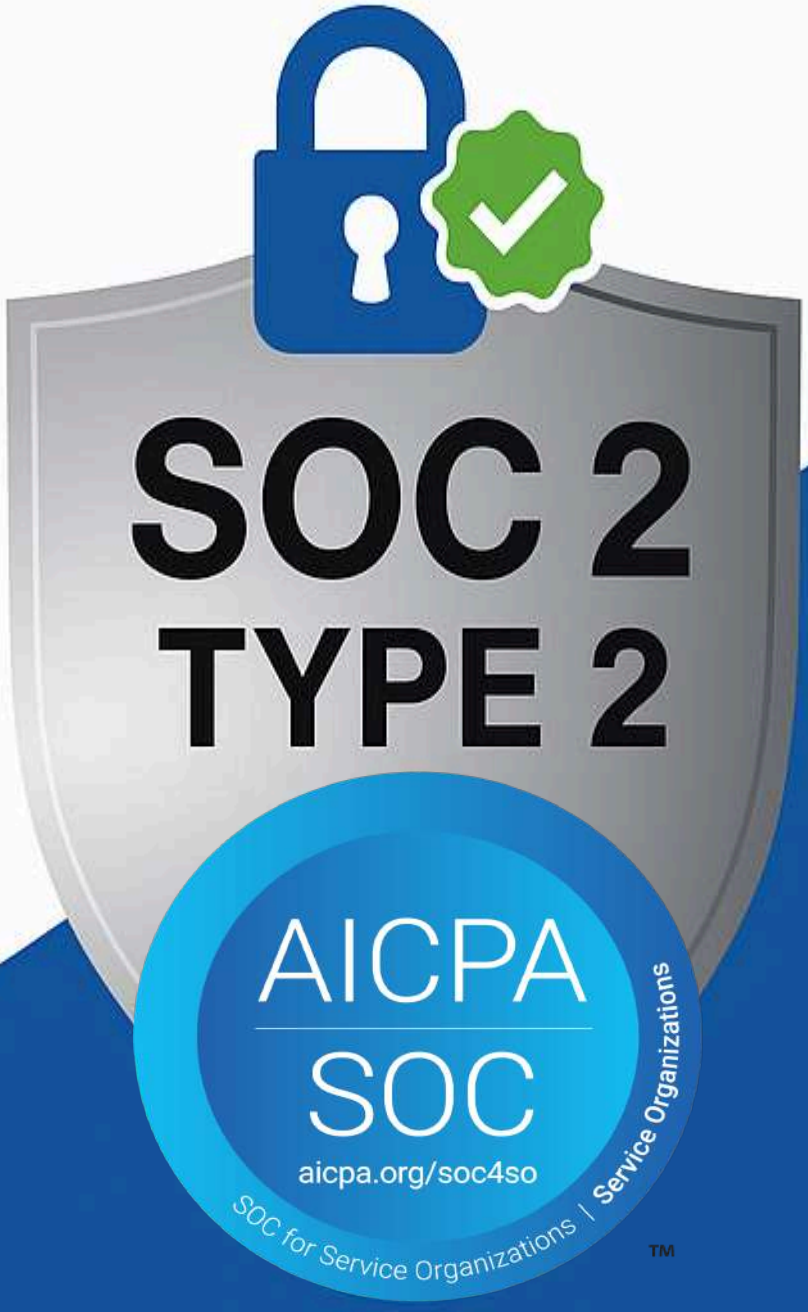

Infinite Open Source Solutions LLP

SYSTEM AND ORGANIZATION CONTROLS (SOC) 2 Type 2
REPORT ON MANAGEMENT'S DESCRIPTION

The Suitability of Design of Controls Relevant to the Controls Placed in Operation and Test of Operating Effectiveness Relevant to Security, Availability, and Confidentiality Trust Criteria

For the period: **December 01, 2024 to December 01, 2025**

Together with Independent Service Auditors' Report

This SOC 2 Type II report is valid for a period of twelve (12) months from the date of the independent service auditor's opinion, which represents the signing date of this report. After this period, users should not rely on the report as a current representation of the system and related controls, unless a subsequent SOC 2 report has been issued.
You may use the SOC for Service Organization's - Service Organization's - Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If, after twelve months, a new report is not issued, must immediately cease use of the SOC for Service Organization's Logo.

Description of the Infinite Open Source Solutions LLP System Relevant to Security, Availability, and Confidentiality

Table of Contents

SOC 2 TYPE 2 REPORT

Section 1: Independent Auditor's Report

SECTION I - INDEPENDENT SERVICE AUDITOR'S REPORT

To: Infinite Open Source Solutions LLP

Scope

We have examined the accompanying 'Description of Infinite Open Source Solutions LLP' from December 01, 2024, to December 01, 2025. This description, along with the suitability of the design and operating effectiveness of controls, has been assessed to meet Infinite Open Source Solutions LLP's service commitments and system requirements based on the applicable trust services criteria for Security, Availability, and Confidentiality throughout the period from December 01, 202,4 to December 01, 2025.

The Security principle focuses on protecting system resources through logical and physical access control measures, ensuring the entity meets its commitments and system requirements related to Security, Availability, and Confidentiality. Controls over system security are designed to prevent or detect the breakdown of segregation of duties, system failures, incorrect processing, theft or unauthorised removal of data or system resources, misuse of software, and improper access to or use, alteration, destruction, or disclosure of information.

Infinite Open Source Solutions LLP Uses

- Infinite Open Source Solutions LLP utilises a robust suite of technologies to ensure the secure and efficient delivery of its services, aligning with SOC 2 trust service criteria. The organisation leverages AWS Cloud Services for scalable, secure, and highly available data storage and processing capabilities.

- These technologies collectively demonstrate Infinite Open Source Solutions LLP's commitment to safeguarding sensitive data, maintaining operational resilience, and complying with the highest security and privacy standards.

The description does not disclose the actual controls at the subservice organisations. Our examination did not include the services provided by the subservice organisations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organisation controls.

The description presents Infinite Open Source Solutions LLP's controls, the applicable trust services criteria, and the types of complementary user entity controls assumed in the design of Infinite Open Source Solutions LLP's controls. The description does not disclose the actual controls at the user entity organisations. Our examination did not include the services provided by the user entity organisations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organisation controls.

Service Organisation's Responsibilities

Infinite Open Source Solutions LLP has provided the accompanying assertion titled "Infinite Open Source Solutions LLP's Management Assertion throughout the period December 01, 2024 to December 01, 2025." about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet Infinite Open Source Solutions LLP's service commitments and system requirements based on the applicable trust services criteria.

Infinite Open Source Solutions LLP is responsible for:

1. Preparing the description and assertion.
2. The completeness, accuracy, and method of presentation of the description and assertion.
3. Providing the services covered by the description.
4. Identifying the risks that would prevent the applicable trust services criteria from being met.
5. Designing, implementing, maintaining, and documenting controls to meet Infinite Open Source Solutions LLP's service commitments and system requirements based on the applicable trust services criteria stated in the description.
6. Specifying the controls that meet Infinite Open Source Solutions LLP's service commitments and system requirements based on the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth outlined in Infinite Open Source Solutions LLP's assertion and on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that the service organisation's commitments and system requirements were met based on applicable trust services criteria.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA).

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether in all material respects.

1. The description is fairly presented based on the description criteria.
2. The controls were suitably designed to provide reasonable assurance that the service organisation's commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria.
3. The controls operated effectively to provide reasonable assurance that the service organisation's commitments and system requirements

were achieved based on the applicable trust services criteria throughout the Period "December 01, 2024 to December 01, 2025".

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to provide reasonable assurance that the service organisation's commitments and system requirements meet the applicable trust services criteria.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the service organisation's commitments and system requirements based on the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own particular needs. Because of their nature and inherent limitations, controls at a service organisation may not always operate effectively to meet the applicable trust services criteria.

Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organisation may become inadequate or fail.

Description of tests of controls

In Section IV, the specific controls tested, the nature and timing, and the results of those tests are listed in the accompanying description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the description criteria described in Infinite Open Source Solutions LLP's assertion and the applicable trust services criteria:

1. The description fairly presents the system that was designed and

implemented throughout the period " December 01, 2024 to December 01, 2025".

2. The controls stated in the description were suitably designed to provide reasonable assurance that the service organizations commitments and system requirements would be achieved if the controls operated effectively based on the applicable trust services criteria and if sub-service organizations and user entities applied the controls contemplated in the design of Infinite Open Source Solutions LLP's controls throughout the Period "December 01, 2024 to December 01, 2025".

3. The controls tested, which were those necessary to provide reasonable assurance that the service organisation's commitments and system requirements based on the applicable trust services principles criteria were met, operated effectively throughout the period from December 01, 2024, to December 01, 2025.

Restricted Use

This report, including the description of tests of controls and results thereof, is intended solely for information and use of user entities of Infinite Open Source Solutions LLP throughout the Period " December 01, 2024 to December 01, 2025", and prospective user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organisation.
- How the service organisation's system interacts with the user entities, subservice organisations, or other parties.
- Internal controls and their limitations.
- Complementary subservice organisations and complementary user entity controls, and how those controls interact with the controls at the service organisations to achieve the service organisation's service commitments and system requirements.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

CPA's Name: Percilchofe CPA LLC

License No.: 1188

Date: 21-Jan-2026

SOC 2 TYPE 2 REPORT

Section 2:
Management's Assertion

SECTION II - MANAGEMENT'S ASSERTION

Infinite Open Source Solutions LLP Management Assertion for the Period December 01, 2024, to December 01, 2025.

We have prepared the attached description titled "Description of Infinite Open Source Solutions LLP's" for the Period "December 01, 2024 to December 01, 2025". (Security, Availability, and Confidentiality), based on the criteria in items (a) (I)–(ii) below, which are the criteria for a description of a service organization's system given in DC Section 200 prepared by AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2® Guide Working Group to be used in conjunction with the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, Privacy and Processing Integrity (the description criteria).

The description is intended to provide users with information about the services provided by Infinite Open Source Solutions LLP, which may be useful when assessing the risks from interactions with the system throughout the Period "December 01, 2024 to December 01, 2025". Particularly, information about the suitability of the design and operating effectiveness of controls to meet Infinite Open Source Solutions LLP service commitments and system requirements based on the criteria related to Security, Availability, and Confidentiality (applicable trust services criteria) outlined in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Privacy, and Processing Integrity (AICPA, Trust Services Criteria).

Infinite Open Source Solutions LLP Uses

- Infinite Open Source Solutions LLP utilises a robust suite of technologies to ensure the secure and efficient delivery of its services, aligning with SOC 2 trust service criteria. The organisation leverages AWS Cloud Services for scalable, secure, and highly available data storage and processing capabilities.
- These technologies collectively demonstrate Infinite Open Source Solutions LLP's commitment to safeguarding sensitive data, maintaining operational resilience, and complying with the highest security and privacy standards.

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

Solutions LLP's controls, the applicable trust services criteria, and the types of complementary user entity organisation controls assumed in the design of Infinite Open Source Solutions LLP's controls. The description does not disclose the actual controls at the user entity organisations.

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

1. The description fairly presents the services provided by Infinite Open Source Solutions LLP throughout the Period "December 01, 2024 to December 01, 2025". The criteria for description are identified below under the heading "Description Criteria".

2. The controls stated in the description were suitably designed and operated effectively to meet Infinite Open Source Solutions LLP's service commitments and system requirements based on the applicable trust services criteria throughout the Period "December 01, 2024 to December 01, 2025", to meet the applicable trust services criteria.

For Infinite Open Source Solutions LLP

Authorized Signatory

Name:

SOC 2 TYPE 2 REPORT

Section 3:
Description of the system

SECTION III - Description of Infinite Open Source Solutions LLP

Overview:

Infinite Open Source Solutions LLP (iOSS) is a technology company providing comprehensive Software services. iOSS was founded in the year 2009 by a group of five young and vibrant entrepreneurs who aim to succeed in life by serving software consumers across the globe. The company specializes in advanced Software, e-commerce, CMS, and Mobile Application development. iOSS has assisted many companies to attain profitable ROI through value-based consultancy and strategic software implementation.

Since our inception, iOSS has built a superior reputation as a master in Web Enterprise solutions and custom software applications. iOSS specializes in enterprise solutions for Network Marketing, transportation, and logistics. Further, it also incorporates state-of-the-art technology and innovation, catering to the best-in-class solutions.

IOSS has a clientele base spanning across the globe. Time-framed delivery of projects with budget precision earned us the loyalty of our customers with a long-term partnership. So far, we take pride in our key success of consistently delivering projects on time without any delays. We supplied software solutions for many large companies and had an influential presence in the Asia- Pacific, North America, Europe, the Middle East, and the African region.

Principal Service Commitments and System Requirements

Introduction:

iOSS (Infinite Open Source Solutions) is a global software development and technology services company delivering high-quality, end-to-end custom software solutions to businesses of all sizes. Headquartered in Calicut, Kerala (India), and supported by strategic international offices in the UAE, Malaysia, Germany, Italy, and the USA, iOSS combines deep technical expertise with a client-centric approach to drive digital transformation across industries.

1. Security

Objective: To ensure that all application systems, development environments, infrastructure, and information assets are protected against unauthorized physical and logical access. This objective is achieved by implementing appropriate access controls, authentication mechanisms, monitoring practices, and security policies to prevent unauthorized system use, data breaches, service disruption, improper code changes, or unauthorized access, modification, disclosure, or loss of customer and company data.

Service Commitments:

- **Access Controls:** Infinite Open Source Solutions LLP commits to

implementing robust access control mechanisms, ensuring that only authorized personnel can access sensitive data and system resources. This includes multi-factor authentication (MFA), role-based access controls (RBAC), and regular access reviews.

- **Physical Security:** Physical access to offices is controlled through security measures such as ID cards & Access Cards, security personnel, and surveillance systems.
- **Network Security:** Our network is secured using security measures provided by our cloud service providers.
- **Encryption:** Data in transit and at rest is encrypted using industry-standard encryption algorithms.

System Requirements:

- Regular updates and patching of systems to address vulnerabilities.
- Encryption of sensitive data and secure key management practices.
- Continuous monitoring and logging of security events.

2. Availability

Objective: The objective is to ensure that information and systems are available for operation and use as committed or agreed, to support the achievement of Infinite Open Source Solutions LLP's business and service delivery objectives.

Service Commitments:

- **System Uptime:** Infinite Open Source Solutions LLP commits to maintaining high system availability with minimal unplanned downtime to ensure continuity of operations.
- **Disaster Recovery and Business Continuity:** Regular backups are conducted and securely stored, with disaster recovery procedures in place to ensure timely restoration of services.
- **Capacity Management:** We regularly assess and optimize system capacity to meet current and future customer demands.

System Requirements:

- Implementation of redundant systems, including power, network, and hardware components.
- Regular testing and updating of DR and BC plans.
- Continuous monitoring of system performance and capacity.

3. Confidentiality

Objective: To ensure that information designated as confidential is protected throughout its lifecycle from collection or creation to final disposition against

unauthorized access, use, or disclosure, in accordance with the entity's contractual, regulatory, or internal obligations.

Service Commitments:

- **Data Classification:** Infinite Open Source Solutions LLP classifies data based on sensitivity and implements appropriate controls to protect confidential information.
- **Access Controls:** Access to confidential data is restricted to authorized personnel only, following the principle of least privilege.
- **Data Encryption:** Confidential data is encrypted both at rest and in transit using strong encryption protocols.
- **Data Disposal:** We commit to securely disposing of or anonymizing confidential data when it is no longer required.

System Requirements:

- Implementation of data classification policies and encryption standards.
- Regular access reviews to ensure compliance with confidentiality requirements.
- Secure methods for data destruction or anonymisation.
- Policies and procedures guide how confidential information is created, accessed, stored, transmitted, and destroyed.

Conclusion:

Infinite Open Source Solutions LLP is committed to maintaining the highest levels of security, availability, and confidentiality. These commitments are supported by robust internal controls and systems designed to meet and exceed industry standards, ensuring the trust and satisfaction of all customers.

Such requirements are communicated in Infinite Open Source Solutions LLP system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organisation-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 networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System used to provide services.

A. Infrastructure & Network Architecture

The infrastructure includes the physical and virtual resources used to deliver Infinite Open Source Solutions LLP services.

The production infrastructure for the Infinite Open Source Solutions is hosted on AWS in their various regions across ap-southeast-1, eu-central-1, and ap-south-1.

Infinite Open Source Solutions uses a virtual and secure network environment on top of AWS infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. Infinite Open Source Solutions application ensures there are only specific authorised points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the AWS Internet Gateway, over to a Virtual Private Cloud that

- Houses the entire application runtime
- Protects the application runtime from any external networks

The internal networks of AWS are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

Physical office: Infinite Open Source Solutions LLP has a physical office at Sahya Building, Govt Cyberpark, Nellikode P. All IT development will be handled by this unit.

B. Software

Infinite Open Source Solutions LLP is responsible for managing the development and operation of the platform, including infrastructure components such as servers, databases, and storage systems. The in-scope Infinite Open Source Solutions infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	Business Function / Description	Underlying Operating System & Storage	Physical Location
PMT, DESKLOG	Desklog is a workforce-intelligent	Desklog is a cloud-based	Desklog is hosted in the

Primary Infrastructure and Software			
	time tracking and productivity software that helps teams and businesses accurately monitor work hours, tasks, projects, and employee performance. It offers automated time tracking, project & task tracking, timesheets, attendance management, idle time analysis, and productivity insights to boost efficiency and support smarter decision-making.	SaaS application hosted on AWS infrastructure. The platform runs on Amazon EC2 instances using Ubuntu OS, ensuring scalability, reliability, and secure access. It uses Amazon RDS (MySQL) for structured database storage and Amazon S3 for storing files and other application data, providing high availability, data durability, and efficient storage management.	Asia Pacific (Mumbai) AWS Region, ensuring low latency and reliable service delivery for users in Asia and nearby regions.
AWS IAM	Identity and access management console for AWS resources.	AWS Proprietary	AWS
AWS Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs, and back-end firewalls segregate the database servers from internal traffic.	AWS Proprietary	AWS
Bitbucket	Source code repository, version control system, and build software.	Bitbucket	Bitbucket Cloud
Google workspace	Identity/Email provider for all Infinite Open Source Solutions LLP employees	Google Workspace Proprietary	Google workspace

Supporting Tools	
System / Application	Business Function / Description

PHP	Programming Language used
Desklog	Provide continuous compliance monitoring of the company's system.
Google workspace	Office communication services

C. People

Infinite Open Source Solutions LLP staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

- **Senior Management:** Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement are required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

- **Information Security Officer:** The Senior Management assigns the role of Information Security Officer to one of its staff members, who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

- **Compliance Program Manager:** The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls across all functions/departments of the organization.

- **System Users:** The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members who access IT resources are provided with annual security awareness training.

D. IT Policies and Procedures

Formal policies and procedures have been established to support the Infinite Open Source Solutions LLP software application. These policies cover:

- Code of Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor Management
- Physical security
- Risk management
- Password management
- Incident management
- Endpoint security
- Encryption
- Disaster Recovery
- Data classification
- Business continuity
- Confidentiality
- Access control
- Acceptable usage
- Asset Management

Via the Desklog, PMT, and Firewall platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Infinite Open Source Solutions LLP also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the

services or systems provided by the IOSS in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

E. Data

Data, as defined by Infinite Open Source Solutions LLP, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

All data that is managed, processed, and stored as part of the Infinite Open Source Solutions is classified as per the Data Classification Policy, which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data • Customer PII • Anything subject to a confidentiality agreement with a customer.

Company Confidential	Information that originated or is owned internally, or was entrusted to Infinite Open Source Solutions LLP by others. Company confidential information may be shared with authorized employees, contractors, and business partners, but not released to the general public.	• Infinite Open Source Solutions LLP Unpublished financial information • Documents and processes explicitly marked as confidential • Unpublished goals, forecasts, and initiatives marked as confidential • Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases • Public website

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up, as documented in the Data backup policy.

F. Physical Security

The in-scope system and supporting infrastructure are hosted by Amazon Web Services (AWS). As such, Amazon Web Services (AWS) is responsible for the physical security controls of the in-scope system. Infinite Open Source Solutions LLP reviews the SOC 2 report provided by Amazon Web Services (AWS) on an annual basis to ensure its controls are in accordance with the standards expected by the customers of Infinite Open Source Solutions.

G. Logical Access

Infinite Open Source Solutions use role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software applications and authenticates to the database.

Infinite Open Source Solutions LLP has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as

well as a role-based access matrix, prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires multi-factor authentication (MFA) wherever possible. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Infinite Open Source Solutions LLP customer data. Staff is encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special- character based. Password configuration settings are configured on each critical system. Additionally, company-owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

H. Change Management

A documented Change Management policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the system are reviewed, deployed, and managed. The policy covers all changes made to the system, regardless of their size, scope, or potential impact.

The change management policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc

A change to the Infinite Open Source Solutions systems can be initiated by a staff member with an appropriate role. Infinite Open Source Solutions LLP uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process, which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and Manual testing, known as a pull request. For all code changes, the

reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

I. Incident Management

Infinite Open Source Solutions LLP has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Infinite Open Source Solutions LLP via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event of problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analysed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self- healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of Infinite Open Source Solutions LLP being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.

- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.

- **High severity incidents** are problems an active security attack has not yet happened, but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.

- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage was caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post- mortems may include updates to the security program or changes to systems required as a result of incidents.

J. Cryptography

User requests to Infinite Open Source Solutions LLP's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Infinite Open Source Solutions LLP web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit.

K. Asset Management (Hardware & Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Infinite Open Source Solutions LLP uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets, with the potential to store or process information, is maintained.

L. Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

M. Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include, but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

N. Availability

Infinite Open Source Solutions LLP has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

O. Boundaries of the system

The scope of this report includes Infinite Open Source Solutions. It also includes the people, processes, and IT systems that are required to achieve our service

commitments toward the customers of this application.

Infinite Open Source Solutions LLP depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

Relevant Aspects of the Infinite Open Source Solutions LLP Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of the design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Infinite Open Source Solutions LLP's description of the system. This section provides information about the five interrelated components of internal control at Infinite Open Source Solutions LLP, including

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

Control Environment

The internal control objectives related to Infinite Open Source Solutions LLP's Customer Services System are to provide reasonable, though not absolute, assurance that controls are appropriately designed and functioning effectively to align with our risk appetite. These objectives ensure that assets are safeguarded against unauthorized access or misuse, transactions are conducted according to management's authorization and client directives, and customer data remains secure.

Management at Infinite Open Source Solutions LLP has established and maintains a framework of controls designed to monitor adherence to established policies and procedures. This section outlines the "tone at the top" set by the company's leadership, reflecting the integrity, ethical values, and competence expected of all employees. It also covers the policies and procedures that guide the execution of controls by employees and management, the risk management and monitoring processes, and the roles of key control groups within the organization.

The internal control structure is established and continuously refined based on Infinite Open Source Solutions LLP's ongoing assessment of the inherent and residual risks facing the organization. This approach ensures that the control environment remains

robust and responsive to evolving risks, thereby supporting the achievement of the organization's objectives.

Integrity and Ethical Values

At Infinite Open Source Solutions LLP, we believe that the effectiveness of controls is intrinsically linked to the integrity and ethical values of the individuals who design, implement, and monitor them. Integrity and ethical conduct form the cornerstone of our control environment, influencing the design, management, and oversight of our service organization components. These values are shaped by our company's ethical and behavioral standards, the methods through which they are communicated, and how they are reinforced in daily practices.

Our commitment to integrity and ethical behavior includes management's proactive steps to eliminate or reduce incentives and temptations that could lead personnel to engage in dishonest, illegal, or unethical activities. We ensure that our entity values and behavioral standards are consistently communicated to all personnel through formal policy statements, codes of conduct, and leading by example.

The following specific control activities have been implemented by the service organization in this area:

- **Formal Documentation:** Organizational policy statements and codes of conduct are formally documented to communicate entity values, behavioral standards, and the consequences of non-compliance to all personnel.
- **Effective Communication:** Policies and procedures are effectively communicated by requiring employees to sign an acknowledgment form, confirming they have received access to the Policies and understand their responsibility to adhere to their contents.
- **Confidentiality Assurance:** A confidentiality statement, which includes a commitment not to disclose proprietary or confidential information (including client information) to unauthorized parties.
- **Background Checks:** Background checks are conducted as part of the hiring process to ensure the integrity and trustworthiness of employees.

Commitment to Competence

Management at Infinite Open Source Solutions LLP defines competence as the combination of knowledge and skills necessary to perform tasks associated with employees' roles and responsibilities. Our commitment to competence includes evaluating the required competence levels for various jobs and translating those levels into the necessary skills and knowledge.

The following specific control activities have been implemented by the service organization in this area:

- **Competence Assessment:** Management has thoroughly assessed the competence levels required for different job roles and has detailed these requirements in written position descriptions.
- **Ongoing Training:** We provide ongoing training to maintain and enhance the skill levels of personnel in specific positions, ensuring they remain competent to meet their responsibilities effectively.

Management's Philosophy and Operating Style

Infinite Open Source Solutions LLP's management philosophy and operating style are key determinants of how the organization manages and mitigates business risks. This philosophy encompasses management's approach to various operational aspects, including information processing, handling confidential and privacy-related data, accounting functions, and personnel management.

Specific control activities implemented in this area include:

- **Regulatory and Industry Updates:** Employees are periodically briefed on regulatory and industry changes affecting the services provided by Infinite Open Source Solutions LLP, ensuring that the organization stays compliant and competitive.
- **Executive Management Meetings:** Regular executive management meetings are held to discuss significant initiatives and address issues that could impact the business, ensuring that leadership is aligned and responsive to emerging challenges.

Organizational Structure and Assignment of Authority and Responsibility

Infinite Open Source Solutions LLP's organizational structure serves as the foundation for planning, executing, controlling, and monitoring activities aimed at achieving company-wide objectives. Management has designed an organizational structure that fits the company's size and the nature of its service offerings.

Key elements of the assignment of authority and responsibility include:

- **Authority and Responsibility Assignment:** Clearly defined authority and responsibility for operating activities, ensuring that employees understand their roles within the organization.
- **Reporting Relationships and Authorization Hierarchies:** Established reporting relationships and authorization hierarchies that promote accountability and clarity in decision-making.
- **Policies on Business Practices:** Policies that define appropriate business practices and ensure that personnel have the necessary knowledge and experience to perform their duties effectively.

- **Communication of Objectives:** Clear communication of the organization's objectives, ensuring that employees understand how their actions contribute to these goals and what they will be held accountable for.

Governance and Oversight: Human Resource Policies and Practices

Infinite Open Source Solutions LLP's success is deeply rooted in its commitment to sound business ethics, efficiency, and high ethical standards. This commitment is reflected in the organization's ability to consistently hire and retain top-quality personnel, which in turn ensures that the service organization operates at peak efficiency. The human resource policies and practices at Infinite Open Source Solutions LLP encompass various aspects of employee management, including hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary actions.

Specific control activities implemented in this area include:

- **Employee Onboarding Checklists:** Comprehensive checklists are used during employee onboarding to ensure that new hires receive all necessary information and resources to integrate smoothly into the organization.
- **Acknowledgment and Confidentiality Agreements:** New employees are required to sign an acknowledgment form confirming their understanding of the Policies, along with a confidentiality agreement, during their orientation on their first day of employment.
- **Annual Employee Evaluations:** All employees undergo an annual evaluation process to assess their performance, identify areas for development, and align individual goals with organizational objectives.
- **Employee Termination Procedures:** Documented termination procedures are in place, guided by a termination checklist, to ensure that the process is handled consistently and in accordance with company policies.

Information Systems and Communication

The effective management and control of Infinite Open Source Solutions LLP's operations rely on a well-structured process that encompasses the primary classes of transactions within the organization, including the reliance on and complexity of information technology systems. Information is identified, captured, processed, and reported through various information systems, as well as through communication with clients, vendors, regulators, and employees.

Risk Assessment

Infinite Open Source Solutions LLP's risk assessment process is a critical component of its ability to deliver reliable services to user organizations. This ongoing process involves management identifying and addressing significant risks that are inherent in the products or services provided. The company's approach includes identifying the underlying sources of risk, measuring the potential impact on the organization,

establishing acceptable risk tolerance levels, and implementing appropriate measures to monitor and manage these risks. This structured process is documented in the Risk Assessment and Risk Treatment Matrix.

Types of Risks Identified and Managed:

1. **Operational Risk Management:**
    a. Focuses on managing changes in the environment, personnel, management, and technology partners that could affect service delivery.
    b. Ensures that operational risks, such as those arising from internal processes or external events, are mitigated effectively.
2. **Strategic Risk Management:**
    a. Manages risks related to the adoption of new technologies, evolving business models, and shifts within the industry that could impact Infinite Open Source Solutions LLP's strategic objectives.
    b. Ensures the company remains competitive and responsive to market changes.
3. **Compliance Management:**
    a. Manages risks associated with legal and regulatory changes, ensuring that Infinite Open Source Solutions LLP remains in compliance with applicable laws and regulations.
    b. Includes monitoring regulatory environments and adjusting internal processes to maintain compliance.

Information and Communication

Information and communication processes are integral to Infinite Open Source Solutions LLP's internal control system. These processes ensure that information is identified, captured, and exchanged in the appropriate form and within the necessary time frame to support the management and control of the organization's operations. The communication channels and information systems used by the company facilitate the management of primary transactions, the handling of complex information technology, and the dissemination of critical information.

Key Aspects of Information and Communication:

1. **Information Identification and Capture:** Information relevant to Infinite Open Source Solutions LLP's operations, whether from internal or external sources, is systematically identified and captured.
2. **Information Processing and Reporting:** The organization processes and reports information through various automated and manual systems. This ensures that all relevant parties, including clients, vendors, regulators, and employees, receive

timely and accurate information.

3. **Internal and External Communication:** Effective communication is maintained with all stakeholders, ensuring that key information is conveyed accurately and promptly to support decision-making and operational activities.

Control Activities

Infinite Open Source Solutions LLP controls activities are defined through its established policies and procedures, which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Communication

Infinite Open Source Solutions LLP employs a comprehensive set of controls to manage communication both internally (with personnel) and externally (with customers, partners, and other entities).

Internal Communication:

1. **Organizational Chart:** A documented organizational chart is maintained, showing the structure, reporting lines, and areas of authority. This chart is periodically reviewed by management to ensure it remains relevant.

2. **Job Descriptions and Responsibilities:** Infinite Open Source Solutions LLP has defined roles and responsibilities in written job descriptions that are communicated to all personnel. Management regularly reviews these job descriptions and updates them as needed.

3. **Employee Policies:** Upon hiring, employees are required to review, sign, and accept the Policies and code of conduct agreement. Additionally, newly hired employees must complete information security training during onboarding and annually thereafter.

4. **Access to Policies and Procedures:** Documented policies and procedures for significant processes are available on OneDrive for employee access.

External Communication:

1. **Customer Responsibilities:** Customer responsibilities are detailed in contracts, with general guidelines communicated through the company's website.

2. **Service Level Compliance:** Internal and subservice organization processes are monitored via service level management procedures to ensure compliance with service level agreements. Security and privacy commitments are also communicated to external users through the company's website.

Physical Security

Infinite Open Source Solutions LLP has established physical security controls that are defined and implemented in accordance with its policies and procedures. These controls are regularly assessed for compliance, focusing on location security, asset management, access control, and related activities.

Logical Security

Infinite Open Source Solutions LLP utilizes Amazon Web Services as its cloud service provider, as well as for production systems, source code control, and backups.

Employee Access Control:

- **Onboarding Process:** When an employee is onboarded, the hiring manager completes an access checklist to specify the systems the employee will need access to. Infinite Open Source Solutions LLP IT then grants access and maintains a record of all employees and their access privileges in a spreadsheet.
- **Offboarding Process:** Upon an employee's departure, Infinite Open Source Solutions LLP IT deactivates their access using the same record-keeping system.
- **Access Reviews:** A quarterly review/audit of this system and related access records is conducted to ensure accuracy.

Monitoring

Vulnerability Scanning and Monitoring:

- **Security Reviews and Vulnerability Assessment:** Infinite Open Source Solutions LLP conducts annual security reviews and vulnerability assessments. This Annual assessment is documented and the results are communicated to management.

Availability Monitoring:

- **Incident Response:** Incident response policies and procedures guide personnel in reporting and responding to IT incidents, including system security breaches. These procedures ensure that incidents are properly identified, reported, and acted upon.
- **Capacity Monitoring:** Infinite Open Source Solutions LLP monitors the capacity utilization of computing infrastructure to ensure service delivery aligns with service-level agreements. This includes monitoring service response times, database storage, and response time.
- **Patch Management:** A patch management process is in place to ensure systems are patched according to vendor recommendations. Authorized personnel assess the impacts of patches and are responsible for ensuring all necessary patches are applied and validated.

This comprehensive approach to communication, security, and monitoring ensures that Infinite Open Source Solutions LLP maintains high standards of reliability, security, and efficiency in its operations.

Complementary Customer Control (CUEC)

Infinite Open Source Solutions LLP's controls related to Infinite Open Source Solutions LLP cover a subset of the overall internal control for each user of the software application. The control objectives related to Infinite Open Source Solutions LLP cannot be achieved solely by the controls put in place by Infinite Open Source Solutions LLP; each customer's internal controls need to be considered along with Infinite Open Source Solutions LLP's controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Related Criteria	CUEC Description
CC5.1 CC5.2 CC5.3 CC6.1	Customers are responsible for managing their organization's account as well as establishing any customized security solutions or automated processes through the use of setup features
CC5.2 CC6.3	Customers are responsible for ensuring that authorized users are appointed as administrators to grant access to their account
CC7.2 CC7.3 CC7.4	Customers are responsible for notifying Infinite Open Source Solutions LLP of any unauthorized use of any password or account, or any other known or suspected breach of security related to the use of Infinite Open Source Solutions
CC8.1	Customers are responsible for any changes made to user and organization data stored within the Infinite Open Source Solutions
CC7.2 CC7.3 CC7.4	Customers are responsible for communicating relevant security and availability issues and incidents to Infinite Open Source Solutions LLP through identified channels

Complementary Subservice Organization Controls (CSOC)

Infinite Open Source Solutions LLP uses subservice organizations in support of its system. Infinite Open Source Solutions LLP's controls related to the system cover only a portion of the overall internal control for user entities. It is not feasible for the trust services criteria to be achieved solely by Infinite Open Source Solutions LLP. Therefore, user entity controls must be evaluated in conjunction with Infinite Open Source Solutions LLP's controls described in Section IV of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Infinite Open Source Solutions LLP periodically reviews the quality of the outsourced operations by various methods, including:

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and
- Non-disclosure agreements

Subservice Organization	Applicable Criteria	CSOC Description
Amazon Web Services (AWS)	CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 7.2	Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.
	CC 6.4 CC 6.5	Physical access and security to the data centre facility are restricted to authorized personnel.
	CC 6.4 A 1.2	Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.
	A 1.3	Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.
	A 1.2	Policies and procedures to document repairs and modifications to the physical components of a facility, including, but not limited to, hardware, walls, doors, locks, and other physical security components.
	C 1.1	A defined data classification policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.
	C 1.2	A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.

	CC 6.1	Encryption methods are used to protect data in transit and at rest.

SOC 2 TYPE 2 REPORT

Section 4:

Auditor's Tests of Controls & Results

SECTION IV - TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the services provided by Infinite Open Source Solutions LLP. The scope of the testing was restricted to Infinite Open Source Solutions LLP and its boundaries as defined in Section 3. Infinite Open Source Solutions LLP conducted the examination testing for the observation period from "December 01, 2024, to December 01, 2025".

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the test of controls, Infinite Open Source Solutions LLP considered various factors, including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.

Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approval, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, we utilise professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. We, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness before selecting samples. In some instances, full populations were tested in cases including but not limited to the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted" in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors

SECURITY PRINCIPLES AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organisation		
CC1.0: CONTROL ENVIRONMENT		**Test Of Controls**	**Results**
CC1.1: COSO Principle 1: The Entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The Entity has formally documented behavioural and ethical standards within the HR policy and made it accessible to all employees through the company's intranet portal.	**Inquiry**: Inquired of Human Resources and management regarding how behavioral and ethical standards are defined for employees and how such standards are communicated and made accessible to employees across the organization. **Inspection**: Inspected the Entity's Human Resource (HR) Policy to verify that it formally documents behavioral, ethical, and professional conduct standards applicable to employees, including expectations related to workplace behavior, ethical conduct, compliance with laws and regulations, disciplinary actions, and reporting of concerns. Additionally, inspected evidence demonstrating that the HR Policy is made available to employees through the company intranet portal. **Observation:** Observed that the Entity has formally documented behavioral and ethical standards within its HR Policy and has made the policy accessible to employees via the company intranet.	No exceptions noted.
CC 1.1.2	The Entity has established documented procedures to identify, document, investigate, and address deviations from expected standards of conduct,	**Inquiry:** Inquired of management regarding the process followed to identify, document, investigate, and address employee misconduct	No exceptions noted

	including violations of policies, procedures, and the Code of Ethics.	and deviations from expected standards of conduct, including violations of organizational policies, procedures, and the Code of Ethics. **Inspection:** Inspected the Entity's Human Resource Policy to verify the existence of documented procedures for identifying, documenting, investigating, and addressing deviations from expected standards of conduct. The policy was observed to include a Code of Conduct defining expected employee behavior and ethical standards, disciplinary procedures outlining actions to be taken in response to violations, a Whistle Blower Policy establishing mechanisms for reporting suspected misconduct and unethical behavior, and a Grievance Policy describing the process for raising, investigating, and resolving employee complaints. **Observation:** Observed that the Entity has established documented procedures to identify, document, investigate, and address deviations from expected standards of conduct.	
CC 1.1.3	The Entity requires employees to periodically review and formally acknowledge organizational policies to reinforce expectations for ethical behavior, compliance with policies, and accountability.	**Inquiry:** Inquired of Human Resources regarding the process used to require employees to review organizational policies and formally acknowledge their understanding and acceptance of those policies, including the frequency of such acknowledgments. **Inspection:** Inspected a sample of Employee Acknowledgment for Annual Policy Review evidencing	No exceptions noted

		that an employee reviewed, understood, and acknowledged the Entity's policies. **Observation:** Observed that the Entity requires employees to formally acknowledge review and understanding of organizational policies on a periodic basis.	
CC1.2: COSO Principle 2: The Senior Management demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The Entity's Senior Management reviews and approves all company policies.	**Inquiry**: Inquired with the Information Security team to understand the process for annual policy review and approval. It was confirmed that updated policies are reviewed internally and then submitted for approval to senior management prior to being uploaded on the company intranet. **Inspection**: Inspected a sample of policy documents and noted the version history, including dates of last review and approvals by Senior Management during the audit period. **Observation:** Observed that the annual policy review and approval process is in place, with policies reviewed and approved by Senior Management as evidenced by documented version histories	No exceptions noted
CC1.2.2	The Entity's Senior Management reviews and approves the Organisational Chart for all employees annually.	**Inquiry:** Inquired with the HR regarding how the organization's structure is reviewed and approved. They confirmed that the Organizational Chart is reviewed annually to reflect any changes in reporting lines, leadership, or departmental restructuring and that the updated version is approved by	No exceptions noted

		Senior Management prior to publication. **Inspection:** Inspected the IOSS Organizational Chart, which outlines the reporting hierarchy, roles, and responsibilities across business functions. **Observation:** Observed that the organisational chart is maintained and reflects the current structure of the organization, as made available for internal reference.	
CC1.3: COSO Principle 3: Management establishes, oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The Entity maintains an Organizational Structure to define authorities, facilitate information flow, and establish responsibilities.	**Inquiry**: Inquired with Senior management about how the organizational structure is developed and maintained and confirmed that it is designed to clearly define reporting lines, decision-making authorities, and responsibilities across departments. **Inspection**: Inspected the organizational chart showing hierarchy, reporting relationships, and departmental roles. **Observation:** Observed that the entity maintains an organizational structure that defines reporting lines, decision-making authorities, and departmental responsibilities.	No exceptions noted
CC1.3.2	The Entity defines and documents clear roles and responsibilities for key personnel through formal job descriptions to support operational effectiveness and accountability.	**Inquiry:** Inquired of management and Human Resources regarding how roles and responsibilities are defined for key personnel and how clarity in job responsibilities supports effective execution of operational and strategic objectives.	No exceptions noted

		Inspection: Inspected a few samples of job descriptions for leadership, operational oversight, technology management, financial analysis, and cross-functional coordination, demonstrating that key roles have defined accountability to support effective operations. **Observation:** Observed that job descriptions align with the entity's operational objectives, outlining specific duties and performance expectations to ensure clarity of roles and enhance organizational effectiveness.	
CC1.4: COSO Principle 4: The Entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The Entity defines required qualifications, skills, and responsibilities for key roles to ensure personnel are competent to perform their assigned duties.	**Inquiry:** Inquired of management and Human Resources regarding how roles, responsibilities, and competency expectations are defined for employees, including how required skills and qualifications are established for key roles. **Inspection:** Inspected a sample of Job Descriptions for key roles to verify that positions include defined responsibilities, required qualifications, skills, and role expectations relevant to operational, technical, and governance functions. **Observation:** Observed that the Entity has formally documented job descriptions that define role-specific responsibilities and competency requirements, supporting the assignment of qualified personnel to roles necessary to achieve the Entity's	No exceptions noted

		objectives.	
CC 1.4.2	The Entity communicates expectations regarding professional conduct, compliance, and ethical behavior to support the development and retention of competent personnel.	**Inquiry:** Inquired of management and Human Resources regarding how expectations for professional conduct, ethical behavior, and compliance are defined and communicated to employees. **Inspection:** Inspected the Entity's Human Resource Policy to verify that expectations related to professional conduct, ethical behavior, compliance with organizational policies, disciplinary actions, grievance handling, and whistleblower reporting are formally documented and applicable to all employees. **Observation:** Observed that the Entity has established documented expectations for professional conduct and ethical behavior within its HR Policy and has communicated these expectations to employees through formally approved documentation.	No exceptions noted
CC1.5: COSO Principle 5:The Entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The Entity defines roles, responsibilities, and expectations for internal control activities and holds personnel accountable through documented policies, job responsibilities, and disciplinary procedures.	**Inquiry:** Inquired of management and Human Resources regarding how roles, responsibilities, and expectations related to internal control activities are defined and how personnel are held accountable for fulfilling those responsibilities. **Inspection:** Inspected a sample of job descriptions to verify that roles and responsibilities for key functions are formally defined and aligned with operational and	No exceptions noted

		control-related expectations. Additionally, inspected the Human Resource Policy to verify that accountability mechanisms, including disciplinary procedures and consequences for non-compliance with policies and expected conduct, are documented and applicable to employees. **Observation:** Observed that the Entity defines roles, responsibilities, and expectations for internal control activities through documented job responsibilities and enforces accountability through formally established HR policies and disciplinary procedures.	
CC 1.5.2	The Entity establishes and maintains a structured compliance and role-based training program to ensure that employees receive onboarding and periodic training on internal policies, procedures, and role-specific responsibilities relevant to their job functions.	**Inquiry:** Inquired of management and Human Resources regarding the Entity's employee training program, including how onboarding training, role-specific training, and ongoing learning activities are planned, delivered, and tracked to ensure employees understand applicable internal policies, procedures, and job responsibilities. **Inspection:** Inspected the Entity's documented training artifacts, including the formal Training Plan, employee onboarding materials, role-based training schedules, and training records, to verify that a structured compliance and role-specific training program has been established and implemented. The inspection included review of onboarding documentation outlining training timelines, policy awareness sessions, system and tool	No exceptions noted

		training, and role-specific responsibilities, as well as evidence of periodic training sessions tailored to different business functions such as development, operations, and administrative roles. **Observation:** Observed that the Entity has implemented a comprehensive training framework that includes formal onboarding, role-specific instructional sessions, hands-on practice, assessments, and periodic reviews.	
CC 1.5.3	The Entity has established a formal performance evaluation process to assess employee performance against defined roles, responsibilities, and behavioral expectations, and to support accountability and ongoing professional development.	**Inquiry:** Inquired of management and Human Resources regarding the Entity's process for evaluating employee performance, including how performance criteria are defined, assessed, reviewed, and documented. **Inspection:** Inspected a sample of Performance Evaluation Form to verify that the Entity has implemented a structured performance assessment process. The inspection included review of evaluation criteria covering job knowledge, quality and quantity of work, task execution, punctuality, reliability, initiative, judgment, cooperation, and attendance; the defined rating scale; employee self-assessment sections; supervisor assessment sections; and areas for professional development and improvement. The form also evidences supervisory review and HR involvement, demonstrating that employee performance is formally evaluated and documented on a periodic basis.	No exceptions noted

		Observation: Observed that the Entity performs formal, documented performance evaluations using standardized criteria and rating scales, with both employee and supervisor input, to assess performance against defined responsibilities and support accountability and professional development.	

CC2.0: COMMUNICATION AND INFORMATION		**Test Of Controls**	**Results**
CC2.1: COSO Principle 13: The Entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC 2.1.1	The Entity generates and uses system and security monitoring information to support decision-making related to internal controls.	**Inquiry:** Inquired of the IT Infrastructure and Security teams to understand the mechanisms for collecting and utilizing system performance and security data. Personnel confirmed that AWS CloudWatch is the primary tool used to aggregate real-time metrics and logs from the production environment. They explained that this data is reviewed to identify operational anomalies, assess system health, and inform capacity planning or security hardening decisions. **Inspection:** Inspected the AWS CloudWatch management console dashboards to verify the generation and availability of system and security-relevant information. The inspection confirmed that the Entity has configured automated monitoring for its cloud infrastructure, specifically tracking key performance and health indicators across multiple instance IDs. Evidence showed active data visualization for CPU Utilization, Network throughput, and Disk activity. The dashboard	No exceptions noted

		was observed to provide real-time and historical telemetry, with integrated visual indicators for alarm status to facilitate rapid identification of system anomalies. **Observation:** Observed that the entity has an established automated monitoring framework within the AWS environment.	
CC 2.1.2	The Entity displays the most current information about its services on its website, which is accessible to its customers.	**Inquiry:** Inquired with the marketing and team to understand the process followed for updating service-related content on the website. **Inspection:** Inspected the entity's website to verify that service-related information, product descriptions, and feature updates are current and accurately described. **Observation:** Observed that the entity maintains an accessible and updated website that provides customers with relevant and accurate service information.	No exceptions noted
CC 2.2: COSO Principle 14: The Entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC 2.2.1	The Entity communicates expectations regarding professional conduct, compliance, and ethical behavior to support the development and retention of competent personnel.	**Inquiry:** Inquired of management and Human Resources regarding how expectations for professional conduct, ethical behavior, and compliance are defined and communicated to employees. **Inspection:** Inspected the Entity's Human Resource Policy to verify that expectations related to professional conduct, ethical behavior, compliance with organizational policies, disciplinary actions, grievance handling, and whistleblower	No exceptions noted

		reporting are formally documented and applicable to all employees. **Observation:** Observed that the Entity has established documented expectations for professional conduct and ethical behavior within its HR Policy and has communicated these expectations to employees through formally approved documentation.	
CC 2.2.2	The Entity makes all policies and procedures available to all staff members via the company intranet.	**Inquiry**: Inquired with the HR to confirm that all company policies and procedures are hosted on the internal intranet, and that employees are notified and required to access and review them. **Inspection**: Inspected the policy and procedure repository on the company intranet to confirm the availability of current policy documents. **Observation**: Observed a demonstration of the intranet policy repository and confirmed that employees have access to relevant policies.	No exceptions noted
CC 2.2.3	The Entity has documented and communicated procedures to employees on how to report information security incidents, system failures, and security concerns through a formal incident management process.	**Inquiry:** Inquired of the Information Security and IT teams regarding how employees are informed of the process for reporting information security incidents, system failures, or security concerns, including the channels available for incident reporting. **Inspection:** Inspected the Security Incident Management Policy to verify that it defines procedures for identifying and reporting information security	No exceptions noted

		incidents, including employee responsibilities, reporting channels through the IT Help Desk, escalation to the Information Security Officer, incident categorization, and communication requirements. **Observation:** Observed that the Entity has formally documented and communicated incident reporting procedures that provide employees with guidance on how to report information security incidents, system failures, and security concerns.	
CC2.3: COSO Principle 15: The Entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The Entity displays the most current information about its services on its website, which is accessible to its customers.	**Inquiry**: Inquired with the Marketing to understand the process for reviewing and updating information on the website, including frequency of updates, responsible roles, and approval workflows. **Inspection**: Inspected evidence of website content reviews, including the latest version of the service description pages showing recent updates or approvals, to confirm that website content was reviewed and maintained during the audit period. **Observation**: Observed the entity's public-facing website and confirmed that the published service information was accurate and reflected the latest internal documentation and offerings.	No exceptions noted
CC 2.3.2	The Entity provides customers with documented and accessible communication channels to report service-related issues, incidents, concerns, or complaints	**Inquiry:** Inquired of the Customer Support and Operations management regarding the availability and documentation of communication channels for	No exceptions noted

	related to the systems and services provided by the Entity.	external stakeholders. Management confirmed that the Entity maintains multiple dedicated channels including email, telephone, and web-based intake forms to ensure customers can report service-related issues, security concerns, or general complaints. These channels are documented on the public-facing website to ensure high accessibility. **Inspection:** Inspected the Entity's official "Contact Us" web pages and support documentation to verify the availability of public-facing communication channels for reporting service-related issues and concerns. The inspection confirmed that the Entity provides multiple accessible pathways, including a dedicated support email address (support@ioss.in) and specific telephonic contact lines. **Observation:** Observed that the Entity provides clear, multi-modal communication pathways that are easily accessible to customers.	

CC3.0: RISK ASSESSMENT		Test Of Controls	Results
CC3.1: COSO Principle 6: The Entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The Entity performs a formal risk assessment exercise annually, as detailed in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	**Inquiry:** Inquired with the Senior Manager about the Inquired with the risk management and information security teams about the frequency, ownership, and scope of the formal risk assessment process. **Inspection:** Inspected the Risk Management Policy and Risk	No exceptions noted

		Assessment Methodology to confirm that the entity has defined procedures for identifying, evaluating, and prioritizing risks based on likelihood and impact. **Observation:** Observed that the entity conducts a formal annual risk assessment exercise, with clearly defined procedures for identifying, evaluating, and prioritizing risks based on likelihood and impact, as evidenced by the Risk Management Policy, Risk Assessment Methodology, and confirmations from risk management and information security teams.	
CC3.1.2	The Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	**Inquiry:** Inquired with the Information Security Officer and Risk Management team regarding the frequency and process of conducting formal risk assessments. They confirmed that a comprehensive risk assessment exercise is conducted annually, as mandated by the Information Risk Management Policy. The assessment involves identifying potential threats and vulnerabilities across infrastructure, data, and business processes, evaluating their likelihood and impact, and documenting results within the Risk Register. **Inspection:** Inspected the Information Risk Management Policy, which outlines the formal procedure for conducting risk assessments, including steps for risk identification, evaluation, treatment, and review. The policy mandates that the assessment be	No exceptions noted

		carried out at least annually and upon any significant change to the organization's systems, processes, or infrastructure. Reviewed the Risk Register, which includes distinct sections for Risk Identification, Risk Assessment, Risk Treatment, and Risk Review. Each record specifies risk details such as the risk name, source, likelihood, impact, risk rating, existing controls, treatment plan, residual risk, risk owner, and review date. **Observation:** Observed that the entity performs a structured and documented risk assessment process annually, as evidenced by the Risk Register and the supporting Risk Management Policy.	
CC3.2: COSO Principle 7: The Entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	**Inquiry:** Inquired with the Information Security Officer and Risk Management team regarding the frequency and process of conducting formal risk assessments. They confirmed that a comprehensive risk assessment exercise is conducted annually, as mandated by the Information Risk Management Policy. The assessment involves identifying potential threats and vulnerabilities across infrastructure, data, and business processes, evaluating their likelihood and impact, and documenting results within the Risk Register. **Inspection:** Inspected the Information Risk Management Policy, which outlines the formal procedure for conducting risk assessments, including steps for	No exceptions noted

		risk identification, evaluation, treatment, and review. The policy mandates that the assessment be carried out at least annually and upon any significant change to the organization's systems, processes, or infrastructure. Reviewed the Risk Register, which includes distinct sections for Risk Identification, Risk Assessment, Risk Treatment, and Risk Review. Each record specifies risk details such as the risk name, source, likelihood, impact, risk rating, existing controls, treatment plan, residual risk, risk owner, and review date. **Observation:** Observed that the entity performs a structured and documented risk assessment process annually, as evidenced by the Risk Register and the supporting Risk Management Policy.	
CC3.2.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	**Inquiry:** Inquired with the senior management team to understand how risks are scored, how likelihood and impact are determined, and how mitigation strategies are associated with each identified risk. **Inspection:** Inspected the Risk Management Policy and risk assessment methodology to confirm that they define a standardized approach for evaluating risks. Reviewed the Risk Register to verify that risks were assigned scores based on likelihood and impact, and that each risk was mapped to documented mitigating controls or treatment plans. **Observation:** Observed that each risk is assessed using a	No exceptions noted

		standardized approach defined in the Risk Assessment Methodology, with risk scores assigned based on likelihood and impact, and corresponding mitigating controls or treatment plans documented in the Risk Register.	
CC3.3: COSO Principle 8: The Entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The Entity considers fraud risks as part of its overall risk assessment process to identify and evaluate risks that could adversely impact the achievement of security, availability, and confidentiality objectives.	**Inquiry**: Inquired of management regarding how fraud risks are considered within the Entity's risk assessment process, including whether potential fraudulent activities are evaluated when identifying risks that could impact system security, availability, or confidentiality. **Inspection**: Inspected the Entity's risk assessment documentation and risk register to verify that the risk assessment process includes documented risk register entries related to potential fraudulent or malicious activities, and that such risks are identified and evaluated for their potential impact on the achievement of security, availability, and confidentiality objectives. **Observation:** Observed that the Entity's risk assessment process incorporates consideration of fraud-related risks as part of the overall evaluation of risks to security, availability, and confidentiality objectives.	No exceptions noted
CC3.4: COSO Principle 9: The Entity identifies and assesses changes that could significantly impact the system of internal control.			

CC3.4.1	The Entity performs a formal risk assessment exercise annually, as detailed in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	**Inquiry:** Inquired with the Senior Manager about the Inquired with the risk management and information security teams about the frequency, ownership, and scope of the formal risk assessment process. **Inspection:** Inspected the Risk Management Policy and Risk Assessment Methodology to confirm that the entity has defined procedures for identifying, evaluating, and prioritizing risks based on likelihood and impact. **Observation:** Observed that the entity conducts a formal annual risk assessment exercise, with clearly defined procedures for identifying, evaluating, and prioritizing risks based on likelihood and impact, as evidenced by the Risk Management Policy, Risk Assessment Methodology, and confirmations from risk management and information security teams.	No exceptions noted
CC3.4.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	**Inquiry:** Inquired with the senior management team to understand how risks are scored, how likelihood and impact are determined, and how mitigation strategies are associated with each identified risk. **Inspection:** Inspected the Risk Management Policy and risk assessment methodology to confirm that they define a standardized approach for evaluating risks. Reviewed the Risk Register to verify that risks were assigned scores based on likelihood and impact, and that	No exceptions noted

		each risk was mapped to documented mitigating controls or treatment plans. **Observation:** Observed that each risk is assessed using a standardized approach defined in the Risk Assessment Methodology, with risk scores assigned based on likelihood and impact, and corresponding mitigating controls or treatment plans documented in the Risk Register.	

CC4.0: MONITORING ACTIVITIES		Test Of Controls	Results
CC4.1: COSO Principle 16: The Entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The Entity maintains an inventory of information assets to ensure that infrastructure and software assets are identified, recorded, and tracked for appropriate management and protection.	**Inquiry:** Inquired of the IT and Operations teams regarding how information assets, including infrastructure and software assets, are identified, documented, and maintained to support effective asset management and security. **Inspection:** Inspected the Information Asset Register to verify that infrastructure and software assets are documented and tracked, including details such as asset name, asset type, ownership, usage, and status, supporting the identification and management of assets within the entity's environment. **Observation:** Observed that the Entity maintains a structured inventory of its information assets.	No exceptions noted

CC4.1.2	The Entity uses continuous monitoring tools to track the operational health and security-relevant conditions of its information systems.	**Inquiry:** Inquired of the Information Security and DevOps teams to determine how the Entity monitors the continuous operational health and security posture of its information systems. Personnel confirmed that AWS CloudWatch is utilized as a centralized monitoring platform to aggregate telemetry data from the cloud infrastructure. **Inspection:** Inspected the AWS CloudWatch management console to verify that the Entity utilizes automated tools for the continuous monitoring of its information systems. The inspection confirmed that the dashboard is configured to aggregate and visualize real-time telemetry data for critical performance and security-relevant metrics, including CPU Utilization, Disk Activity (Read/Write Bytes and Operations), and Network Traffic (In/Out and Packets). Furthermore, the inspection verified that the monitoring environment includes status indicators for system alarms, which are designed to track the operational health and integrity of the cloud infrastructure. **Observation:** Observed that the Entity maintains an automated and continuous monitoring environment through AWS CloudWatch.	No exceptions noted
CC4.1.3	The Entity's Senior Management reviews and approves the Organisational Chart for all employees.	**Inquiry:** Inquired with the HR regarding how the organization's structure is reviewed and approved. They confirmed that the Organizational Chart is reviewed annually to reflect any changes in reporting lines,	No exceptions noted

		leadership, or departmental restructuring and that the updated version is approved by the Senior Management prior to publication. **Inspection:** Inspected the IOSS's Organizational Chart, which outlines the reporting hierarchy, roles, and responsibilities across business functions. **Observation:** Observed that the organisational chart is maintained and reflects the current structure of the organization, as made available for internal reference.	
CC4.2: COSO Principle 17: The Entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management as appropriate.			
CC4.2.1	The Entity has documented and communicated procedures to employees on how to report information security incidents, system failures, and security concerns through a formal incident management process.	**Inquiry:** Inquired of the Information Security and IT teams regarding how employees are informed of the process for reporting information security incidents, system failures, or security concerns, including the channels available for incident reporting. **Inspection:** Inspected the Security Incident Management Policy to verify that it defines procedures for identifying and reporting information security incidents, including employee responsibilities, reporting channels through the IT Help Desk, escalation to the Information Security Officer, incident categorization, and communication requirements. **Observation:** Observed that the Entity has formally documented and communicated incident reporting procedures that provide	No exceptions noted

		employees with guidance on how to report information security incidents, system failures, and security concerns.	
CC4.2.2	The Entity uses continuous monitoring tools to track the operational health and security-relevant conditions of its information systems.	**Inquiry:** Inquired of the Information Security and DevOps teams to determine how the Entity monitors the continuous operational health and security posture of its information systems. Personnel confirmed that AWS CloudWatch is utilized as a centralized monitoring platform to aggregate telemetry data from the cloud infrastructure. **Inspection:** Inspected the AWS CloudWatch management console to verify that the Entity utilizes automated tools for the continuous monitoring of its information systems. The inspection confirmed that the dashboard is configured to aggregate and visualize real-time telemetry data for critical performance and security-relevant metrics, including CPU Utilization, Disk Activity (Read/Write Bytes and Operations), and Network Traffic (In/Out and Packets). Furthermore, the inspection verified that the monitoring environment includes status indicators for system alarms, which are designed to track the operational health and integrity of the cloud infrastructure. **Observation:** Observed that the Entity maintains an automated and continuous monitoring environment through AWS CloudWatch.	No exceptions noted
CC4.2.3	The Entity's Senior Management reviews and approves all company	**Inquiry**: Inquired with the Information Security team to	No exceptions noted

	policies.	understand the process for annual policy review and approval. It was confirmed that updated policies are reviewed internally and then submitted for approval to senior management prior to being uploaded on the company intranet. **Inspection**: Inspected a sample of policy documents and noted the version history, including dates of last review and approvals by Senior Management during the audit period. **Observation:** Observed that the annual policy review and approval process is in place, with policies reviewed and approved by Senior Management as evidenced by documented version histories	

CC5.0: CONTROL ACTIVITIES		Test Of Controls	Results
CC5.1: COSO Principle 10: The Entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	**Inquiry**: Inquired of management regarding the policies established by the Entity to define expected behavior, ethical standards, and control responsibilities, and how these policies support the overall control environment. **Inspection:** Inspected a set of approved organizational policies, including information security, access control, endpoint security, incident response, and related policies, to verify that they define expected behavior, roles and responsibilities, enforcement mechanisms, and compliance expectations intended to support the Entity's control environment.	No Exceptions Noted

		Observation: Observed that the Entity has formally documented and approved a set of policies that establish expected standards of behavior, accountability, and control responsibilities.	
CC5.1.2	The Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	**Inquiry:** Inquired with Human Resources and department heads to understand how responsibilities are segregated across functional roles. **Inspection:** Inspected the organizational chart, role-specific job descriptions, and the role-based matrix to verify that duties are clearly assigned and distributed in a manner that prevents conflicting responsibilities. **Observation:** Observed that roles and responsibilities are formally defined and distributed across individuals and functions, as reflected in the organizational chart, job descriptions, and role-based access matrix.	No exceptions noted
CC5.1.3	The Entity has a documented Acceptable Usage Policy and makes it available for all staff on the company intranet.	**Inquiry**: Inquired with the HR team to understand how the Acceptable Usage Policy is communicated to employees. **Inspection**: Inspected the Acceptable Usage Policy to verify that it defines expected behavior regarding the use of corporate systems. **Observation**: Observed the location of the AUP on the company intranet and confirmed that it is accessible to all staff.	No exceptions noted
CC5.2: COSO Principle 11: The Entity also selects and develops general control activities over technology to support the achievement of objectives.			

CC5.2.1	The Entity implements monitoring controls to identify system events and conditions that could affect the achievement of objectives.	**Inquiry:** Inquired of the IT Operations team regarding the monitoring tools and alerting mechanisms used to identify system errors, performance issues, and anomalous conditions. **Inspection:** Inspected AWS CloudWatch monitoring dashboards to verify that infrastructure and application components hosted in the cloud environment are continuously monitored. This included a review of CloudWatch dashboards displaying metrics related to application errors, resource utilization, and system health, as well as an inspection of associated CloudWatch alarm configurations to confirm that alerts are generated when predefined thresholds are exceeded. **Observation:** Observed that the Entity has implemented monitoring and alerting controls that provide visibility into system conditions and events, supporting timely identification of issues that could impact system objectives.	No exceptions noted
CC5.2.2	The Entity selects and implements logical access controls over systems and applications to restrict access to authorized users.	**Inquiry:** Inquired of the Information Security and IT teams regarding how access to systems and applications is restricted to authorized users, including authentication requirements and access authorization principles. **Inspection:** Inspected the approved Access Control Policy to verify that it formally defines requirements for user registration, authentication, authorization, role-based access, access provisioning and de-provisioning, periodic access reviews, and enforcement of the principle of	No exceptions noted

		least privilege. Additionally, inspected multi-factor authentication (MFA) configuration evidence to confirm that MFA is enabled and enforced for access to critical systems. Further inspected supporting access control documentation to verify that access rights are granted only to registered and authorized users and that access control requirements are documented and governed through formally approved policies. **Observation:** Observed that the Entity has implemented documented logical access control requirements, including authentication and authorization mechanisms, to restrict system access to authorized users in support of its control objectives.	
CC5.2.3	The Entity's Senior Management reviews and approves the Organisational Chart for all employees.	**Inquiry:** Inquired with the HR regarding how the organization's structure is reviewed and approved. They confirmed that the Organizational Chart is reviewed annually to reflect any changes in reporting lines, leadership, or departmental restructuring and that the updated version is approved by the Head of HR and Senior Management prior to publication. **Inspection:** Inspected the IOSS's Organizational Chart, which outlines the reporting hierarchy, roles, and responsibilities across business functions. **Observation:** Observed that the organisational chart is maintained and reflects the current structure of the organization, as made available for internal reference.	No exceptions noted

CC5.2.4	The Entity's Senior Management reviews and approves the Risk Assessment Report annually.	**Inquiry:** Inquired with the Information security and Senior Management teams regarding the process for performing, reviewing, and approving the organization's annual risk assessment. They confirmed that a comprehensive risk assessment is conducted annually to identify, analyze, and evaluate operational, information security, and compliance-related risks. **Inspection:** Inspected the Risk Register, which contained detailed entries under sections such as Risk Identification, Risk Assessment, Risk Treatment, and Risk Review. Each record listed the Risk ID, Date Identified, Risk Name, Details, Likelihood (L), Impact (I), Risk Rating, Controls in Place, Treatment Plan, Residual Risk, Risk Owner, Status, and Review Date. The register was updated, demonstrating that the entity actively tracks risks and mitigation actions. The metadata within the document showed review and update activity consistent with the annual review process. **Observation**: Observed that the risk assessment process is documented and reviewed at least once annually by Senior Management.	No exceptions noted
CC5.3: COSO Principle 12: The Entity deploys control activities through policies that establish what is expected and in procedures that put policies into action			
CC5.3.1	The Entity makes all policies and procedures available to all staff members via the company intranet.	**Inquiry**: Inquired with the HR to confirm that all company policies and procedures are hosted on the internal intranet, and that employees are notified and required to access and review them.	No exceptions noted

		Inspection: Inspected the policy and procedure repository on the company intranet to confirm the availability of current policy documents. Reviewed intranet access logs and a sample of employee acknowledgment forms to verify that employees accessed and acknowledged the policies. **Observation**: Observed a demonstration of the intranet policy repository and confirmed that employees have access to relevant policies and that the system tracks acknowledgment activity.	
CC5.3.2	The Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	**Inquiry:** Inquired with the Information Security and IT teams to understand the process for developing, reviewing, and disseminating core policies that support the company's control environment. **Inspection:** Inspected a sample of policies to confirm they are documented, version-controlled, and aligned with organizational objectives. Verified that each policy was approved by authorized personnel and reflects current practices and control requirements. **Observation:** Observed the central policy repository (intranet) and confirmed that all listed policies were accessible to appropriate employees. They included revision history, approval records, and assigned ownership.	No exceptions noted

CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS		Test Of Controls	Results
CC6.1: The Entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	The Entity has developed and approved an Access Control Policy that defines requirements for user provisioning and de-provisioning to ensure that only authorized users are registered and granted access credentials, and that access is modified or revoked upon role change or separation.	**Inquiry:** Inquired of the Information Security and IT teams regarding how user access to systems and applications is governed, including the processes for user registration, authorization, access modification, and de-registration. **Inspection:** Inspected the approved Access Control Policy to verify that it defines requirements for user provisioning and de-provisioning, including management authorization prior to granting access, role-based access assignment, periodic access reviews, and the timely removal of user access upon termination or role change **Observation:** Observed that the Entity has formally documented and approved an Access Control Policy that establishes governance over user access lifecycle activities, including authorization, provisioning, modification, and de-registration, supporting the restriction of system access to authorized users in alignment with the principle of least privilege during the period under review.	No exceptions noted
CC6.1.2	The entity maintains a role-based access control (RBAC) matrix that maps staff roles to their corresponding system permissions, ensuring that access to system components is restricted to authorized personnel based on job responsibilities.	**Inquiry:** Inquired with the Human Resources and IT Security team regarding how role-based access is defined and maintained across the organization. Confirmed that an access control matrix is maintained, which defines system access entitlements based on job	No exceptions noted

		roles and responsibilities. Role changes are reviewed and updated within the HR and IT systems to align with the access requirements of the new designation. **Inspection**: Inspected the Role Access Matrix, which maps specific user roles to system permissions, confirming that access entitlements are documented and segregated by role. Reviewed role change records and employment history in the HR system, which showed changes in designations along with effective dates and approval details. Verified that updates to employee roles are reflected in the access matrix and provisioning process. **Observation:** Observed that the access control matrix is formally maintained and that role-to-permission mapping is consistently enforced.	
CC 6.1.3	The Entity maintains an inventory of information assets to ensure that infrastructure and software assets are identified, recorded, and tracked for appropriate management and protection.	**Inquiry:** Inquired of the IT and Operations teams regarding how information assets, including infrastructure and software assets, are identified, documented, and maintained to support effective asset management and security. **Inspection:** Inspected the Information Asset Register to verify that infrastructure and software assets are documented and tracked, including details such as asset name, asset type, ownership, usage, and status, supporting the identification and management of assets within the entity's environment. **Observation:** Observed that the Entity maintains a structured inventory of its information assets.	No exceptions noted

CC 6.1.4	The entity has implemented logical network security controls within its cloud-based architecture to restrict unauthorized access to production systems, including the use of managed cloud services, secure network boundaries, encrypted communications, and token-based authentication mechanisms.	**Inquiry:** Inquired of the IT and engineering teams regarding the logical network security controls implemented within the cloud environment to restrict unauthorized access to production systems, including the use of managed cloud services, secure communication channels, and authentication mechanisms **Inspection:** Inspected the entity's logical network architecture documentation to verify that production systems are hosted within a cloud-based environment utilizing managed services, including API Gateway and serverless backend components, with encrypted communications (HTTPS/TLS) between clients and backend services, controlled access paths, and token-based authentication mechanisms for interactions with internal and external services. **Observation:** Observed that the entity's production environment is architected using managed cloud services with defined network boundaries, encrypted communication channels, and authentication controls.	No exceptions noted
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized			
C6.2.1	The Entity has established and approved an Access Control Policy that defines requirements for granting, modifying, reviewing, and removing system credentials and access rights to ensure access is restricted to authorized users based on roles and responsibilities.	**Inquiry:** Inquired of the Information Security and IT teams regarding how access to systems and information assets is governed, including how access requirements, authorization principles, and user responsibilities are documented and enforced through policy.	No exceptions noted

		Inspection: Inspected the approved Access Control Policy to verify that it defines access control requirements, including user registration and de-registration, role-based authorization, privilege management, access reviews, password management, segregation of duties considerations, and enforcement mechanisms. **Observation:** Observed that the Entity has formally documented and approved an Access Control Policy that establishes governance over system credentials and access rights.	
CC6.2.2	The Entity maintains a role-based access control matrix that defines system access entitlements for each user role, ensuring that access to information systems and resources is granted strictly based on job function and business need.	**Inquiry:** Inquired with the Information Security Officer and System Administrators regarding how access rights are determined and maintained. Confirmed that access entitlements are defined according to job responsibilities and documented within a Role Access Matrix, which is reviewed periodically to ensure accuracy and alignment with organizational roles. **Inspection**: Inspected the Role Access Matrix and verified that it documents user roles and corresponding system access permissions across critical applications and infrastructure. Reviewed the Access Control Policy to confirm that it establishes the principle of least privilege and mandates the maintenance of a formal access entitlement matrix. Confirmed that access entitlements for various functional roles are mapped to the systems and data required to perform their designated duties.	No exceptions noted

		Observation: Observed that access privileges are formally defined and documented based on user roles, ensuring appropriate segregation of duties and adherence to the least-privilege principle.	
CC6.3: The Entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	The Entity maintains a role-based access control matrix that defines system access entitlements for each user role, ensuring that access to information systems and resources is granted strictly based on job function and business need.	**Inquiry:** Inquired with the Information Security Officer and System Administrators regarding how access rights are determined and maintained. Confirmed that access entitlements are defined according to job responsibilities and documented within a Role Access Matrix, which is reviewed periodically to ensure accuracy and alignment with organizational roles. **Inspection**: Inspected the Role Access Matrix and verified that it documents user roles and corresponding system access permissions across critical applications and infrastructure. Reviewed the Access Control Policy to confirm that it establishes the principle of least privilege and mandates the maintenance of a formal access entitlement matrix. Confirmed that access entitlements for various functional roles are mapped to the systems and data required to perform their designated duties. **Observation:** Observed that access privileges are formally defined and documented based on user roles, ensuring appropriate segregation of duties and adherence to the least-privilege principle.	No exceptions noted

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC 6.4.1	The Entity restricts physical access to office facilities and areas housing information assets by implementing access card–based entry controls, CCTV surveillance, and on-site physical security measures. The Entity also maintains fire safety equipment to protect facilities and physical assets from damage or disruption.	**Inquiry:** Inquired of Facilities Management and Administration regarding the physical security controls in place to restrict access to office facilities, including the use of access cards, CCTV monitoring, and fire safety equipment. **Inspection:** Inspected physical access control mechanisms, including access card systems at facility entry points, CCTV camera installations and monitoring areas, and the presence of fire extinguishers within the office premises. **Observation:** Observed that access to office facilities is restricted to authorized personnel through access cards, CCTV surveillance is in place to monitor facility entry and activity, and fire safety equipment is installed to protect physical assets.	No exceptions noted
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC 6.5.1	The Entity establishes and maintains a formal policy for the secure decommissioning and disposal of information assets containing classified information to prevent unauthorized access and data exposure.	**Inquiry:** Inquired of the Information Security and IT teams regarding the procedures for decommissioning assets that store classified data. Personnel confirmed that a formal Media Disposal Policy is in place to guide the secure destruction or sanitization of both physical and electronic media. **Inspection:** Inspected the Entity's formal Media Disposal Policy to verify that documented guidance is provided for the secure decommissioning of information	No exceptions noted

		assets containing classified data. The inspection confirmed that the policy establishes a comprehensive framework for identifying, classifying, and disposing of various media types, including digital storage devices, physical documents, and mobile hardware. Specifically, the policy mandates the use of secure disposal methods such as physical destruction (degaussing or crushing) or certified data wiping for electronic media, and cross-cut shredding for physical records. **Observation:** Observed that the Entity provides clear, documented guidance for the decommissioning of information assets through its formal policy framework.	
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The Entity enforces multi-factor authentication (MFA) for personnel accessing critical information systems to strengthen authentication and protect against unauthorized access to sensitive data.	**Inquiry:** Inquired of the IT and Information Security teams regarding the authentication requirements for accessing critical development and production environments. Personnel confirmed that multi-factor authentication (MFA) is a mandatory security requirement for all staff members accessing the systems. **Inspection:** Inspected a sample of user account security configuration settings to verify the implementation of multi-factor authentication (MFA) for staff members accessing critical information systems. **Observation:** Observed that the Entity has successfully implemented and enforced multi-factor authentication for its critical systems during the period under review.	No exceptions noted

CC6.6.2	The Entity has a documented Endpoint Security Policy and makes it available for all staff on the company intranet.	**Inquiry:** Inquired of the IT Security team regarding the entity's endpoint security governance, including how endpoint security requirements are documented and communicated to personnel. **Inspection:** Inspected the approved Endpoint Security Policy to verify that it defines endpoint security requirements, including antivirus and anti-malware controls, firewall usage, encryption requirements, access controls, patch management, incident reporting, and enforcement provisions **Observation:** Observed that the entity has formally documented and approved an Endpoint Security Policy that establishes security requirements and responsibilities for protecting endpoints, supporting the entity's objective to safeguard information assets during the period under review.	No exceptions noted
CC 6.6.3	The Entity enforces security configurations on all company-owned endpoints, including an automated screen lock after a defined period of inactivity, to protect against unauthorized physical access to sensitive information.	**Inquiry:** Inquired of the IT Operations and Information Security teams regarding the baseline security configurations for employee workstations and laptops. Personnel confirmed that all company-owned endpoints are required to have an automated screen lock enabled. **Inspection:** Inspected a sample of system configuration profiles and security settings on company-owned endpoints to verify the implementation of automated screen lock requirements. The inspection confirmed that devices are configured with a mandatory inactivity timeout set to 5 minutes,	No exceptions noted

		after which the system automatically initiates a screen lock. Furthermore, it was verified that the configuration requires valid user credentials to regain access, effectively preventing unauthorized use of unattended workstations. **Observation:** Observed that the Entity has successfully operationalized the inactivity timeout control across its endpoint fleet.	
CC6.7: The Entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Information transmitted between users, endpoints, and application components is protected through encryption in transit and device-level security controls, and access is restricted to authorized users and processes.	**Inquiry:** Inquired of the IT and Engineering teams regarding how information is protected during transmission and how access to systems and data is restricted to authorized users, including the use of device security controls, and authentication mechanisms. **Inspection:** Inspected TLS Certification and HTTPS Enforcement evidence to confirm that application endpoints are configured to enforce encrypted communication over HTTPS. Inspected Multi-Factor Authentication (MFA) configuration evidence to confirm that access to the entity's systems requires multi-factor authentication for authorized users. **Observation:** Observed that the entity has implemented technical controls to protect information during transmission and on user devices.	No exceptions noted

CC6.7.2	The Entity secures user access to the application by enforcing HTTPS and leveraging Transport Layer Security (TLS) encryption to protect the confidentiality and integrity of data in transit between users and the application.	**Inquiry:** Inquired of the Security and DevOps teams regarding the protocols used to secure data transmitted over public networks. Personnel confirmed that all external access to the entity's application is restricted to HTTPS. They stated that the environment is configured to reject non-encrypted HTTP connections and utilizes industry-standard TLS encryption to protect user sessions and sensitive data from interception or tampering. **Inspection:** Inspected the application's transport layer configurations and certificate management interface to verify that user access is secured through encrypted communication channels. The inspection confirmed that the Entity has implemented SSL/TLS certificates issued by a recognized Certificate Authority to enable HTTPS across all public-facing application endpoints. **Observation:** Observed that the Entity has successfully implemented encryption for data in transit.	No exceptions noted
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The Entity implements network-level security controls, including automated threat protection and intrusion prevention systems, to prevent, detect, and respond to the introduction of unauthorized or malicious software.	**Inquiry:** Inquired of the Information Security and IT Infrastructure teams regarding the technical controls used to secure the network perimeter. Personnel confirmed that a centralized network security platform is utilized to provide multi-layered defense. **Inspection:** Inspected the Sophos Network Security "Control Center" dashboard to verify the	No exceptions noted

		implementation of technical controls designed to prevent and detect unauthorized or malicious software. The inspection confirmed that the Entity utilizes a centralized security platform that integrates intrusion prevention, zero-day protection, and application-level filtering. Verification of the dashboard interface showed active monitoring for network attacks and zero-day incidents, as well as the categorization and blocking of unauthorized application types. **Observation:** Observed that the Entity maintains a robust network security posture through the use of an integrated firewall and threat management system.	

CC7.0: SYSTEM OPERATIONS		Test Of Controls	Results
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The Entity establishes, documents, and implements secure configuration standards for IT assets, leveraging industry best practices and automated monitoring to maintain a hardened system environment.	**Inquiry:** Inquired of the IT Infrastructure and Information Security teams regarding the process for hardening systems and maintaining configuration standards. Personnel confirmed that the Entity has established a formal Configuration Management Policy that mandates the use of standard, secure templates for all hardware, software, and network services. **Inspection:** Inspected the Entity's formal Configuration Management Policy and relevant enterprise management tool configurations to verify the implementation of system hardening standards. The inspection confirmed that the Entity has established a comprehensive policy framework that mandates the use of pre-defined, secure configuration templates incorporating industry-standard hardening benchmarks like CIS for all hardware, software, and networks prior to production deployment. **Observation:** Observed that the Entity has operationalized a structured configuration management framework.	No exceptions noted
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	The Entity has defined and implemented detection policies,	**Inquiry:** Inquired of the Information Security and IT	No exceptions noted

	procedures, and automated tools across its infrastructure to identify potential intrusions, unauthorized access, and system anomalies.	Operations teams regarding the strategy for detecting security incidents and anomalies. Personnel confirmed that the Entity maintains formal policies, such as the Configuration Management Policy, which establish the requirement for continuous monitoring of information technology assets. **Inspection:** Inspected the Entity's formal Configuration Management Policy to verify the implementation of detection tools and procedures. The inspection confirmed that the Entity's policy framework mandates the continuous monitoring of IT assets to prevent and detect unauthorized or incorrect changes. Technical verification showed that AWS CloudWatch is actively used to track infrastructure-level metrics such as network traffic spikes and processing anomalies that may indicate an intrusion. Simultaneously, the inspection of GitHub/GitLab groups and project settings confirmed that the system is used to identify inappropriate access or unauthorized modifications to the codebase through centralized visibility of user roles and repository activity. **Observation:** Observed that the Entity has successfully implemented detection capabilities across both its cloud infrastructure and software development environment.	
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The Entity uses continuous monitoring tools to automatically track system health, endpoint	**Inquiry:** Inquired of the IT Operations team regarding the tools used for continuous	No exceptions noted

	security status, and application or infrastructure conditions, and to generate alerts when predefined thresholds or security-relevant events occur.	monitoring of endpoints, systems, and cloud infrastructure, including how security status, system health, and error conditions are monitored and how automated alerts are generated. **Inspection:** Inspected the dashboards showing firewall protections enabled and active on user systems, as well as cloud monitoring configurations demonstrating AWS CloudWatch configured to automatically detect and alert on backend application errors and predefined infrastructure conditions. **Observation:** Observed that the Entity has implemented continuous monitoring mechanisms across endpoints and cloud infrastructure that automatically track security status and system conditions and generate alerts when defined thresholds or error conditions are met, supporting ongoing visibility into the security and operational health of systems during the period under review.	
CC7.4: The Entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The entity has documented and approved an Incident Response Plan that defines roles, responsibilities, and procedures for identifying, assessing, responding to, and recovering from information security incidents.	**Inquiry:** Inquired of the Information Security team regarding the entity's incident management and response framework, including how information security incidents are identified, assessed, contained, eradicated, and recovered from, and how the Incident Response Plan is communicated and made available to employees. **Inspection:** Inspected the approved Incident Response Plan	No exceptions noted

		to verify that it documents a structured incident response process, including incident identification, assessment, classification, containment, eradication, recovery, post-incident review, roles and responsibilities, communication requirements, and training and awareness provisions, and that the plan is intended to be made available to staff for reference via internal channels. **Observation:** Observed that the entity has formally documented an Incident Management and Response Plan that defines end-to-end procedures for responding to information security incidents and establishes roles, escalation, communication, and review requirements, indicating that incident response expectations are defined and communicated to personnel during the period under review.	
CC7.5: The Entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The entity has documented Business Continuity and Disaster Recovery (BCDR) policies and procedures to support the continuation of business operations in the event of a disruption or security incident.	**Inquiry:** Inquired of management and the Information Security and IT Operations teams regarding the entity's approach to business continuity and disaster recovery, including how continuity and recovery procedures are documented, communicated, and maintained to support the continuation of critical business operations during disruptive events or security incidents. **Inspection:** Inspected the approved Business Continuity and Disaster Recovery Policy to verify that it establishes a formal framework for responding to business disruptions and security incidents, defines roles and	No exceptions noted

		responsibilities, and outlines requirements for business continuity planning, disaster recovery planning, testing, and periodic review. Additionally, inspected the Internal Business Continuity Playbook to verify that it documents practical continuity procedures, including incident classification, escalation protocols, recovery objectives (RTO/RPO), department-level response playbooks, backup and recovery processes, vendor dependencies, communication flows, and testing and review activities **Observation:** Observed that the entity has formally documented business continuity and disaster recovery policies and supporting procedures that define how critical operations are to be maintained or restored in the event of a disruption or security incident.	
CC7.5.2	The entity has a formally documented and approved Data Backup Policy that is made available to all staff via the company intranet.	**Inquiry:** Inquired with the IT team regarding the documentation, approval, and communication of the Data Backup Policy. The teams confirmed that the policy outlines backup schedules, storage locations, encryption requirements, and restoration procedures for critical data and systems. **Inspection:** Inspected the Data Backup Policy to confirm that it defines the frequency and scope of data backups, responsibilities of designated personnel, and retention requirements for backup data. Verified that the policy has been formally approved by Senior Management and uploaded to the company intranet for staff reference. **Observation:** Observed that the	No exceptions noted

		Data Backup Policy is communicated and made available to relevant personnel through the company intranet, ensuring that employees are aware of the entity's data protection and restoration practices.	

CC8.0: CHANGE MANAGEMENT		Test Of Controls	Results
CC8.1: The Entity authorizes, designs, develops, or acquires, configures, documents, tests, approves and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The entity has a documented Change Management Policy, which is available to all Staff Members via the company intranet.	**Inquiry:** Inquired with the IT team to confirm that the Change Management Policy is documented, approved, and made accessible to all staff via the company intranet. **Inspection:** Inspected the documented Change Management Policy and verified its availability on the company intranet for access by all employees. **Observation:** Observed that the Change Management Policy is documented and approved, and is available to all staff members via the company intranet, as confirmed through inquiry with the IT team and inspection of the policy's availability on the intranet.	No exceptions noted
CC8.1.2	The Entity utilizes a centralized version control system to manage, organize, and restrict access to application code repositories, ensuring that all changes are tracked and attributable to authorized users.	**Inquiry:** Inquired of the Engineering and DevOps teams regarding the platform used for source code management and change tracking. Personnel confirmed that GitLab is used to manage code repositories and group structures. **Inspection:** Inspected the GitLab management interface to verify	No exceptions noted

		the implementation of a structured code management system. The inspection confirmed that the Entity maintains multiple distinct groups, each representing different functional modules or development projects, which serves as the foundation for tracking and logging code-level changes. Specifically, verified that each group has a designated "Owner" assigned to ensure accountability for the code and access permissions within that repository. The inter face further demonstrates that the system tracks the number of projects and active contributors within each group, providing a transparent and auditable trail of the organizational structure of the source code. **Observation:** Observed that the Entity has established a formal environment for managing application code through GitLab.	

CC9.0: RISK MITIGATION			
CC9.1: The Entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The Entity performs a formal risk assessment exercise annually, as detailed in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	**Inquiry:** Inquired with the Senior Manager about the Inquired with the risk management and information security teams about the frequency, ownership, and scope of the formal risk assessment process. **Inspection:** Inspected the Risk Management Policy and Risk Assessment Methodology to confirm that the entity has defined procedures for identifying, evaluating, and prioritizing risks based on likelihood and impact.	No exceptions noted

		Observation: Observed that the entity conducts a formal annual risk assessment exercise, with clearly defined procedures for identifying, evaluating, and prioritizing risks based on likelihood and impact, as evidenced by the Risk Management Policy, Risk Assessment Methodology, and confirmations from risk management and information security teams.	
CC9.1.2	The Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	**Inquiry:** Inquired with the Information Security Officer and Risk Management team regarding the frequency and process of conducting formal risk assessments. They confirmed that a comprehensive risk assessment exercise is conducted annually, as mandated by the Information Risk Management Policy. The assessment involves identifying potential threats and vulnerabilities across infrastructure, data, and business processes, evaluating their likelihood and impact, and documenting results within the Risk Register. **Inspection:** Inspected the Information Risk Management Policy, which outlines the formal procedure for conducting risk assessments, including steps for risk identification, evaluation, treatment, and review. The policy mandates that the assessment be carried out at least annually and upon any significant change to the organization's systems, processes, or infrastructure. Reviewed the Risk Register, which includes distinct sections for Risk Identification, Risk Assessment,	No exceptions noted

		Risk Treatment, and Risk Review. Each record specifies risk details such as the risk name, source, likelihood, impact, risk rating, existing controls, treatment plan, residual risk, risk owner, and review date. **Observation:** Observed that the entity performs a structured and documented risk assessment process annually, as evidenced by the Risk Register and the supporting Risk Management Policy.	
CC9.1.3	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	**Inquiry:** Inquired with the senior management team to understand how risks are scored, how likelihood and impact are determined, and how mitigation strategies are associated with each identified risk. **Inspection:** Inspected the Risk Management Policy and risk assessment methodology to confirm that they define a standardized approach for evaluating risks. Reviewed the Risk Register to verify that risks were assigned scores based on likelihood and impact, and that each risk was mapped to documented mitigating controls or treatment plans. **Observation:** Observed that each risk is assessed using a standardized approach defined in the Risk Assessment Methodology, with risk scores assigned based on likelihood and impact, and corresponding mitigating controls or treatment plans documented in the Risk Register.	No exceptions noted
CC9.2: The entity assesses and manages risks associated with vendors and business partners			

CC9.2.1	The entity has a documented Risk Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated.	**Inquiry**: Inquired with senior management to confirm that a Risk Assessment and Management Policy is formally documented and approved, and that it includes defined processes for identifying, assessing, and mitigating risks related to business objectives, service commitments, and system requirements. **Inspection**: Reviewed the Risk Management Policy and supporting risk assessment methodology to verify that they outline structured procedures for identifying and evaluating risks. Examined the risk register to confirm that documented risks reflect alignment with the entity's business objectives, service commitments, and system requirements. **Observation**: Observed that the entity maintains a formal Risk Assessment and Management Policy supported by a consistent methodology and documented risk register. The process includes regular identification, evaluation, and mitigation of risks associated with business operations, demonstrating alignment with the entity's service commitments and system requirements.	No exceptions noted
CC9.2.2	The entity has a documented Vendor Management Policy that provides guidance to staff on performing risk assessments of third-party vendors.	**Inquiry**: Inquired with the Procurement and Information Security teams regarding how vendor relationships are assessed and managed. Specifically asked how staff are guided to evaluate and mitigate risks related to third-party vendors. **Inspection**: Inspected the Vendor Management Policy, which outlines the process for onboarding,	No exceptions noted

		evaluating, and periodically reassessing third-party vendors. Verified that the policy includes criteria for determining vendor criticality, risk assessment procedures, and responsibilities for staff involved in vendor selection and oversight. **Observation**: Observed that the policy is formally documented and available to relevant personnel. It includes detailed procedures for performing vendor risk assessments and sets expectations for due diligence, ongoing monitoring, and contract requirements. The policy serves as a foundational document ensuring that vendor-related risks are managed consistently across the organisation.	

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE			
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY		**Test Of Controls**	**Results**
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	The entity ensures that confidential information is retained only for as long as necessary unless required.	**Inquiry:** Inquired of the Information Security and IT Operations teams regarding the process for defining retention periods for confidential information, including how legal, regulatory, and business requirements are considered, how retention periods are approved, and how periodic reviews of retention periods are performed. **Inspection:** Inspected the approved Data Retention Policy to verify that it defines specific retention periods for various categories of data, requires data	No exceptions noted

		to be retained only for defined periods based on legal, compliance, and business requirements, mandates annual review of retention periods by data owners, and requires formal approval for any changes to retention periods. **Observation:** Observed that the entity has documented retention requirements for confidential information, including defined retention periods, review mechanisms, and approval workflows for retention changes.	
C1.1.2	The entity has a documented Data Classification Policy and makes it available for all staff on the company intranet.	**Inquiry**: Inquired with the Information Security and Compliance teams regarding how data classification requirements are defined, approved, and communicated to employees. Management confirmed that the Entity has formally documented a Data Classification Policy approved by senior management, which defines data categories (Public, Internal, Confidential), handling requirements, retention expectations, and protection standards. **Inspection**: Inspected the Data Classification Policy to verify that it is formally documented, approved, and current. Verified that the policy defines data classification categories, roles and responsibilities, labeling requirements, handling controls, retention and destruction requirements, and enforcement provisions. Additionally, inspected the demonstration that the policy is published and accessible to employees through the company intranet, confirming availability to	No exceptions noted

		staff. **Observation:** Observed that the Entity has established a formally documented and approved Data Classification Policy that clearly defines how information is classified, handled, protected, retained, and destroyed.	
C1.1.3	The Entity identifies and defines confidential information through formal contractual agreements and requires employees to acknowledge and protect such information through executed Non-Disclosure Agreements (NDAs).	**Inquiry:** Inquired of management regarding how the Entity identifies confidential information and communicates confidentiality requirements to employees and relevant personnel. **Inspection:** Inspected a sample of Entity's executed Non-Disclosure Agreement (NDA) to verify that confidential information is formally identified and defined. The NDA was observed to include a clear definition of confidential information, specify the types of information considered confidential, outline obligations for protecting such information, restrict unauthorized disclosure or use, and define the duration for which confidentiality obligations apply, including post-employment requirements. **Observation:** Observed that the Entity identifies confidential information through formal contractual agreements and requires employees to acknowledge and protect such information by executing a Non-Disclosure Agreement.	No exceptions noted
C1.2: The Entity disposes of confidential information to meet the entity's objectives related to confidentiality.			

C1.2.1	The Confidential information is disposed of in accordance with documented data retention and secure disposal policies.	**Inquiry**: Inquired of the Information Security and IT Operations teams regarding the process for retaining and disposing of confidential information, including how retention periods are defined, how disposal approvals are obtained, and how secure disposal is enforced once retention requirements are met. **Inspection**: Inspected the approved Data Retention Policy to verify that it defines retention periods for various categories of data, specifies approval requirements prior to disposal, and establishes secure disposal methods for confidential and sensitive information, including destruction requirements after the completion of retention periods. **Observation**: Observed that the entity has established and documented retention and secure disposal requirements for confidential information, including defined retention periods, approval workflows, and authorized disposal methods	No exceptions noted

A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY		**Test Of Controls**	**Results**
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.			
A1.1.1	The Entity utilizes automated monitoring tools to track infrastructure performance and resource utilization metrics, ensuring system capacity is managed to support ongoing availability objectives.	**Inquiry:** Inquired of the IT Infrastructure and DevOps teams regarding the process for managing system capacity and resource availability. Personnel confirmed that AWS CloudWatch is used to establish a continuous monitoring baseline for the	No exceptions noted

		production environment. They explained that real-time CPU, disk, and network metrics is used to identify utilization trends and ensure that infrastructure resources are appropriately scaled to meet operational demands. **Inspection:** Inspected the AWS CloudWatch management console dashboards to verify that the Entity tracks system capacity and infrastructure performance metrics. The inspection confirmed the active monitoring of several key resource utilization indicators for various instance IDs, including CPU Utilization, Network throughput (NetworkIn, NetworkOut, and NetworkPackets), and Disk activity (Read/Write bytes and operations). The dashboard was observed to provide real-time telemetry and visualization of these metrics, allowing the Entity to establish performance baselines and identify utilization trends or deviations. **Observation:** Observed that the Entity maintains a centralized, automated system for tracking infrastructure performance.	
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	The Entity ensures that data backups are periodically restored and tested to validate the integrity and recoverability of backup data.	**Inquiry:** Inquired of management and IT operations personnel regarding the Entity's backup and recovery procedures, including how backups are maintained, how restoration testing is performed, and how the integrity and recoverability of backup data are	No exceptions noted

		validated. **Inspection:** Inspected the Entity's backup inventory and system records documenting key systems subject to backup, including Git repositories, CRM systems, ERP systems, and employee-related applications. The inspection included review of documented backup frequency, retention periods, and access controls applied to backup data. Additionally, inspected evidence of backup server logs and restoration-related records maintained within the audit log repository, demonstrating that backup data is periodically accessed and validated to support recovery and integrity verification. **Observation:** Observed that the Entity maintains documented backups for critical systems with defined retention periods and access controls, and performs periodic restoration and validation activities to confirm the integrity and recoverability of backup data	
A1.2.2	The entity has documented a Business Continuity & Disaster Recovery Policy, which establishes guidelines and procedures on continuing business operations in case of a disruption or a security incident.	**Inquiry:** Inquired with the Entity's Information Security and IT Operations teams to understand whether a formal Business Continuity and Disaster Recovery Policy is established, approved, and communicated, and how it defines responsibilities, recovery objectives, and procedures for responding to business disruptions and security incidents. **Inspection:** Inspected the documented Business Continuity and Disaster Recovery Policy provided by the Entity, verified that the policy is formally	No exceptions noted

		documented, version-controlled, and approved by management. Confirmed that the policy defines business continuity and disaster recovery objectives, scope, roles and responsibilities, recovery strategies, incident escalation procedures, backup and restoration expectations, and periodic testing requirements to support continuity of operations during disruptive events. **Observation:** Observed that the Entity has established and documented a Business Continuity & Disaster Recovery Policy that provides structured guidance for maintaining and restoring business operations in the event of operational disruptions or security incidents.	
A1.3: The Entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	The Entity has documented Business Continuity and Disaster Recovery (BCDR) Policies that define procedures for resuming operations in the event of a disruption, and performs periodic disaster recovery and backup restoration tests to validate their effectiveness.	**Inquiry:** Inquired with the Information Security, Technology, and Operations teams regarding how business continuity and disaster recovery requirements are defined, implemented, and tested. The teams explained that the Entity maintains formally documented BCDR policies and an internal continuity plan that defines recovery procedures, roles and responsibilities, communication protocols, and recovery objectives (RTOs and RPOs). **Inspection:** Inspected the approved Business Continuity and Disaster Recovery Policy and Plan to verify that they formally document recovery objectives, system and process recovery procedures, escalation and	No exceptions noted

		communication workflows, and assigned roles and responsibilities. Additionally, inspected a sample of periodic disaster recovery and backup restoration testing, including backup snapshot logs, restoration capability records, and alerts related to backup failures, to confirm that recovery procedures are exercised and validated during the audit period. **Observation:** Observed that the Entity has established and maintained comprehensive business continuity and disaster recovery documentation and performs periodic recovery testing activities.	