Test (PT) to analyze web-facing Internet Protocols (IP) and servers owned and managed by Yotta. A detailed PT report is generated and shared with the CISO team for review. Identified vulnerabilities and associated risks are documented in a comprehensive risk register. The respective operations teams evaluate these vulnerabilities, prioritize them based on severity, and enable their timely remediation based on risk assessment. The identified risks and mitigation progress are systematically reviewed and discussed during MRM with Yotta leadership.

Security, Capacity and Network Monitoring:

Yotta has defined procedure for capacity management which is reviewed Yotta senior management on an annual basis. Yotta has a dedicated monitoring team who monitors critical systems and IS events that are recorded in the Zabbix application and the IBMQradar applications.

The Corporate IT team monitors the utilization of system resources and performance of the IT assets and initiates changes if required as per the change management policy. In addition to real-time resource utilization monitoring, optimization of network devices is conducted to help ensure efficient resource allocation and maximize performance. Performance monitoring is of network components is conducted using the Zabbix application. An analysis of the device outages, availability events, and capacity utilization is prepared and reviewed by the Network team and the NOC team. Monitoring of network event logs, patch management, inatallation, capturing errors, security issues from network activity and application logs is logged and monitored in the IBMQradar application. The monitoring is performed by the SOC team.

MRM which includes Yotta management, is conducted on a periodic basis to monitor and review the effectiveness of controls and to drive continual improvement within the organization. The meeting summary as minutes is shared with all the stakeholders and senior management.

Business Continuity Plan and Disaster Recovery

Yotta has a documented Business Continuity Plan (BCP) and Disaster Recovery (DR) plan and is reviewed and approved by the Chief Digital Officer. BCP tests and DR drills are conducted based on drill calendar.

The BCP process at Yotta is conducted at an enterprise level, extending beyond the recovery of technological infrastructure to encompass all critical business functions. This includes personnel, physical workspace, IT systems and services, data management, and related operational dependencies. The Business Continuity Management (BCM) framework incorporates the management's commitment, scope definition, policy formulation, risk assessment, and continuous monitoring, analysis, and evaluation to ensure the program's effectiveness and alignment with organizational objectives.

Yotta has established High Availability (HA) infrastructure by leveraging advanced infrastructure strategies to establish seamless service continuity during component failures. Additionally, mock drills are conducted on periodic basis at all locations. The results of the mock drills are recorded in drill report and the risk associated with the results are documented in the data sheet maintained by DC Operations team and approved by the Head GRC on an annual basis.

INFORMATION AND COMMUNICATION

Management have defined procedures for periodic and formal reporting of activities for their user entities. Communication with user entities is through calls, e-mail or OneYotta, a portal dedicated for user entity use.

The intranet hosts the information such as information relating to internal policies, announcements, periodic email updates and hence serves as an important internal communication medium.

Yotta follows an open-door policy towards accessibility of senior management to employees. Employees can approach their respective Managers to discuss any issues relating to work.

Internal Communication

Yotta uses the Darwin Box application for internal communication, announcements, any changes to the organization structure. Yotta policies and procedures are accessible to employees through ATHENA. General updates to the entire firm on security policies and procedures are communicated through emails that are encrypted. To discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization, internal meetings are conducted on a quarterly basis. The summary of updates of such meetings is shared through email.

Internal transfers, new hires and exits are informed internally to appropriate personnel through email. Employee grievances if any are reported through emails to the HR team. Additionally, sessions are scheduled on a periodic basis where the management interacts with the employees and provides insights and updates on the various firm wide activities. Key issues affecting the organization and its employees are also communicated to employees during such sessions. In addition, Yotta shares security updates through desktop screensaver and wallpapers.

External Communication

Yotta communicates externally with the stakeholders and user entities through emails, telephonic conversations, video conferencing and personal meetings. Major changes / incidents affecting the user entity, security breaches and other monthly updates are shared with the user entity and other stakeholders through emails. Component health, performance and capacity information are uploaded on the OneYotta application dedicated for user entity. User entities can also submit request through the Helpdesk team, which is a centralised point for managing and addressing inquires.

GENERAL OPERATING ENVIRONMENT

Information Security

Yotta, through ISO and PCI DSS certification, strives to incorporate IS principles into the organization's culture, by making it the responsibility of every stakeholder to build and maintain a robust IS environment. Yotta has defined and documented an IS policy which outlines maintaining security, confidentiality, availability, and privacy of information within Yotta processes including services provided to user entities. Yotta has also defined underlying procedures which serve as guidelines for Yotta users in incorporating IS in day-to-day operations. IS policy is reviewed and approved annually by Chief Digital Officer.

At Yotta Information Security, Privacy and Compliance training is imparted to new joiners as a part of the induction training which is required to be completed within a week of their joining date. Further, refresher training is conducted for the entire firm on an annual basis which includes information security and privacy trainings.

Yotta has developed and communicated policies and procedures across functions including information security, HR, logical security, network security, infrastructure management, physical and environmental security, backup, and restoration, change management, and incident management to its employees. The roles and responsibilities of the team members are defined in the policy and procedure documents.

CISO team shares phishing simulation emails to Yotta employees on a monthly basis. The CISO team monitors the status of the phishing emails on caniphish.com application used to manage phishing simulation emails. The CISO team will share the list of users whose ID was compromised upon clocking the email. The employees whose IDs were compromised undertakes mandatory IS trainings.

Operations Security Policies

Yotta's System Hardening policy defines the guidelines for implementing security configurations on workstations and servers to mitigate vulnerabilities and protect them from threats. The policy includes guidelines on endpoint encryption such as installation of antivirus, disk encryption, endpoint firewall, USB block and restricted admin rights. For server hardening, a golden image is defined reflecting a standard set of configurations and is approved by the CISO on an annual basis. Yotta has defined data classification policy which defines guidelines to classify the data between confidential, external and internal.

Password Policy

- This policy governs the creation and protection of passwords in Yotta for access to the domain and network.
- Yotta uses complex password parameters which include:
    - minimum length of eight characters
    - special character
    - an upper case
    - a numeric value
    - password validity of maximum 90 days
    - account lockout after three invalid logon attempts
    - password history of five

Human Resources

- The HR department has docuemnted policy procedures which includes employee onboarding, employee probation and confirmation policy, leave and absence management policy, suspension, and termination as potential sanctions for employee misconduct. The policies are reviewed by Head HR and approved by Co-founder and Chief Executive Officer (CEO) on an annual basis.
- The HR department is responsible for carrying out activities i.e. recruitment, onboarding, induction, performance evaluation, performance improvement and offboarding. The HR department is responsible for the development of policies and procedures pertaining to HR which can be referred by employees in the organization for developing competency of the workforce in their respective job responsibilities.
- The job descriptions outline the roles, responsibilities, required experience, and qualifications necessary to perform assigned duties in a professional and competent manner. The organization identifies the knowledge and skills essential for fulfilling these responsibilities and recruits candidates based on the specified skill set and job requirements.

- Job requisitions, containing detailed job descriptions, are either uploaded on Darwin Box or communicated via email by the Business Head or Managers to the HR team. For recruitment, the HR team conducts an initial screening to evaluate candidates' alignment with the job description. Shortlisted candidates proceed through technical and HR interview rounds, during which their skills and competencies are assessed against the job requirements.
- Following the assessment process, a candidate may be selected for the role. Upon hiring, a comprehensive background check which comprises of education qualification, past employement and criminal record verification is conducted. If discrepancies arise during the background verification process, the Head of GRC reviews the findings and an exception approval is granted on the case to case basis to proceed with the hire, if necessary.
- Yotta has a Code of Business Conduct policy in place which is designed to protect the confidential information about the company and user entities received by the employees. This policy restricts employees from sharing the data on need-to-know basis only. At the time of joining, employees sign Letter of Understanding and Security Guidelines and appointment letter which includes Non-Disclosure Agreement (NDA), code of conduct, security, privacy and confidentiality clauses.
- Each employee undergoes training for a specified period post joining. The employees are provided induction training on processes of Yotta services based on a pre-defined training schedule. Employees have access to Standard Operating Procedures (SOP) that describe the process / activities of their respective operational area. Periodic training is imparted to the employees to facilitate their knowledge enhancement.
- Mandatory refresher training is conducted on an annual basis. The progress of the training for each employee is tracked through the Darwinbix application. In case of non compliance, the HR team shares reminder emails to the employee.
- New joiner and existing employees are required to undergo mandatory IS, Cyber security and Privacy trainings. Employees are required to undergo IS training in case the employee has clicked on phishing simulation email shared by the CISO monthly. Relevant actions are taken in case of non-compliance of training.
- For performance management, the employees undergo an annual appraisal cycle. The performance of employee is rated by the employee's superior on a quarterly basis.

Colocation

Yotta provides data centre infrastructure for user entities to host and manage their systems based on the services opted by them. Yotta has provided dedicated cages with rack keys to each user entity to establish restricted physical access to authorized personnel.

A Service Request (SR) is raised through the Tussom application by the Helpdesk team to install or setup infrastructure for new user entities. The SRs are then assigned to respective tower operations team to process the request based on the subscription opted by the user entity. User entity email ID is onboarded on Tussom application which enables the user entity to raise the SR directly on Tussom. User entity can also contact or call the helpdesk team to raise and SR on the Tussom application on their behalf.

Physical Security and Access Control

There exists a documented Physical Security policy for controlling physical access to general and restricted areas, including the data centre hosting facility. The policy is reviewed and approved by the CISO and Head of security on an annual basis.

Physical Access Creation

Access to Yotta employees is given based on their job responsibilities. The DC Security and DC Operations team have access to the data centres. Employees are required to display their identity (ID) cards while in the office facilities and DC. Yotta has installed biometric and access card devices to restrict the access of employees in the office facilities and internally to restrict access to specific work areas. The Security team manages biometric access by using the Milestone (for Mumbai and Navi Mumbai) and Genetics (for Noida and Gift city) application. The HR team informs the DC security team through email and provides the date of joining of an employee. The DC security team grants access upon approval from department head.

Physical Access Revocation

On the last working day of an employee, an automated mail is sent from DarwinBox to the DC Security team to deactivate the physical access rights of the employee to the Yotta data centres. The HR will also send list of users whose access from the data centre has to be revoked to the DC security team. The DC Security team deactivates the accesses associated with the employee's access card and sends a confirmation email to the Human Resources team.

Visitors and Vendors Access

To facilitate visitor access for vendors, auditors, consultants, or user entity, a request ticket must be initiated in the Tussom application. Once the ticket is raised, an auto-generated link of the Visitor Management System (VMS) from Tussom application will be sent to the visitor via email. Through this link, the visitor will be required to provide all necessary details, including signing a Non-Disclosure Agreement (NDA). The information, along with the signed NDA, will be captured in the VMS.

The DC Security team will review and verify the submitted details before issuing an E-Visitor pass, which is sent to the visitor via email. Upon arrival, the on-site security guard will scan the E-Visitor Pass, and the visitor's details will be displayed on the VMS, allowing them to proceed to reception. At reception, the visitor's government issued, or company photo ID will be verified prior to granting entry to the general area. To help ensure the right level of vigilance is practiced, Yotta issues different access lanyards defined as below for employees, user entity personnel and vendors/sub-contractors. Visitors accessing the restricted areas are escorted by personnel from DC Operations team.

Colour	Visitor type
Blue	Yotta employee
White	User entity
Yellow	Visitor
Black	Project contractors
Orange	Operational contractors
Grey	Service personnel
Light blue	Consultant

To enable utmost protection of critical assets hosting user entities' data and the data centres, the security mechanisms are organized into seven layers of security.

- Layer 7 Vehicle checks, ID verification.

- Layer 6 ID check at full height turnstile, under vehicle scanning system.

- Layer 5 X-ray scanning and frisking at the lobby.

- Layer 4 Visitor management system and turnstile.

- Layer 3 Key management / verification.

- Layer 2 Frisking at the server hall entry.

- Layer 1 Mantrap, access card and biometric access control system at the server hall.

For user entity accessing server racks, which are secured with lock and key, the key details along with entry date and time is updated in the visitor register prior to accessing server room. The security guard stationed outside the server room verifies the approval granted by the DC Operations team for visit along with the rack details shared by the user entity.

Physical Security – CCTV Monitoring

The data centre operates under 24/7 CCTV surveillance, with a dedicated room for monitoring footage. Monitoring is conducted in 12-hour shifts. If any unauthorized access is detected at the door, an alarm is automatically triggered by the Genetics or Milestone applications. The DC Security team will raise an incident ticket in the Tussom application and immediately alert the on-site security guard to survey the area.

CCTV logs are retained across locations for 90 days. A daily MIS report is prepared and shared with the security assistant for log review, and subsequently forwarded to the security officer for verification. In the event of a critical issue, the Head Security and Safety is notified, along with the report, and actions are taken as needed.

Physical Access Review

On a bi-annual basis, the Head of Department of the DC Security team reviews the system-generated list of individuals with access to the data centre. Discrepancies identified if any are actioned upon after consultation with the respective department heads.

Environmental Controls

To prevent and reduce the risk of damage and interference to Yotta's infrastructure due to physical and environmental threats, Yotta has a documented Physical and Environmental Security policy which is reviewed and approved by the Head of DC Security on an annual basis. Yotta has defined Data Centre Maintenance policy which includes maintenance of data centre utilities and security equipment and disposal of waste which is reviewed and approved by Head – DC Operations on an annual basis.

The data centre is equipped with advanced environmental protection systems including cooling systems, smoke detectors, fire suppression system, smoke detectors, temperature and humidity monitoring system to safeguard the data centre environment. The data centre operates on uninterruptible power supply (UPS) and diesel generator and maintains a backup of 48 hours in case of any electricity outage. The power control is divided into two sections/ blocks which is block A and block B which works as secondary power supply to each other.

A dedicated temperature and humidifier control system continuously monitors the temperature and humidity levels at the server hall. The DC Operations team members monitor the system for any deviation. In case of any deviation, the system triggers an alarm, and the DC Operations team will take relevant actions.

The DC Operations team conducts the preventive maintenance of critical equipment in the data centre as per preventive maintenance schedule. This activity is performed to maintain the continued operability of the equipment.

The DC Operations team maintains a preventive maintenance calendar, structured according to the maintenance requirements of each component. When a maintenance date is approaching, a reminder email is sent to the vendor. On the scheduled date, the vendor visits the data centre to inspect and service the components. Following each maintenance, the vendor issues a service report. Turnaround time (TAT) is agreed between Yotta and vendor. Any discrepancies identified are reviewed by the DC Operations Head, who oversees corrective actions as necessary.

To document any discrepancies and corresponding corrective actions, a ticket is raised in the Tussom application. If a component issue arises that necessitates replacement and impacts user entity service, user entity approval for downtime is obtained prior to replacement.

At the Mumbai (Airoli and Panvel) and Delhi (Noida) locations, critical spare parts are stored on-site in dedicated facilities called the storage room for emergencies. In addition to this, parts owned by Yotta are stored at the vendor's warehouse. All parts are stored at the vendor's warehouse. Apart from the details maintained in material management tool, a register is kept at the store to maintain record of spare parts.

The DC Operations team conducts regular checks to help ensure that all components, whether stored on Yotta premises or at the vendor's location, remain operational and in good condition. Additionally, on an annual basis, the Yotta DC Operations team conducts on-site reviews of procured products at the vendor's location to verify performance and maintenance compliance.

Vendor Management

A Third-Party and Outsourcing Security policy has been established and implemented for the outsourcing of any service to third-party vendors. Yotta has defined a standard contract template that includes defined terms, conditions, and responsibilities for vendors and subcontractors. These contracts address security, confidentiality, availability, and privacy commitments as applicable. They also include requirements such as background check results for contracted employee partners and notifications in the event of security, confidentiality, availability, or privacy violations or breaches.

The Procurement team maintains list of all the vendors based on their criticality. At the time of onboarding, the Procurement team performs due diligence of vendors based on the products or services they provide. For technical verification, the respective operations teams evaluate the vendor's offerings and capabilities. Vendors are rated on various parameters, with the ratings reviewed and approved by three key authorities:

1. Project Head
2. Operations Head
3. Technical Head

Logical Access

Yotta has documented a logical access procedure as a part of IS Policy. IS Policy is reviewed on an annual basis by the CISO. Logical access procedures are defined to protect against unauthorized access to information resources and services to prevent disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves as per business requirements. Access to key application and Servers is authenticated through Sectona PAM tool. The appropriate level of access to infrastructure and information is determined based upon the business need, job functions, and role.

Access to the restricted servers and applications is provided only after obtaining approval of the respective operations team head. Operating System (OS) level and network level controls are established to protect un-authorized logical access to IT infrastructure. User access rights are reviewed on a quarterly basis by the head of respective departments. Access rights of the user are disabled within 24 hours post receiving intimation from HR.

User Registration/De-registration

When a new employee joins Yotta, the HR department sends an email to the Corporate IT team requesting the creation of the employee's account in the Yotta Active Directory (AD). Upon receiving the request, the Corporate IT team creates ID on Yotta Active Directory (AD). Additionally, the Corporate IT team provides access to designated applications that are pre-approved by the respective application / operation heads. These pre-approved application lists are subject to periodic review by each operations head to verify their relevance and compliance. Once the AD access is created, the Corporate IT team sends an email to the employee with instructions for setting up a password in accordance with the AD password policy.

In the case of an employee's resignation or termination, the HR department notifies the Corporate IT team via email to revoke the employee's access. Upon receiving this notification, the Corporate IT team secures a backup of the required user data for archiving purpose and deactivates the employee's login ID from the AD. Following the completion of all necessary formalities, the login ID is permanently disabled within 90 days, subject to the approval of the Corporate IT Head. This process ensures secure and efficient management of user access, with periodic reviews conducted to maintain alignment with organizational security policies.

Privileged Account Access

A privileged account on a system is a user account that has elevated permissions and access rights, allowing it to perform administrative or critical functions beyond those available to standard user accounts. These accounts are typically used for tasks such as configuring systems, managing security settings, accessing sensitive data, and maintaining infrastructure. Privileged access to the infrastructure is granted based on roles and authorized approvals outlined in the Information Security policy. Access to the servers is enabled through Sectona- PAM and access to network components is enabled through CISCO ISE. Privileged access rights are reviewed by the respective Operation heads on a quarterly basis. Request for termination of such access rights is communicated to the respective operations team. Additionally, IT team also pro-actively checks with the employees for continuation / termination of privileged rights during its quarterly review.

Network and Antivirus Management

Network management

Yotta has configured FortiGate Unified Threat Management (UTM) device at the perimeter of network to prevent it from external threats. The Network security teaam and the NOC team manages deliverables such as internet bandwidth, rack, electricity, power, cross connect, remote connectivityand network design provided to the user entity. List of network components are maintained in the CMDB module within the Tussom application.

The Network team reviews network configuration based on pre-approved hardening checklist. In case of configuration level changes, the vendor performs changes post approval from the Network team.

The Network team monitors the network components through CISCO Identity Services Engine (ISE). Privilege activity is logged and monitored through CISCO ISE. Logical access to the perimeter firewalls and network devices has been restricted to authorized personnel from Cyber Security team using CISCO ISE. Authentication is granted via Sectona- PAM tool.

Firmware upgrades are performed by the Network team when latest patches are released or to resolve a bug issue. The upgrades are tested (Pre-check) by the vendor prior to implementation on network components. After implementation, post-checks are performed to verity the system stability. Precheck and post-check activities are documented in the Tussom application. In case of downtime, the user entity are notified. Roll back strategy is in place in case of failure during upgrades. Data encryption has been enabled on OneYotta application using Secure Hash Algorithm (SHA)- 256.

Antivirus Management

The Crowdstrike application is configured on the endpoints (workstations and servers) to prevent the threat of virus, malware and ransomware. The antivirus is configured to receive updates from live update server whereas the endpoints are configured to install automatic updates of signature files on daily basis. The endpoints are configured to perform system scans on a realtime basis. The antivirus is configured to block activity such as port scans based on the ruleset defined within the application. It displays potential risks on the dasshboard and the monitoring team sends a notification to the respective operations team and raises a ticket in Tussom application simultaneously. Activities related to virus protection are logged and maintained in the SIEM tool.

Change Management

Yotta has a documented Change Management process for management of changes (application, OS, database, domain and network devices) to prevent or mitigate business losses including degradation of the environment, health, and safety as the result of changes made in Yotta. The policy is reviewed on an annual basis by the Head- Service Management.

Changes are categorized into four different types namely Emergency, Planned,Pre- approved and Retrospective.

Change type	Description	Risk associated
Pre- approved	Changes like patches, vulnerabilities, configurations to infrastructure that are preauthorized by the change management team. Category	Low
Planned	Change to a service or infrastructure for which the risk is assessed and are approved case-to-case by the Change Advisory Board (CAB).	Moderate
Emergency	Change to repair an error within the environment and are approved by the CAB for each case	High
Retrospective	Emergency changes that are implemented first and the ticket is logged and discussed int the next weekly CAB meeting	High

Change requests are raised on the Tussom application for approval and review. The life cycle of the change request is divided into stages, that is Submission, Analysis, Approval, Implementation, Review, and Closure. The change is initiated by a change requestor. The technical approver evaluates the change and either approves or rejects the change based on their analysis. The change manager reviews the analysis and forwards the change to the Change Advisory Board (CAB) members. The CAB members will analyse the change during the CAB meeting. If approved, the change is forwarded to the development manager for testing and validation. Upon successful validation, the implementor pushes the change into production enviroment. The change auditor verifies whether the changes are functioning correctly in the production enviroment as per expected test results. A rollback plan is applied in case the changes are not functioning as per the test results. Yotta has a Change Advisory Board (CAB) which meets on a weekly basis to discuss pre-approved and planned changes. Approval for emergency changes is provided immediately once the change is raised.

Patch Management

Database servers

Upgrades for databases managed by Yotta are performed on a quarterly basis. A ticket is raised on the Tussom application by the Cloud team. For the databases managed by the user entity, a request is raised from the registered ID which logs a ticket on the Tussom application. The user entity can also call the Helpdesk team to raise a ticket regarding upgrades. All the upgrades follow the change management process.

Incident and Problem Management

Yotta has a documented Incident Management policy which defines the process of reporting interruptions in the daily operations due to unplanned events or incidents. The policy is reviewed on an annual basis by the Head- Service Management. The incidents and service requests are either raised on Tussom application directly or an email is shared with Yotta helpdesk team and a member from the helpdesk team will raise a ticket in the Tussom application. The incidents are raised, managed and resolved as per the Incident Management policy. Incidents are categorized based on severity into S1, S2, S3 and S4 levels. S1 severity represents the highest level of severity incidents.

Categorisation of incidents based on their severity:

Severity	Description
Severity 1 (S1)	Leading to business impact
Severity 2 (S2)	Leading to slowness in business
Severity 3 (S3)	Leading to impacting the setup. No impact on business
Severity 4 (S4)	Auto tickets generated based on threshold configurations

Severity	Description
Service Request (S4)	Requests from end users

Incidents are tracked, monitored, prioritized based on severity, assigned to respective Operations team through Tussom application. The respective Operations team will analyse and track the incident to closure. Incidents with S1 severity have a problem ticket associated with it and root cause analysis is documeted in the problem ticket. Service Level Agreements (SLA) for closure of incidents have been established and defined in the policy document. Tussom application SLAs are also configured within the Tussom application which automatically highlights SLA breaches in the ticket. SLA compliance and delays/ breaches are monitored in the management review meeting.

In the event of a security incident, the Information Security team conducts a thorough investigation of actual or suspected breaches. This includes analyzing the incident, assessing potential vulnerabilities, and reviewing relevant internal procedures and controls in collaboration with the impacted department. Following the investigation, the CISO delivers actionable recommendations to mitigate risks and oversees their implementation. Monthly review meetings are conducted with management to discuss the incidents occurred, resolution performed and SLA breach if any.

Backup Operations

Yotta has a Backup policy in place which intends to address the company's requirement to backup copies of essential business information, data and support information is taken regularly in a manner such that it is available for restoration of business operations whenever required within the stipulated period. The policy is reviewed by Head – Backup and Restoration on an annual basis. The Business Continuity and Disaster Recovery Plans are tested periodically to verify continuation of business including but not limited to mock restoration of data, testing remote connections and replication services.

Backups are configured and enabled through Commvault application. The backups of files and folders are scheduled for each servers / folders onboarded on Commvault application. Backups are performed on a daily (incremental) and weekly (full) basis. Backup of Yotta internal servers and user entity servers is taken using the Commvault application managed by Yotta. The responsibility of data on user entity server lies solely with the user entity as mentioned in the contract. The servers are given unique identification to distinguish between internal Yotta servers and external (user entity) servers.

Apart from the daily schedule, backup is taken upon request from Yotta operations team for internal servers and user entity for external servers. The request is initiated through a backup request form, and the backup team, performs the backup based on the specified requirements in the form.

The Backup team receives a status notification indicating whether the backup was successful or encountered an issue. In the event of a backup failure, an incident ticket is promptly raised in the Tussom application, triggering corrective actions by the Backup team.

Failed backups are scheduled to restart automatically after 24 hours. However, if an immediate reattempt is necessary, the Backup Operations team can manually trigger the backup. Permissions to modify backup configurations are exclusively granted to the Yotta backup team. Data at rest is encrypted using AES 256 for security. Backup activity logs are recorded directly within the Commvault application.

Storage and restoration

The retention period and management of backups for Yotta internal servers are overseen by the respective Operations team. Backup tapes are securely stored in dedicated vaults located within the data Centre premises. Backup data is stored in a dedicated storage area, with the retention period tailored to meet the user entity's subscription plan. For user entity opting for tape storage, magnetic tapes are securely transported to a secondary location by Iron Mountain. Additionally, the servers are backed up at a seperate geographical location.

Privacy

Yotta has defined privacy policy and is published on its corporate website: https://yotta.com/privacy-policy. Yotta's Privacy policy is regularly reviewed by its Legal Team and updated as needed to reflect current business practices. The policy describes how Yotta collects, uses, and protects customers' personal data across its websites, products, services, events, and experiences.

To help ensure robust data privacy, Yotta has developed and implemented a data privacy awareness and training program for its employees which is conducted on an annual basis. Privacy awareness modules are also incorporated as a part of the Information Security training provided to all employees.

Yotta has defined Data Protection policy which covers logging and monitoring of privacy breaches. The policy document is reviewed by Head Legal and Data Protection Officer (DPO). To maintain data privacy standards, Yotta conducts continuous monitoring of its privacy controls, helping ensure their effectiveness and promptly addressing any identified issues through corrective actions.

A dedicated email ID: dpo@yotta.com is maintained for redressal of complaints. The Data Privacy Officer is responsible for addressing the complaints or any incidents of non-compliance.

The DPO plays a key role in:

- Documenting and approving the data protection and privacy policy
- Addressing nature and scope of data privacy breach, if any
- Potential impact of the breach
- Remedial actions taken to mitigate the risk associated with any breach.

Privacy Governance

The Yotta Privacy policy applies to data under Yotta's management. As user entities are responsible for data collection and appropriateness of usage of data, user entities privacy policies are applicable to such data.

CONTROL ACTIVITIES

Trust Services Criteria and Related Activities

Relevant trust services criteria and Yotta's related controls are included in section 4 of this report, "Trust Services Criteria, Controls Test Procedures and Tests Results", to eliminate the redundancy that would result from listing them in this section and repeating them in section 4. Although the applicable trust services criteria and related controls are presented in section 4, they are, nevertheless, an integral part of Yotta's System description.

Controls to be excercised by User Entity

In the design of their controls, Yotta has envisaged certain controls to be exercised by user entity. These controls are listed in section 4 for each control objective under the heading "Complementary User Entity Controls". The responsibility for design, implementation, and operating effectiveness of these controls rests with user entity unless subscribed. This information has been provided to user entity and to their auditors to be taken into consideration when making assessments of control risk for user entity.

Although, the Complementary User Entity Controls are included, they do not form part of scope of the report:

- User entities are responsible for managing the infrastructure, accessing the infrastructure, taking backup of the data and restoration of the backup.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

I. Mapping of Criteria with Control Description

Criteria #	Criteria Description	Control number	Control Description
CC 1.0 Common Criteria Related to Control Environment			
CC 1.1	The entity demonstrates a commitment to integrity and ethical values.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.1.2	Yotta has defined ISMS based on International Organization for Standardization (ISO) 27001:2022 framework.
		CC 1.1.3	Standard contractual agreements signed between Yotta and its user entities include Yotta's security, availability, privacy and confidentiality commitments as applicable regarding the system.
		CC 1.1.4	Confidentiality agreement and Non-disclosure agreement (NDA) is signed by new joiners on the date of joining the organization as part of employment letter.
		CC 1.1.5	Yotta has established disciplinary standards and guidelines for employee behavior as part of Code of Business Conduct policy which include suspension, and termination as potential sanctions for employee misconduct and the policy is reviewed and approved by the Head HR on an annual basis.
		CC 1.1.6	New joiners are required to read and accept the Code of Conduct (CoC) agreement consisting of terms and conditions on the day of their joining.
		CC 1.1.7	Employees must clear a background check covering minimum of previous employment, education and criminal records before they are confirmed by the management. Exceptional approvals are taken for specific unsuccessful background verification cases from Head HR/ CEO of Yotta.
CC 1.2	The Board of Directors (BoD) demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC 1.2.1	Management has established a board charter to determine the requirement and composition of Board of Directors (BoD).
		CC 1.2.2	Yotta has a defined organizational structure, reporting lines, authorities, and responsibilities. As part of its business planning process, ongoing risk assessment and management process, Yotta revises the structure when necessary to help meet the commitments and requirements.
		CC 1.2.3	The organization's BoD has members who are independent of executive management such that they are objective in evaluation and decision making.

Criteria #	Criteria Description	Control number	Control Description
CC 1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.2.1	Management has established a board charter to determine the requirement and composition of Board of Directors (BoD).
		CC 1.2.2	Yotta has a defined organizational structure, reporting lines, authorities, and responsibilities. As part of its business planning process, ongoing risk assessment and management process, Yotta revises the structure when necessary to help meet the commitments and requirements.
		CC 1.3.1	Roles and responsibilities are defined in written job descriptions and reviewed on an annual basis. Roles and responsibilities documents are uploaded on Yotta's intranet portal.
		CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.
CC 1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC 1.1.7	Employees must clear a background check covering minimum of previous employment, education and criminal records before they are confirmed by the management. Exceptional approvals are taken for specific unsuccessful background verification cases from Head HR/ CEO of Yotta.
		CC 1.4.1	There exists formally documented Employee Onboarding Policy document that provides guidance for employee onboarding, approved by Co-founder and CEO on an annual basis. These policies are made available to employees on the Yotta intranet.
		CC 1.4.2	Job requirements are documented in the job descriptions, and candidates' abilities, experience and knowledge to meet these requirements are evaluated as part of the hiring evaluation process.
		CC 1.4.3	Candidates are evaluated based on their technical skills and non-technical skills during the interview evaluation process.
		CC 1.4.4	Management establishes requisite skillsets for employees and provides continued training about its commitments and requirements for employees to support the achievement of objectives.
		CC 1.4.5	Employee performance across organization is measured against the defined goals and objectives on a quarterly basis.

Criteria #	Criteria Description	Control number	Control Description
CC 1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC 1.1.5	Yotta has established disciplinary standards and guidelines for employee behavior as part of Code of Business Conduct policy which include suspension, and termination as potential sanctions for employee misconduct and the policy is reviewed and approved by the Head HR on an annual basis.
		CC 1.3.1	Roles and responsibilities are defined in written job descriptions and reviewed on an annual basis. Roles and responsibilities documents are uploaded on Yotta's intranet portal.
		CC 1.4.5	Employee performance across organization is measured against the defined goals and objectives on a quarterly basis.
		CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet. The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.
CC 2.0 Common Criteria Related to Communication and Information			
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC 2.1.1	There exists a formally documented Information Classification policy that includes classification of data based on its criticality and sensitivity. The document is reviewed and approved by Yotta's management on an annual basis.
		CC 2.1.2	Yotta has a defined Change Management Procedure specifying the change management process to be followed for key applications. The policy is reviewed and approved by Head Service Management on an annual basis.
		CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and approved by Head Service Management on an annual basis.
		CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.
		CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The

Criteria #	Criteria Description	Control number	Control Description
			SRs are approved and tracked to closure by the respective operation tower personnel.
		CC 2.1.6	Operations team personnel follow defined protocols to perform Root Cause Analysis (RCA). for evaluating severity one (S1) incidents
		CC 2.1.7	There exists a policy and procedure document for capacity management which defines the process to be followed for monitoring and planning asset capacity. This policy and procedure document are reviewed by Yotta senior management on an annual basis.
		CC 2.1.8	Zabbix application is utilized to monitor availability, system performance and health and generate alerts when specific predefined thresholds are breached and corrective actions are taken by respective team.
		CC 2.1.9	Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.
		CC 2.1.10	Resolution of incidents are reviewed on a monthly basis by the senior management in the review meetings.
		CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.
		CC 2.1.12	An asset inventory of Yotta's network components is maintained for accounting of asset additions and removals for management's use and is reviewed by the Head - IT Operations (Network).
		CC 2.1.13	An asset inventory of Yotta's system components (servers, end-user systems) is maintained for accounting of asset additions and removals for management's use and is reviewed by the team lead from Corporate IT and Cloud Operation team.
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.1.3	Standard contractual agreements signed between Yotta and its user entities include Yotta's security, availability, privacy and confidentiality commitments as applicable regarding the system.

Criteria #	Criteria Description	Control number	Control Description
		CC 1.2.2	Yotta has a defined organizational structure, reporting lines, authorities, and responsibilities. As part of its business planning process, ongoing risk assessment and management process, Yotta revises the structure when necessary to help meet the commitments and requirements.
		CC 1.3.1	Roles and responsibilities are defined in written job descriptions and reviewed on an annual basis. Roles and responsibilities documents are uploaded on Yotta's intranet portal.
		CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.
		CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and approved by Head Service Management on an annual basis.
		CC 2.2.1	Management conducts information security trainings upon compromise of employee emails after phishing simulations.
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.1.2	Yotta has defined ISMS based on International Organization for Standardization (ISO) 27001:2022 framework.
		CC 1.1.3	Standard contractual agreements signed between Yotta and its user entities include Yotta's security, availability, privacy and confidentiality commitments as applicable regarding the system.
		CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and confidentiality commitments applicable to the vendors and third parties.
		CC 2.3.2	Operations team performs a preliminary vendor risk assessment prior to entering into any business relationship with a new vendor. Such assessments are used to assess the risk of the company's relationship with the vendor.
CC 3.0 Common Criteria Related to Risk Assessment, and Design and Implementation of Controls			

Criteria #	Criteria Description	Control number	Control Description
CC 3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC 1.1.2	Yotta has defined ISMS based on International Organization for Standardization (ISO) 27001:2022 framework.
		CC 1.2.2	Yotta has a defined organizational structure, reporting lines, authorities, and responsibilities. As part of its business planning process, ongoing risk assessment and management process, Yotta revises the structure when necessary to help meet the commitments and requirements.
		CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.
		CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 3.1.2	Identified vulnerabilities are rated using a risk evaluation process and ratings provided are reviewed by the GRC and the CISO team.
		CC 3.1.3	The deficiencies identified as part of the vulnerability assessment are documented in risk register along with the corrective action plan and date of closure.
		CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape
CC 3.2	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.	CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 3.1.2	Identified vulnerabilities are rated using a risk evaluation process and ratings provided are reviewed by the GRC and the CISO team.
		CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape

Criteria #	Criteria Description	Control number	Control Description
		CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on critical servers on a quarterly basis and tracked to closure.
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on critical servers on a quarterly basis and tracked to closure.
		CC 3.3.1	There exists formally documented whistle blower policy and procedures that provide guidance regarding fraud, whistle blower mechanism and protection to whistle blower. The policy is reviewed and approved by Co-founder & CEO on an annual basis.
		CC 3.3.2	Management has established whistle-blower e-mail ID available to internal and external users.
		CC 3.3.3	There exists defined policy related to disposal of media/ waste with confidential information it holds, if any, in electronic and paper form. The policy is reviewed periodically and is approved by Head-DC operations.
		CC 3.3.4	The GRC team communicates the internal audit observations to the relevant stakeholders and senior management annually.
		CC 3.3.5	Annual Penetration testing is performed by a third-party. Reports are shared with relevant stakeholders and reviewed by the senior management. The vulnerabilities identified are evaluated and closed based on risk assessment.
		CC 3.3.6	Netskope DLP application is configured on the endpoint devices to scan for sensitive information transferred on the removable media. Incidents detected are analyzed and tracked to closure.
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.

Criteria #	Criteria Description	Control number	Control Description
		CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape
		CC 3.3.4	The GRC team communicates the internal audit observations to the relevant stakeholders and senior management annually.
CC 4.0 Common Criteria Related to Monitoring Activities			
CC 4.1	The entity selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.
		CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.
		CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 3.3.4	The GRC team communicates the internal audit observations to the relevant stakeholders and senior management annually.
		CC 3.3.5	Annual Penetration testing is performed by a third-party. Reports are shared with relevant stakeholders and reviewed by the senior management. The vulnerabilities identified are evaluated and closed based on risk assessment.
		CC 4.1.1	The GRC team conducts internal audit annually. Gaps identified as part of the internal audit are tracked to closure.
		CC 4.1.2	Yotta is ISO 27001:2022 and PCI-DSS certified. Surveillance audit is conducted annually for effectiveness of internal controls.
		CC 4.1.3	An end-point asset inventory of assets is maintained in the Tussom application and hardened based on hardening checklist.
		CC 4.1.4	Hardening guidelines are established for network devices and are reviewed by the Head - IT Operations (Network) annually.

Criteria #	Criteria Description	Control number	Control Description
		CC 4.1.5	There exists an Internal Audit Framework document that describes the internal audit planning and methodology
		CC 4.1.6	Business continuity and Disaster Recovery (DR) drills are conducted based on DR drill calendar and exceptions noted, if any, are tracked to closure.
CC 4.2	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 BoD, as appropriate.	CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.
		CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 3.1.3	The deficiencies identified as part of the vulnerability assessment are documented in risk register along with the corrective action plan and date of closure.
		CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 3.3.4	The GRC team communicates the internal audit observations to the relevant stakeholders and senior management annually.
		CC 4.1.1	The GRC team conducts internal audit annually. Gaps identified as part of the internal audit are tracked to closure.
		CC 4.2.1	On a quarterly basis, a risk acceptance analysis for recurring non- impactful risks is approved by the CISO and Business team.
CC 5.0 Common Criteria Related to Control Activities			
CC 5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.

Criteria #	Criteria Description	Control number	Control Description
		CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet. The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.
		CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape
		CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 5.1.1	Control owners are identified post identification of vulnerabilities as part of risk assessments. Control owners are documented in the risk register and risk register is reviewed and approved by Head – GRC on an annual basis.
CC 5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet. The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.

Criteria #	Criteria Description	Control number	Control Description
		CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 5.1.1	Control owners are identified post identification of vulnerabilities as part of risk assessments. Control owners are documented in the risk register and risk register is reviewed and approved by Head – GRC on an annual basis.
CC 5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.1.2	Yotta has defined ISMS based on International Organization for Standardization (ISO) 27001:2022 framework.
		CC 1.1.4	Confidentiality agreement and Non-disclosure agreement (NDA) is signed by new joiners on the date of joining the organization as part of employment letter.
		CC 1.1.5	Yotta has established disciplinary standards and guidelines for employee behavior as part of Code of Business Conduct policy which include suspension, and termination as potential sanctions for employee misconduct and the policy is reviewed and approved by the Head HR on an annual basis.
		CC 1.1.6	New joiners are required to read and accept the Code of Conduct (CoC) agreement consisting of terms and conditions on the day of their joining.
		CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet. The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.
		CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and approved by Head Service Management on an annual basis.

Criteria #	Criteria Description	Control number	Control Description
CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
CC 6.1	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.	CC 2.1.12	An asset inventory of Yotta's network components is maintained for accounting of asset additions and removals for management's use and is reviewed by the Head - IT Operations (Network).
		CC 2.1.13	An asset inventory of Yotta's system components (servers, end-user systems) is maintained for accounting of asset additions and removals for management's use and is reviewed by the team lead from Corporate IT and Cloud Operation team.
		CC 3.3.6	Netskope DLP application is configured on the endpoint devices to scan for sensitive information transferred on the removable media. Incidents detected are analyzed and tracked to closure.
		CC 4.1.3	An end-point asset inventory of assets is maintained in the Tussom application and hardened based on hardening checklist.
		CC 6.1.1	There exists a Password and Account Management policy document that describes the password policies configured on the domain controller and applications in Yotta which includes password parameters such as minimum password length, password complexity, maximum password age and account lockout after unsuccessful attempts.
		CC 6.1.2	An authentication mechanism is implemented for key applications, network devices and servers, by implementing password policies as per defined password policy.
		CC 6.1.3	Privileged access to the network components follows the principle of least privilege by granting defined user roles through CISCO ISE and logical access to these roles are approved by authorized personnel. This access is reviewed on a quarterly basis.
		CC 6.1.4	Yotta has defined its Network Functional Procedure document to provide guidelines to employees utilizing the Virtual Private Network (VPN) to access the Yotta network in a secure manner. Policy is reviewed and approved on an annual basis by Head – IT Operations: Network
		CC 6.1.5	Firewall rules limit the types of activities and service requests that can be performed from external connections.
		CC 6.1.6	Data stored in Yotta managed databases are encrypted using AES 256 bit encryption.

Criteria #	Criteria Description	Control number	Control Description
CC 6.2	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.	CC 6.1.1	There exists a Password and Account Management policy document that describes the password policies configured on the domain controller and applications in Yotta which includes password parameters such as minimum password length, password complexity, maximum password age and account lockout after unsuccessful attempts.
		CC 6.1.2	An authentication mechanism is implemented for key applications, network devices and servers, by implementing password policies as per defined password policy.
		CC 6.1.3	Privileged access to the network components follows the principle of least privilege by granting defined user roles through CISCO ISE and logical access to these roles are approved by authorized personnel. This access is reviewed on a quarterly basis.
		CC 6.2.1	Employee user IDs are created in the Active Directory (AD) by the Corporate IT team as on date of joining of the employee upon approval from HR and Corporate IT team personnel.
		CC 6.2.2	A formal user approval process has been implemented that requires authorization by appropriate management for granting and modifying access to key applications upon approval from application owners
		CC 6.2.3	A formal user approval process has been implemented that requires authorization by appropriate management for granting access to Yotta managed databases upon approval from the Cloud team personnel.
		CC 6.2.4	Employee user IDs for resigned/ terminated personnel are disabled in Active Directory (AD) within 24 hours of the last working day as per the timelines defined in the Employee Exit process document.
		CC 6.2.5	The user access to the key applications is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.
		CC 6.2.6	The user access to Yotta Managed databases is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.
		CC 6.2.7	Quarterly user access review is performed for user IDs having access to active directory (AD). Discrepancies noted during the review are communicated to respective teams for resolution.
		CC 6.2.8	Quarterly user access review is performed for user IDs having access to key applications. Discrepancies noted during the review are communicated to respective teams for resolution.

Criteria #	Criteria Description	Control number	Control Description
		CC 6.2.9	Quarterly user access review is performed for user IDs having access to the databases (MYSQL, MSSQL and Oracle). Discrepancies noted during the review are communicated to respective teams for resolution.
CC 6.3	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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC 6.1.1	There exists a Password and Account Management policy document that describes the password policies configured on the domain controller and applications in Yotta which includes password parameters such as minimum password length, password complexity, maximum password age and account lockout after unsuccessful attempts.
		CC 6.1.2	An authentication mechanism is implemented for key applications, network devices and servers, by implementing password policies as per defined password policy.
		CC 6.1.3	Privileged access to the network components follows the principle of least privilege by granting defined user roles through CISCO ISE and logical access to these roles are approved by authorized personnel. This access is reviewed on a quarterly basis.
		CC 6.2.1	Employee user IDs are created in the Active Directory (AD) by the Corporate IT team as on date of joining of the employee upon approval from HR and Corporate IT team personnel.
		CC 6.2.2	A formal user approval process has been implemented that requires authorization by appropriate management for granting and modifying access to key applications upon approval from application owners
		CC 6.2.3	A formal user approval process has been implemented that requires authorization by appropriate management for granting access to Yotta managed databases upon approval from the Cloud team personnel.
		CC 6.2.4	Employee user IDs for resigned/ terminated personnel are disabled in Active Directory (AD) within 24 hours of the last working day as per the timelines defined in the Employee Exit process document.
		CC 6.2.5	The user access to the key applications is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.
		CC 6.2.6	The user access to Yotta Managed databases is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.
		CC 6.2.7	Quarterly user access review is performed for user IDs having access to active directory (AD). Discrepancies noted during the review are communicated to respective teams for resolution.

Criteria #	Criteria Description	Control number	Control Description
		CC 6.2.8	Quarterly user access review is performed for user IDs having access to key applications. Discrepancies noted during the review are communicated to respective teams for resolution.
		CC 6.2.9	Quarterly user access review is performed for user IDs having access to the databases (MYSQL, MSSQL and Oracle). Discrepancies noted during the review are communicated to respective teams for resolution.
		CC 6.3.1	For employees and contractors leaving the organization, exit checklist is signed by employee and manager, which then is transferred to the IT team who is responsible to revoke access to the domain within 24 hours of the employees last working date.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, DC, facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC 6.4.1	There exists a Physical Access Control Policy that describes the process for controlling physical access to the facilities and server room. This document is reviewed and approved by the Head DC security and safety.
		CC 6.4.2	Employees' and visitors' access to premises is restricted using access cards. Access to general and restricted areas within premises is granted after receiving approval from authorized personnel of Yotta.
		CC 6.4.3	Employees access to server hall is restrict to authorized employees using biometric access control system and mantrap. DC Operations team grants the access to server hall based on the approval from DC Security team.
		CC 6.4.4	Visitors and vendors requiring access to data centres are issued identification badge and escorted by authorized DC Security team personnel.
		CC 6.4.5	On a Quarterly basis restricted area access reports are generated and shared with the designated owner for the premises for review. Any discrepancies noted are tracked to closure.
		CC 6.4.6	At the time of separation from the organization, employee's and contractor's ID cards and access cards are returned to the security department, and access to the premises is disabled within 24 hours of the last working day.
		CC 6.4.7	Data centre facilities are secured by power fence at the perimeter, full height turnstiles at the entry gate and security guards are stationed at entry and exit point to monitor movement of employees and visitors.
		CC 6.4.8	Dedicated zones are defined for each area allowing only authorized personnel to access specific areas
		CC 6.4.9	Employees, visitors and contractors are issued unique lanyards based on the type of the visitor at the time of entry.

Criteria #	Criteria Description	Control number	Control Description
		CC 6.4.10	At the facilities entry point vehicles and personal belongings are scanned.
CC 6.5	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.	CC 3.3.3	There exists defined policy related to disposal of media/ waste with confidential information it holds, if any, in electronic and paper form. The policy is reviewed periodically and is approved by Head-DC operations.
		CC 6.2.4	Employee user IDs for resigned/ terminated personnel are disabled in Active Directory (AD) within 24 hours of the last working day as per the timelines defined in the Employee Exit process document.
		CC 6.2.5	The user access to the key applications is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.
		CC 6.2.6	The user access to Yotta Managed databases is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet. The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.
		CC 3.3.5	Annual Penetration testing is performed by a third-party. Reports are shared with relevant stakeholders and reviewed by the senior management. The vulnerabilities identified are evaluated and closed based on risk assessment.
		CC 4.1.4	Hardening guidelines are established for network devices and are reviewed by the Head - IT Operations (Network) annually.
		CC 6.1.3	Privileged access to the network components follows the principle of least privilege by granting defined user roles through CISCO ISE and logical access to these roles are approved by authorized personnel. This access is reviewed on a quarterly basis.
		CC 6.6.1	Privilege activity of network and database servers is logged within the PAM application. Security incidents are notified and corrective actions are taken to resolve the incidents.
		CC 6.6.2	Antivirus is configured to perform a scan on a real time basis. Yotta monitors the antivirus compliance on a periodic basis.

Criteria #	Criteria Description	Control number	Control Description
		CC 6.6.3	Firewall is configured at the perimeter of Yotta's network to restrict internet access as per defined policy.
		CC 6.6.4	Firewall is configured with Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) to monitor Yotta's networks and report threats.
CC 6.7	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.	CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet. The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.
		CC 2.1.9	Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.
		CC 3.3.6	Netskope DLP application is configured on the endpoint devices to scan for sensitive information transferred on the removable media. Incidents detected are analyzed and tracked to closure.
		CC 4.1.4	Hardening guidelines are established for network devices and are reviewed by the Head - IT Operations (Network) annually.
		CC 6.6.3	Firewall is configured at the perimeter of Yotta's network to restrict internet access as per defined policy.
		CC 6.6.4	Firewall is configured with Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) to monitor Yotta's networks and report threats.
		CC 6.7.1	Management has restricted access to external media such as USB, CD and external hard drives. Exception request for the use of removable media is approved by CISO.
		CC 6.7.2	Backup media are encrypted to prevent data loss.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 3.3.6	Netskope DLP application is configured on the endpoint devices to scan for sensitive information transferred on the removable media. Incidents detected are analyzed and tracked to closure.

Criteria #	Criteria Description	Control number	Control Description
		CC 6.6.2	Antivirus is configured to perform a scan on a real time basis. Yotta monitors the antivirus compliance on a periodic basis.
		CC 6.6.3	Firewall is configured at the perimeter of Yotta's network to restrict internet access as per defined policy.
		CC 6.6.4	Firewall is configured with Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) to monitor Yotta's networks and report threats.
CC 7.0 Common Criteria Related to System Operations			
CC 7.1	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.	CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 3.3.5	Annual Penetration testing is performed by a third-party. Reports are shared with relevant stakeholders and reviewed by the senior management. The vulnerabilities identified are evaluated and closed based on risk assessment.
		CC 3.3.6	Netskope DLP application is configured on the endpoint devices to scan for sensitive information transferred on the removable media. Incidents detected are analyzed and tracked to closure.
		CC 4.1.3	An end-point asset inventory of assets is maintained in the Tussom application and hardened based on hardening checklist.
		CC 4.1.4	Hardening guidelines are established for network devices and are reviewed by the Head - IT Operations (Network) annually.
		CC 6.6.1	Privilege activity of network and database servers is logged within the PAM application. Security incidents are notified and corrective actions are taken to resolve the incidents.
		CC 6.6.4	Firewall is configured with Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) to monitor Yotta's networks and report threats.
		CC 7.1.1	Database upgrades (patches) for Yotta managed databases are applied after analysis by Yotta. Patches are deployed through the change management process.
CC 7.2	The entity monitors system components and the operation of those components for anomalies	CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and

Criteria #	Criteria Description	Control number	Control Description
	that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		approved by Head Service Management on an annual basis.
		CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.
		CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The SRs are approved and tracked to closure by the respective operation tower personnel.
		CC 2.1.8	Zabbix application is utilized to monitor availability, system performance and health and generate alerts when specific predefined thresholds are breached and corrective actions are taken by respective team.
		CC 2.1.9	Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.
		CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape
		CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on a critical server on a quarterly basis, and tracked to closure
		CC 6.6.1	Privilege activity of network and database servers is logged within the PAM application. Security incidents are notified and corrective actions are taken to resolve the incidents.
		CC 6.6.2	Antivirus is configured to perform a scan on a real time basis. Yotta monitors the antivirus compliance on a periodic basis.
CC 7.3	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	CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.
		CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and

Criteria #	Criteria Description	Control number	Control Description
	actions to prevent or address such failures.		approved by Head Service Management on an annual basis.
		CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.
		CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The SRs are approved and tracked to closure by the respective operation tower personnel.
		CC 2.1.6	Operations team personnel follow defined protocols to perform Root Cause Analysis (RCA). for evaluating severity one (S1) incidents
		CC 2.1.9	Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.
		CC 2.1.10	Resolution of incidents are reviewed on a monthly basis by the senior management in the review meetings.
		CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and approved by Head Service Management on an annual basis.
		CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.
		CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The SRs are approved and tracked to closure by the respective operation tower personnel.
		CC 2.1.10	Resolution of incidents are reviewed on a monthly basis by the senior management in the review meetings.
CC 7.5	The entity identifies, develops, and implements	CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and

Criteria #	Criteria Description	Control number	Control Description
	activities to recover from identified security incidents.		approved by Head Service Management on an annual basis.
		CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.
		CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The SRs are approved and tracked to closure by the respective operation tower personnel.
		CC 2.1.6	Operations team personnel follow defined protocols to perform Root Cause Analysis (RCA). for evaluating severity one (S1) incidents
		CC 7.5.1	Yotta has a defined Business Continuity Management Policy which describes the process of continuing the business in case of any disruptions. The policy is reviewed and approved by the Chief Digital Officer on an annual basis or in case of any changes.
		CC 7.5.2	Business continuity and Disaster Recovery (DR) drills are conducted based on DR drill calendar and exceptions noted, if any, are tracked to closure.
		CC 7.5.3	Vulnerabilities identified during monthly/yearly mock drills are evaluated and discussed in Management Review Meetings.
CC 8.0 Common Criteria Related to Change Management			
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC 2.1.2	Yotta has a defined Change Management Procedure specifying the change management process to be followed for key applications. The policy is reviewed and approved by Head Service Management on an annual basis.
		CC 4.1.3	An end-point asset inventory of assets is maintained in the Tussom application and hardened based on hardening checklist.
		CC 4.1.4	Hardening guidelines are established for network devices and are reviewed by the Head - IT Operations (Network) annually.
		CC 7.1.1	Database upgrades (patches) for Yotta managed databases are applied after analysis by Yotta. Patches are deployed through the change management process.
		CC 8.1.1	Changes are approved by authorized personnel in accordance with the nature of the change prior to development and implementation of change.

Criteria #	Criteria Description	Control number	Control Description
		CC 8.1.2	Changes are tested and approved prior to implementing the changes into production.
		CC 8.1.3	Emergency changes are approved by CAB members before implementation of change.
		CC 8.1.4	There exists a logically separate environment for development, test and production for key applications and developer access to the production environment is restricted.
		CC 8.1.5	Changes (Pre-planned, Emergency and Retrospective) are reviewed on a weekly basis by the Service Management team and CAB team
CC 9.0 Common Criteria Related to Risk Mitigation			
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.
		CC 1.1.2	Yotta has defined ISMS based on International Organization for Standardization (ISO) 27001:2022 framework.
		CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.
		CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape
		CC 3.3.4	The GRC team communicates the internal audit observations to the relevant stakeholders and senior management annually.
		CC 4.1.1	The GRC team conducts internal audit annually. Gaps identified as part of the internal audit are tracked to closure.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and

Criteria #	Criteria Description	Control number	Control Description
			confidentiality commitments applicable to the vendors and third parties.
		CC 2.3.2	Operations team performs a preliminary vendor risk assessment prior to entering into any business relationship with a new vendor. Such assessments are used to assess the risk of the company's relationship with the vendor.
		CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.
		CC 9.2.1	The organization has documented process for terminating vendor relationship as part of the Procurement Procedure document which is reviewed and approved by Head – Procurement and Asset Management on an annual basis.
ADDITIONAL CRITERIA FOR AVAILABILITY			
A 1.1	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.	A 1.1.1	The management has established a process for maintaining redundancy of network components.
		CC 2.1.7	There exists a policy and procedure document for capacity management which defines the process to be followed for monitoring and planning asset capacity. This policy and procedure document are reviewed by Yotta senior management on an annual basis.
		CC 2.1.8	Zabbix application is utilized to monitor availability, system performance and health and generate alerts when specific predefined thresholds are breached and corrective actions are taken by respective team.
		CC 2.1.9	Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.
A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors	A 1.2.1	CCTV cameras are installed at the entry and exit points of the premises and critical areas. The video surveillance is reviewed on a real time basis, recordings are retained for a minimum period of 90 days and reviewed by the Administration team.

Criteria #	Criteria Description	Control number	Control Description
	environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A 1.2.2	Environmental protections have been installed at Yotta include the following: • Cooling systems • Smoke detectors • Sprinklers • Fire Extinguisher • Battery and diesel generators • UPS • Fire Alarm
		A 1.2.3	Environmental protections receive periodic maintenance as per defined schedule for each equipment.
		A 1.2.4	Management has implemented detection controls to identify environmental anomalies.
		A 1.2.5	Secondary backup of power supply is installed to be utilized in case of power failure.
		A 1.2.6	The DC Operations team performs monitoring of temperature for network and UPS rooms during each shift.
		A 1.2.7	Yotta has a defined Backup Management procedure specifying the backup process to be followed for key applications and servers. The policy is reviewed and approved by Head Storage and Backup on an annual basis.
		A 1.2.8	Data backups are performed for key applications and servers as per pre-defined schedules.
		A 1.2.9	Data backups are monitored for successful completion and any errors/failures are tracked to closure. Only authorized employees are allowed to modify backup. Ticket is raised in the Tussom application in case of backup failures.
		A 1.2.10	Backup media tapes are transferred to the offsite storage location on monthly basis and backup transfer records are recorded and documented by the authorized IT team personnel in the ticket raised on Tussom application.
		A 1.2.11	Backup restoration testing is performed by the Yotta team upon request. The restoration test results are reviewed by the respective Team lead and exceptions identified are followed up through the problem management process.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A 1.2.5	Secondary backup of power supply is installed to be utilized in case of power failure.
		A 1.2.7	Yotta has a defined Backup Management procedure specifying the backup process to be followed for key applications and servers. The policy is reviewed and approved by Head Storage and Backup on an annual basis.

Criteria #	Criteria Description	Control number	Control Description
		A 1.2.9	Data backups are monitored for successful completion and any errors/failures are tracked to closure. Only authorized employees are allowed to modify backup. Ticket is raised in the Tussom application in case of backup failures.
		A 1.2.11	Backup restoration testing is performed by the Yotta team upon request. The restoration test results are reviewed by the respective Team lead and exceptions identified are followed up through the problem management process.
		A 1.3.1	Backups are retained based on defined policy
		A 1.3.2	Server hall is supported by Uninterruptible Power Supply (UPS) systems and Diesel Generator Sets (DG sets), for continuous operation of hardware equipment in the event of a component or power failure.
		CC 7.5.1	Yotta has a defined Business Continuity Management Policy which describes the process of continuing the business in case of any disruptions. The policy is reviewed and approved by the Chief Digital Officer on an annual basis or in case of any changes.
		CC 7.5.2	Business continuity and Disaster Recovery (DR) drills are conducted based on DR drill calendar and exceptions noted, if any, are tracked to closure.
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C 1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	A 1.3.1	Backups are retained based on defined policy.
		CC 1.1.3	Standard contractual agreements signed between Yotta and its user entities include Yotta's security, availability, privacy and confidentiality commitments as applicable regarding the system.
		CC 1.1.4	Confidentiality agreement and Non-disclosure agreement (NDA) is signed by new joiners on the date of joining the organization as part of employment letter.
		CC 1.1.6	New joiners are required to read and accept the Code of Conduct (CoC) agreement consisting of terms and conditions on the day of their joining.
		CC 2.1.1	There exists a formally documented Information Classification policy that includes classification of data based on its criticality and sensitivity. The document is reviewed and approved by Yotta's management on an annual basis.
		CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and confidentiality commitments applicable to the vendors and third parties.

Criteria #	Criteria Description	Control number	Control Description
		CC 3.3.3	There exists defined policy related to disposal of media/ waste with confidential information it holds, if any, in electronic and paper form. The policy is reviewed periodically and is approved by Head-DC operations.
		CC 6.1.1	There exists a Password and Account Management policy document that describes the password policies configured on the domain controller and applications in Yotta which includes password parameters such as minimum password length, password complexity, maximum password age and account lockout after unsuccessful attempts.
		C 1.1.1	There exists a formal Removable Media policy that describes the process for usage of external devices at Yotta. This policy is reviewed and approved by the Head Corporate IT.
ADDITIONAL CRITERIA FOR PRIVACY			
P 1.1	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.	CC 1.1.3	Standard contractual agreements signed between Yotta and its user entities include Yotta's security, availability, privacy and confidentiality commitments as applicable regarding the system.
		CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and confidentiality commitments applicable to the vendors and third parties.
		P 1.1.1	Policy and procedure documents relating to privacy are uploaded on Yotta's intranet.
		P 1.1.2	Yotta provides user entities with its Privacy Notice by publishing the notice on Yotta website. Yotta Privacy Notice addresses the following: • The choices available regarding collection, use, retention, disclosure, and disposal of personal information. • The information collected by Yotta, how it is used, shared, secured, retained and/or disclosed. • The scope of the notice's applicability.
		P 1.1.3	Yotta informs user entities of changes made to Yotta Privacy notice through Yotta website.
P 2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the	A 1.3.1	Backups are retained based on defined policy
		CC 3.3.3	There exists defined policy related to disposal of media/ waste with confidential information it holds, if any, in electronic and paper form. The policy is reviewed periodically and is approved by Head-DC operations.

Criteria #	Criteria Description	Control number	Control Description
	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.	P 1.1.2	Yotta provides user entities with its Privacy Notice by publishing the notice on Yotta website. Yotta Privacy Notice addresses the following: • The choices available regarding collection, use, retention, disclosure, and disposal of personal information. • The information collected by Yotta, how it is used, shared, secured, retained and/or disclosed. • The scope of the notice's applicability.
		P 1.1.3	Yotta informs user entities of changes made to Yotta Privacy notice through Yotta website.
P 3.1	Personal information is collected consistent with the entity's objectives related to privacy.	P 1.1.2	Yotta provides user entities with its Privacy Notice by publishing the notice on Yotta website. Yotta Privacy Notice addresses the following: • The choices available regarding collection, use, retention, disclosure, and disposal of personal information. • The information collected by Yotta, how it is used, shared, secured, retained and/or disclosed. • The scope of the notice's applicability.
P 3.2	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.	CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and confidentiality commitments applicable to the vendors and third parties.
		P 3.2.1	User entities are required to accept Yotta Privacy terms at the time of subscription.
P 4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and confidentiality commitments applicable to the vendors and third parties.
		P 1.1.2	Yotta provides user entities with its Privacy Notice by publishing the notice on Yotta website. Yotta Privacy Notice addresses the following: • The choices available regarding collection, use, retention, disclosure, and disposal of personal information.

Criteria #	Criteria Description	Control number	Control Description
			• The information collected by Yotta, how it is used, shared, secured, retained and/or disclosed. • The scope of the notice's applicability.
		P 1.1.3	Yotta informs user entities of changes made to Yotta Privacy notice through Yotta website.
P 4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	NA	Service organization responsibilities do not include retention of personal data of user entities. Hence, the criteria related to retention of personal information is not applicable.
P 4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	NA	Service organization responsibilities do not include disposal of personal data of user entities' data subjects. Hence, the criteria related to disposal of personal information is not applicable.
P 5.1	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.	NA	Service organization responsibilities do not include granting access to identified and authenticated data subjects to access personal information of user entities' data subjects. Hence, the criteria related to granting access of personal information is not applicable.
P 5.2	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.	NA	Service organization responsibilities do not include correction or amendments or correction to personal information of user entities' data subjects. Further, service organization do not have access to user entities personal information. Hence, the criteria related to correction of personal information is not applicable.
P 6.1	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	NA	Service organization responsibilities do not include disclosure of personal data to third parties. Hence, the criteria related to disclosure of personal information to third parties is not applicable.

Criteria #	Criteria Description	Control number	Control Description
	entity's objectives related to privacy.		
P 6.2	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.	NA	Service organization responsibilities do not include disclosure of personal data to user entities' data subjects and third parties. Hence, the criteria related to disclosure of personal information is not applicable.
P 6.3	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.	CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.
		P 6.3.1	There exists Data Protection policy covering the logging and monitoring of the privacy breaches as part of the incident management. Policy is reviewed and approved annually by Head Legal and Data Protection Officer.
P 6.4	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.	NA	Service organization responsibilities do not include granting access to personal information to vendors and third parties. Hence criteria related to obtaining privacy commitments from vendors and third parties is not applicable.
P 6.5	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.	NA	Service organization responsibilities do not include disclosure of personal data to third parties. Hence, the criteria related to disclosure of personal information is not applicable.

Criteria #	Criteria Description	Control number	Control Description
P 6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.
		P 6.3.1	There exists Data Protection policy covering the logging and monitoring of the privacy breaches as part of the incident management. Policy is reviewed and approved annually by Head Legal and Data Protection Officer.
P 6.7	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.	NA	Service organization responsibilities do not include disclosure of personal data to data subjects. Hence, the criteria related to disclosure of personal information is not applicable.
P 7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	NA	Service organization responsibilities do not include collections and maintenance of personal data. Hence, the criteria related to personal information lifecycle management is not applicable.
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 identified deficiencies are made or taken in a timely manner.	CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.
		CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The SRs are approved and tracked to closure by the respective operation tower personnel.
		P 8.1.1	Yotta has established a mailbox for internal users through which the Data Privacy Officer (DPO) monitors privacy related complaints and takes necessary actions.

II. Control description and Test of Operating Effectiveness

Control number	Control Description	Test procedure	Conclusion
CC 1.1.1	There exists formally documented Information Security (IS) policies and procedures that provide guidance for IS management within the organization, and include roles and responsibilities of the organization's personnel with reference to IS. These policies are made available to employees on the Yotta intranet.	○ Inquired with the Chief Information Security Officer (CISO) regarding the formally documented IS policy and procedure. ○ Inspected the IS policy to determine whether it included guidance for IS management within the organization, responsibilities for organization's personnel with reference to IS, and whether the policy was reviewed and approved annually, or in case of any major changes by Chief Digital Officer ○ Inspected the Yotta intranet portal, ATHENA to determine whether the IS policy was made available to Yotta employees.	No relevant exceptions noted.
CC 1.1.2	Yotta has defined ISMS based on International Organization for Standardization (ISO) 27001:2022 framework.	○ Inquired with the GRC team personnel regarding the implementation of ISO 27001:2022 framework. ○ Inspected the ISO 27001:2022 certificate to determine whether the organization had implemented ISMS based on ISO 27001:2022 framework.	No relevant exceptions noted.
CC 1.1.3	Standard contractual agreements signed between Yotta and its user entities include Yotta's security, availability, privacy and confidentiality commitments as applicable regarding the system.	○ Inquired with the Legal team personnel regarding the standard contractual agreements signed between Yotta and its user entities include Yotta's confidentiality and privacy commitments. ○ For selection of user entities, inspected the Master Service Agreement (MSA) signed with the user entities to determine whether the availability, confidentiality and privacy commitments were defined in the MSA.	No relevant exceptions noted.
CC 1.1.4	Confidentiality agreement and Non-Disclosure Agreement (NDA) is signed by new joiners on the date of joining the	○ Inquired with the Human Resources (HR) team personnel regarding the process of signing Confidentiality and NDA	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	organization as part of employment letter.	agreement for new joiners on the date of joining. o For a selection of new joiners, inspected the employment letter to determine whether confidentiality agreement and NDA was signed by the employees on the date of joining the organization.	
CC 1.1.5	Yotta has established disciplinary standards and guidelines for employee behavior as part of Code of Business Conduct policy which include suspension, and termination as potential sanctions for employee misconduct and the policy is reviewed and approved by the Head HR on an annual basis.	o Inquired with the HR team personnel regarding the process of establishing disciplinary standards and guidelines for employee behaviour. o Inspected the disciplinary standards and guidelines along with its revision history to determine whether standards and guidelines for employee behaviour were established as a part of Code of Business Conduct policy which includes, suspension, and termination as potential sanctions for employee misconduct and the policy was reviewed and approved by Head HR on an annual basis.	No relevant exceptions noted.
CC 1.1.6	New joiners are required to read and accept the Code of Conduct (CoC) agreement consisting of terms and conditions on the day of their joining.	o Inquired with the HR team personnel regarding the signing of Code of conduct (CoC) by the new joiners on the date of joining the organization. o For a selection of new joiners, inspected the Code of conduct (CoC) agreement to determine whether the agreement was signed on the date of joining the organization.	No relevant exceptions noted.
CC 1.1.7	Employees must clear a background check covering minimum of previous employment, education and criminal records before they are confirmed by the management. Exceptional approvals are taken for specific unsuccessful background verification cases from Head HR/ CEO of Yotta.	o Inquired with the HR team personnel regarding the process of background verification check for the new joiners. o For a selection of new joiners, inspected the background check reports to determine whether background check covering minimum of previous employment, education and criminal records was performed	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
CC 1.2.1	Management has established a board charter to determine the requirement and composition of Board of Directors (BoD).	○ Inquired with the GRC team personnel regarding existence of Board of Directors and its composition. ○ Inspected Yotta's website and organization structure to determine whether the requirement and composition of Board of Directors was defined.	No relevant exceptions noted.
CC 1.2.2	Yotta has a defined organizational structure, reporting lines, authorities, and responsibilities. As part of its business planning process, ongoing risk assessment and management process, Yotta revises the structure when necessary to help meet the commitments and requirements.	○ Inquired with the GRC team and the HR team personnel regarding the organization structure, reporting lines, authorities, and responsibilities. ○ Inspected the organizational structure, and the roles and responsibilities document to determine whether organizational structure, reporting lines, authorities, and responsibilities to manage the organization's security, confidentiality and availability commitments and requirements were defined.	No relevant exceptions noted.
CC 1.2.3	The organization's BoD has members who are independent of executive management such that they are objective in evaluation and decision making.	○ Inquired with the GRC team personnel regarding existence of Board of Directors and its independence from the Yotta management. ○ Inspected Yotta's website and the organization structure to determine whether the Board of Directors were independent of the management and objective in evaluation and decision making.	No relevant exceptions noted.
CC 1.3.1	Roles and responsibilities are defined in written job descriptions and reviewed on an annual basis. Roles and responsibilities documents are uploaded on Yotta's intranet portal.	○ Inquired with the HR team personnel regarding roles and responsibilities in the job descriptions along with the review and approval. ○ Inspected the job descriptions with defined roles and responsibilities along with the revision history to determine whether the written job descriptions were uploaded on the intranet and were reviewed and approved by the Yotta management on a periodic basis.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
CC 1.3.2	The GRC team meets annually to discuss risk considerations critical to business as part of management review meetings.	○ Inquired with the GRC team personnel regarding the review meetings conducted in Yotta. ○ Inspected the Management Review Meeting (MRM) invite and data sheet to determine whether risk considerations critical to business were discussed as part of management review meeting.	No relevant exceptions noted.
CC 1.4.1	There exists formally documented Employee Onboarding Policy document that provides guidance for employee onboarding, approved by Co-founder and CEO on an annual basis. These policies are made available to employees on the Yotta intranet.	○ Inquired with the HR team personnel regarding the existence of Employee Onboarding Policy document. ○ Inspected the Employee Onboarding Policy document and revision history to determine whether there exists formally documented Employee Onboarding Policy document that provides guidance for employee onboarding approved by Head-Corporate IT on an annual basis. ○ Inspected the Yotta intranet portal, ATHENA to determine whether the Employee Onboarding policy was made available to Yotta employees	No relevant exceptions noted.
CC 1.4.2	Job requirements are documented in the job descriptions, and candidates' abilities, experience and knowledge to meet these requirements are evaluated as part of the hiring evaluation process.	○ Inquired with the HR team personnel regarding the documentation for job descriptions and evaluation of candidates' abilities to meet the specified requirements. ○ Inspected the written job description documents to determine whether the job requirements were defined in job description. ○ For a selection of new joiners, inspected the interview evaluation sheet to determine whether the candidates' abilities, experience, and knowledge to meet the requirements were evaluated as part of the hiring evaluation process.	No relevant exceptions noted.
CC 1.4.3	Candidates are evaluated based on their technical skills and non-	○ Inquired with the HR team personnel regarding technical and	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	technical skills during the interview evaluation process.	on technical interview evaluation process. o For a selection of new joiners, inspected the evaluation sheets to determine whether candidates were evaluated based on their technical skills and non-technical skills during the interview evaluation process.	
CC 1.4.4	Management establishes requisite skillsets for employees and provides continued training about its commitments and requirements for employees to support the achievement of objectives.	o Inquired with the HR team personnel regarding the training programs for employees across Yotta. o For a selection of new joiners, inspected the business induction and Information Security training completion records to determine whether trainings were completed by the employees. o Inspected the training tracker to determine whether the HR team personnel monitor compliance of Yotta employees with the training requirements.	No relevant exceptions noted.
CC 1.4.5	Employee performance across organization is measured against the defined goals and objectives on a quarterly basis.	o Inquired with the HR team personnel regarding the process of performance evaluations against the defined goals and objectives. o For a selection of employees, inspected the goals defined and the performance evaluation conducted by their respective managers through performance development dashboard maintained by the HR team personnel to determine whether the employee performance across organization was measured against established goals and objectives on a quarterly basis.	No relevant exceptions noted.
CC 1.5.1	Management has defined policies and procedures for information security encompassing access management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures and made available on the Yotta intranet.	o Inquired with the GRC team personnel regarding the formulation of IS policies and procedures for information security processes. o Inspected the IS policies and procedures to determine whether Management had defined policies and procedures for information security encompassing access	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	The policy and procedure documents are reviewed and approved by operations head on an annual basis or in case of any changes.	management, change management, incident management, communication and network security, business continuity planning and disaster recovery procedures. o Inspected the Yotta's intranet, ATHENA to determine whether the IS policies and procedures were defined and were made available for the Yotta employees and the policy and procedure documents were reviewed and approved by the Head of the Departments on an annual basis or in case of any changes.	
CC 2.1.1	There exists a formally documented Information Classification policy that includes classification of data based on its criticality and sensitivity. The document is reviewed and approved by Yotta's management on an annual basis.	o Inquired with the GRC team personnel regarding the existence and review of an Information Classification policy. o Inspected the Information Classification policy document and revision history to determine whether the document included the classification of data based on its criticality and sensitivity and whether the policy was reviewed and approved by Yotta management on an annual basis.	No relevant exceptions noted.
CC 2.1.2	Yotta has a defined Change Management Procedure specifying the change management process to be followed for key applications. The policy is reviewed and approved by Head Service Management on an annual basis.	o Inquired with the Service Management team personnel regarding the Change Management Procedure document which describes the handling of change requests based on change category. o Inspected the Change Management Procedure document and revision history to determine whether the process for implementation and approval of emergency, pre-planned and normal changes was documented and reviewed by Head- Service Management on an annual basis.	No relevant exceptions noted.
CC 2.1.3	Yotta has a defined Incident Management procedure specifying the incident handling process and escalation matrix to be followed. The policy is reviewed and approved by Head	o Inquired with the Service Management team personnel regarding the process documented for managing an internal as well	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	Service Management on an annual basis.	as user entity reported incidents or service requests. o Inspected the Incident Management policy document and revision history to determine whether the incident logging, prioritization, assignment and escalation process was documented and approved by the Head Service Management on an annual basis.	
CC 2.1.4	Incidents are logged, prioritized and assigned in the Tussom application. The incident is analyzed and resolved by respective team as per the defined SLA. Further if needed, escalation procedures are followed and documented for incidents not closed within defined SLA.	o Inquired with the Service Management team personnel regarding the process for incident logging, prioritization, assignment and escalation as well as user entity reported events. o For a selection of incidents, inspected the incident tickets logged in the Tussom application to determine whether the incidents were logged, prioritized, assigned, analysed and resolved by respective team as per the defined SLA.	No relevant exceptions noted.
CC 2.1.5	Service requests (SR) for installation of new infrastructure are logged in the Tussom application. The SRs are approved and tracked to closure by the respective operation tower personnel.	o Inquired with the Service Management team personnel regarding the process for raising service requests. o For a selection of service requests, inspected the service ticket workflow from Tussom application to determine whether requests are logged in the Tussom application and were tracked to closure by the respective operation tower personnel.	No relevant exceptions noted.
CC 2.1.6	Operations team personnel follow defined protocols to perform Root Cause Analysis (RCA). for evaluating severity one (S1) incidents	o Inquired with the Service Management team personnel regarding the process of handling high severity incidents. o For a selection of severity one (S1) incidents, inspected the RCA documents attached as part of the incident tickets to determine whether operations team personnel follow defined protocols for evaluating reported events.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
CC 2.1.7	There exists a policy and procedure document for capacity management which defines the process to be followed for monitoring and planning asset capacity. This policy and procedure document are reviewed by Yotta senior management on an annual basis.	○ Inquired with the IT team personnel regarding the existence of a policy and procedure document for capacity management. ○ Inspected the Capacity Management document to determine whether the process for monitoring and planning asset capacity was defined and documented and was reviewed and approved by Yotta management on an annual basis.	No relevant exceptions noted.
CC 2.1.8	Zabbix application is utilized to monitor availability, system performance and health and generate alerts when specific predefined thresholds are breached and corrective actions are taken by respective team.	○ Inquired with the IT team regarding the process of monitoring the system health and capacity. ○ Inspected the asset report extracted from the Zabbix application to determine whether all the systems are on boarded in Zabbix application for monitoring. ○ Inspected the capacity monitoring report extracted from the Zabbix application to determine whether the system availability, performance and health was monitored, and actions were taken in case of any breaches/ incidents. ○ For a selection of incidents, inspected the ticket and workflow in Tussom application to determine whether corrective actions were taken by respective team.	No relevant exceptions noted.
CC 2.1.9	Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.	○ Inquired with the SOC team regarding the process of monitoring the system for security breaches. ○ Inspected the asset report extracted from the IBMQradar application to determine whether all the systems are on boarded in SIEM application for monitoring. ○ Inspected the incident monitoring report extracted from the IBMQradar application to determine whether the system was	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		monitored, and actions were taken in case of any breaches	
CC 2.1.10	Resolution of incidents are reviewed on a monthly basis by the senior management in the review meetings.	○ Inquired with the Service Management team personnel regarding the process of reviewing the incident tickets. ○ For a selection of months, inspected the meeting invite and the presentation summary to determine whether resolution and the root cause analysis were reviewed by the senior management team on a monthly basis.	No relevant exceptions noted.
CC 2.1.11	CISO team monitors security incidents (including privacy breaches) on a daily basis. The team follows defined protocols to resolve, escalate and track security incidents to closure.	○ Inquired with the CISO team personnel regarding the monitoring of security incidents in Yotta. ○ Inspected the dashboard of IBMQradar application to determine incidents/ events were monitored on real time basis by CISO team personnel. ○ For a selection of incidents, inspected the workflow and analysis of the incidents in Tussom application to determine whether the CISO team follows defined protocols to resolve, escalate and track security incidents to closure.	No relevant exceptions noted. We were informed that there were no instances of security incidents that qualified to be privacy breaches during the examination period.
CC 2.1.12	An asset inventory of Yotta's network components is maintained for accounting of asset additions and removals for management's use and is reviewed by the Head - IT Operations (Network).	○ Inquired with the Network and NOC team personnel regarding the asset inventory management process. ○ Inspected the Yotta network components asset inventory list along with the review performed to determine whether list of Yotta system components were maintained for accounting of additions and removals for management's use.	No relevant exceptions noted.
CC 2.1.13	An asset inventory of Yotta's system components (servers, end-user systems) is maintained for accounting of asset additions and	○ Inquired with the Cloud team personnel regarding the asset inventory management process.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	removals for management's use and is reviewed by the team lead from Corporate IT and Cloud Operation team.	○ Inspected the Yotta server components inventory list along with the review performed to determine whether a list of Yotta system components were maintained for accounting of additions and removals for management's use.	
CC 2.2.1	Management conducts information security trainings upon compromise of employee emails after phishing simulations.	○ Inquired with the CISO team personnel regarding the information security awareness programs required to be completed upon compromise of employee emails after phishing simulations. ○ For a selection of employees, inspected the result of the phishing simulation and compared it with the information security training records of the employees to determine whether the information security awareness trainings were completed by those employees whose IDs have been compromised in the phishing simulation.	No relevant exceptions noted.
CC 2.3.1	Management has signed master service agreements that include clearly defined terms, conditions, and responsibilities for vendors and third parties. These master service agreements include availability and confidentiality commitments applicable to the vendors and third parties.	○ Inquired with the DC Operations team personnel regarding the terms, conditions, and responsibilities defined for the vendors and third parties in the master service agreements. ○ Inquired with the DC Operations team personnel regarding the confidentiality clause in the master service agreements with vendors and third parties. ○ For a selection of vendors, inspected the master service agreement to determine whether it included the defined terms, conditions, responsibilities and confidentiality commitments applicable to vendors.	No relevant exceptions noted.
CC 2.3.2	Operations team performs a preliminary vendor risk assessment prior to entering into any business relationship with a new vendor. Such assessments are used to assess the risk of the	○ Inquired with the vendor operations team personnel regarding the process followed for performing preliminary vendor	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	company's relationship with the vendor.	risk assessment prior to onboarding of new vendors. o For a selection of vendors inspected vendor risk assessment performed to determine whether the risk of association with the vendor was assessed before entering into business relationship.	
CC 3.1.1	Management has defined and documented a formal Risk Management process that specifies risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood. The document is reviewed and approved by the Head-GRC and CISO on annual basis or in case of any changes.	o Inquired with the GRC team personnel regarding the risk management process for evaluating risks based on severity, occurrence and likelihood in Yotta. o Inspected the Risk Management Framework to determine whether risk tolerances and the process for evaluating risks based on severity, occurrence and likelihood were included and to determine whether the document was reviewed and approved by the Yotta the Head- GRC and CISO on annual basis or in case of any changes.	No relevant exceptions noted.
CC 3.1.2	Identified vulnerabilities are rated using a risk evaluation process and ratings provided are reviewed by the GRC and the CISO team.	o Inquired with the CISO and GRC team personnel regarding the rating of identified vulnerabilities. o Inspected the risk register document to determine whether the vulnerabilities identified were rated according to the risk evaluation process and ratings provided were reviewed by the GRC and the CISO team.	No relevant exceptions noted.
CC 3.1.3	The deficiencies identified as part of the vulnerability assessment are documented in risk register along with the corrective action plan and date of closure.	o Inquired with the CISO and GRC team personnel regarding the documentation of vulnerability assessment and corrective actions within the gap tracker. o Inspected the risk register, corrective actions and stakeholders identified for each vulnerability to determine whether the deficiencies were documented in risk register along with the corrective action plan and date of closure.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
CC 3.1.4	There exists a risk register which records and maintain risk description, impact, likelihood, and rating for system components. Furthermore, risk register is updated by the respective operations team and reviewed by the GRC team in response to changes in environmental, regulatory and technological landscape	○ Inquired with the CISO and GRC team personnel regarding the maintenance of risk register of the Yotta's risk component. ○ Inspected the risk register document to determine whether the risk description, impact, likelihood and rating were documented for system components and whether the risk register was updated by the respective operations team and reviewed by the respective team and GRC team in response to changes in environmental, regulatory and technological landscape.	No relevant exceptions noted.
CC 3.2.1	There exists documented Vulnerability Assessment plan which is reviewed annually or in case of change by the CISO.	○ Inquired with the CISO team personnel regarding the process followed for vulnerability assessment. ○ Inspected the Vulnerability Assessment plan and revision history to determine whether the plan was reviewed and approved annually or in case of any major changes by the CISO.	No relevant exceptions noted.
CC 3.2.2	Internal vulnerability assessment is performed on ongoing basis by Yotta. Corrective action is taken on the identified critical vulnerabilities on critical servers on a quarterly basis and tracked to closure.	○ Inquired with the CISO team personnel regarding the process followed for vulnerability assessment. ○ Inspected the Qualys application dashboard to determine whether internal vulnerability assessment was performed on ongoing basis. ○ For a selection of quarters, inspected the dashboard of Qualys application to determine whether the vulnerabilities were monitored on a quarterly basis. ○ For a selection of quarters, inspected the assessment report to determine whether the findings noted during the vulnerability assessment were reported to the management. ○ Inspected the VA tracker of subsequent quarters to determine whether the vulnerabilities were	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		tracked to closure for critical servers.	
CC 3.3.1	There exists formally documented whistle blower policy and procedures that provide guidance regarding fraud, whistle blower mechanism and protection to whistle blower. The policy is reviewed and approved by Co-founder & CEO on an annual basis.	○ Inquired with the HR team personnel regarding the existence of Whistle blower policy document describing the process for fraud and whistle blower. ○ Inspected the Whistle blower policy and revision history to determine whether the policy included guidance for fraud, whistle blower mechanism, and protection to whistle blower, and was reviewed and approved annually or in case of any major changes by Co-founder & CEO on an annual basis.	No relevant exceptions noted.
CC 3.3.2	Management has established whistle-blower e-mail ID available to internal and external users.	○ Inquired with the GRC team personnel regarding the employee grievance functional mailbox established by the Yotta's management. ○ Inspected the grievance mailbox: trustline@yotta.com to determine whether a separate email ID was used for complaint redressal for internal employees.	No relevant exceptions noted. We were informed that no whistle blower complaints were logged during the examination period
CC 3.3.3	There exists defined policy related to disposal of media/ waste with confidential information it holds, if any, in electronic and paper form. The policy is reviewed periodically and is approved by Head-DC operations.	○ Inquired with the DC Operations team personnel regarding the policy related to disposal of media with confidential information if any, in electronic and paper form. ○ Inspected the Data Centre Maintenance Policy document of Yotta IT equipment and waste along with revision history to determine whether the management had an established guidelines related to disposal of media with confidential information it holds, if any, in electronic and paper form and whether the policy was reviewed periodically and was approved by the Head-DC operations.	No relevant exceptions noted.
CC 3.3.4	The GRC team communicates the internal audit observations to the relevant stakeholders and senior management annually.	○ Inquired with the GRC team personnel regarding the communication of internal audit	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		observations to stakeholders and senior management. o Inspected the email communication with the relevant stakeholders and management review meeting invite to determine whether internal audit observations were communicated to the relevant stakeholders and senior management annually	
CC 3.3.5	Annual Penetration testing is performed by a third-party. Reports are shared with relevant stakeholders and reviewed by the senior management. The vulnerabilities identified are evaluated and closed based on risk assessment.	o Inquired with the GRC team personnel regarding the annual penetration testing performed by the third party. o Inspected the third-party penetration report to determine whether penetration test was performed on an annual basis o Inspected the management review meeting invites and data sheets to determine whether penetration testing reports were shared with senior management for review and vulnerabilities were evaluated. Additionally, inspected the risk assessment performed by the service organization for open vulnerabilities, to determine whether the vulnerabilities impacted user entities' servers or data.	No relevant exceptions noted.
CC 3.3.6	Netskope DLP application is configured on the endpoint devices to scan for sensitive information transferred on the removable media. Incidents detected are analyzed and tracked to closure.	o Inquired with the CISO team personnel regarding the configuration of DLP application and monitoring of DLP incidents. o Inspected the endpoint devices integrated with the Netskope application and endpoint device asset inventory to determine whether DLP was configured on endpoint devices. o For a selection of incidents, inspected the impact analysis to determine whether the incidents were analysed and tracked to closure.	No relevant exceptions noted.
CC 4.1.1	The GRC team conducts internal audit annually. Gaps identified as	o Inquired with the GRC team personnel regarding the internal audits conducted in Yotta.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	part of the internal audit are tracked to closure.	○ Inspected the Internal Audit reports conducted by the GRC team to determine whether internal audit was performed on an annual basis, and whether the vulnerabilities / gaps identified were tracked to closure.	
CC 4.1.2	Yotta is ISO 27001:2022 and PCI-DSS certified. Surveillance audit is conducted annually for effectiveness of internal controls.	○ Inquired with the GRC team personnel regarding the ISO and PCI DSS certification and audit conducted on an annual basis. ○ Inspected the ISO 27001:2022 and PCI-DSS Version 4.0 certificate to determine whether the organization was ISO and PCI DSS certified.	No relevant exceptions noted.
CC 4.1.3	An end-point asset inventory of assets is maintained in the Tussom application and hardened based on hardening checklist.	○ Inquired with the Corporate IT team personnel regarding the asset inventory management process. ○ Inspected the Yotta end-points asset inventory list along with the review performed to determine whether a list of Yotta system components were maintained for accounting of additions and removals for management's use. ○ For selected new asset assigned, inspected the hardening status from Manage Engine application to determine whether end-point asset was hardened	No relevant exceptions noted.
CC 4.1.4	Hardening guidelines are established for network devices and are reviewed by the Head - IT Operations (Network) annually.	○ Inquired with the Network and NOC team personnel regarding the hardening guidelines established for network components and its review. ○ Inspected the Hardening guidelines along with the approval to determine whether the hardening guidelines were established for network components and were reviewed by the Head - IT Operations (Network) on an annual basis. ○ For a selection of network devices, inspected the console screenshot to determine whether the network devices were	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		hardened according to hardening checklist.	
CC 4.1.5	There exists an Internal Audit Framework document that describes the internal audit planning and methodology	○ Inquired with the GRC team personnel regarding the Internal Audit Policy specifying the scope of assessment and controls relating to each tower/ operation. ○ Inspected the Internal Audit Policy document to determine whether the framework and the internal audit process was included and the document was reviewed and approved by Head-GRC on annual basis or in case of any changes.	No relevant exceptions noted.
CC 4.1.6	Business continuity and Disaster Recovery (DR) drills are conducted based on DR drill calendar and exceptions noted, if any, are tracked to closure.	○ Inquired with the GRC team personnel regarding BCP and DR plans and its testing. ○ Inspected the BCP and DR plans to determine whether the plans were developed and reviewed on an annual basis. ○ Inspected the BCP and DR drill reports to determine whether BCP and DR drills were performed on an annual basis, and exceptions noted were tracked to closure.	No relevant exceptions noted.
CC 4.2.1	On a quarterly basis, a risk acceptance analysis for recurring non- impactful risks is approved by the CISO and Business team.	○ Inquired with the CISO and GRC team personnel regarding risk acceptance procedure. ○ For a selection of quarters, inspected the risk associated with the vulnerabilities identified, analysis of the risk, risk acceptance form and approval from CISO along with business team to determine whether the risk acceptance analysis was performed for recurring non-impactful risks and was approved by the CISO and Business team.	No relevant exceptions noted.
CC 5.1.1	Control owners are identified post identification of vulnerabilities as part of risk assessments. Control owners are documented in the risk register and risk register is	○ Inquired with the GRC team personnel regarding the identification of control owners based on the vulnerabilities identified during the assessment.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	reviewed and approved by Head – GRC on an annual basis.	○ Inspected the risk register to determine whether control owners were identified based on the vulnerabilities identified during assessment and the document was reviewed and approved by Head-GRC.	
CC 6.1.1	There exists a Password and Account Management policy document that describes the password policies configured on the domain controller and applications in Yotta which includes password parameters such as minimum password length, password complexity, maximum password age and account lockout after unsuccessful attempts.	○ Inquired with the GRC team personnel regarding the password configuration for domain controller and in-scope applications and servers. ○ Inspected the Password policy document to determine whether the password parameters for domain controller and in-scope applications were documented. ○ Inspected the password configuration on domain controller and applications to determine whether password controls such as minimum password length, password complexity, maximum password age and account lockout after unsuccessful attempts were configured on domain controller and applications as per documented password policy.	No relevant exceptions noted.
CC 6.1.2	An authentication mechanism is implemented for key applications, network devices and servers, by implementing password policies as per defined password policy.	○ Inquired with the GRC team personnel regarding the password configuration for domain controller and in-scope applications and servers. ○ Inspected the password configuration on domain controller, applications and servers to determine whether password controls such as minimum password length, password complexity parameters, maximum password age and account lockout after unsuccessful attempts were configured on key applications, network devices and servers as per documented password policy.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
CC 6.1.3	Privileged access to the network components follows the principle of least privilege by granting defined user roles through CISCO ISE and logical access to these roles are approved by authorized personnel. This access is reviewed on a quarterly basis.	○ Inquired with the Network IT team personnel regarding the process of granting logical access to the Yotta network. ○ Inspected the list of users having logical access to Yotta network components through CISCO ISE to determine whether principle of least privileges was followed, and access was granted only to authorized personnel and whether admin access was restricted to L3 users from Network IT team. ○ For a selection of new joiners, inspected the Tussom ticket and approval workflow to determine whether logical access to Yotta network components was created at the time of onboarding post approval by Network team personnel. ○ For a selection of quarters, inspected the user access review email to determine whether access was reviewed on a quarterly basis.	No relevant exceptions noted.
CC 6.1.4	Yotta has defined its Network Functional Procedure document to provide guidelines to employees utilizing the Virtual Private Network (VPN) to access the Yotta network in a secure manner. Policy is reviewed and approved on an annual basis by Head – IT Operations: Network	○ Inquired with the IT team personnel regarding the documented Remote Working Policy for VPN access. ○ Inspected the Remote Working document and Network Functional Procedure to determine whether the guidelines for utilizing the VPN solution to access the Yotta network in a secure manner was defined and documented and policy was review and approved on an annual basis by Head – IT Operations: Network.	No relevant exceptions noted.
CC 6.1.5	Firewall rules limit the types of activities and service requests that can be performed from external connections.	○ Inquired with the Firewall IT team personnel regarding the rulesets configured on the firewall to limit type of activities from external connections. ○ Inspected the ruleset configured in the firewall to determine whether deny all rule was configured by default and only explicit inbound and outbound	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		traffic was allowed the firewall to limit the types of activities and service requests that can be performed from external connections.	
CC 6.1.6	Data stored in Yotta managed databases are encrypted using AES 256 bit encryption.	○ Inquired with the Cloud team personnel regarding the encryption mechanism of data residing within the database servers. ○ Inspected the configuration from the system specifying encryption of AES 256 to determine whether data stored in Yotta managed databases were encrypted using AES 256 bit encryption.	No relevant exceptions noted.
CC 6.2.1	Employee user IDs are created in the Active Directory (AD) by the Corporate IT team as on date of joining of the employee upon approval from HR and Corporate IT team personnel.	○ Inquired with the Corporate IT team personnel regarding the process of granting logical access to the Active Directory (AD). ○ For a selection of new joiners, inspected the Tussom ticket, approval workflow, HR list and screenshot from AD to determine whether logical access to Yotta domain was created at the time of onboarding post approval from HR and Corporate IT team personnel.	No relevant exceptions noted.
CC 6.2.2	A formal user approval process has been implemented that requires authorization by appropriate management for granting and modifying access to key applications [2]upon approval from application owners	○ Inquired with the Application team personnel regarding the process of granting logical access to the application ○ For a selection of user IDs created and modified, inspected the Tussom ticket, approval workflow and screenshot from the application to determine whether logical access to key applications PAM, SFDC and CISO ISE was created by application IT team personnel post approval from application owners.	No relevant exceptions noted.

[2] Key application: PAM, SFDC and CISO ISE

Control number	Control Description	Test procedure	Conclusion
CC 6.2.3	A formal user approval process has been implemented that requires authorization by appropriate management for granting access to Yotta managed databases upon approval from the Cloud team personnel.	○ Inquired with the Application team personnel regarding the process of granting logical access to Yotta managed databases. ○ For a user ID created, inspected the email approval and date of creation from the PAM application to determine whether a formal user approval process had been implemented that requires authorization by appropriate management for granting access to Yotta managed databases upon approval from the Cloud team personnel.	No relevant exception noted.
CC 6.2.4	Employee user IDs for resigned/ terminated personnel are disabled in Active Directory (AD) within 24 hours of the last working day as per the timelines defined in the Employee Exit process document.	○ Inquired with the Corporate IT team personnel regarding the process for employee user ID removal from Yotta AD. ○ For a selection of resigned/ terminated employees, inspected the last working date of the employee in HR records and the deactivation date in AD to determine whether the ID was disabled within 24 hours of employee's last working date	No relevant exceptions noted.
CC 6.2.5	The user access to the key applications is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.	○ Inquired with the Application team personnel regarding the process for employee user ID removal to applications. ○ For a selection of separated employees, inspected the last working date of the employee in HR records and the deactivation date in the applications to determine whether the logical access was revoked within 24 hours of intimation received from the HR post employee's last working date.	No relevant exceptions noted.
CC 6.2.6	The user access to Yotta Managed databases is revoked within 24 hours from intimation from HR as per the timelines defined in the Employee Exit process document.	○ Inquired with the Cloud team personnel regarding the process of granting logical access to the Yotta managed databases.	No relevant exceptions noted. We were informed that no user IDs required to be deleted for Yotta managed databases during the examination period.

Control number	Control Description	Test procedure	Conclusion
CC 6.2.7	Quarterly user access review is performed for user IDs having access to active directory (AD). Discrepancies noted during the review are communicated to respective teams for resolution.	○ Inquired with the Corporate IT team personnel regarding the process followed for performing user access review of users having access to AD. ○ For a selection of quarters, inspected the user access review email to determine whether access was reviewed on a quarterly basis and discrepancies noted during the review were communicated to respective teams for resolution.	No relevant exceptions noted.
CC 6.2.8	Quarterly user access review is performed for user IDs having access to key applications. Discrepancies noted during the review are communicated to respective teams for resolution.	○ Inquired with the Application team personnel regarding the process followed for performing user access review of users having access on applications. ○ For a selection of quarters, inspected the user access review email to determine whether access to key applications PAM, SFDC and CISCO ISE was reviewed on a quarterly basis and discrepancies noted during the review were communicated to respective teams for resolution	No relevant exceptions noted.
CC 6.2.9	Quarterly user access review is performed for user IDs having access to the databases (MYSQL, MSSQL and Oracle). Discrepancies noted during the review are communicated to respective teams for resolution.	○ Inquired with the Application team personnel regarding the process followed for performing user access review of users having access on databases. ○ For a selection of quarters, inspected the user access review email to determine whether access to database servers (MYSQL, MSSQL and Oracle) was reviewed on a quarterly basis and discrepancies noted during the review were communicated to respective teams for resolution.	No relevant exceptions noted.
CC 6.3.1	For employees and contractors leaving the organization, exit checklist is signed by employee and manager, which then is transferred to the IT team who is responsible to revoke access to the domain within 24 hours of the employees last working date.	○ Inquired with the HR team personnel regarding the process for employee user ID removal to the Yotta applications ○ For a selection of separated employees, inspected the last working date of the employee in the HR leaver's list and the deactivation date in Darwinbox account to determine whether	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		domain access was revoked within 24 hours of employee's last working date.	
CC 6.4.1	There exists a Physical Access Control Policy that describes the process for controlling physical access to the facilities and server room. This document is reviewed and approved by the Head DC security and safety.	○ Inquired with the DC Security team personnel regarding the existence of a Physical Access Control policy describing the seven-layer security covering the process for controlling physical access to the facilities and data centre and its review and approval. ○ Inspected the Physical Access Control policy and revision history to determine whether it included the seven-layer security covering the process for controlling physical access to the facilities and server room and whether it was reviewed and approved by the Head DC security on an annual basis.	No relevant exceptions noted.
CC 6.4.2	Employees' and visitors' access to premises is restricted using access cards. Access to general and restricted areas within premises is granted after receiving approval from authorized personnel of Yotta.	○ Inquired with the DC Security team personnel regarding the process of granting employee and visitors with access to general and restricted areas within premises. ○ For a selection of new joiners (employee), inspected email from HR to the DC Security team along with the provision date to determine whether access was granted to new joiners only upon receipt of email from HR. ○ For a selection of visitors, inspected the workflow from Tussom application to determine whether the access to authorized visitors was granted on completion of visitor details in the Tussom application.	No relevant exceptions noted.
CC 6.4.3	Employees access to server hall is restrict to authorized employees using biometric access control system and mantrap. DC Operations team grants the access to server hall based on the approval from DC Security team.	○ Inquired with the DC Security team personnel regarding the process of granting biometric access to server room to employees. ○ Performed a physical walkthrough of server hall to determine whether the mantraps	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		were implemented at the entry and exit points of the server hall. o For a selection of new joiners (employees), inspected the date of access creation, email from HR to the DC Security team and approval from DC Security team to determine whether access to server room was granted to new joiners only upon approval from DC Security team.	
CC 6.4.4	Visitors and vendors requiring access to data centres are issued identification badge and escorted by authorized DC Security team personnel.	o Inquired of the DC Security team personnel regarding the process followed for granting visitor access to the server rooms within data centres. o Performed a physical walkthrough of the data centres to determine whether visitors were being issued an identification badge and were required to be escorted by authorized individuals.	No relevant exceptions noted.
CC 6.4.5	On a Quarterly basis restricted area access reports are generated and shared with the designated owner for the premises for review. Any discrepancies noted are tracked to closure.	o Inquired with the DC Security team personnel regarding the process followed for performing user access review of users having access to restricted areas. o For a selection of quarters, inspected the user access review email to determine whether access was reviewed on a quarterly basis and discrepancies were tracked to closure.	No relevant exceptions noted.
CC 6.4.6	At the time of separation from the organization, employee's and contractor's ID cards and access cards are returned to the security department, and access to the premises is disabled within 24 hours of the last working day.	o Inquired with the DC Security team personnel regarding the process for access to the premises is disabled at employee's last working day. o For a selection of separated employees, inspected the last working date of the employee in HR records and the deactivation status of the card from the Genetics system to determine whether access to the premises was disabled within 24 hours of the employee's last working day. o Performed physical walkthrough of the premises to determine	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		whether contractor's ID cards and employee access cards were returned to the security department at the time of exit.	
CC 6.4.7	Data centre facilities are secured by power fence at the perimeter, full height turnstiles at the entry gate and security guards are stationed at entry and exit point to monitor movement of employees and visitors.	○ Inquired with the DC Operations team personnel regarding the process of monitoring entry and exit points and deployment of security guards. ○ Performed a walkthrough of Yotta facilities to determine whether security guards were stationed at entry and exit point to monitor movement of employees and visitors and data centre facilities were secured by power fence at the perimeter and full heighted turnstile at the entry gate.	No relevant exceptions noted.
CC 6.4.8	5.9 Dedicated zones are defined for each area allowing only authorized personnel to access specific areas	○ Inquired with the DC Operations team personnel regarding the segregation of common and restricted areas at the data centre facilities. ○ Performed a walkthrough of Yotta data center facilities to determine whether dedicated zones were defined for each area allowing only authorized personnel to access specific areas.	No relevant exceptions noted.
CC 6.4.9	Employees, visitors and contractors are issued unique lanyards based on the type of the visitor at the time of entry.	○ Inquired with the DC Security team personnel regarding the process of issuing lanyards to employees, visitors and contractors. ○ Performed a walkthrough of Yotta facilities and data centres to determine whether employees, visitors and contractors were issued unique lanyards based on the type of visitor at the time of entry.	No relevant exceptions noted.
CC 6.4.10	At the facilities entry point vehicles and personal belongings are scanned.	○ Inquired with the DC Security team regarding the process of scanning vehicles and personal belongings. ○ Performed a physical walkthrough of a facility to determine whether vehicles and	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		personal belongings are scanned at the entry points of the facility.	
CC 6.6.1	Privilege activity of network and database servers is logged within the PAM application. Security incidents are notified and corrective actions are taken to resolve the incidents.	○ Inquired with the PAM team regarding the process of monitoring the system and servers on PAM application. ○ Inspected the asset report extracted from the PAM application to determine whether all the systems were on boarded on PAM application for monitoring. ○ Inspected the PAM dashboard to determine whether the access to the servers was monitored and actions were taken in case of any breaches.	No relevant exceptions noted.
CC 6.6.2	Antivirus is configured to perform a scan on a real time basis. Yotta monitors the antivirus compliance on a periodic basis.	○ Inquired with the IT team personnel regarding the existence of a policy document describing the process followed for anti-virus scanning and compliance monitoring. ○ Inspected the CrowdStrike and PaloAlto dashboard and list of asset inventory from CrowdStrike and PaloAlto application to determine whether the antivirus application was installed on all endpoint devices and servers and configured to perform a scan on a real time basis.	No relevant exceptions noted.
CC 6.6.3	Firewall is configured at the perimeter of Yotta's network to restrict internet access as per defined policy.	○ Inquired with the Firewall IT team personnel regarding the process of restricting internet access through firewall. ○ Inspected the network diagram to determine whether the external points of connectivity were protected by firewall complex. ○ Inspected the firewall ruleset to determine whether firewall was configured to restrict internet access as per defined policy ○ Inspected the weekly meeting and agenda to determine whether firewall policy was discussed in	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		case of any changes with the Operations team.	
CC 6.6.4	Firewall is configured with Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) to monitor Yotta's networks and report threats.	○ Inquired with the Firewall IT team personnel regarding the configuration of firewall on Yotta network perimeter. ○ Inspected the network diagram to determine whether the external points of connectivity were protected by firewall configured with Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS). ○ Inspected the security policy of the firewall specifying IPS and IDS enabled for defined source and destination IP addresses to determine whether Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) was enabled to monitor Yotta's networks and report threats.	No relevant exceptions noted.
CC 6.7.1	Management has restricted access to external media such as USB, CD and external hard drives. Exception request for the use of removable media is approved by CISO.	○ Inquired with the Corporate IT team personnel regarding the process of restricting access to external media. ○ Inspected the configuration on Manage Engine to determine whether management had restricted access to external media including USB, CD and external hard drives. ○ For a selection of users, inspected the approval granted by the CISO for the use of USB on workstations.	No relevant exceptions noted.
CC 6.7.2	Backup media are encrypted to prevent data loss.	○ Inquired with the Backup team personnel regarding the process of encrypting backup media during creation of backup media. ○ Inspected the configuration settings of backup software encryption configuration to determine whether the back media was encrypted to prevent data loss.	No relevant exceptions noted.
CC 7.1.1	Database upgrades (patches) for Yotta managed databases are applied after analysis by Yotta.	○ Inquired with the Cloud operations team personnel regarding the existence of an	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
	Patches are deployed through the change management process.	approved process document for patch management. o For a selection of patches implemented, inspected tickets raised in Tussom application to determine whether patches were deployed after analysis and as per the change management process.	
CC 7.5.1	Yotta has a defined Business Continuity Management Policy which describes the process of continuing the business in case of any disruptions. The policy is reviewed and approved by the Chief Digital Officer on an annual basis or in case of any changes.	o Inquired with the GRC team personnel regarding existence of Business Continuity Management Policy and plan. o Inspected the Business Continuity Management policy along with revision history to determine whether there exists a documented BCP and DR plan as part of Business Continuity Management policy which was reviewed and approved by the Chief Digital Officer an annual basis or in case of any changes.	No relevant exceptions noted.
CC 7.5.2	Business continuity and Disaster Recovery (DR) drills are conducted based on DR drill calendar and exceptions noted, if any, are tracked to closure.	o Inquired with the GRC team personnel regarding BCP and DR plans and its testing. o Inspected the BCP and DR plans to determine whether the plans were developed and reviewed on an annual basis. o Inspected the BCP and DR drill reports to determine whether BCP and DR drills were performed on an annual basis, and exceptions noted were tracked to closure.	No relevant exceptions noted.
CC 7.5.3	Vulnerabilities identified during monthly/yearly mock drills are evaluated and discussed in Management Review Meetings.	o Inquired with the GRC team personnel regarding vulnerabilities noted during mock drills. o For a selection of months/ year, inspected the mock drill reports to determine whether the mock drills were conducted as per the defined frequencies and vulnerabilities were documented in the mock drill reports. o Inspected the management review meeting MOM and the management review meeting invite to determine whether the	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		identified vulnerabilities were discussed during those review meetings.	
CC 8.1.1	Changes are approved by authorized personnel in accordance with the nature of the change prior to development and implementation of change.	○ Inquired with the Service Management team personnel regarding the process for raising and approval of change requests. ○ For a selection of change requests, inspected the approval in Tussom application to determine whether the changes were approved by the Project Manager in accordance with the nature of the change prior to development and implementation of change.	No relevant exceptions noted.
CC 8.1.2	Changes are tested and approved prior to implementing the changes into production.	○ Inquired with the Service Management team personnel regarding the testing performed for changes. ○ For a selection of change requests, inspected the change request tickets and change testing documents uploaded on Tussom application to determine whether testing was performed, documented and approved in the ticket for changes by the development team.	No relevant exceptions noted.
CC 8.1.3	Emergency changes are approved by CAB members before implementation of change.	○ Inquired with the Service Management team personnel regarding the approval of emergency changes and their implementation in the production environment. ○ For a selection of emergency change requests, inspected the change request tickets from Tussom application to determine whether the Project Manager and CAB approval was obtained before implementation of change.	No relevant exceptions noted.
CC 8.1.4	There exists a logically separate environment for development, test and production for key applications and developer access to the production environment is restricted.	○ Inquired with the Service Management and cloud team personnel regarding the segregation of UAT and production environments. ○ Inspected the URL of development, test and production environments to determine	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		whether production environment was segregated from development and test environments. o Inspected the list of users having deployment access to the production environment and list of users having access to the development environment to determine whether the access rights were segregated.	
CC 8.1.5	Changes (Pre-planned, Emergency and Retrospective) are reviewed on a weekly basis by the Service Management team and CAB team	o Inquired with the Service Management team personnel regarding weekly meetings conducted to review the changes. o For a selection of weeks, inspected the weekly meeting invites, agenda of the meeting and details of the changes that were discussed to determine whether the changes were analysed and reviewed during the weekly meetings with the service management and the CAB team personnel.	No relevant exceptions noted.
CC 9.2.1	The organization has documented process for terminating vendor relationship as part of the Procurement Procedure document which is reviewed and approved by Head – Procurement and Asset Management on an annual basis.	o Inquired with the GRC team personnel regarding process for terminating vendors. o Inspected the Procurement Procedure document and revision history to determine whether the organization had a defined process for terminating vendor relationship and whether the document was reviewed and approved by Head – Procurement and Asset Management on an annual basis.	No relevant exceptions noted.
A 1.1.1	The management has established a process for maintaining redundancy of network components.	o Inquired with the Firewall IT team personnel regarding the process for maintaining redundancy of network components. o Inspected the network architecture diagram to determine whether redundancy was maintained for network components.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
A 1.2.1	CCTV cameras are installed at the entry and exit points of the premises and critical areas. The video surveillance is reviewed on a real time basis, recordings are retained for a minimum period of 90 days and reviewed by the Administration team.	○ Inquired with the DC Operations team personnel regarding the process of deploying CCTVs on entry and exit points for video surveillance. ○ Performed a walkthrough of Yotta facilities to determine whether the video surveillance was reviewed on a real time basis. ○ Inspected system configuration to determine whether recordings were retained for a minimum period of 90 days and reviewed by the DC Operations team.	No relevant exceptions noted.
A 1.2.2	Environmental protections have been installed at Yotta include the following: • Cooling systems • Smoke detectors • Sprinklers • Fire Extinguisher • Battery and diesel generators • UPS • Fire Alarm	○ Inquired with the DC Operations team personnel regarding environmental protection mechanisms deployed. ○ Performed a physical walkthrough to determine whether environmental protections were installed including the following: • Cooling systems • Smoke detectors • Sprinklers • Fire Extinguisher • Battery and diesel generators • UPS • Fire Alarm	No relevant exceptions noted.
A 1.2.3	Environmental protections receive periodic maintenance as per defined schedule for each equipment.	○ Inquired with the DC Operations team personnel regarding the planned maintenance of chillers, fire alarm systems, fire extinguishers, Diesel Generators (DG) and Uninterruptible Power Supply (UPS). ○ Inspected the 52 weeks maintenance calendar to determine whether maintenance of devices was scheduled. ○ For a selection of quarters, inspected the service maintenance reports to determine whether maintenance of chillers, fire alarm systems, Diesel Generators (DG) and Uninterruptible Power Supply (UPS) was performed in	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		accordance with the defined schedule.	
A 1.2.4	Management has implemented detection controls to identify environmental anomalies.	○ Inquired with the DC Operations team personnel regarding the existence of detection control to identify environmental anomalies. ○ Performed a walkthrough of the server room to determine whether detection controls such as CCTV, fire alarms, fire extinguishers, door alarms, temperature and humidity monitoring to identify environmental anomalies were implemented.	No relevant exceptions noted.
A 1.2.5	Secondary backup of power supply is installed to be utilized in case of power failure.	○ Inquired with the DC Operations team personnel regarding the availability of power backup in case of a power failure. ○ Performed a physical walkthrough of block which had the secondary backup setup to determine whether server room was supported by a secondary backup of power supply.	No relevant exceptions noted.
A 1.2.6	The DC Operations team performs monitoring of temperature for network and UPS rooms during each shift.	○ Inquired with the DC Operations team personnel regarding the process to monitor the temperature of network and UPS rooms. ○ Performed a physical walkthrough of network room and UPS room to determine whether the DC Operations team monitored the temperature for network and UPS rooms during each shift.	No relevant exceptions noted.
A 1.2.7	Yotta has a defined Backup Management procedure specifying the backup process to be followed for key applications and servers. The policy is reviewed and approved by Head Storage and Backup on an annual basis.	○ Inquired with the Backup team personnel regarding the process of managing backups ○ Inspected the Backup Management Procedure document to determine whether backup process was defined for key applications and servers. ○ Inspected the Backup Management Procedure document revision history to determine whether the document	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		was reviewed and approved by Head Storage and Backup on an annual basis.	
A 1.2.8	Data backups are performed for key applications and servers as per pre-defined schedules.	○ Inquired with the backup team personnel regarding the frequency, schedule and process followed for data backup. ○ Inspected the backup schedule configured in Commvault application to determine whether backups were configured for key applications as per the pre-defined schedule. ○ For a selection of days/weeks, inspected the status of the backup jobs for key applications to determine whether the backups were executed as per the schedule defined in the Commvault application.	No relevant exceptions noted.
A 1.2.9	Data backups are monitored for successful completion and any errors/failures are tracked to closure. Only authorized employees are allowed to modify backup. Ticket is raised in the Tussom application in case of backup failures.	○ Inquired with the Backup team personnel regarding the process of monitoring of backups for failure. ○ For a selection of days and weeks, inspected the availability of backup logs with the status of backup to determine whether the backups were manually monitored for failure. ○ Inspected the list of users having access to the Commvault application along with roles and responsibilities to determine whether only authorized users were allowed to modify backup. ○ For selected backup failures, inspected the ticket raised on Tussom application to determine whether ticket was raised on Tussom application in case of backup failures.	No relevant exceptions noted.
A 1.2.10	Backup media tapes are transferred to the offsite storage location on monthly basis and backup transfer records are recorded and documented by the authorized IT team personnel in the ticket raised on Tussom application.	○ Inquired with the Backup team personnel regarding the tape storage at a secondary location. ○ For a selection of months, inspected the ticket raised in Tussom application to determine whether backup media tapes were transferred to the offsite storage	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		location on monthly basis and documented by the authorized IT team personnel in the ticket raised in the Tussom application.	
A 1.2.11	Backup restoration testing is performed by the Yotta team upon request. The restoration test results are reviewed by the respective Team lead and exceptions identified are followed up through the problem management process.	○ Inquired with the Backup team personnel regarding the process related to restoration testing. ○ For a selection of restoration test requests, inspected the email request for infrastructure restoration and the workflow ticket raised in Tussom application to determine whether backup restoration testing was performed and the restoration test results were reviewed by the respective Team lead and exceptions identified were followed up through the problem management process	No relevant exceptions noted.
A 1.3.1	Backups are retained based on defined policy	○ Inquired with the Backup team personnel regarding retention period of backup. ○ Inspected the Commvault application configuration to determine whether retention period for the backups were configured	No relevant exceptions noted.
A 1.3.2	Server hall is supported by Uninterruptible Power Supply (UPS) systems and Diesel Generator Sets (DG sets), for continuous operation of hardware equipment in the event of a component or power failure.	○ Inquired with the DC Operations team personnel regarding the availability of UPS systems and DG sets to support the server room for continuous operation of hardware equipment in the event of a component or power failure. ○ Performed a physical walkthrough of the server room to determine whether server room was supported by UPS and DG sets were installed for continuous operation of hardware equipment in the event of a component or power failure.	No relevant exceptions noted.
C 1.1.1	There exists a formal Removable Media policy that describes the process for usage of external devices at Yotta. This policy is reviewed and approved by the Head Corporate IT.	○ Inquired with the Corporate IT team personnel regarding the policy related to disposing of media with confidential information if any, in electronic and paper form.	No relevant exceptions noted.

Control number	Control Description	Test procedure	Conclusion
		○ Inspected the removable media policy document and revision history to determine whether the policy describes the process for usage of external devices at Yotta and whether the policy was reviewed and approved by the Head Corporate IT on an annual basis.	
P 1.1.1	Policy and procedure documents relating to privacy are uploaded on Yotta's intranet.	○ Inquired with GRC team personnel regarding the regarding the formally documented Data Protection policy. ○ Inspected the Data Protection policy to determine whether policy and procedure documents relating to privacy existed, and were reviewed and approved annually or in case of any major changes by Data Protection Officer (DPO). ○ Inspected the Yotta intranet portal, ATHENA to determine whether the Data Protection policy was made available	No relevant exceptions noted.
P 1.1.2	Yotta provides user entities with its Privacy Notice by publishing the notice on Yotta website. Yotta Privacy Notice addresses the following: • The choices available regarding collection, use, retention, disclosure, and disposal of personal information. • The information collected by Yotta, how it is used, shared, secured, retained and/or disclosed. • The scope of the notice's applicability.	○ Inquired with Data Privacy team regarding the process followed for providing privacy notice on Yotta website. ○ Inspected the privacy notice present on Yotta website to determine whether the following points were addressed: • The choices available regarding collection, use, retention, disclosure, and disposal of personal information. • The information collected by Yotta, how it is used, shared, secured, retained and/or disclosed. • The scope of the notice's applicability.	No relevant exceptions noted.
P 1.1.3	Yotta informs user entities of changes made to Yotta Privacy notice through Yotta website.	○ Inquired with Data Privacy team regarding the process of informing user entities of changes made to Yotta Privacy notice.	No relevant exceptions noted. We were informed that there were no changes to the Privacy notice during the examination period.

Control number	Control Description	Test procedure	Conclusion
P 3.2.1	User entities are required to accept Yotta Privacy terms at the time of subscription.	○ Inquired with the Data Privacy team regarding the process of accepting the privacy terms by user entities. ○ Inspected the Yotta website to determine whether User entities were required to accept Yotta Privacy terms at the time of subscription.	No relevant exceptions noted.
P 6.3.1	There exists Data Protection policy covering the logging and monitoring of the privacy breaches as part of the incident management. Policy is reviewed and approved annually by Head Legal and Data Protection Officer.	○ Inquired with the Data Protection Officer (DPO) regarding the formally documented Data Protection policy and procedure. ○ Inspected the Data Protection policy to determine whether it included guidance for logging and monitoring privacy breach as part of incident management. ○ Further inspected the revision history to determine whether the policy was reviewed and approved annually by Head Legal and Data Protection Officer.	No relevant exceptions noted.
P 8.1.1	Yotta has established a mailbox for internal users through which the Data Privacy Officer (DPO) monitors privacy related complaints and takes necessary actions.	○ Inquired with the GRC team personnel regarding the privacy breach functional mailbox established by the Yotta's management. ○ Inspected the grievance mailbox: dpo@yotta.com to determine whether a separate email was established for internal users for complaint redressal.	No relevant exceptions noted.

SECTION 5

ADDITIONAL INFORMATION PROVIDED BY SERVICE ORGANIZATION

DARK WEB MONITORING

Yottas' CISO team monitors dark web using SOCRadar and TechOwl applications. The tool has predefined ruleset to capture anomalies incluing:

- Unauthorized access attempts
- Abnormal traffic
- Compromise of password
- Dark web activities like leaked data, and discussions of cyber-attacks.

In case of any discrepencies detected, the CISO team conducts impact analysis to determine whether the incident represent actual compromise/ exposed credentials or a false positive. Based on the findings, correctve actions are implemented approved by the CISO to mitigate risks effectively.

ABBREVIATIONS

ABBREVIATIONS

Sr. No.	Abbreviations	Expanded Form
1.	AD	Active Directory
2.	Admin	Administration
3.	AV	Anti-Virus
4.	BCP	Business Continuity Plan
5.	BCM	Business Continuity Management
6.	CAB	Change Advisory Board
7.	CCTV	Close Circuit Television
8.	CHT	Customer Happiness Team
9.	CISO	Chief Information Security Officer
10.	CoC	Code of Conduct
11.	Colo	Colocation
12.	CPU	Central Processing Unit
13.	CUEC	Complementary User Entity Controls
14.	DB	Database
15.	DC	Data centre
16.	DLP	Data Leakage Prevention
17.	DR	Disaster Recovery
18.	GRC	Governance Risk Compliance
19.	HA	High Availability
20.	HR	Human Resources
21.	IaaS	Infrastructure as a Service
22.	IDS	Intrusion Detection System
23.	IPS	Intrusion Prevention System
24.	IS	Information Security
25.	ISMS	Information Security Management System
26.	ISO	International Organization for Standardization
27.	IT	Information Technology
28.	JD	Job Description
29.	MIS	Management Information System
30.	MOM	Minutes of Meeting

Sr. No.	Abbreviations	Expanded Form
31.	MRM	Management Review Meeting
32.	MSA	Master Service Agreement
33.	NDA	Non-Disclosure Agreement
34.	NOC	Network Operations Centre
35.	OEM	Original Equipment Manufacturer
36.	OS	Operating System
37.	PCI-DSS	Payment Card Industry Data Security Standard
38.	RAM	Random access Memory
39.	RCA	Root Cause Analysis
40.	SHA	Secure Hash Algorithm
41.	SIEM	Security Information and Event Management
42.	SLA	Service Level Agreement
43.	SOP	Standard Operating Procedure
44.	TAT	Turnaround Time
45.	UAT	User Acceptance Testing
46.	UTM	Unified Threat Management
47.	UPS	Uninterruptible Power Supply
48.	URL	Uniform Resource Locator
49.	USB	Universal Serial Bus
50.	UVSS	Under Vehicle Scanning system
51.	VA	Vulnerability Assessment
52.	VPN	Virtual Private Network