



SOC 2 Type II Report

For the Period of February 1, 2023 to February 29, 2024

**REPORT ON CONTROLS PLACED IN OPERATION AT NAYAONE LIMITED
RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT
INCLUDING TEST PERFORMED AND RESULTS THEREOF.**



CONFIDENTIAL INFORMATION

The information contained in this report is confidential and shall not be duplicated, published, or disclosed in whole or in part, or used for other purposes, without the prior written consent of NayaOne Limited Corporate Entity.

Table of Contents

Section I – NayaOne Limited Management Assertion	1
Section II - Independent Service Auditor’s Report	2
Section III - Description of the NayaOne platform relevant to Security, Availability and Confidentiality throughout the period February 1, 2023 to February 29, 2024	5
Company & System Overview and Background	5
Purpose and Scope of the Report	5
Products and Services offered by NayaOne’s Platform	5
Organizational Structure.....	5
Overview of the company’s Internal Controls.....	6
Control Environment	6
Risk Assessment	7
Control Activities	8
Information and Communication.....	8
Internal Monitoring.....	9
Logical and Physical Access.....	9
Access Control, User, and Permissions Management.....	9
Revocation Process.....	10
Production Environment Logical Access.....	10
Remote Access	10
Physical Access and Visitors.....	10
Software Development Lifecycle (SDLC) Overview	10
Monitoring the Change Management Processes.....	11
Description of the Production Environment	11
Production Environment	11
Network Infrastructure.....	12
Web, Application, and Service Supporting Infrastructure Environment	12
Production Monitoring	12
Security and Architecture	12
Data Center Security.....	13
Infrastructure Security.....	13
Application Security.....	13
Operational Security.....	14
Security Awareness & Training	14
Support	14
Ticketing and Management	14
Incident Management Process	15
Escalation Process	15
Availability Procedures	15
Database Backup	15
Data center availability procedures	15
Disaster Recovery	15
Monitoring Usage	16
Confidentiality Procedures	16
Data Encryption.....	16
Subservice Organization Carved-out Controls: Amazon Web Services (AWS)	17

NayaOne Limited’s Customers’ Responsibilities	17
Section IV - Description of Criteria, Controls, Tests and Results of Tests	19
Testing Performed and Results of Tests of Entity-Level Controls	19
Criteria and controls	19
Control Environment	20
Communication and Information	24
Risk Assessment	28
Monitoring Activities	32
Control Activities.....	33
Logical and Physical Access Controls	36
System Operations.....	45
Change Management	49
Risk Mitigation	51
Availability	53
Confidentiality	56



NayaOne

Section I – NayaOne Limited Management Assertion

April 7, 2024

We have prepared the accompanying “Description of the NayaOne platform relevant to Security, Availability and Confidentiality throughout the period February 1, 2023 to February 29, 2024” (Description) of NayaOne Limited (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the NayaOne platform (System) that may be useful when assessing the risks arising from interactions with the System , particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Carved-out Unaffiliated Subservice Organization: NayaOne Limited uses Amazon Web Services (“AWS”) to provide infrastructure management services. The Description indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at NayaOne Limited to achieve the service commitments and system requirements. The Description presents NayaOne Limited’s controls and the types of complementary subservice organization controls assumed in the design of NayaOne Limited’s controls. The Description does not disclose the actual controls at the carved-out AWS.

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

- a. The Description presents the System that was designed and implemented throughout the period February 1, 2023 to February 29, 2024 in accordance with the Description Criteria.
- b. The controls stated in the Description were suitably designed throughout the period February 1, 2023 to February 29, 2024 to provide reasonable assurance that NayaOne Limited service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and if the carved-out subservice organization applied the controls assumed in the design of NayaOne Limited’s controls throughout that period.
- c. The NayaOne Limited controls stated in the Description operated effectively throughout the period February 1, 2023 to February 29, 2024 to provide reasonable assurance that NayaOne Limited’s service commitments and system requirements were achieved based on the applicable trust services criteria, if the carved-out subservice organization applied the controls assumed in the design of NayaOne Limited’s controls throughout that period.

Signature 

Title **Karan Jain**
CEO

Section II - Independent Service Auditor's Report

To the Management of NayaOne Limited

Scope

We have examined NayaOne Limited's accompanying "Description of the NayaOne platform relevant to Security, Availability and Confidentiality throughout the period February 1, 2023 to February 29, 2024" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022) (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period February 1, 2023 to February 29, 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022), in AICPA Trust Services Criteria.

NayaOne Limited uses AWS (subservice organization) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at NayaOne Limited, to provide reasonable assurance that NayaOne Limited's service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents NayaOne Limited's system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. The Description does not disclose the actual controls at AWS. Our examination did not include the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period February 1, 2023 to February 29, 2024.

NayaOne Limited's responsibilities

NayaOne Limited 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 its service commitments and system requirements were achieved. NayaOne Limited has provided the accompanying assertion titled, Management Assertion of NayaOne Limited (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. NayaOne Limited 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) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated therein to achieve the Service Organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) . Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period February 1, 2023 to February 29, 2024. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization’s service commitments and system requirements
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

We are required to be independent of NayaOne Limited and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1– Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and 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:

- a. the Description presents the NayaOne platform system that was designed and implemented throughout the period February 1, 2023 to February 29, 2024 in accordance with the Description Criteria.
- b. the controls stated in the Description were suitably designed throughout the period February 1, 2023 to February 29, 2024, to provide reasonable assurance that NayaOne Limited's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of NayaOne Limited's controls throughout that period.
- c. the controls stated in the Description operated effectively throughout the period February 1, 2023 to February 29, 2024 to provide reasonable assurance that NayaOne Limited service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and user entity controls assumed in the design of NayaOne Limited's controls operated effectively throughout that period.

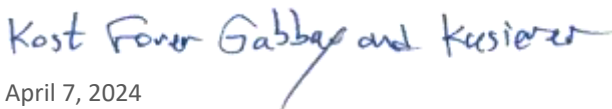
Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of NayaOne Limited, user entities of NayaOne Limited's system during some or all of the period February 1, 2023 to February 29, 2024 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

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

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

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global



April 7, 2024
Tel-Aviv, Israel



Section III - Description of the NayaOne platform relevant to Security, Availability and Confidentiality throughout the period February 1, 2023 to February 29, 2024

Company & System Overview and Background

The platform of NayaOne enables Financial Services firms to connect to FinTechs and datasets and build and evaluate new propositions, before scaling them to production. All financial firms are facing ever-changing market conditions, which requires them to accelerate their innovation. Using a modular, cloud-native, Fintech-as-a-Service and Digital Sandbox platform provides NayaOne partners the flexibility to discover, evaluate and scale third-party solutions. NayaOne is based in London, UK.

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting NayaOne Platform and does not extend to other available software products and services or the controls at third third-party service providers.

Note: Parenthetical references have been included in the following narrative as a cross-reference to the applicable control procedures included in the Description of Criteria, Controls, Tests, and Results of Tests section of this report.

Products and Services offered by NayaOne’s Platform

NayaOne’s platform enables Financial Services firms to connect to FinTechs and datasets and build and evaluate new propositions securely, before scaling them to production. Using a highly modular, cloud-native, Fintech-as-a-Service platform provides NayaOne partners the flexibility to discover, evaluate and scale third party solutions.

Organizational Structure

The organization has defined structures, reporting lines with assigned authority and responsibilities to appropriately meet the security requirements (3). NayaOne's organizational structure provides the overall framework for planning, directing, and controlling operations. The organizational chart is documented and clearly defines management authorities and reporting hierarchy:



Description of key personnel roles & responsibilities

- Chief Executive Officer (CEO): responsible for overseeing the entire organization and making high-level decisions that impact the company's future.
- Head of Engineering: responsible for leading the company's engineering team and overseeing the development and maintenance of the company's products and technology.
- Product Manager: responsible for guiding the development and launch of innovative financial products that meet customer needs and drive company growth.
- Director of Financial Services and Sales: responsible for managing the company's financial operations, including budgeting, financial planning, and reporting.

- Director, Financial Services and Operations: responsible for managing both financial operations and operational processes to ensure efficiency and compliance within the organization.
- Head of Marketing and Growth: responsible for leading marketing initiatives and growth strategies to expand the company's market presence and drive revenue growth.
- Head of Client Solutions: responsible for developing and delivering tailored solutions to meet the needs of clients, ensuring satisfaction and long-term partnerships.
- Ecosystem and Marketplace Manager: responsible for managing relationships and operations within the company's marketplace ecosystem, fostering growth and value for all participants.
- Data Scientist: responsible for using data and advanced analytics to drive decision-making and drive growth across the organization.
- Project Manager: responsible for overseeing the planning, execution, and delivery of projects within the organization, ensuring they are completed on time and meet customer needs.

Overview of the company's Internal Controls

A company's internal control is a process – effected by NayaOne's Boards of Directors, management, and other personnel – designed to enable the achievement of objectives in the following categories:

- Adherence to the organization policies and procedures
- Effectiveness and efficiency of operations
- Compliance with applicable laws and regulations

The following section is a description of the five components of internal controls for NayaOne, namely:

1. Control environment
2. Control activities
3. Risk assessment
4. Information and Communication
5. Internal Monitoring

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the board of directors, and others concerning the importance of controls and the emphasis given to controls in NayaOne's policies, procedures, methods, and organizational structure. The control environment defines a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. A control environment is the base on which NayaOne is to establish an effective system and allow strategic objectives to be met, operate most effectively and efficiently, safeguard assets, and comply with required legal responsibilities.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through NayaOne's:

- Management operating style
- Organizational structure
- Employee job descriptions
- Organizational policies and procedures

Board of directors - The board of directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control **(1)**. The board establishes oversight responsibilities, applies relevant expertise, and operates independently from management. The Board's responsibilities include but are not limited to monitoring the actual performance of the company through its company strategy, and approving equity-based compensation plans in which directors, officers, or employees may participate.



Management Philosophy and Operating Style – The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives (2). They also evaluate risks and threats and discuss security, confidentiality, and availability non-compliance issues. In its role, the management team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The management team designs policies and communications so that personnel understand NayaOne's objectives, know how their actions interrelate and contribute to those objectives, and recognize how and for what they are held accountable.

Human Resources Policy and Practices – Human resources policies and practices related to hiring, orienting, training, evaluating, promoting, and compensating personnel. The competence of NayaOne's personnel is an essential element of its control environment. The organization's ability to recruit and retain highly trained, competent and responsible personnel is dependent to a great extent on its human resources policies and practices. Responsibility and accountability for developing and maintaining the policies are assigned to the relevant personnel and approved on an annual basis by the management team. Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees (4). New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses. Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring process (6). Management monitors employees' compliance with an official signature. The company performs an annual formal evaluation of resourcing and staffing including assessment of employee qualification alignment with the company's objectives. Employees receive feedback on their strengths and weaknesses annually (10).

Commitment to Competence - Competence at NayaOne is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform professional assignments, and (4) through the performance evaluation process, identify opportunities for growth and improvement. The company provides education and training to ensure skill sets and technical competency of employees are developed and maintained (9). The company conducts pre-employment screening checks of candidates commensurate with the employee's position and level, in accordance with local laws and the HR policy (7). New employees go through an onboarding process to be informed of their role responsibilities, organizational policies, and provision of relevant access (8). The company's employees are required to read and accept the code of conduct, acceptable use policy, and Non-Disclosure agreement (NDA) upon their hire. Management monitors employees' compliance with an official signature (5). New hires are granted access to the relevant environments following an HR notification. The permission credentials depend on the employee's role & responsibilities (37).

Risk Assessment

NayaOne is committed to managing and minimizing risk by identifying, analyzing, assessing, mitigating, and treating exposures that may hinder, prevent or otherwise impact the company from achieving its goals and serving its clients. NayaOne recognizes risk management as a strong consideration in strategic and operational planning, daily management, and decision-making at all levels of the company.

Risk identification: The process of identifying, assessing, and managing risks is a critical component of NayaOne's system of internal controls. The purpose of NayaOne's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis identifies key business processes in which potential exposures of some consequence exist. Exposures consider both internal and external influences that may harm NayaOne's ability to provide reliable services. The risk identification process addresses the following at minimum:

- Identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles
- Assessing the criticality of information assets



- Identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events
- Identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, business partners, customers, and others with access to NayaOne's information systems.

Risk assessment: The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance (22). The process is documented and maintained and all remediation activities must be approved by management. Key NayaOne stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. The yearly risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented (23). The assessment process includes instructions on how the risk should be managed and whether to accept, avoid, limit, or transfer the risk.

Risk mitigation: Once the severity and likelihood of a potential risk have been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. Risks are mitigated to acceptable levels based on risk level, including resolution time frames, which are established, documented and approved by management (64).

The risk mitigation process is integrated into the company's risk assessment. IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company (69). In addition, the company assesses, on an annual basis, the risks that vendors and business partners represent to the achievement of the Company's objectives (67).

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks. NayaOne's operating and functional units are required to implement control activities that help achieve business objectives associated with the following:

- Adherence to the organization policies and procedures
- The effectiveness and efficiency of operations
- Compliance with applicable laws and regulations

The control activities are designed to address specific risks associated with NayaOne operations and are reviewed as part of the risk assessment process. NayaOne has developed formal policies and procedures covering various operational matters to document the requirements for the performance of many control activities.

Information and Communication

Information and communication are integral components of NayaOne's internal control system. They involve the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At NayaOne, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Internal Communication

A detailed description of the product architecture and system boundaries is documented and available internally to the company's employees (11). Changes are documented within the system and approved by authorized employees. In



addition, NayaOne's approved policies as well as the process of informing their customers and business partners about breaches of the system Security, Availability, and Confidentiality are communicated to personnel responsible for implementing them in the internal application. The company maintains an internal informational knowledge base describing the company's environment, its boundaries, user responsibilities and services **(13)**. Release notes are available internally upon release of the version to the production environment describing the closed stories that were part of the version **(17)**.

External Communication

The company maintains external documentation describing the product features, system boundaries, user guides, and services commitments **(15)**. New features are communicated to customers through email to update on new product features **(16)**.

Internal Monitoring

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand NayaOne's objectives. The assigned policy owner reviews and approves the policy every year, and responsibility and accountability for developing and maintaining the policies are assigned to NayaOne's relevant teams.

Logical and Physical Access

NayaOne has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. A security policy is documented by NayaOne management and is reviewed and approved on an annual basis.

Access Control, User, and Permissions Management

Access to NayaOne information assets is restricted. NayaOne employees and contractors will not be granted access to any information asset that is not directly needed for their work in NayaOne. The company manages access governance through a role-based access control matrix based on the job description and responsibilities **(26)**. Access to organizational systems above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning **(27)**. Several controls are in place to ensure that access management is properly done:

- Access to the identity management tool is performed using two-factor authentication and is restricted to authorized personnel **(31)**.
- Access to sensitive databases is restricted to authorized users and uses two-factor authentication **(33)**.
- Access to the source control tool is performed using two-factor authentication and is restricted to authorized personnel **(34)**.
- Access to alter and delete backups is restricted to authorized users and uses two-factor authentication **(35)**.
- User access and permissions in restricted environments are reviewed and approved by the company's management on an annual basis **(37)**.

Additionally, access authorization is defined based on work purposes only. The company has established a formal standard for passwords to govern the management and use of authentication mechanisms. Strong password configuration settings, where applicable, are enabled and including:

- (1) Use a minimum of 12 characters
- (2) Use upper case, lower case, numeric, and special character values
- (3) Enforced password history policy with at least 5 previous passwords remembered **(29)**.



Access to system resources is protected by means of the following security measures:

1. The company has established key management process in place to support the organization's use of cryptographic techniques **(36)**.
2. The company secures and controls its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies **(48)**.

Revocation Process

User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination **(38)**.

The company's employees return the organizational assets in their possession upon termination of their employment **(40)**.

Production Environment Logical Access

The production environment access is protected and restricted. Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method **(32)**. Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval **(26)**.

Privileged access rights are defined as any access authorizations created for the employee for their work, temporarily or permanently, beyond those specified in respect of their position in the user permissions table.

Remote Access

All NayaOne employees adhere to and should be connected via company password policy and MFA mechanisms in order to enforce and ensure stringent security measures when connecting to NayaOne via a remote connection.

Physical Access and Visitors

Physical access to the offices is restricted to authorized personnel using codes for each door. The codes are needed within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities **(41)**. While at NayaOne offices, employees are required to wear the company access card.

Visitors to NayaOne offices are required to be accompanied by a NayaOne employee at all times during their stay. Employees encountering an unfamiliar or suspicious person wandering around the office are expected to ask them politely about the nature of their business and if necessary, accompany them to their host. Visitors are not allowed to access or connect to NayaOne company's network or equipment.

Software Development Lifecycle (SDLC) Overview

Tickets are used to document and prioritize change requests within the change management system. Pull requests and change tickets are linked to each other so the code change can be tracked **(58)**. Change management procedures have clearly defined roles and responsibilities. The authorization of change requests is performed by the owner or business unit manager **(59)**. Code changes must be reviewed and approved in order to progress through the SDLC and deploy a version to production **(60)**.

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the change management application. Each change goes through a life cycle. The company developed a process in order to manage emergency changes ('hotfix'). Post approval process is performed for each emergency change **(64)**.



Software Testing and QA Process: Procedures are in place to ensure automated testing is performed on approved data and test plans in order to ensure the overall security status of the production environment. In the event that automated test failures are detected, a notification is sent to relevant stakeholders **(62)**.

Software Release: A successful test result is mandatory in order to continue with the SDLC process and deploy a version to the production environment **(63)**. Deployment of new releases into the production is restricted to authorized personnel and performed automatically **(65)**.

Monitoring the Change Management Processes

Changes that may affect system Security, Availability, and Confidentiality-related issues are communicated through emails to the different team owners. Changes are documented within the system and approved by authorized employees.

Description of the Production Environment

Production Environment

The processes described below are executed within NayaOne's production environment, which is hosted through AWS Virtual Private Cloud - located globally.

The currently utilized cloud provider locations are based in Ireland. The facilities comply with NayaOne's standards of security and reliability, which enable NayaOne to provide its services efficiently and stably.

The company enforces segregation between development, staging and production environments to enforce confidentiality and privacy on customers data **(66)**.

Note: Controls performed by the data center service providers are not included in the scope of this report.

NayaOne's infrastructure runs on top of AWS's Infrastructure as a Service (IaaS) and utilizes various services such as:

- ACM
- CloudFormation
- EC2
- Elastic load balancer
- EBS
- RDS
- S3
- Secret Manager
- CloudFront
- Guard Duty
- CloudTrail
- IAM
- AWS WAF
- CloudWatch

The use of the above AWS services is designed to make web-scale computing easier for NayaOne, and enable NayaOne to perform (but are not limited to) the following:

- Create and run virtual machines utilizing the Cloud provider's infrastructure through the secure and customizable computing service (Compute Engine). This enables resource optimization, data encryption, and reduced computing costs as a result of the utilized virtual machine.
- Vulnerability assessments can be performed automatically using container registry.



- Additionally, other utilized AWS services enable automatic logging of data, system monitoring, and storage functionality to NayaOne.

Network Infrastructure

The company has enabled multiple network security controls, such as VPC security, cloud firewall, SSH restriction, port restriction, VPN, and remote access restriction **(42)**. Robust network infrastructure is essential for reliable and secure real-time data communication between NayaOne's cloud service components. To provide sufficient capacity, NayaOne's network infrastructure relies on platforms provided by AWS. To ensure appropriate network security levels, NayaOne security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality, and availability. NayaOne's security model encompasses the following components:

- Application layer security, including:
 - Various authentication schemas such as multi-factor authentication (MFA), unique ID, and complex password policy
 - Logical security
 - Penetration testing
 - IP address source restriction
 - Customers' data encryption at rest and in transit
- Network and infrastructure security, including:
 - Network architecture
 - Risk management
 - AWS data centers
 - Cloud operation security (change management, monitoring, and log analysis)
 - Network vulnerability scanning
 - Intrusion detection/prevention systems

Web, Application, and Service Supporting Infrastructure Environment

NayaOne utilizes the clustered infrastructure design of AWS to provide redundancy and high availability. In addition, the infrastructure is configured in a way that enables auto-scaling capabilities. This allows for supporting high performance during demand spikes for the services. Intrusion detection system continuously scans for potential security issues and alerts the administrator upon discovering unexpected and potentially malicious activity in the production environment **(49)**.

Production Monitoring

NayaOne has an established internal audit function that evaluates management's compliance with NayaOne's identity management, source code management, and infrastructure controls. A suite of monitoring tools is used by the company to monitor usage, capacity, and performance. Alerts are sent to relevant stakeholders based on predefined rules or anomalies. The notifications are reviewed and processed according to their level of urgency **(70)**. Actions performed in the production environment, including OS, DB, and application are monitored, logged, and reviewed. Audit trail (security logs) is deployed on the production environment continuously to capture actions made directly by the user or a cloud service **(51)**. Audit trail retention is configured for 365 days **(52)**.

Security and Architecture

NayaOne provides a secure, reliable, and resilient Software-as-a-Service platform that has been designed based on industry best practices. The below addresses the network and hardware infrastructure, software, and information security elements that NayaOne delivers as part of this platform, database management system security, application

controls, and intrusion detection monitoring software. Intrusion detection system scans continuously for potential security issues and alerts the administrator upon discovering unexpected and potentially malicious activity in the production environment **(53)**. A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring **(54)**.

Data Center Security

NayaOne relies on the global infrastructure of AWS which can include the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage.

This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards and regulations.

The environmental protection managed by the vendors' policies are:

- **Redundancy** - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- **Fire Detection and Suppression** – Automatic fire detection and suppression equipment have been installed to reduce risk.
- **Redundant Power** – the data center electrical power systems are designed to be fully redundant and maintainable without impact on operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure. Data centers use generators to provide backup power for the entire facility.
- **Climate and Temperature Controls** – maintain a constant operating temperature and humidity level for all hardware.
- **Physical access** - AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures, and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion **(68)**.

Infrastructure Security

- **End-to-End Network Isolation** - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud from being intercepted.
- **External & Internal enforcement points** - All servers are protected by restricted AWS firewall rules. The configuration of the cloud providers' firewall rules is restricted to authorized personnel.
- **Server Hardening** - all servers are hardened according to industry best practices.

Application Security

- **Penetration Testing** - The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner **(25)**.
- **Vulnerabilities Management** - Internal vulnerability scanning is performed by the relevant teams using sufficient tools. Production networks undergo vulnerability scans continuously. When an incident is detected, a ticket is created and assigned to the relevant personnel to resolve the issue in a timely manner **(50)**. Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated in a timely manner **(61)**.

- **Segregation of Customer Data** - During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. Part of NayaOne's logical security procedures is to ensure users are segregated from each other.

Operational Security

- **Configuration and Patch Management** – NayaOne makes use of a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components. Patch management is in process for the company's laptops and servers. Security settings are hardened and cannot be changed by users. Alerts and remediation are triggered automatically when deficiencies are discovered.
- **Security Incident Response Management** - The company has developed a security incident response policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations (56). Whenever a security incident of a physical or electronic nature is suspected or confirmed, NayaOne's engineers are instructed to follow appropriate procedures. Customers and legal authorities are notified as required by Privacy regulations. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet NayaOne's objectives related to privacy.
- **Endpoint Protection** - Endpoint protection platform is installed on employees' devices (i.e., workstations and laptops), centrally managed and configured to receive updates regularly (49). Alerts are sent to the security owner in case the agent has identified suspicious activity on the endpoint device.

Security Awareness & Training

All NayaOne employees need to be well aware of their information security responsibilities. Awareness is achieved by communicating NayaOne's security policies and guidelines to employees in various ways. The NayaOne security team works to implement security awareness and responsibilities based on the NayaOne security awareness program.

NayaOne's management encourages security-related professional development and education. Adequate funding and resources are dedicated to relevant professional development and education, according to the global NayaOne training plan and security awareness program.

The company has established a security awareness training program and requires all employees to complete this training every year (12).

The NayaOne security awareness training includes the following:

- Common security risks and threats, compliance matters, regulations, and Acceptable Use Policy
- Information security, proper data protection, and privacy of customers' data
- Mobile devices (laptops) security
- Training on Social engineering, fraud, and phishing

Support

Customers are notified of service interruptions through the company's website, based on the service level agreement (SLA) (18). Response time to customer's issues is defined at the SLA. The agreement is communicated to the customers as part of the contract (20). Customers can contact the support team through dedicated support channels. Client issues are reported to the company via a dedicated support email address. Support issues are handled by using a ticketing system (19). Customers, business partners, and suppliers are provided with communication channels on the website to report failures, incidents, and other complaints to the company (21).

Ticketing and Management

NayaOne opens a ticket when a client raises an issue or when an issue is proactively identified. NayaOne uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution.

Incident Management Process

NayaOne has a defined and implemented Incident Management Policy. Within the policy, there are defined processes and procedures to be followed for respective incident types. The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents (56). The detailed Incident Management Policy includes and details the different phases of incident management and response, including the various response protocols - which detail the appropriate reporting and escalation procedures and personnel to contact for each respective incident type. A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring (50). A root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution (57).

Escalation Process

NayaOne's goal is to resolve issues efficiently. The issue is tracked and updated in the support ticketing system. The escalation process is defined and documented by Customer Support. The company uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders by an internal communication tool, based on predefined rules. The notifications are reviewed and processed according to their level of urgency.

Availability Procedures

As part of its current backup retention policy, NayaOne utilizes the services of cloud storage for all files saved to network drives. Corporate cloud storage is on AWS Workplace associated with NayaOne company email accounts and shared Drive. In addition, Production logs are backed up in AWS cloud storage.

NayaOne has implemented the operations management controls described below to manage and execute production operations. Daily incremental backups are performed using a cloud service. The backup is retained for 14 days (73).

Database Backup

The backup schedule for servers and databases is as follows:

- Full daily backups (snapshots)
- Backups are performed automatically based on a time-interval
- Backups are stored in a secure and restricted area in AWS cloud services in different availability zones.

Data center availability procedures

The NayaOne production environment is located in several availability zones to maintain high availability standards (72).

Disaster Recovery

The company conducts disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results and lessons learned from the tests (75).

The company has developed a disaster recovery plan (DRP) to continue to provide critical services in the event of a disaster. The DRP is reviewed on an annual basis (74). This is to coordinate the recovery of critical business functions in managing and supporting the business recovery in the event of a service disruption or facility disaster. A disaster is defined as any event that renders a business and its facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.

The DR plan for NayaOne includes the following phases:

1. Discovery phase



2. Crisis management phase
3. Assessment and decision phase
4. Recovery/continuity phase.

Testing is essential to validate that those plans remain effective, personnel is familiar with the DR Plan, and the information contained within is correct, thus helping assure that the plans will work when needed. The purpose of this section is to identify and document the procedures for testing the Disaster Recovery Plan. NayaOne performs a full Disaster Recovery test at least once a year. The test simulates at least one of the emergency scenarios and involves the DMT and all relevant departments.

Disaster Recovery tests are fully documented. A “Lessons learned” meeting takes place after each test, to analyze NayaOne’s performance during the test. The DR plan is updated according to the findings of this meeting.

Monitoring Usage

A suite of monitoring tools is used by the company to monitor usage, capacity, and performance. Alerts are sent to relevant stakeholders based on predefined rules or anomalies. The notifications are reviewed and processed according to their level of urgency. Critical NayaOne system components are replicated across multiple Availability Zones and backups are maintained. Actions performed in the production environment, including OS, DB, and application are monitored, logged, and reviewed. A formal report is prepared to reflect the system's availability.

Confidentiality Procedures

Customer confidentiality is a key factor in NayaOne. As such, NayaOne has implemented security measures to ensure the confidentiality of its customers' sensitive personal information. The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the SRE Engineer on an annual basis **(24)**. All active devices in the production network are included for tracking and reporting purposes. Within the information asset inventory, classification and categorization of assets are performed based on the type of access, type of data, the sensitivity of data, and the criticality level of the asset impact to the business and the continuation of its operations. The company has implemented the capability of tracking and identifying customer data in its assets (i.e., databases, storage, backups) **(77)**. Data assets containing customer and confidential information are identified and protected. Data retention depends on the type of asset and the management commitments **(76)**. Data loss prevention (DLP) system is used to validate that employees do not send sensitive or critical information outside sensitive environments. The DLP system classifies regulated, confidential, and business-critical data and identifies violations of policies defined by the company. Alerts are sent to the administrator upon breach of the policy **(47)**.

Upon Customer request at the end of a contract agreement, NayaOne will dispose of customer confidential information. The company has procedures in place to dispose of confidential information according to the company's data retention and disposal policy **(78)**. In addition, customers' passwords are hashed and salted within the company's user database **(43)**. Business partners are required to sign an agreement containing a confidentiality clause.

Confidentiality commitments included in agreements with vendors and third parties with restricted access are reviewed by NayaOne and the third party at the time of contract creation or renewal.

Data Encryption

NayaOne uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk. Processes are in place to protect encryption keys during generation, storage, use, and destruction. The company's employees use a secure password manager to save, store and organize their passwords and logins in a vault encrypted to their device **(30)**. Apps and software installations are restricted to a defined list of approved software. Installation of new software needs to be requested and approved by the IT department **(44)**.



Data in Transit

Encrypted communication between the company's customers and the company's assets is enabled using a valid HTTPS TLS 1.2 authenticated certificate **(44)**.

Data at Rest

Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted **(45)**. Customer content stored at rest is encrypted, without any action required from the customer, using one or more encryption mechanisms; data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key; data encryption keys are stored with the data, and encrypted with key encryption keys that are exclusively stored and used inside the providers' central key management services; which are redundant and globally distributed. Memory storage of the company's operational devices (i.e. workstations and laptops) is encrypted to ensure safety of sensitive information **(46)**.

Subservice Organization Carved-out Controls: Amazon Web Services (AWS)

The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict the access to the virtual and physical servers, software, firewalls and physical storage to authorized individuals and to review the list of users and permissions on a regular basis.
- Implement controls to:
 - Provision access only to authorized persons
 - Remove access when no longer appropriate
 - Secure the facilities to permit access only to authorized persons
 - Monitor access to the facilities
- Be consistent with defined system security as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, related policies.
- Provide that only authorized tested and documented changes are made to the system.
- Implement and maintain procedures exist and measures consistent with the risk assessment to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

NayaOne Limited's Customers' Responsibilities

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with NayaOne.
- Ensuring timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with NayaOne's services.
- Maintaining authorized, secure, timely, and complete transactions for user organizations relating to NayaOne's services.
- Protecting data that is sent to NayaOne by using appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- Implementing controls requiring additional approval procedures for critical transactions relating to NayaOne's services.
- Reporting to NayaOne in a timely manner any material changes to their overall control environment that may adversely affect services being performed by NayaOne.



Description of the NayaOne relevant to Security, Availability and Confidentiality for the Period
February 1, 2023 to February 29, 2024

- Notifying NayaOne in a timely manner of any changes to personnel directly involved with services performed by NayaOne. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by NayaOne.
- Adhering to the terms and conditions stated within their contracts with NayaOne.
- Developing, and if necessary, implementing a business continuity and disaster recovery plan (DRP) that will aid in the continuation of services provided by NayaOne.

Section IV - Description of Criteria, Controls, Tests and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by NayaOne Limited, KFGK considered the aspects of NayaOne Limited control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of NayaOne Limited. The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

Description of Criteria, Controls, Tests and Results of Tests

Control Environment

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The board of directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	Inspected the invitations and minutes for a sample of board of directors meetings and determined that the board of directors met quarterly, demonstrated independence from management, and exercised oversight of the development and performance of internal control.	No deviations noted.
5	The company's employees are required to read and accept the code of conduct, acceptable use policy, and Non-Disclosure agreement (NDA) upon their hire. Management monitors employees' compliance with an official signature.	<p>Inspected the signed acceptable use policy and code of conduct monitored in the HR platform for a sample of new employees hired during the audit period and determined that NayaOne's employees were required to read and accept the code of conduct and acceptable use policy upon their hire. Management monitored employees' compliance with an official signature.</p> <p>Inspected the NDA for a sample of new employees hired during the audit period and determined that NayaOne's employees were required to read and accept the Non-Disclosure agreement (NDA) upon their hire.</p>	No deviations noted.
69	IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company.	Inspected the IT vendors terms and conditions agreement and determined that IT vendors that engaged in business with the company were subjected to information security, confidentiality, and privacy commitments as part of their agreements with the company.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The board of directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	Inspected the invitations and minutes for a sample of board of directors meetings and determined that the board of directors met quarterly, demonstrated independence from management, and exercised oversight of the development and performance of internal control.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives.	Inspected the invitations and minutes for a sample of management meetings and determined that the management of the company convened a meeting on a monthly basis and had a fixed agenda to oversight the company's objectives.	No deviations noted.
3	The organization has defined structures, reporting lines with assigned authority and responsibilities to appropriately meet the security requirements.	Inspected the company's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were defined.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.	
6	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	<p>Inspected job descriptions in a job recruitment platform and determined that job descriptions were documented and maintained within a job recruitment platform.</p> <p>Inspected documentation of the pre-employment screening for a sample of new employees hired during the audit period and the recruitment platform determined that candidates' abilities to meet the jobs' requirements were evaluated as part of the hiring process.</p>	No deviations noted.
7	The company conducts pre-employment screening checks of candidates commensurate with the employee's position and level, in accordance with local laws and the HR policy.	<p>Inspected documentation of the pre-employment screening for a sample of new employees hired during the audit period and determined that NayaOne conducted pre-employment screening checks of candidates commensurate with the employee's position and level.</p> <p>Inspected the company's HR policy and determined that NayaOne conducted pre-employment screening checks of candidates commensurate in accordance with local laws and the HR policy.</p>	No deviations noted.
8	New employees go through an onboarding process to be informed of their role responsibilities, organizational policies, and provision of relevant access.	Inspected the onboarding checklists for a sample of new employees hired during the audit period and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different policies.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	The company provides education and training to ensure skill sets and technical competency of employees are developed and maintained.	Inspected the training materials and the record of employees' participation and determined that NayaOne provided education and training to relevant departments to ensure skill sets and technical competency of employees were developed and maintained.	No deviations noted.
12	The company has established a security awareness training program and requires all employees to complete this training every year.	Inspected the security awareness training materials and determined that NayaOne has established a security awareness training for employees on an annual basis. Inspected the security awareness training records for a sample of the company's employees and determined that NayaOne's employees were required to complete this training.	No deviations noted.
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
10	The company performs an annual formal evaluation of resourcing and staffing including assessment of employee qualification alignment with the company's objectives. Employees receive feedback on their strengths and weaknesses annually.	Inspected the annual feedback records for a sample of the company's employees and determined that NayaOne performed an annual formal evaluation of resourcing and staffing including assessment of employee qualification alignment with the company's objectives. Employees received feedback on their strengths and weaknesses annually.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

Communication and Information

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis. Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.	No deviations noted.
11	A detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.	Inspected the company's product architecture diagram and determined that a detailed description of the product architecture and system boundaries was documented. Inspected the company's internal portal and determined that the company's product architecture was available internally to the company's employees.	No deviations noted.
15	The company maintains external documentation describing the product features, system boundaries, user guides, and services commitments.	Inspected the company's website and determined that NayaOne maintained external documentation describing the product features, system boundaries, user guides, and services commitments.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The board of directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	Inspected the invitations and minutes for a sample of board of directors meetings and determined that the board of directors met quarterly, demonstrated independence from management, and exercised	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		oversight of the development and performance of internal control.	
2	The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives.	Inspected the invitations and minutes for a sample of management meetings and determined that the management of the company convened a meeting on a monthly basis and had a fixed agenda to oversight the company's objectives.	No deviations noted.
3	The organization has defined structures, reporting lines with assigned authority and responsibilities to appropriately meet the security requirements.	Inspected the company's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were defined.	No deviations noted.
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis. Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.	No deviations noted.
12	The company has established a security awareness training program and requires all employees to complete this training every year.	Inspected the security awareness training materials and determined that NayaOne has established a security awareness training for employees on an annual basis. Inspected the security awareness training records for a sample of the company's employees and determined that NayaOne's employees were required to complete this training.	No deviations noted.
13	The company maintains an internal informational knowledge base describing the company's environment, its boundaries, user responsibilities and services.	Inspected the company's internal portal and determined that NayaOne maintained an internal informational knowledge base describing the company's environment, its boundaries, user responsibilities and services.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	Release notes are available internally upon release of the version to the production environment describing the closed stories that were part of the version.	Inspected the release notes available to employees during the audit period and determined that release notes were available internally upon release of the version to the production environment describing the closed stories that were part of the version.	No deviations noted.
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.
69	IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company.	Inspected the IT vendors terms and conditions agreement and determined that IT vendors that engaged in business with the company were subjected to information security, confidentiality, and privacy commitments as part of their agreements with the company.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	The company has established a security awareness training program and requires all employees to complete this training every year.	<p>Inspected the security awareness training materials and determined that NayaOne has established a security awareness training for employees on an annual basis.</p> <p>Inspected the security awareness training records for a sample of the company's employees and determined that NayaOne's employees were required to complete this training.</p>	No deviations noted.
15	The company maintains external documentation describing the product features, system boundaries, user guides, and services commitments.	Inspected the company's website and determined that NayaOne maintained external documentation describing the product features, system boundaries, user guides, and services commitments.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	New features are communicated to customers through email to update on new product features.	Inspected the release notes sent to customers during the audit period and determined that new features were communicated to customers through email to update on new product features.	No deviations noted.
18	Customers are notified of service interruptions through the company's website, based on the service level agreement (SLA).	Inspected the uptime report and determined that no service interruptions occurred during the audit period.	No deviations noted.
19	Client issues are reported to the company via a dedicated support email address. Support issues are handled by using a ticketing system.	Inspected the customer support mailbox and determined that client issues were reported to the company via a dedicated support email address. Inspected the ticket details for a sample of client support related issues submitted during the audit period and determined that client support issues were handled by using a ticketing system.	No deviations noted.
20	Response time to customer's issues is defined at the SLA. The agreement is communicated to the customers as part of the contract.	Inspected the SLA and determined that response time to customer's issues was defined at the SLA. Inspected a sample of contracts with customers and determined that the agreement was communicated to the customers as part of the contract.	No deviations noted.
21	Customers, business partners, and suppliers are provided with communication channels on the website to report failures, incidents, and other complaints to the company.	Inspected the company's communication channels and determined that customers, business partners, and suppliers were provided with communication channels on the website to report failures, incidents, and other complaints to the company.	No deviations noted.
69	IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company.	Inspected the IT vendors terms and conditions agreement and determined that IT vendors that engaged in business with the company were subjected to information security, confidentiality, and privacy commitments as part of their agreements with the company.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

Risk Assessment

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	<p>The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance.</p>	<p>Inspected the risk assessment and treatment policy and determined that the company maintained a formal risk management program to continuously discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers.</p> <p>Inspected the risk assessment matrix and determined that risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the risk assessment matrix and determined that a formal risk control matrix was updated annually.</p> <p>Inspected the risk assessment matrix and determined that the company's management acknowledged risk treatment decisions and approved risk acceptance.</p>	<p>No deviations noted.</p>
23	<p>The yearly risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.</p>	<p>Inspected the invitation for the risk assessment meeting and determined that senior management met on an annually basis.</p> <p>Inspected the meeting minutes documentation for the risk assessment meeting and determined minutes of the meeting and action items were documented.</p>	<p>No deviations noted.</p>

Description of Criteria, Controls, Tests and Results of Tests

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance.	<p>Inspected the risk assessment and treatment policy and determined that the company maintained a formal risk management program to continuously discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers.</p> <p>Inspected the risk assessment matrix and determined that risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the risk assessment matrix and determined that a formal risk control matrix was updated annually.</p> <p>Inspected the risk assessment matrix and determined that the company's management acknowledged risk treatment decisions and approved risk acceptance.</p>	No deviations noted.
23	The yearly risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	<p>Inspected the invitation for the risk assessment meeting and determined that senior management met on an annually basis.</p> <p>Inspected the meeting minutes documentation for the risk assessment meeting and determined minutes of the meeting and action items were documented.</p>	No deviations noted.
24	The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the SRE Engineer on an annual basis.	Inspected the asset mapping documentation and determined that NayaOne identified, classified and managed the inventory of information assets.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the assets mapping documentation and determined that the assets inventory was reviewed by the SRE Engineer on an annual basis.	
67	The company assesses, on an annual basis, the risks that vendors and business partners represent to the achievement of the Company's objectives.	Inspected the vendors assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
68	The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	Inspected the review of the data center SOC 2 report performed by NayaOne and determined that the review was performed annually and included investigation of deviations, auditor's opinion and identifying and documenting the controls in place at Nilus to address the CUECs.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance.	<p>Inspected the risk assessment and treatment policy and determined that the company maintained a formal risk management program to continuously discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers.</p> <p>Inspected the risk assessment matrix and determined that risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the risk assessment matrix and determined that a formal risk control matrix was updated annually.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the risk assessment matrix and determined that the company's management acknowledged risk treatment decisions and approved risk acceptance.	
23	The yearly risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	<p>Inspected the invitation for the risk assessment meeting and determined that senior management met on an annually basis.</p> <p>Inspected the meeting minutes documentation for the risk assessment meeting and determined minutes of the meeting and action items were documented.</p>	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance.	<p>Inspected the risk assessment and treatment policy and determined that the company maintained a formal risk management program to continuously discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers.</p> <p>Inspected the risk assessment matrix and determined that risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the risk assessment matrix and determined that a formal risk control matrix was updated annually.</p> <p>Inspected the risk assessment matrix and determined that the company's management acknowledged risk treatment decisions and approved risk acceptance.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
23	The yearly risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	<p>Inspected the invitation for the risk assessment meeting and determined that senior management met on an annually basis.</p> <p>Inspected the meeting minutes documentation for the risk assessment meeting and determined minutes of the meeting and action items were documented.</p>	No deviations noted.
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.

Monitoring Activities

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives.	Inspected the invitations and minutes for a sample of management meetings and determined that the management of the company convened a meeting on a monthly basis and had a fixed agenda to oversight the company's objectives.	No deviations noted.
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	<p>Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis.</p> <p>Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
25	An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.	Inspected the penetration test report and determined that an external web application penetration test was conducted annually. Inspected the penetration test report and determined that there were no high or critical issues.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives.	Inspected the invitations and minutes for a sample of management meetings and determined that the management of the company convened a meeting on a monthly basis and had a fixed agenda to oversight the company's objectives.	No deviations noted.
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis. Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.	No deviations noted.

Control Activities

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives.	Inspected the invitations and minutes for a sample of management meetings and determined that the management of the company convened a meeting on a	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		monthly basis and had a fixed agenda to oversight the company's objectives.	
22	The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance.	<p>Inspected the risk assessment and treatment policy and determined that the company maintained a formal risk management program to continuously discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers.</p> <p>Inspected the risk assessment matrix and determined that risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the risk assessment matrix and determined that a formal risk control matrix was updated annually.</p> <p>Inspected the risk assessment matrix and determined that the company's management acknowledged risk treatment decisions and approved risk acceptance.</p>	No deviations noted.
26	Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.	<p>Inspected the list of users with access to the production environment and the permissions policy of the production environment and determined that developers did not have access to the production environment.</p> <p>Inspected a sample of access requests and determined that developers were granted temporary access for emergency purposes and these accesses were documented and included an approval.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The management of the company convenes a meeting on a monthly basis, and has a fixed agenda to oversight the company's objectives.	Inspected the invitations and minutes for a sample of management meetings and determined that the management of the company convened a meeting on a monthly basis and had a fixed agenda to oversight the company's objectives.	No deviations noted.
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis. Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.	No deviations noted.
38	User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination.	Inspected the offboarding checklists as a sample of terminated employees and determined that user accounts were disabled or deleted on the production and other organizational information assets timely upon notification of job termination.	No deviations 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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis. Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.

Logical and Physical Access Controls

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	A detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.	Inspected the company's product architecture diagram and determined that a detailed description of the product architecture and system boundaries was documented. Inspected the company's internal portal and determined that the company's product architecture was available internally to the company's employees.	No deviations noted.
24	The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the SRE Engineer on an annual basis.	Inspected the asset mapping documentation and determined that NayaOne identified, classified and managed the inventory of information assets. Inspected the assets mapping documentation and determined that the assets inventory was reviewed by the SRE Engineer on an annual basis.	No deviations noted.
26	Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.	Inspected the list of users with access to the production environment and the permissions policy of the production environment and determined that developers did not have access to the production environment.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected a sample of access requests and determined that developers were granted temporary access for emergency purposes and these accesses were documented and included an approval.	
27	Access to organizational systems above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.	Inspected the access request ticketing board and a sample of access requests and determined that access to organizational systems above least privileged, including administrator accounts, was approved by appropriate personnel prior to access provisioning.	No deviations noted.
28	The company manages access governance through a role-based access control matrix based on the job description and responsibilities.	Inspected the access control matrix and determined that NayaOne managed access governance through a role-based access control matrix based on the job description and responsibilities.	No deviations noted.
29	The company has established a formal standard for passwords to govern the management and use of authentication mechanisms. Strong password configuration settings, where applicable, are enabled and including: (1) Use a minimum of 12 characters (2) Use upper case, lower case, numeric, and special character values (3) Enforced password history policy with at least 5 previous passwords remembered.	Inspected the SSO password configuration and determined that NayaOne established a formal standard for passwords to govern the management and use of authentication mechanisms. Strong password configuration settings, where applicable, were enabled and including: (1) use a minimum of 12 characters, (2) use upper case, lower case, numeric, and special character values, (3) enforced password history policy with at least 5 previous passwords remembered.	No deviations noted.
30	The company's employees use a secure password manager to save, store and organize their passwords and logins in a vault encrypted to their device.	Inspected the password configuration of the password management tool and determined that NayaOne's employees used a secure password manager to save, store and organize their passwords and logins in a vault encrypted to their device.	No deviations noted.
31	Access to the identity management tool is performed using two-factor authentication and is restricted to authorized personnel.	Inspected the list of users with access to the identity management tool and determined that access was restricted to authorized personnel.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the identity management tool configuration and determined that two factor authentication was enabled.	
32	Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method.	<p>Inspected the list of users with access to production environment console and determined that access to the production environment console was restricted to authorized personnel.</p> <p>Inspected the two-factor authentication configuration and determined that the access to the production environment console was performed using a two-factor authentication method.</p>	No deviations noted.
33	Access to sensitive databases is restricted to authorized users and uses two-factor authentication.	<p>Inspected the list of users with access to the databases and determined that access to the production environment console was restricted to authorized personnel.</p> <p>Inspected the two-factor authentication configuration and determined that the access to the databases was performed using a two-factor authentication method.</p>	No deviations noted.
34	Access to the source control tool is performed using two-factor authentication and is restricted to authorized personnel.	<p>Inspected the list of users with access to the source control tool and determined that access was restricted to authorized personnel.</p> <p>Inspected the two-factor authentication configuration and determined that two factor authentication was enabled.</p>	No deviations noted.
35	Access to alter and delete backups is restricted to authorized users and uses two-factor authentication.	Inspected the list of users with access to alter and delete backups and determined that access was restricted to authorized users.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the configuration of the access to alter and delete backups and determined that access was performed using two-factor authentication.	
36	The company has established key management process in place to support the organization’s use of cryptographic techniques.	Inspected the KMS configuration and determined that NayaOne established a key management process in place to support the organization’s use of cryptographic techniques.	No deviations noted.
45	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	Inspected the database encryption configuration, backup encryption configuration and the storage encryption configuration and determined that restricted information assets containing sensitive customer data hosted on databases, storage, and backups were at least disk-level encrypted.	No deviations noted.
46	Memory storage of the company’s operational devices (i.e. workstations and laptops) is encrypted to ensure safety of sensitive information.	Inspected the compliance platform laptop storage encryption evidence and determined that memory storage of the company’s operational devices (i.e. workstations and laptops) was encrypted to ensure safety of sensitive information.	No deviations noted.
66	The company enforces segregation between development, staging and production environments to enforce confidentiality and privacy on customers data.	Inspected the segregation between environments and determined that NayaOne enforced segregation between development, staging, and production environments to enforce confidentiality and privacy of customers' data.	No deviations noted.
76	Data assets containing customer and confidential information are identified and protected. Data retention depends on the type of asset and the management commitments.	<p>Inspected the company's records management policy and determined that data assets containing customer and confidential information were identified and protected.</p> <p>Inspected the assets inventory documentation and determined that data retention depended on the type of asset and the management commitments.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
27	Access to organizational systems above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.	Inspected the access request ticketing board and a sample of access requests and determined that access to organizational systems above least privileged, including administrator accounts, was approved by appropriate personnel prior to access provisioning.	No deviations noted.
37	New hires are granted access to the relevant environments following an HR notification. The permission credentials depend on the employee's role & responsibilities.	Inspected the HR notification for a sample of new employees hired during the audit period and determined that new employees' access to the relevant environments was granted following a HR notification. Inspected the onboarding checklists for a sample of new employees hired during the audit period and determined that the permission credentials depended on the employee's role & responsibilities.	No deviations noted.
38	User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination.	Inspected the offboarding checklists as a sample of terminated employees and determined that user accounts were disabled or deleted on the production and other organizational information assets timely upon notification of job termination.	No deviations noted.
39	User access and permissions in restricted environments are reviewed and approved by the company's management on an annual basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on an annual basis.	No deviations noted.
40	The company's employees return the organizational assets in their possession upon termination of their employment.	Inspected the offboarding checklists as a sample of terminated employees and determined that NayaOne's employees returned the organizational assets in their possession upon termination of their employment.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
27	Access to organizational systems above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.	Inspected the access request ticketing board and a sample of access requests and determined that ccess to organizational systems above least privileged, including administrator accounts, was approved by appropriate personnel prior to access provisioning.	No deviations noted.
28	The company manages access governance through a role-based access control matrix based on the job description and responsibilities.	Inspected the access control matrix and determined that NayaOne managed access governance through a role-based access control matrix based on the job description and responsibilities.	No deviations noted.
38	User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination.	Inspected the offboarding checklists as a sample of terminated employees and determined that user accounts were disabled or deleted on the production and other organizational information assets timely upon notification of job termination.	No deviations noted.
39	User access and permissions in restricted environments are reviewed and approved by the company's management on an annual basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on an annual basis.	No deviations 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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
41	Physical access to the offices is restricted to authorized personnel using codes for each door. The codes are needed within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	Inspected the company's physical security policy and determined that physical access to the offices was restricted to authorized personnel using codes for each door. Inspected the company's physical security policy and determined that the codes were needed within the	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
40	The company's employees return the organizational assets in their possession upon termination of their employment.	Inspected the offboarding checklists as a sample of terminated employees and determined that NayaOne's employees returned the organizational assets in their possession upon termination of their employment.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
42	The company has enabled multiple network security controls, such as VPC security, cloud firewall, SSH restriction, port restriction, VPN, and remote access restriction.	Inspected the security groups and determined that NayaOne enabled multiple network security controls as VPC security, cloud firewall, SSH restriction, port restriction, VPN, and remote access restriction.	No deviations noted.
43	Customers' passwords are hashed and salted within the company's user database.	Inspected the database's password configuration and determined that customers' passwords were hashed and salted within NayaOne's user database.	No deviations noted.
44	Encrypted communication between the company's customers and the company's assets is enabled using a valid HTTPS TLS 1.2 authenticated certificate.	Inspected the encryption certificate and determined that encrypted communication between the company's customers and the company assets was enabled using a valid HTTPS TLS 1.2 authenticated certificate.	No deviations noted.
45	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	Inspected the database encryption configuration, backup encryption configuration and the storage encryption configuration and determined that restricted information assets containing sensitive customer data hosted on databases, storage, and backups were at least disk-level encrypted.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
43	Customers' passwords are hashed and salted within the company's user database.	Inspected the database's password configuration and determined that customers' passwords were hashed and salted within NayaOne's user database.	No deviations noted.
44	Encrypted communication between the company's customers and the company's assets is enabled using a valid HTTPS TLS 1.2 authenticated certificate.	Inspected the encryption certificate and determined that encrypted communication between the company's customers and the company assets was enabled using a valid HTTPS TLS 1.2 authenticated certificate.	No deviations noted.
45	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	Inspected the database encryption configuration, backup encryption configuration and the storage encryption configuration and determined that restricted information assets containing sensitive customer data hosted on databases, storage, and backups were at least disk-level encrypted.	No deviations noted.
46	Memory storage of the company’s operational devices (i.e. workstations and laptops) is encrypted to ensure safety of sensitive information.	Inspected the compliance platform laptop storage encryption evidence and determined that memory storage of the company’s operational devices (i.e. workstations and laptops) was encrypted to ensure safety of sensitive information.	No deviations noted.
47	Data loss prevention (DLP) system is used to validate that employees do not send sensitive or critical information outside sensitive environments. The DLP system classifies regulated, confidential, and business-critical data and identifies violations of policies defined by the company. Alerts are sent to the administrator upon breach of the policy.	<p>Inspected the data loss prevention system and determined that data loss prevention (DLP) system was used to validate that employees did not send sensitive or critical information outside sensitive environments. The DLP system classified regulated, confidential, and business-critical data and identified violations of policies defined by the company.</p> <p>Inspected the company's DLP policy in the data loss prevention system and a sample of an alert and determined that alerts were sent to the administrator upon breach of the policy.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
48	The company secures and controls its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.	Inspected evidence from the unified endpoint management tool within the compliance platform and determined that NayaOne secured and controlled its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.	No deviations noted.
49	Endpoint protection platform is installed on employees' devices (i.e., workstations and laptops), centrally managed and configured to receive updates regularly.	Inspected the endpoint configurations and the malware detection report and determined that endpoint protection platform was installed on employees' devices (i.e., workstations and laptops), and configured to receive updates regularly.	No deviations 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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
46	Memory storage of the company's operational devices (i.e. workstations and laptops) is encrypted to ensure safety of sensitive information.	Inspected the compliance platform laptop storage encryption evidence and determined that memory storage of the company's operational devices (i.e. workstations and laptops) was encrypted to ensure safety of sensitive information.	No deviations noted.
48	The company secures and controls its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.	Inspected evidence from the unified endpoint management tool within the compliance platform and determined that NayaOne secured and controlled its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.	No deviations noted.
49	Endpoint protection platform is installed on employees' devices (i.e., workstations and laptops), centrally managed and configured to receive updates regularly.	Inspected the endpoint configurations and the malware detection report and determined that endpoint protection platform was installed on employees' devices (i.e., workstations and laptops), and configured to receive updates regularly.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

System Operations

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
50	Production networks undergo vulnerability scans continuously. When an incident is detected, a ticket is created and assigned to the relevant personnel to resolve the issue in a timely manner.	<p>Inspected the vulnerability scan configuration and determined that production networks underwent vulnerability scan continuously.</p> <p>Inspected the high issue findings and determined that when a critical incident was detected, alerts were sent to relevant stakeholders for investigation and resolutions in a timely manner.</p>	No deviations noted.
61	Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated in a timely manner.	<p>Inspected the vulnerability scan configuration and determined that vulnerability scans for the source code were performed continuously to identify security issues as part of the SDLC.</p> <p>Inspected the high issues findings and determined that high/critical issues were remediated.</p>	No deviations 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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
51	Audit trail (security logs) is deployed on the production environment continuously to capture actions made directly by the user or a cloud service.	Inspected the audit logs configuration and the logs file integrity validation configuration and determined that audit trail (security logs) was deployed on the production environment continuously to capture actions made directly by the user or a cloud service.	No deviations noted.
52	Audit trail retention is configured for 365 days.	Inspected the audit log configuration and determined that audit trail logs were configured for 365 days.	No deviations noted.
53	Intrusion detection system scans continuously for potential security issues and alerts the administrator	Inspected the intrusion detection findings report and determined that intrusion detection system scanned	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	upon discovering unexpected and potentially malicious activity in the production environment.	continuously for potential security issues and alerted the administrator upon discovering unexpected and potentially malicious activity in the production environment.	
54	A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring.	Inspected a sample of tickets and determined that a ticketing system was used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
53	Intrusion detection system scans continuously for potential security issues and alerts the administrator upon discovering unexpected and potentially malicious activity in the production environment.	Inspected the intrusion detection findings report and determined that intrusion detection system scanned continuously for potential security issues and alerted the administrator upon discovering unexpected and potentially malicious activity in the production environment.	No deviations noted.
54	A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring.	Inspected a sample of tickets and determined that a ticketing system was used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring.	No deviations noted.
55	The company has developed a security incident response policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	Inspected the company's incident response policy and determined that NayaOne developed a security incident response policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	No deviations noted.
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		updated to reflect emerging continuity risks and lessons learned from past incidents.	

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
18	Customers are notified of service interruptions through the company's website, based on the service level agreement (SLA).	Inspected the uptime report and determined that no service interruptions occurred during the audit period.	No deviations noted.
50	Production networks undergo vulnerability scans continuously. When an incident is detected, a ticket is created and assigned to the relevant personnel to resolve the issue in a timely manner.	Inspected the vulnerability scan configuration and determined that production networks underwent vulnerability scan continuously. Inspected the high issue findings and determined that when a critical incident was detected, alerts were sent to relevant stakeholders for investigation and resolutions in a timely manner.	No deviations noted.
55	The company has developed a security incident response policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	Inspected the company's incident response policy and determined that NayaOne developed a security incident response policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	No deviations noted.
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.
57	A root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution.	Inspected the root cause analysis report for a sample of security incident occurrences during the audit period and determined that a root cause analysis was prepared and reviewed by management for high severity	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		incidents. Change requests were prepared based on the root cause analysis to remediation and resolution.	

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
18	Customers are notified of service interruptions through the company's website, based on the service level agreement (SLA).	Inspected the uptime report and determined that no service interruptions occurred during the audit period.	No deviations noted.
57	A root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution.	Inspected the root cause analysis report for a sample of security incident occurrences during the audit period and determined that a root cause analysis was prepared and reviewed by management for high severity incidents. Change requests were prepared based on the root cause analysis to remediation and resolution.	No deviations noted.
74	The company has developed a disaster recovery plan (DRP) to continue to provide critical services in the event of a disaster. The DRP is reviewed on an annual basis.	Inspected the company's business continuity plan and determined that it outlined the steps to be undertaken in case of disaster. Inspected the company's business continuity plan and determined that the disaster recovery plan was reviewed on an annual basis.	No deviations noted.
75	The company conducts disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results and lessons learned from the tests.	Inspected the disaster recovery drill report and determined that NayaOne conducted disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. Inspected the disaster recovery drill report and determine that team members that participated in the DR exercise developed testing plans and post mortems	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		which documented the results and lessons learned from the tests.	

Change Management

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
26	Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.	<p>Inspected the list of users with access to the production environment and the permissions policy of the production environment and determined that developers did not have access to the production environment.</p> <p>Inspected a sample of access requests and determined that developers were granted temporary access for emergency purposes and these accesses were documented and included an approval.</p>	No deviations noted.
58	Tickets are used to document and prioritize change requests within the change management system. Pull requests and change tickets are linked to each other so the code change can be tracked.	<p>Inspected the details for a sample of pull request tickets and determined that tickets were used to document and prioritize change requests within the change management system.</p> <p>Inspected the change management tickets for a sample of pull requests and determined that pull requests and change tickets were linked to each other so the code change could be tracked.</p>	No deviations noted.
59	Change management procedures have clearly defined roles and responsibilities. The authorization of change requests is performed by the owner or business unit manager.	Inspected the change management configuration and determined that change management procedures clearly defined roles and responsibilities.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the change management tickets for a sample of pull requests and determined that the authorization of change requests was performed by the owner or business unit manager.	
60	Code changes must be reviewed and approved in order to progress through the SDLC and deploy a version to production.	Inspected the details for a sample of pull request tickets and determined that code review took place as part of the change management approval process.	No deviations noted.
61	Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated in a timely manner.	Inspected the vulnerability scan configuration and determined that vulnerability scans for the source code were performed continuously to identify security issues as part of the SDLC. Inspected the high issues findings and determined that high/critical issues were remediated.	No deviations noted.
62	Procedures are in place to ensure automated testing is performed on approved data and test plans in order to ensure the overall security status of the production environment. In the event that automated test failures are detected, a notification is sent to relevant stakeholders.	Inspected the tests configuration and the details for a sample of pull request tickets and determined that procedures were in place to ensure automated testing was performed on approved data and test plans in order to ensure the overall security status of the production environment. Inspected a failed test notification and determined that in the event that automated test failures were detected, a notification was sent to relevant stakeholders.	No deviations noted.
63	A successful test result is mandatory in order to continue with the SDLC process and deploy a version to the production environment.	Inspected the tests configuration and the details for a sample of pull request tickets and determined that a successful test result was mandatory in order to continue with the SDLC process and deploy a version to the production environment.	No deviations noted.
64	The company developed a process in order to manage emergency changes ('hotfix'). Post approval process is performed for each emergency change.	Inspected the company's SDLC policy and a sample of emergency changes and determined that NayaOne developed a process in order to manage emergency	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		changes ('hotfix'). Post approval process was performed for each emergency change.	
65	Deployment of new releases into the production is restricted to authorized personnel and performed automatically.	Inspected the list of users with permission to deploy to production and determined that deployment of new releases into the production was restricted to the authorized personnel. Inspected the deployment approval flow and determined that deployment of new releases into the production was performed automatically.	No deviations noted.
66	The company enforces segregation between development, staging and production environments to enforce confidentiality and privacy on customers data.	Inspected the segregation between environments and determined that NayaOne enforced segregation between development, staging, and production environments to enforce confidentiality and privacy of customers' data.	No deviations noted.

Risk Mitigation

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.
72	The NayaOne production environment is located in several availability zones to maintain high availability standards.	Inspected the production availability zone configuration and determined that availability zones were enabled to maintain high availability standards.	No deviations noted.
75	The company conducts disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios,	Inspected the disaster recovery drill report and determined that NayaOne conducted disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results and lessons learned from the tests.	communication plans, fail-over scenarios, operational transition, and other emergency responses. Inspected the disaster recovery drill report and determine that team members that participated in the DR exercise developed testing plans and post mortems which documented the results and lessons learned from the tests.	

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
67	The company assesses, on an annual basis, the risks that vendors and business partners represent to the achievement of the Company's objectives.	Inspected the vendors assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
68	The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	Inspected the review of the data center SOC 2 report performed by NayaOne and determined that the review was performed annually and included investigation of deviations, auditor's opinion and identifying and documenting the controls in place at NayaOne to address the CUECs.	No deviations noted.
69	IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company.	Inspected the IT vendors terms and conditions agreement and determined that IT vendors that engaged in business with the company were subjected to information security, confidentiality, and privacy commitments as part of their agreements with the company.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

Availability

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
70	A suite of monitoring tools is used by the company to monitor usage, capacity, and performance. Alerts are sent to relevant stakeholders based on predefined rules or anomalies. The notifications are reviewed and processed according to their level of urgency.	<p>Inspected the monitoring dashboards and determined that a suite of monitoring tools was used by the company to monitor usage, capacity, and performance.</p> <p>Inspected the monitoring tool configuration and determined that alerts were sent to relevant stakeholders based on predefined rules or anomalies.</p> <p>Inspected a sample of a notifications from a capacity alert generated from the audit period and determined that the notification was reviewed and processed according to its level of urgency.</p>	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix is updated annually. The company's management acknowledges risk treatment decisions and approves risk acceptance.	<p>Inspected the risk assessment and treatment policy and determined that the company maintained a formal risk management program to continuously discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers.</p> <p>Inspected the risk assessment matrix and determined that risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		<p>Inspected the risk assessment matrix and determined that a formal risk control matrix was updated annually.</p> <p>Inspected the risk assessment matrix and determined that the company's management acknowledged risk treatment decisions and approved risk acceptance.</p>	
70	<p>A suite of monitoring tools is used by the company to monitor usage, capacity, and performance. Alerts are sent to relevant stakeholders based on predefined rules or anomalies. The notifications are reviewed and processed according to their level of urgency.</p>	<p>Inspected the monitoring dashboards and determined that a suite of monitoring tools was used by the company to monitor usage, capacity, and performance.</p> <p>Inspected the monitoring tool configuration and determined that alerts were sent to relevant stakeholders based on predefined rules or anomalies.</p> <p>Inspected a sample of a notifications from a capacity alert generated from the audit period and determined that the notification was reviewed and processed according to its level of urgency.</p>	No deviations noted.
72	<p>The NayaOne production environment is located in several availability zones to maintain high availability standards.</p>	<p>Inspected the production availability zone configuration and determined that availability zones were enabled to maintain high availability standards.</p>	No deviations noted.
73	<p>Daily incremental backups are performed using a cloud service. The backup is retained for 14 days.</p>	<p>Inspected the database backup configuration and the database backup snapshots and determined that monthly incremental backups were performed using the cloud services.</p> <p>Inspected the database backup configuration and determined that the backups were retained for 14 days.</p>	No deviations noted.
74	<p>The company has developed a disaster recovery plan (DRP) to continue to provide critical services in the event of a disaster. The DRP is reviewed on an annual basis.</p>	<p>Inspected the company's business continuity plan and determined that it outlined the steps to be undertaken in case of disaster.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the company's business continuity plan and determined that the disaster recovery plan was reviewed on an annual basis.	
75	The company conducts disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results and lessons learned from the tests.	<p>Inspected the disaster recovery drill report and determined that NayaOne conducted disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses.</p> <p>Inspected the disaster recovery drill report and determine that team members that participated in the DR exercise developed testing plans and post mortems which documented the results and lessons learned from the tests.</p>	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
56	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inspected the company's incident response policy and determined that the NayaOne's contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.
74	The company has developed a disaster recovery plan (DRP) to continue to provide critical services in the event of a disaster. The DRP is reviewed on an annual basis.	<p>Inspected the company's business continuity plan and determined that it outlined the steps to be undertaken in case of disaster.</p> <p>Inspected the company's business continuity plan and determined that the disaster recovery plan was reviewed on an annual basis.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
75	The company conducts disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results and lessons learned from the tests.	<p>Inspected the disaster recovery drill report and determined that NayaOne conducted disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses.</p> <p>Inspected the disaster recovery drill report and determine that team members that participated in the DR exercise developed testing plans and post mortems which documented the results and lessons learned from the tests.</p>	No deviations noted.

Confidentiality

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Formal policies and procedures are documented, reviewed and approved on an annual basis by the management and are available to the company's employees.	<p>Inspected the company's policies and procedures and determined that policies and procedures were documented, reviewed and approved by management on an annual basis.</p> <p>Inspected the company's the HR platform and determined that policies and procedures were available to employees on the HR platform.</p>	No deviations noted.
24	The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the SRE Engineer on an annual basis.	<p>Inspected the asset mapping documentation and determined that NayaOne identified, classified and managed the inventory of information assets.</p> <p>Inspected the assets mapping documentation and determined that the assets inventory was reviewed by the SRE Engineer on an annual basis.</p>	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
43	Customers' passwords are hashed and salted within the company's user database.	Inspected the database's password configuration and determined that customers' passwords were hashed and salted within NayaOne's user database.	No deviations noted.
44	Encrypted communication between the company's customers and the company's assets is enabled using a valid HTTPS TLS 1.2 authenticated certificate.	Inspected the encryption certificate and determined that encrypted communication between the company's customers and the company assets was enabled using a valid HTTPS TLS 1.2 authenticated certificate.	No deviations noted.
45	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	Inspected the database encryption configuration, backup encryption configuration and the storage encryption configuration and determined that restricted information assets containing sensitive customer data hosted on databases, storage, and backups were at least disk-level encrypted.	No deviations noted.
46	Memory storage of the company's operational devices (i.e. workstations and laptops) is encrypted to ensure safety of sensitive information.	Inspected the compliance platform laptop storage encryption evidence and determined that memory storage of the company's operational devices (i.e. workstations and laptops) was encrypted to ensure safety of sensitive information.	No deviations noted.
48	The company secures and controls its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.	Inspected evidence from the unified endpoint management tool within the compliance platform and determined that NayaOne secured and controlled its employees' laptops to enforce its security settings, including hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.	No deviations noted.
49	Endpoint protection platform is installed on employees' devices (i.e., workstations and laptops), centrally managed and configured to receive updates regularly.	Inspected the endpoint configurations and the malware detection report and determined that endpoint protection platform was installed on employees' devices (i.e., workstations and laptops), and configured to receive updates regularly.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
68	The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	Inspected the review of the data center SOC 2 report performed by NayaOne and determined that the review was performed annually and included investigation of deviations, auditor's opinion and identifying and documenting the controls in place at NayaOne to address the CUECs.	No deviations noted.
69	IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company.	Inspected the IT vendors terms and conditions agreement and determined that IT vendors that engaged in business with the company were subjected to information security, confidentiality, and privacy commitments as part of their agreements with the company.	No deviations noted.
76	Data assets containing customer and confidential information are identified and protected. Data retention depends on the type of asset and the management commitments.	Inspected the company's records management policy and determined that data assets containing customer and confidential information were identified and protected. Inspected the assets inventory documentation and determined that data retention depended on the type of asset and the management commitments.	No deviations noted.
77	The company has implemented the capability of tracking and identifying customer data in its assets (i.e., databases, storage, backups).	Inspected the company's database and determined that NayaOne has implemented the capability of tracking and identifying customer data in its assets (i.e., databases, storage, backups).	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the SRE Engineer on an annual basis.	Inspected the asset mapping documentation and determined that NayaOne identified, classified and managed the inventory of information assets.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the assets mapping documentation and determined that the assets inventory was reviewed by the SRE Engineer on an annual basis.	
77	The company has implemented the capability of tracking and identifying customer data in its assets (i.e., databases, storage, backups).	Inspected the company's database and determined that NayaOne has implemented the capability of tracking and identifying customer data in its assets (i.e., databases, storage, backups).	No deviations noted.
78	The company has procedures in place to dispose of confidential information according to the company's data retention and disposal policy.	Inspected the company's records management policy and determined that NayaOne had procedures in place to dispose of confidential information according to the company's data retention and disposal policy. During the audit period this situation did not occur.	No deviations noted.
