suneratech

Simplifying Cloud | Accelerating Innovation

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT

For the period September 1, 2022, through February 28, 2023

Report Date – March 22, 2023

AICPA SOC

aicpa.org/soc4so

SOC for Service Organizations | Service Organizations

Attinkom

We verify your trust

TABLE OF CONTENTS

{Remainder of the page intentionally left blank}

SECTION I ASSERTION OF SUNERATECH'S MANAGEMENT

MANAGEMENT'S ASSERTION

March 22, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Suneratech's "Software Development, Application Management Services, Product Engineering, Quality Engineering, Cloud Migration, Cloud Infrastructure and Managed Services" (system) throughout the period September 1, 2022, to February 28, 2023, to provide reasonable assurance that Suneratech's service commitments and system requirements relevant to security, availability, confidentiality, processing integrity, and privacy were achieved. Our description of the boundaries of the system is presented in the Attachment A and identifies aspects of the system covered by our assertion.

Suneratech utilizes cloud services by Oracle (subservice organization) for hosting their products, to provide Cloud Migration, Cloud Infrastructure and Managed services, and various other functional activities. The description (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary along with controls at Suneratech, to achieve Suneratech's service commitments and system requirements based on the applicable trust services criteria. The description presents Suneratech's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Suneratech's controls. The description presented in Attachment A does not extend and disclose the actual controls at the subservice organization.

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

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2022, to February 28, 2023, to provide reasonable assurance that Suneratech's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA Trust Services Criteria).

Suneratech's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2022, to February, 2023, to provide reasonable assurance that Suneratech's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, if subservice organization and user entities applied the complementary controls assumed in the design of Suneratech's controls throughout the period September 1, 2022, to February 28, 2023.

- ***Sunera Technologies Private Limited***

ATTACHMENT A

ATTACHMENT A

DESCRIPTION OF SUNERATECH'S SYSTEM RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, PROCESSING INTEGRITY AND PRIVACY

Company Background & Overview of Services

Sunera Technologies Private Limited was established in 2005, primarily as a SI company. Suneratech is Oracle's Platinum Partner, Oracle's leading Cloud Managed Service Provider and Managed Service Provider across Cloud Migration, Data Center Migration, Infrastructure Managed Services, and Oracle Applications Managed Services including Oracle BI and Data Warehouse Service. Over the past 10 years, Suneratech has invested heavily in building IT Automation Platforms for industry across various functions. Suneratech's customers benefit by leveraging its IT Automation Platforms-based services e.g., CloudTestr, AutoMap, Ring Master Studio, AI-enabled ServiceDesk platform, etc. Suneratech provides a wide spectrum of services e.g., Cloud Managed Service, Cloud Migration Service, Infra Managed Service, Application Managed Service, Database Managed Service, Integration Services, BI, Data Analytics & Data Warehouse Services, Cloud Security and Compliance Services.

Suneratech's IP led platform services are:

1. Testing Automation Service by CloudTestr
2. Patch Automation Service by RingMaster Studio
3. Application Management Services by AMS
4. Supply Chain Solution by eSeal

Further information about Suneratech is available on the website, www.suneratech.com.

Boundaries of System

The boundaries of the system are the specific aspects of Suneratech's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customer are not included within the boundaries of the system.

Subservice Organization

Suneratech utilizes cloud services by Oracle (subservice organization) for hosting their products, to provide Cloud Migration, Cloud Infrastructure and Managed services, and various other functional activities and is not included in the scope of this examination. The cloud provider provides robust security capabilities for the organization to implement and maintain security and data protection.

Oracle has achieved many compliance certifications including SOC Attestation (SOC 1, SOC 2, SOC3) to provide its customers with assurance that its platform meets security requirements and industry standards. https://www.oracle.com/in/corporate/cloud-compliance/.

The criteria that relate to controls at the subservice organization includes all criteria related to the Trust Service Principles of Security, Confidentiality, and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Suneratech include:

- The systems are protected against unauthorized access (both physical and logical).
- The systems are available for operation and use and in the capacities, as committed or agreed.
- Environmental protections have been installed and monitored for incidents or events that impact subservice organization's assets.
- Policies and procedures exist related to security and availability and are implemented and followed.

System Components

Suneratech has defined processes and teams for Information Systems (IS), Information Technology (IT), Network Communication, Change Management, Incident Management, Logical access, Backup and Recovery, Business Continuity, Physical Access, and Human Resources (HR) to support the delivery of services to its clients.

Infrastructure

Suneratech's Information Technology (IT) landscape is built on a centralized Windows Active Directory architecture and secured VPN Networks for providing authentication and restricted access to systems. Suneratech's Enterprise Applications and Service Desk provides End-user IT and business services. Suneratech's server rooms are equipped with Uninterruptible Power Supply (UPS), backup generators, and fire detection systems to protect systems from environmental hazards.

Industry-standard firewalls are installed and managed to protect Suneratech's systems by residing on the network to inspect all ingress connections routed to the Suneratech's environment. Suneratech uses cryptographic controls to ensure the security of its data. Suneratech prevents unauthorized physical access to the workplace and appropriate environment housing of customer information.

An inventory of hardware and software used in the network is maintained and updated as necessary. Logging and monitoring software are configured to collect data from in-scope systems to monitor system performance, potential security vulnerabilities, capacity utilization, and alert upon detection of unusual system activity.

Software

Software includes key assets in providing Software Development, Application Management Services, Product Engineering, Quality Engineering, Cloud Migration, Cloud Infrastructure and Managed Services.

People

Suneratech is responsible for the management and supervision of personnel involved in providing services delivered to its clients. The categories of personnel involved in the operation and use of the system are Executive Management, GRC Team, IT Team, Operations Team, Delivery Team, InfoSec Team, Administration Team, Legal Team, Finance Team, and the Human Resources (HR) Team. Each team has defined responsibilities and accountabilities outlined in the policies of the organization.

Procedures

Suneratech has developed the Information Security Management System (ISMS), Privacy Management, Information Technology Service Management (ITSM), and Quality Management System policies and procedures. The ISMS, Privacy, ITSM, and QMS policies and procedures are reviewed periodically and changes if any, are authorized by the Chief Information Security Officer (CISO) and GRC Practice Head.

Data

Suneratech has established written policies and procedures related to Information classification, labeling of information, storing, isolating confidential information, and disposal in its Information Security Policy and Asset Management Procedure.

Relevant Aspects of Control Environment, Risk Assessment, Information and Communication, Monitoring Activities, Policies and Practices

I. Control Environment

The control environment at Suneratech is the foundation for other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; management's commitment to competence; its organization structure; the assignment of authority and responsibility; and the oversight and direction provided by the Senior Management and the Executive Leadership Team.

Integrity and Ethical Values

Suneratech requires Directors, Senior Management, Officers, and all employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Suneratech promotes values as its core ethical values of the company and all employees are expected to fulfil their responsibilities based on these principles and comply with all applicable laws and regulations.

Suneratech promotes an environment of open, transparent communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted. Core values are communicated from the Executive Leadership Team to personnel through policies, directives, guidelines, and the code of conduct.

Senior Management and Executive Committee Participation

Suneratech’s control consciousness is influenced significantly by the participation of the Executive Leadership Team. Responsibilities of the Executive Leadership Team are documented and understood by Executive and Senior Management personnel.

Communication and Enforcement of Integrity and Ethical Values

To maintain a fair and productive working environment, Suneratech has a documented and approved code of conduct. The code of conduct reflects its continued commitment to ethical business practices and compliance. Employees are made aware of the organization's code of conduct during orientation training.

In addition, new joiners are assigned a task in the Enterprise Portal to provide their acceptance to the organization's code of conduct. Management monitors personnel compliance with the code of conduct through monitoring of customer and workforce member complaints and takes required necessary action. Suneratech has implemented a whistle-blower program to ensure significant deviations, non-compliances, and wrong practices are reported on time. Any complaints raised are promptly and thoroughly investigated.

Management Philosophy and Operating Style

Suneratech's management philosophy is to look for ways to continuously improve; provide quality service to clients and, most of all, take pride in work and setting high standards. Suneratech's management holds quarterly business review meetings to communicate information needed to fulfil their roles with respect to the achievement of Suneratech's service commitments and system requirements.

Townhall meetings are conducted quarterly by the Leadership team & All-Hands meet are conducted within Business Units on a monthly basis by People Partners to provide a platform for a successful dialogue between the Management Team and employees.

Commitment to competence

Suneratech's management defines competence as the knowledge and skills necessary to accomplish tasks that define personnel roles and responsibilities. Management commitment to competence includes management's consideration of the competence level of jobs and how those levels translate into requisite skills and knowledge. Written job descriptions are in place to clarify and enhance communication which serves as the foundation for developing interview questions, conducting performance evaluations, setting goals, and growth paths. Suneratech has implemented a structured interview process to ascertain the standout candidates matching the qualifications, relevant experience, skills, and expertise needed for a job position.

The training focused on the technology domain, and soft skills are conducted periodically for employees as a part of the learning and development initiatives of the organization. Suneratech has defined & implemented the 'Career Development Matrix 'to guide employees towards career progression, internal job rotations, and promotions. Management establishes key performance indicators (KPI) at all levels of the organization considering the achievement of both long terms and short-term objectives and ensuring the whole organization is aligned to achieving them.

Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. The performance of the internal controls implemented within the environment is assigned to appropriate process owners and operational personnel based on defined roles and responsibilities. Segregation of duties is in place for critical functions and departments.

Organizational Structure

Organizational structure is in place to communicate areas of authority, responsibility, and lines of reporting to the personnel. These are periodically reviewed and made available to employees via Enterprise Portal. Authority Limits, delegation of power, and roles and responsibilities are in place for significant roles.

II. Risk Assessment

A documented Risk Management Procedure is in place which provides a systematic approach to identify, assess, and counter security risks faced by the information and information systems of Suneratech. The CISO is responsible for developing the risk management procedure and ensuring adherence to the procedure. A formal risk assessment is performed at least annually or when significant events occur, and results are documented.

III. Information and Communication

Suneratech's management realizes that effective communication with personnel is vital to align Suneratech's business strategies and goals with operating performance. Suneratech communicates its service commitments to clients as appropriate. It also communicates those commitments and associated system requirements to internal employees to enable them to carry out their responsibilities. There are standard communication mechanisms for smooth and coherent communication and understanding between all the groups within Suneratech.

Suneratech has also implemented various methods of communication to help assure that clients understand their roles and responsibilities in the use of their products and services and communication of significant events. Project teams communicate with clients regularly through emails, telephone calls, and personal meetings. Periodic reporting on operations and other relevant reports are shared with the client as agreed.

IV. Monitoring Activities

Suneratech has established a Governance, Risk, and Compliance Function (GRC) independent of the operations team to assist the organization better identify, understand, and manage dynamic interrelationships between risks and compliance. Internal Audits are conducted periodically to verify the effectiveness of the implemented controls, identify gaps, and discover improvement opportunities.

Suneratech supports many user entities in their efforts to meet the regulatory demands of their industry. Suneratech has assisted user entities by successfully meeting the requirements of many certifications and regulatory demands.

- ISO 9001: 2015 Quality Management System
- ISO/IEC 27001: 2013 Information Security Management System (ISMS)
- ISO/IEC 20000-1:2018 Information technology — Service management
- GDPR

CMMI V2.0 Appraisal Suneratech has undergone CMMI V2.0 appraisal for Development projects from the Enterprise application Modernization and Sunera Support units, as well as Support projects from Infra Cloud Transformation and Enterprise application Modernization. CMMi Development & Services 2.0 Maturity Level 3 Benchmark appraisal was successfully completed for Suneratech.

Alerts and logs are monitored through the respective system. Management review meetings headed by CISO are held annually to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

V.Policies and Practices

Physical and Environmental Security

Physical and Environmental Security policy and procedure document set out the security standards for access to Suneratech premises. Physical access is controlled through a biometric (fingerprint)/ RFID card access control system, video surveillance, round the clock security guards deployed at the main entrance to the premises to monitor the movement of people and equipment in an out of the premises. Close Circuit Television (CCTV) cameras are installed at suitable locations within the premises.

Environmental protections have been installed which includes the following:

- Cooling systems
- Power backup in the event of power failure
- Redundant communications lines
- Smoke detectors
- Fire Extinguishers
- Fire Alarm

Logical Security

User access control policy and procedure are formally documented and approved at least on an annual basis by the CISO. User accounts for the Suneratech domain are created by the IT Team for authorized new joiners based on the request raised by the HR as part of the on-boarding process. Access is granted on the 'least privilege' basis as default and any additional access needs to be approved. Privileges granted to users is reviewed monthly. Control self-assessments that include logical and physical access review is performed by the IT Team and reviewed by Director - IT / IT Manager monthly. Logical access to domain and systems is disabled as a component of the separation process.

Data Security

Suneratech endeavors to meet leading standards and regulations for data protection and privacy. DLP systems have been installed to detect and prevent potential data breaches/data ex-filtration transmissions in the organization's network. Full Disk Encryption is enabled on user's workstations. Use of removable media is prohibited by policy except when authorized by management.

Network & Endpoint Security

Suneratech's delivery center is equipped with the latest hardware, software, and networking infrastructure. Firewall is implemented to protect the network from external threats and vulnerabilities. The firewall provides unified threat management (UTM) services such as intrusion protection, web filtering and inbound and out bound traffic filtering. Network administrative access is restricted to authorized user accounts.

Management has defined configuration and hardening standards that include requirements for the implementation of security groups, access control, configuration settings, and standardized policies in Information Security Policies and Procedures. IT Infrastructure and workstations are hardened as per the standards.

Suneratech utilizes a SIEM solution for managing security events, provides insights and track record of the activities within the IT environment.

Antivirus and Antimalware software is installed on workstations and servers. End-User do not have permission to install software on the workstations. The ability to install software on workstations and laptops is restricted to IT support personnel.

The patch management activity is done regularly as per the patch management calendar or as and when any critical changes to the computing environment.

Remote working

Suneratech has implemented an SSL VPN over the internet to enable the authorized employees to get connected to Suneratech's environment to access their system through an encrypted tunnel. Multifactor authentication is implemented for remote connectivity. This allows an authorized remote user to connect to the network using the internet, through any Internet Service Provider (ISP).

Cloud Security

Cloud Infrastructure is hardened as per the industry best practices. Cloud monitoring solution is implemented to provide a holistic overview of the entire cloud infrastructure. A role-based security process has been defined within the cloud infrastructure based on the job requirements. The production system is protected by security groups rules set up for the virtual cloud networks (VCN). VCN has been set up and all production servers are within the private subnet.

Internet Connectivity

Internet Connectivity across Suneratech is through multiple service providers for redundancy and resiliency.

Vulnerability Assessment & Penetration Testing

Vulnerability scanning tool is implemented to discover, assess, prioritize, and patch critical vulnerabilities in real time and across IT landscape. Identified vulnerabilities are remediated and tracked to closure by the InfoSec Team. Suneratech engages with third-party security consulting firms to perform annual penetration testing. Identified vulnerabilities are remediated and revalidation testing is conducted to confirm the status of closure.

Human Resources

Suneratech has documented its HR policies and procedures which provide structure, control, and fairness. They also ensure compliance with employment legislation and inform employees of their responsibilities and the company's expectations. HR procedures that are followed for regular employees are also applied to the contingent staff.

Hiring procedures require that proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff. Shortlisted candidates are issued offer of appointment letters with employment terms and conditions. New joiners are required to sign a 'Non-Disclosure Agreement' at the time of joining.

Suneratech conducts background checks via the third party at the discretion of the company and/or for the clients who request it. New employees participate in an induction program that acquaints them with Suneratech organization, functions, values, and an overview of services, key policies, and Information Security best practices. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, and continuing education programs.

The training focused on the technology domain, and soft skills are conducted periodically for employees as a part of the learning and development initiatives of the organization. Performance evaluation is conducted annually via Suneratech Annual Performance Evaluation System (SAPES) configured on the EP Portal. Suneratech has defined & implemented the 'Career Development Matrix 'to guide employees towards career progression, internal job rotations, and promotions.

Grievance handling procedure is in place to manage employees' grievances. Employees are encouraged to use informal methods for resolving disputes or disagreements. Employees can also formally raise their grievances to their Reporting Manager/ HR People Partner.

Termination of employment is processed as per Suneratech's exit process. If an employee intends to resign, he or she will provide a letter of resignation to his or her immediate supervisor with the required notice period as per the terms of employment. Access privileges are revoked upon termination of the employment.

Information Security

Suneratech has developed an Information Security Policy to provide a management directive for Information Security and to maintain appropriate information security controls. The Chief Information Security Officer (CISO) has been appointed with the authority and responsibility of maintaining and enforcing the Information security policies and procedures at an organizational level.

Information Security Policy is reviewed at least annually or when significant changes occur and approved by the Chief Information Security Officer (CISO). Suneratech's Information Security Framework consists of a set of standards, guidelines, and practices created with the purpose to protect the organization and client's information assets from all threats, whether internal or external, deliberate, or accidental. Suneratech ensures that appropriate information security controls are applied and integrated into existing processes to ensure continual protection of information from risks affecting confidentiality, integrity, and availability thereby enhancing the confidence of clients and adding value to the organization.

Information Security requirements are communicated to new hires upon joining Suneratech and regular updates are formally communicated to existing employees through training, awareness sessions, and campaigns periodically. Information Security Policy is made available to employees via Enterprise Portal.

A formal disciplinary action process is defined for employees, contractors, or third-party users who have violated Suneratech's security policies and procedures. Disciplinary action is decided based on the severity of the incident.

Change Management

Suneratech has defined its Change Management procedure for managing changes to all the assets, infrastructure, processes, software, third party activities, etc. The Chief Information Security Officer is responsible for reviewing the change management process and ensuring Information Security requirements are met in this process. There exists a Change Advisory Board (CAB) responsible for authorizing non-standard and emergency changes. All changes are recorded, approved, implemented, tested, and versioned before moving to the production environment.

Information Security Incident Management

Documented Incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. Incidents raised are tracked to closure and the resolution is submitted in the incident management tool. Root cause analysis is performed for all critical/high incidents for identifying the cause(s) and contributing factors of an incident.

A formal disciplinary action process is defined for employees, contractors, or third-party users who have violated Suneratech's security policies and procedures. Disciplinary action is decided based on the severity of the incident. Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives. Lessons learned exercise is conducted by the Incident Response team wherever necessary.

Release Management

Suneratech's Release Management process enables the project teams to perform the releases by establishing the guidelines of Continuous Integration/Continuous Development/ Continuous Testing. It also enforces the best practice of deliverables demos and retrospection for each release. Implementation of the Release management process ensures the Continuous Integration/ Continuous Development Automation, Release Notes, Build Management Guidelines, Deployment Manual, User Manual, Deliverables Demo Signoff, and Retrospection. The release management process enables the team to produce repeatedly quality software with shorter times to market, which allows Suneratech to be more responsive to the operating environment.

SDLC Model

Suneratech has defined the rules and guidelines for the secure development of software and systems in its SDLC procedural document. The software development life cycle is the collection of phases through which a software product/ project passes from initial conception to customer acceptance.

Business Continuity Management

Suneratech has developed a Business Continuity Policy and associated Business Continuity Management Procedure document to help realize and implement its Business Continuity Management program. The Business Continuity Plan is reviewed at least on an annual basis or when there is a material change to the situation.

Backup and Recovery

Backup and Recovery procedure is defined to ensure adequate back-up for recovering essential business information and computing resources. Restoration testing of the backups is performed as a planned activity or when significant event/s occur.

Capacity Management

Suneratech has implemented a systematic process for resource planning to keep track of its resources, utilizing them according to the project plan, improve the project's delivery, and attain desired operational performance.IT Capacity Planning is performed to ensure that the organization has ample IT capacity to meet business needs.

Third Party Vendor Management

Agreements are established with service providers/vendors that include clearly defined terms, conditions, and responsibilities for service providers, and vendors. Risk related to the vendor is assessed through a formal risk assessment process to ensure that the use of service provided by the supplier/vendor does not create an unacceptable potential business disruption or a negative impact on business performance.

IT Helpdesk

IT team receives requests for support through Emails/ IT Chatbot/ Helpdesk. Suneratech has implemented IT Avanthi Chatbot – Digital Assistant to improve overall ITSM efficiency and productivity by handling routine employee issues much faster. It interacts with the users through a conversational UI to solve queries faster and is available 24/7.

Privacy

Suneratech is committed to protecting personal data under the regulatory system and in accordance with the data protection laws (e.g., GDPR) and maintain a robust and structured program for compliance adherence and monitoring. Suneratech has implemented various technical and organizational measures to ensure compliance with data protection requirements discussed in other sections of the report.

On an annual basis, GRC Team performs privacy risk assessment to identify and mitigate privacy risks. In the scope of providing services to user entities, Suneratech acts in the capacity of the data processor and does not have control over communication with data subjects nor does it have a direct interface with the data subjects.

Data Protection Impact Assessment is performed for all the client projects to identify and manage privacy risks arising from new projects. A Data Processing Agreement is signed between client and Suneratech to regulate the terms and conditions of data processing.

Suneratech has developed, implemented, and maintained a Privacy and Data Protection Training Program to educate personnel on their responsibilities of protecting personal information and organizational procedures.

Complementary User Entity Controls

Suneratech's controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of Suneratech's controls are suitably designed and operating effectively, along with related controls at Suneratech.

{Remainder of the page intentionally left blank}

ATTACHMENT B

ATTACHMENT B
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Suneratech makes commitments related to security, availability, confidentiality, processing integrity, privacy, SLA adherence & compliance with relevant laws and regulations to its customers and has established system requirements as part of the service. Service commitments to customers are documented and communicated in the Vendor Services Agreement and SOW as well as in the description of the service offerings provided online.

Suneratech establishes operational requirements that support the achievement of security, availability, confidentiality, processing integrity and privacy commitments, SLA adherence, compliance with relevant laws and regulations, and other system requirements. Such requirements are communicated in Suneratech's system policies and procedures, system design documentation, and contracts with clients.

Information Security Management System policy (ISMS policy) is a document with high-level requirements for establishing an Information Security Management System in Suneratech and demonstrate compliance to ISO/IEC 27001:2013. Information security policies define an organization wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of Suneratech's system.

Information Technology Service Management System (SMS Catalog) is to provide the highest level of service to Suneratech's clients and ensure that Suneratech continually improves the delivery of services to clients. The existence of the SMS catalog is a testimony to management's commitment to continually improve the service management and its commitment to ISO/IEC 20000-1:2018 requirement.

Quality Management System Policy is to provide the highest level of service to Suneratech's clients and ensure that it continually improves the delivery of services to clients. The existence of the QMS Policy is a testimony to management's commitment to continually improve the quality and its commitment to ISO 9001:2015 requirements. CMMi Development & Services 2.0 Maturity Level 3 Benchmark appraisal was successfully completed for Suneratech.

{Remainder of the page intentionally left blank}

SECTION II INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Management of Sunera Technologies Private Limited

Scope

We have examined Sunera Technologies Private Limited (also referred to as "Suneratech" or "service organization") accompanying assertion titled "Assertion of Suneratech's Management" (assertion) that the controls within Suneratech's Software Development, Application Management Services, Product Engineering, Quality Engineering, Cloud Migration, Cloud Infrastructure and Managed Services (system) were effective throughout the period September 1, 2022, to February 28, 2023 to provide reasonable assurance that Suneratech's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy (AICPA, Trust Services Criteria).

As indicated in the description, Suneratech utilizes cloud services by Oracle (subservice organization) for hosting their products, to provide Cloud Migration, Cloud Infrastructure and Managed services, and various other functional activities and is not included in the scope of this examination. The description includes only the controls of Suneratech and excludes controls of the subservice organization. The description also indicates that certain trust services criteria can be met only if the subservice organization's controls, contemplated in the design of Suneratech's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to the controls of subservice organization.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of Suneratech's controls are suitably designed and operating effectively, along with the related controls at the service organization. Our examination did not extend to such complementary user entity controls.

Service Organization Responsibilities

Suneratech is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Suneratech's service commitments and system requirements were achieved. Suneratech has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Suneratech is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Suneratech's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Suneratech's service commitments and system requirements based on the applicable trust services criteria.

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, management's assertion that the controls within Suneratech's system were effective throughout the period September 1, 2022, to February 28, 2023 to provide reasonable assurance that Suneratech's service commitments and system requirements were achieved based on the applicable trust service criteria, is fairly stated, in all material respects, if subservice organization and user entity controls assumed in the design of Suneratech's controls operated effectively throughout the period September 1, 2022, to February 28, 2023.

Truly Yours,

Attinkom LLC

March 22, 2023

ATTINKOM LLC
CERTIFIED
PUBLIC
ACCOUNTANT
WE VERIFY YOUR TRUST

Appendix A: Glossary

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access.

commitments. Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided, or the product, production, manufacturing, or distribution specifications.

controls. Policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

criteria. The benchmarks used to measure or evaluate the subject matter.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network elements.

internal control. A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

personal information. Information that is or can be about or related to an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the bases for procedures.

practitioner. A CPA who performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

security incident. A security event that requires action on the part of an entity in order to protect information assets and resources.

system. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives in accordance with management specified requirements.

system components. Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

Appendix A: Glossary

system boundaries. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function or provide a service. When systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ.

SOC 3 Engagement. An examination engagement to report on management's assertion about whether controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to one or more of the trust services categories (applicable trust services criteria.)

system requirements. Specifications regarding how the system should function to (a) meet the entity's commitments to customers and others (such as customers' customers); (b) meet the entity's commitments to suppliers and business partners; (c) comply with relevant laws, and regulations, and guidelines of industry groups, such as business or trade associations; and (d) achieve other entity objectives that are relevant to the trust services category or categories addressed by the description. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations.

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

subservice organization. A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

trust services. A set of professional attestation and advisory services based on a core set of criteria related to security, availability, processing integrity, confidentiality, or privacy.

unauthorized access. Access to information or system components that (a) has not been approved by a person designated to do so by management and (b) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

vendor. (or supplier). An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the entity that are necessary to achieve the entity's objectives), it also might be a service provider.

Appendix B: Abbreviations

Abbreviation	Expanded Form
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
BI	Business Intelligence
CAB	Change Advisory Board
CCTV	Close Circuit Television
CDM	Career Development Matrix
CISO	Chief Information Security Officer
CSAT	Customer Satisfaction
DG	Diesel Generator
DLP	Data Loss Prevention
DPA	Data Processing Agreement
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
EP	Enterprise Portal
GRC	Governance, Risk and Compliance
HR	Human Resources
HTTPS	Hypertext Transfer Protocol Secure
IQA	Internal Quality Audit
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITSM	Information Technology Service Management
KPI	Key Performance Indicator
ML	Machine Learning
NC	Non-Conformance
NDA	Non-Disclosure Agreement
QMS	Quality Management System
RSN	Report Serial Number
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMS	Service Management System
UPS	Uninterruptible Power Supply
VA	Vulnerability Assessment
VCN	Virtual Cloud Network
VPN	Virtual Private Network

USA | INDIA | SINGAPORE | UAE | CANADA