

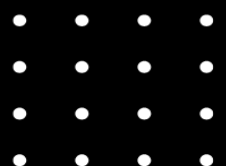
INTERNXT

Internxt Universal Technologies SL

System and Organization Controls (SOC 2®) Type II Report

Description of Internxt software applications relevant to the Trust Services Criteria of Security, Availability and Confidentiality

September 1, 2025, through November 30, 2025



STATEMENT OF CONFIDENTIALITY

This report, including the Description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Internxt, user entities of Internxt software applications during some or all of the period September 1, 2025 through November 30, 2025, business partners of Internxt subject to risks arising from interactions with Internxt's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the system and its related internal controls. This report is not intended to be and should not be used by anyone other than these specified parties. Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

1 Independent Service Auditors' Report	5
2 Management Assertion Provided by Internxt Universal Technologies SL	10
3 Description of Systems Provided by the Service Organization	13
4 Information Provided by Independent Service Auditor Except for Applicable Trust Services Criteria and Control Activities.....	49



SECTION 1

INDEPENDENT SERVICE AUDITORS' REPORT

1 INDEPENDENT SERVICE AUDITORS' REPORT

To the management of Internxt Universal Technologies SL

Scope

We have examined the description of the system provided by Management of Internxt Universal Technologies SL (the "Service Organization" or "Internxt") included in Section 3, "Description of Systems Provided by Service Organization" of its Internxt software applications throughout the period September 1, 2025 to November 30, 2025 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period September 1, 2025 to November 30, 2025, to provide reasonable assurance that Internxt's service commitments and system requirements would be 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, in AICPA Trust Services Criteria.

Internxt uses OVHCloud ("Subservice Organization") for cloud hosting services. The Description indicates that complementary Subservice Organization controls that are suitably designed and operating effectively are necessary, along with controls at Internxt, to achieve Internxt's service commitments and system requirements based on the applicable trust services criteria. The Description presents Internxt's controls, the applicable trust services criteria, and the types of complementary Subservice Organization controls assumed in the design of Internxt's controls. The Description does not disclose the actual controls at the Subservice Organization. Our examination did not include the services provided by the Subservice Organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary Subservice Organization controls.

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

Service Organization's Responsibilities

Management of Internxt 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 Internxt service commitments and system requirements would be achieved. Management of Internxt has provided the accompanying assertion in Section 2 titled, "Management Assertion Provided by Internxt Universal Technologies SL" (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Management of Internxt is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and

identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and operating effectiveness of controls stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the Internxt's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that Internxt achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the Description.

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

Service Auditor's Independence and Quality Control

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

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and therefore may not include every aspect of the system that each individual report user may consider important to meet their informational needs. There are inherent limitations in any

system of internal control, including the possibility of human error and the circumvention of controls.

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

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4, "Information Provided by the Service auditor: Test of controls".

Opinion

In our opinion, in all material respects:

- a) The Description presents Internxt's system that was designed and implemented throughout the period September 1, 2025 to November 30, 2025, in accordance with the description criteria.
- b) The controls stated in the Description were suitably designed throughout the period September 1, 2025 to November 30, 2025, to provide reasonable assurance that Internxt'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 Organization and user entities applied the complementary controls assumed in the design of Internxt's controls throughout that period.
- c) The controls stated in the Description operated effectively throughout the period September 1, 2025 to November 30, 2025, to provide reasonable assurance that Internxt's service commitments and system requirements would be achieved based on the applicable trust services criteria, provided that the complementary controls assumed in the design of Internxt's controls at the Subservice Organization and user entities also operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Internxt, user entities of Internxt software applications during some or all of the period September 1, 2025 to November 30, 2025, business partners of Internxt subject to risks arising from interactions with the Internxt's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by Internxt.
- How Internxt's system interacts with user entities, business partners, Subservice Organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary Subservice Organization controls and how they interact with related controls at Internxt to achieve Internxt's commitments and system requirements.

- User entity responsibilities and how they may affect the user entity's ability to effectively use Internxt's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of Internxt'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.

Accorp Partners CPA LLC

ACCORP PARTNERS CPA LLC

License No.: PAC-FIRM-LIC-47383

Kalispell, Montana

Date: December 18, 2025



SECTION 2

MANAGEMENT'S
ASSERTION
PROVIDED
BY SERVICE
ORGANIZATION

MANAGEMENT ASSERTION PROVIDED BY INTERNXT UNIVERSAL TECHNOLOGIES SL

For the period from September 1, 2025 through November 30, 2025

We have prepared the accompanying System Description Provided by Service Organization (Description) of Internxt Universal Technologies SL (the "Service Organization" or "Internxt") 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 Internxt software applications (System) that may be useful when assessing the risks arising from interactions with the System throughout the period September 1, 2025 to November 30, 2025, 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 (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Internxt uses OVHCloud ("Subservice Organization") for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Internxt, to achieve Internxt's service commitments and system requirements based on the applicable trust services criteria. The description presents Internxt's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Internxt controls. The description does not disclose the actual controls at the subservice organization. The description does not extend to controls of the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Internxt, to achieve Internxt's service commitments and system requirements based on the applicable trust services criteria. The description presents Internxt's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Internxt's controls. The description does not extend to controls of the user entities.

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

- a. The description presents the System that was designed and implemented throughout the period September 1, 2025 to November 30, 2025 in accordance with the description Criteria.
- b. The controls stated in the description were suitably designed throughout the period September 1, 2025 to November 30, 2025, to provide reasonable assurance that Internxt's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Internxt's controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period September 1, 2025 to November 30, 2025, to provide reasonable assurance that Internxt's service commitments and system requirements were achieved based on

the applicable trust services criteria, if the subservice organizations and user entities applied the complementary controls assumed in the design of Internxt's controls operated effectively throughout that period.

For Internxt Universal Technologies SL

A handwritten signature in blue ink, consisting of a stylized 'J' followed by a long horizontal line.

Name: Fran Villalba Segarra
Title: CEO
Date: December 18th, 2025

A blue ink stamp with the text "INTERNXT UNIVERSAL TECHNOLOGIES SL" in a bold, sans-serif font, tilted at an angle.



SECTION 3

DESCRIPTION OF THE SYSTEM

3 DESCRIPTION OF SYSTEMS PROVIDED BY THE SERVICE ORGANIZATION

3.1 Overview of service organization and in-scope services

Internxt Drive, S3, Antivirus, Send, VPN, Cleaner (Collectively referred as Internxt software applications) are cloud-hosted software applications built by Internxt Universal Technologies SL.

Following are the in-scope applications provided by Internxt:

Internxt Drive

- Internxt Drive is a secure cloud storage service that allows users to store, synchronize, back up, and share files across supported desktop and mobile platforms.
- All files are encrypted end-to-end on the user's device prior to transmission, ensuring that Internxt does not have access to unencrypted customer data or encryption keys.
- Data is protected using industry-standard cryptographic controls during transmission and at rest, supporting confidentiality and integrity objectives.
- The service provides file versioning, sharing links with access controls, and optional backup functionality to support availability and recoverability.
- Internxt Drive is designed in accordance with zero-knowledge principles and GDPR requirements.

Internxt S3 (Object Storage)

- Internxt S3 is an object storage service designed for developers and businesses requiring scalable, encrypted storage compatible with S3-style APIs.
- Data stored through Internxt S3 is encrypted prior to storage, supporting confidentiality and protection against unauthorized access.
- The service is designed to support high availability and durability through distributed infrastructure.
- Access to stored objects is controlled through authentication and authorization mechanisms aligned with least-privilege principles.
- Internxt S3 supports secure integration with third-party applications and internal systems.

Internxt Antivirus

- Internxt Antivirus is a client-side security service designed to detect, block, and remove malware and other malicious software from user devices.
- The service operates locally on the user's device, helping to protect system integrity without requiring access to user files stored in Internxt Drive.
- Threat detection mechanisms are designed to operate in real time and through scheduled scans.
- The antivirus service contributes to overall platform security by reducing the risk of compromised endpoints accessing cloud services.

Internxt Send

- Internxt Send is a secure file-transfer service that allows users to share files through encrypted links.
- Files shared via Internxt Send are encrypted before upload and automatically expire after 15 days.
- The service supports confidentiality by ensuring that only authorized recipients can access shared files.
- Internxt Send does not require recipients to create an account, reducing exposure while maintaining secure delivery.
- Files are automatically deleted after expiration, supporting data minimization principles.

Internxt VPN

- Internxt VPN is a privacy-focused virtual private network service that encrypts user internet traffic and masks IP addresses.
- The service uses secure tunneling protocols to protect data in transit over public or untrusted networks.
- Internxt VPN operates under a no-logs policy, minimizing the collection and retention of user activity data.
- The service enhances user privacy and security when accessing online services, particularly on public Wi-Fi networks.
- VPN access is authenticated and controlled to prevent unauthorized use.

Internxt Cleaner

- Internxt Cleaner is a device optimization and privacy tool designed to remove unnecessary files, cache data, and temporary system artifacts.
- The service helps improve device performance and reduce the local storage of residual data that may pose privacy risks.
- Cleaner operates locally on the user's device and does not transmit cleaned data to Internxt systems.
- The tool supports privacy and data hygiene by enabling users to manage and delete unused or obsolete data.
- Internxt Cleaner complements other security services by reducing attack surface on user endpoints.

3.2 Principal Service Commitments and System Requirements

Internxt designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Internxt makes to customers and the compliance requirements that Internxt has established for their services.

Security commitments to user entities are documented and communicated in Internxt's customer agreements, as well as in the description of the service offering provided online. Internxt's security commitments are standardized and based on some common principles.

These principles include but are not limited to, the following:

- The fundamental design of Internxt's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- Internxt implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Internxt and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

Internxt establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Internxt's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how staff is hired.

3.3 Components of the System used to provide services

Infrastructure & Network Architecture

The production infrastructure for the Internxt software applications is hosted on OVHCloud in their various regions across Europe.

Internxt software applications uses a virtual and secure network environment on top of OVHCloud infrastructure to ensure that the software application is always protected. Internxt software applications ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

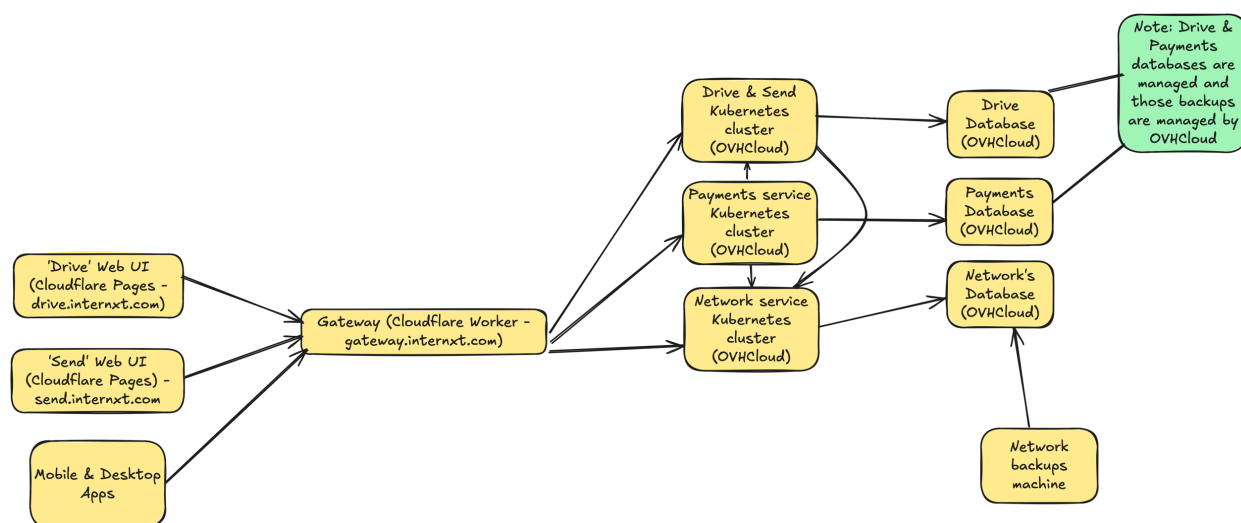
When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the OVHCloud Internet Gateway, over to a Virtual Private Cloud that

1. Houses the entire application runtime.

Description of the System

2. Protects the application runtime from any external networks.

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



Software

Internxt is responsible for managing the development and operation of the Internxt software applications including infrastructure components such as servers, databases, and storage systems. The in-scope Internxt infrastructure and software components are shown in the table below:

System/ Application	Business Function / Description
Internxt software applications	Access to the Internxt SaaS application is through a web/mobile interface and user authentication.
OVHCloud IAM	Identity and access management console for OVHCloud resources.
OVHCloud Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.
GitHub	Source code repository, version control system, and build software.
Hostinger	Identity/Email provider for all Internxt Universal Technologies SL employees.

People

Internxt's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is

required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

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

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

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

Data

Data, as defined by Internxt, constitutes the following:

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

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

Data Sensitivity	Description	Examples
Customer confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	- Customer system and operating data - Customer PII - Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally or was entrusted to Internxt by others. Company confidential information may be shared with authorized employees,	- Internxt's PII - Unpublished financial information

Data Sensitivity	Description	Examples
	contractors, and business partners but not released to the general	- Documents and processes explicitly marked as confidential - Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	- Press releases - Public website

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

Procedures and Policies

Formal policies and procedures have been established to support the Internxt software applications. These policies cover:

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

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal

control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Internxt also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Internxt software applications, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

3.4 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. This section provides information about the five interrelated components of internal control at Internxt, including:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring controls

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Internxt's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Internxt's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Internxt and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members.
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Internxt's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.

Management Philosophy and Operating Style

Internxt's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information.

Internxt's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities that the Internxt has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.

Organizational Structure and Assignment of Authority and Responsibility

Internxt's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational

charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources

Internxt's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

Specific control activities that the Internxt has implemented in this area are described below:

- Validation of identity, past performance, and other background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

Internxt's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Internxt identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Internxt software applications, and the management has implemented various measures designed to manage these risks. Internxt believes that effective risk management is based on the following principles:

- Senior management's commitment to the security of Internxt software applications.
- The involvement, cooperation, and insight of all Internxt staff.
- Initiating risk assessments with discovery and identification of risks.
- A thorough analysis of identified risks.
- Commitment to the strategy and treatment of identified risks.
- Communicating all identified risks to the senior management.
- Encouraging all Internxt staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Internxt software applications. The Internxt risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Internxt's Information Security Officer and the department or individuals responsible for the area being assessed. All Internxt staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

Internxt uses a number of vendors to meet its business objectives. Internxt understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Internxt employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Internxt assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Internxt's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Internxt management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Internxt identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Internxt's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Information and Communication

Internxt maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Internxt also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff.

Monitoring Controls

Internxt management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Control Activities

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

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

Physical Security

The in-scope system and supporting infrastructure are hosted by OVHCloud. As such, OVHCloud are responsible for the physical security controls of the in-scope system. Internxt reviews the SOC 2 report provided by OVHCloud on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Internxt software applications.

Logical Access Control

The Internxt software applications uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

Internxt has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

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

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

Change Management

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

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

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

A change to the Internxt software applications can be initiated by a staff member with an appropriate role. Internxt uses a version control system to manage and record activities related to the change management process.

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

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

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

Incident Management

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

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

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

- Low severity incidents are those that do not require immediate remediation. These typically include a partial service of Internxt being unavailable (for which workarounds

exist). These do not require someone to be paged or woken up beyond normal work hours.

- Medium severity incidents are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- High severity incidents are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.
- Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

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

Cryptography

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

Asset Management (Hardware and Software)

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

Vulnerability Management

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

Endpoint Management

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

Availability

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

Boundaries of the System

The scope of this report includes the Internxt software applications. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

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

Significant Events and Conditions

Internxt has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the software application.

3.5 Complementary User Entity Controls

Internxt's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Internxt customers.

For customers to rely on the information processed through the Internxt's software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

Complementary User Entity Controls	Applicable Criteria
Customers are responsible for managing their organization's Internxt software applications account as well as establishing any customized security solutions or automated processes through the use of setup features.	CC5.1, CC5.2, CC5.3, CC6.1
Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Internxt software applications account	CC5.2, CC6.3
Customers are responsible for notifying Internxt of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Internxt software	CC7.2, CC7.3, CC7.4

Complementary User Entity Controls	Applicable Criteria
applications.	
Customers are responsible for any changes made to user and organization data stored within the Internxt software applications.	CC8.1
Customers are responsible for communicating relevant security and availability issues and incidents to Internxt through identified channels.	CC7.2, CC7.3, CC7.4

3.6 Complementary Subservice Organization Controls

Controls at Service organization and controls at User organization related to Internxt software applications to its customers relevant to the Security, Availability, and Confidentiality ("in-scope trust service criteria"), cover only a portion of the overall internal control structure of its clients. The control objectives cannot be achieved without taking into consideration operating effectiveness of controls at Subservice Organization providing services to service organization to perform services provided to user entity that are likely to be relevant to those user entity internal control over financial reporting.

This section highlights those internal control structure responsibilities, Internxt believes should be present at all applicable Subservice Organization, and which Internxt has considered in developing its control structure policies and the procedures described in this report.

The Subservice Organization used by Internxt relevant to providing services related to Internxt software applications is shown below:

Subservice Organization	Service Provided
OVHCloud	Cloud computing services

Control Activity Expected to be Implemented by Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	CC6.4, A1.2
Encryption methods are used to protect data in transit and at rest.	CC6.1
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	A1.2
A defined Data Classification Policy specifies classification levels and control requirements to meet the company's commitments related to confidentiality.	C1.1

Control Activity Expected to be Implemented by Subservice Organization	Applicable Criteria
A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.	C1.2

3.7 Trust services criteria and Description of Related Controls:

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
Control Environment			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	SDC-1	Entity has a documented policy to define behavioral standards and acceptable business conduct.
		SDC-6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC-12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	SDC-24	Entity's Senior Management reviews and approves all company policies annually.
		SDC-25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
		SDC-26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC-27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC-29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in	SDC-2	Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.
		SDC-3	Entity has established procedures to communicate with staff about their roles and responsibilities.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	the pursuit of objectives.	SDC-22	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.
		SDC-25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
		SDC-154	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.
		SDC-396	Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.
		SDC-397	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	SDC-4	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.
		SDC-5	Entity has established procedures to perform security risk screening of individuals before authorizing access.
		SDC-7	Entity provides information security and privacy training to staff that is relevant to their job function.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	SDC-7	Entity provides information security and privacy training to staff that is relevant to their job function.
		SDC-9	Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
		SDC-12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC-383	Entity requires that all staff members complete Information Security Awareness training annually.
		SDC-387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.
		SDC-388	Entity documents, monitors, and retains individual training activities and records.
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.	SDC-11	Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.
		SDC-13	Entity makes all policies and procedures available to all staff members for their perusal.
		SDC-14	Entity displays the most current information about its services on its website, which is accessible to its customers.
		SDC-71	Entity has a documented policy outlining guidelines for the disposal and retention of information.
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.	SDC-1	Entity has a documented policy to define behavioral standards and acceptable business conduct.
		SDC-6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC-12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC-13	Entity makes all policies and procedures available to all staff members for their perusal.
		SDC-15	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
			systems provided by the entity in the event there are problems.
		SDC-135	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.
		SDC-383	Entity requires that all staff members complete Information Security Awareness training annually.
		SDC-387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.
		SDC-388	Entity documents, monitors, and retains individual training activities and records.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	SDC-14	Entity displays the most current information about its services on its website, which is accessible to its customers.
		SDC-16	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.
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.	SDC-18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
		SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a	SDC-6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC-18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	basis for determining how the risks should be managed.		threats that could impair systems' security commitments and requirements.
		SDC-19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC-21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
		SDC-55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.
		SDC-68	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	SDC-20	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	SDC-18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
		SDC-19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
		SDC-21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
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.	SDC-22	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.
		SDC-23	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC-24	Entity's Senior Management reviews and approves all company policies annually.
		SDC-25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
		SDC-26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC-27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC-29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		SDC-30	Entity reviews and evaluates all Subservice Organizations periodically, to ensure commitments to Entity's customers can be met.
		SDC-154	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.
		SDC-389	Entity periodically updates and reviews the inventory of systems as a part of

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
			installations, removals, and system updates.
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.	SDC-15	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.
		SDC-23	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC-24	Entity's Senior Management reviews and approves all company policies annually.
		SDC-25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
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.	SDC-31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
		SDC-32	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.
		SDC-69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems
		SDC-105	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support	SDC-23	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	the achievement of objectives.	SDC-24	Entity's Senior Management reviews and approves all company policies annually.
		SDC-25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
		SDC-26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC-27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC-28	Entity's Infosec officer reviews and approves the list of people with access to production console annually
		SDC-29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		SDC-30	Entity reviews and evaluates all Subservice Organizations periodically, to ensure commitments to Entity's customers can be met.
		SDC-31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
		SDC-108	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.
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.	SDC-6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC-12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC-13	Entity makes all policies and procedures available to all staff members for their perusal.
		SDC-31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
		SDC-33	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.
		SDC-53	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.
		SDC-58	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal
		SDC-64	Entity has documented policies and procedures to manage changes to its operating environment.
		SDC-65	Entity has procedures to govern changes to its operating environment.
		SDC-66	Entity has established procedures for approval when implementing changes to the operating environment.
		SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements
		SDC-69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems
		SDC-135	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.
		SDC-391	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
Logical and Physical Access Controls			
CC6.1	The entity implements logical access security software, infrastructure, and	SDC-33	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system

Description of the System

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	architectures over protected information assets to protect them from security events to meet the entity's objectives.		credentials which grant the ability to access the critical systems.
		SDC-34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.
		SDC-38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
		SDC-42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC-43	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC-108	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.
		SDC-135	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.
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	SDC-33	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.
		SDC-34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.
		SDC-35	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Description of the System

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	access is no longer authorized.		
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.	SDC-33	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.
		SDC-34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.
		SDC-35	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.
		SDC-37	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.
		SDC-42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC-43	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC-108	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.
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		Not applicable as all the applications and information are hosted on cloud services provided by OVHCloud.

Description of the System

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	to meet the entity's objectives.		
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.	SDC-35	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.
		SDC-48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	SDC-38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
		SDC-39	Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor authentication.
		SDC-44	Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.
		SDC-45	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.
		SDC-46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.
		SDC-47	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.
		SDC-50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.
		SDC-104	Entity has documented policies and procedures for endpoint security and related controls.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
		SDC-141	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.
		SDC-390	Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.
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.	SDC-45	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.
		SDC-49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.
		SDC-51	Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.
		SDC-52	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.
		SDC-100	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.
		SDC-106	Entity has a documented policy to manage encryption and cryptographic protection controls.
		SDC-141	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.
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.	SDC-46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.
		SDC-50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
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.	SDC-23	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC-55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC-56	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC-61	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats
		SDC-62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC-108	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.
		SDC-391	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
		SDC-394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.
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	SDC-23	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC-55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC-56	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	represent security events.	SDC-61	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats
		SDC-62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC-391	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
		SDC-394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.
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.	SDC-46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.
		SDC-54	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.
		SDC-55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC-56	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC-61	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.
		SDC-62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC-63	Entity identifies vulnerabilities on the company platform through an annual

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
			penetration testing exercise conducted by a qualified third-party service provider.
		SDC-391	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
		SDC-394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.
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.	SDC-53	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.
		SDC-54	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	SDC-54	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.
		SDC-58	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal
		SDC-392	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident
		SDC-393	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.
Change Management			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and	SDC-52	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
	implements changes to infrastructure, data, software, and procedures to meet its objectives.	SDC-64	Entity has documented policies and procedures to manage changes to its operating environment.
		SDC-65	Entity has procedures to govern changes to its operating environment.
		SDC-66	Entity has established procedures for approval when implementing changes to the operating environment.
Risk Mitigation			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	SDC-18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
		SDC-19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC-56	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC-58	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal
		SDC-59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.
		SDC-60	Entity tests backup information periodically to verify media reliability and information integrity.
		SDC-62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The

Description of the System

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
			objectives incorporate the Entity's service commitments and system requirements
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	SDC-21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
		SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements
		SDC-68	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.
Additional Criteria for Availability			
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	SDC-62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
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.	SDC-58	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal
		SDC-59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.
		SDC-60	Entity tests backup information periodically to verify media reliability and information integrity.
		SDC-392	Entity has documented guidelines to manage Disaster Recovery that establish quidelines and procedures for continuing

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
			business operations in case of a disruption or a security incident
		SDC-393	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	SDC-60	Entity tests backup information periodically to verify media reliability and information integrity.
		SDC-97	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.
		SDC-392	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident
		SDC-393	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.
Additional Criteria for Confidentiality			
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	SDC-6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC-12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC-45	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.
		SDC-49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.
		SDC-69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems
		SDC-70	Entity performs physical and/or logical labelling of information systems as per the

Description of the System

TSC Ref. #	Criteria	Control Ref. #	Control Activity as specified by Internxt
			guidelines documented policy defined for data classification
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	SDC-48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.
		SDC-71	Entity has a documented policy outlining guidelines for the disposal and retention of information.



SECTION 4

INFORMATION
PROVIDED BY THE
SERVICE AUDITOR:
TEST OF CONTROLS

4 INFORMATION PROVIDED BY INDEPENDENT SERVICE AUDITOR EXCEPT FOR APPLICABLE TRUST SERVICES CRITERIA AND CONTROL ACTIVITIES

4.1 Objective of Our Examination

This report, including the description of tests of controls and results thereof in this section are intended solely for the information and use of Internxt, user entities of the Internxt system related to Internxt software applications during some or all of the period September 1, 2025 through November 30, 2025, business partners of Internxt subject to risks arising from interactions with Internxt's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service Organization.
- how the service Organization's system interacts with user entities, Subservice Organizations, and other parties.
- internal control and its limitations.
- complementary user-entity controls and how they interact with related controls at the service Organization to meet the applicable trust services criteria; the applicable trust services criteria.
- and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This section presents the following information provided by Internxt:

- The controls established and specified by Internxt to achieve the specified trust services criteria.

Also included in this section is the following information provided by auditors:

- A description of the tests performed by auditors to determine whether Internxt's controls were operating with sufficient effectiveness to achieve specified trust services criteria. Auditors determined the nature, timing, and extent of the testing performed.
- The results of tests of controls.

The examination was conducted in accordance with the criteria as set forth in DC Section 200. 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2025 to November 30, 2025 to provide reasonable assurance that Internxt's 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, of the American Institute of Certified Public Accountants (AICPA), and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18). SSAE 18 is inclusive of the following: (1) AT-C 105, Concepts Common to all Attestation Engagements; and (2) AT-C 205, Examination Engagements. Our testing of Internxt's controls was restricted to the controls identified by Internxt to meet the criteria related to Security,

Availability and Confidentiality listed in Section 1 of this report and was not extended to controls described in Section 3 but not included in Section 4, or to controls that may be in effect at user Organizations or Subservice Organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and Subservice Organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, Subservice Organizations, and Internxt's controls should be evaluated together. If effective user entity or Subservice Organizations controls are not in place, Internxt's controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Internxt our procedures included tests of the following relevant elements of the Internxt control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication
4. Monitoring
5. Control Activities

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Internxt activities and operations, inspection of Internxt documents and records, and re-performance of the application of Internxt controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine the Internxt description of the system related to Internxt as well as the suitability of the design and operating effectiveness of controls for a representative number of samples throughout the period of September 1, 2025 to November 30, 2025.

In selecting particular tests of the operational effectiveness of controls, we considered the (a) nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the trust services principles and criteria to be achieved and (d) the expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of information provided by Internxt is also a component of the testing procedures performed. Information we are utilizing as evidence may include, but is not limited to:

1. Standard 'out of the box' reports as configured within the system.
2. Parameter-driven reports generated by Internxt systems.

3. Custom-developed reports that are not standard to the application such as scripts, report writers, and queries.
4. Spreadsheets that include relevant information utilized for the performance or testing of a control.
5. Internxt prepared analyses, schedules, or other evidence manually prepared and utilized by the Company.

While these procedures are not specifically called out in the test procedures listed in this section, they are completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Internxt.

4.4 Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Internxt. Our tests of controls were performed on controls as they existed during the period of September 1, 2025 through November 30, 2025, and were applied to those controls relating to the trust services principles and criteria.

Tests performed of the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because auditors does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, auditor reports all deviations.

4.5 Testing Procedures Performed by Independent Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC1.1 CC2.2	SDC-1	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected code of conduct document and acceptable usage policy to ascertain whether entity has a documented policy to define behavioral standards and acceptable business conduct.	No exception noted.
CC1.1 CC2.2 CC3.2 CC5.3 C1.1	SDC-6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no new joiners during the audit period.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC1.1 CC1.5 CC2.2 CC5.3 C1.1	SDC-12	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, policy acceptance logs and HR policies information to ascertain whether entity has established procedures for staff to acknowledge applicable company policies periodically.	No exception noted.
CC1.2 CC4.1 CC4.2 CC5.2	SDC-24	Entity's Senior Management reviews and approves all company policies annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			to ascertain whether entity's Senior Management reviews and approves all company policies annually.	
CC1.2 CC1.3 CC4.1 CC4.2 CC5.2	SDC-25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.</p>	No exception noted.
CC1.2 CC4.1 CC5.2	SDC-26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected organization chart and its review records to ascertain whether entity's Senior Management reviews and approves the Organizational Chart for all employees annually.</p>	No exception noted.
CC1.2 CC4.1 CC5.2	SDC-27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected risk assessment report and review evidence to ascertain whether entity's Senior Management reviews and approves the Risk Assessment Report annually.</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC1.2 CC4.1 CC5.2	SDC-29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor assessment register and reports to ascertain whether entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	No exception noted.
CC1.3	SDC-2	Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure to ascertain whether entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	No exception noted.
CC1.3	SDC-3	Entity has established procedures to communicate with staff about their roles and responsibilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no new joiners during the audit period.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC1.3 CC4.1	SDC-22	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure and roles and responsibility document of Information Security Officer to ascertain whether entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			maintain an enterprise-wide cybersecurity and privacy program.	
CC1.3 CC4.1	SDC-154	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected asset register to ascertain whether entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.</p>	No exception noted.
CC1.3	SDC-396	Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected organizational structure and roles and responsibility document of People Operations Officer to ascertain whether entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.</p>	No exception noted.
CC1.3	SDC-397	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected organizational structure and roles and responsibility document of compliance program manager to ascertain whether entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC1.4	SDC-4	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no new joiners during the audit period.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC1.4	SDC-5	Entity has established procedures to perform security risk screening of individuals before authorizing access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no new joiners during the audit period.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC1.4 CC1.5	SDC-7	Entity provides information security and privacy training to staff that is relevant to their job function.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected attendance records from the last Security and privacy training to ascertain whether entity provides information security and privacy training to staff that is relevant to their job function.	No exception noted.
CC1.5	SDC-9	Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected annual evaluation records to ascertain whether entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC1.5 CC2.2	SDC-383	Entity requires that all staff members complete Information Security Awareness training annually.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected attendance records from the last Security awareness training session to ascertain whether entity requires that all staff members complete Information Security Awareness training annually.</p>	No exception noted.
CC1.5 CC2.2	SDC-387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Noted that there were no new joiners during the audit period.</p>	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC1.5 CC2.2	SDC-388	Entity documents, monitors, and retains individual training activities and records.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected attendance records from the last Security and privacy training to ascertain whether entity documents, monitors, and retains individual training activities and records.</p>	No exception noted.
CC2.1	SDC-11	Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected logs from event monitoring tool to ascertain whether entity systems generate information that is reviewed and evaluated to</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			determine impacts on the functioning of internal controls.	
CC2.1 CC2.2 CC5.3	SDC-13	Entity makes all policies and procedures available to all staff members for their perusal.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Noted that the policies and processes are shared with all the employees using Sprinto. Inspected the Sprinto functionality to ascertain whether Entity makes all policies and procedures available to all staff members for their perusal.</p>	No exception noted.
CC2.1 CC2.3	SDC-14	Entity displays the most current information about its services on its website, which is accessible to its customers.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected their publicly accessible website to ascertain whether entity displays the most current information about its services on its website, which is accessible to its customers.</p>	No exception noted.
CC2.1 C1.2	SDC-71	Entity has a documented policy outlining guidelines for the disposal and retention of information.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected data disposal and retention policy to ascertain whether entity has a documented policy outlining guidelines for the disposal and retention of information.</p>	No exception noted.
CC2.2 CC4.2	SDC-15	Entity has provided information to employees, via various Information Security Policies/procedures, on how to	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected Information Security policy and procedures to ascertain whether entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	
CC2.2 CC5.3 CC6.1	SDC-135	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected password management policy and password configuration to ascertain whether entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.</p>	No exception noted.
CC2.3	SDC-16	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected incident management and sample of incident tickets to ascertain whether entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.</p>	No exception noted.
CC3.1 CC3.2	SDC-18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC3.4 CC9.1		procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected risk register to ascertain whether entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	
CC3.1 CC3.2 CC5.3 CC9.1 CC9.2	SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements</p>	No exception noted.
CC3.2 CC3.4 CC9.1	SDC-19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected documented risk mitigation strategy within risk register to ascertain whether each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.</p>	No exception noted.
CC3.2 CC3.4 CC9.2	SDC-21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		critical to the systems' security commitments and requirements.	Inspected vendor risk assessment forms to ascertain whether entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	
CC3.2 CC7.1 CC7.2 CC7.3	SDC-55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected vulnerability scans and action plans to ascertain whether entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.</p>	No exception noted.
CC3.1 CC3.2 CC5.3 CC9.1 CC9.2	SDC-67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements</p>	No exception noted.
CC3.2 CC9.2	SDC-68	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected vendor management policy to ascertain whether entity has a documented policy and procedures to manage Vendors/third-party</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			suppliers and provides guidance to staff on performing a risk assessment of such vendors.	
CC3.3	SDC-20	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected risk register, and risks related to fraud to ascertain whether entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.</p>	No exception noted.
CC4.1 CC4.2 CC5.2 CC7.1 CC7.2	SDC-23	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected monitoring logs the monitoring tool to ascertain whether entity uses a monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.</p>	No exception noted.
CC4.1 CC5.2	SDC-30	Entity reviews and evaluates all Subservice Organizations periodically, to ensure commitments to Entity's customers can be met.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected SOC 2 type II reports of Subservice Organization and evaluation report prepared by entity to ascertain whether entity reviews and evaluates all Subservice Organizations periodically, to ensure commitments to entity's customers can be met.</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC4.1	SDC-389	Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected asset register to ascertain whether entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.</p>	No exception noted.
CC5.1 CC5.2 CC5.3	SDC-31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected information security policy and acceptable usage policy to ascertain whether entity has documented a set of policies and procedures that establish expected behavior with regard to the Company's control environment.</p>	No exception noted.
CC5.1	SDC-32	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected user access list to ascertain whether entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.</p>	No exception noted.
CC5.1 CC5.3 C1.1	SDC-69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected Information Security Policy to ascertain whether entity has a documented Information</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			Security Policy that governs the confidentiality, integrity, and availability of information systems.	
CC5.1	SDC-105	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected information security policy and acceptable usage policy to ascertain whether entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.</p>	No exception noted.
CC5.2	SDC-28	Entity's Infosec officer reviews and approves the list of people with access to production console annually	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected user access review records to ascertain whether entity's Infosec officer reviews and approves the list of people with access to production console annually.</p> <p>Noted that no changes were requested as part of the user access review activity.</p>	No exception noted.
CC5.2 CC6.1 CC6.3 CC7.1	SDC-108	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected logs from monitoring tool to ascertain whether entity uses a continuous monitoring tool to alert the security team to update the access</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			levels of team members whose roles have changed.	
CC5.3 CC6.1 CC6.2 CC6.3	SDC-33	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected Access Control policy to ascertain whether entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.</p>	No exception noted.
CC5.3 CC7.4	SDC-53	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected incident management policy to ascertain whether entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.</p>	No exception noted.
CC5.3 CC7.5 CC9.1 A1.2	SDC-58	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected Backup policy to ascertain whether entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.</p>	No exception noted.

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC5.3 CC8.1	SDC-64	Entity has documented policies and procedures to manage changes to its operating environment.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected change management policy and SDLC process document to ascertain whether entity has documented policies and procedures to manage changes to its operating environment.</p>	No exception noted.
CC5.3 CC8.1	SDC-65	Entity has procedures to govern changes to its operating environment.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected change management policy and SDLC process document to ascertain whether entity has procedures to govern changes to its operating environment.</p>	No exception noted.
CC5.3 CC8.1	SDC-66	Entity has established procedures for approval when implementing changes to the operating environment.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected, for sample changes, approval and testing records to ascertain whether entity has established procedures for approval when implementing changes to the operating environment.</p>	No exception noted.
CC5.3 CC7.1 CC7.2 CC7.3	SDC-391	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected information security policy and vulnerability management policy to ascertain whether entity has a documented policy and</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
			procedures to establish guidelines for managing technical vulnerabilities.	
CC6.1 CC6.2 CC6.3	SDC-34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no new joiners during the audit period.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC6.1 CC6.6	SDC-38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected firewall configuration and database access ruleset to ascertain whether entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	No exception noted.
CC6.1 CC6.3	SDC-42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest user access review records to ascertain whether entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	No exception noted.
CC6.1 CC6.3	SDC-43	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected latest user access review records to ascertain whether entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	
CC6.2 CC6.3 CC6.5	SDC-35	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no leavers during the audit period.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC6.3	SDC-37	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected list of users having access to production databases to ascertain whether entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	No exception noted.
CC6.5 C1.2	SDC-48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset disposal policy to ascertain whether entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC6.6	SDC-39	Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor authentication.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected MFA configuration to ascertain whether entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor authentication.</p>	No exception noted.
CC6.6	SDC-44	Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected, for sample endpoint, anti-virus and malware protection software version and installation status to ascertain whether where applicable, entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.</p>	No exception noted.
CC6.6 CC6.7 C1.1	SDC-45	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected, for sample endpoint, encryption status to ascertain whether entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.</p>	No exception noted.
CC6.6 CC6.8 CC7.3	SDC-46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected latest security patching report to</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		establishment of the internal connection.	ascertain whether entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	
CC6.6	SDC-47	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected screen lock configuration at domain level to ascertain whether entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.</p>	No exception noted.
CC6.6 CC6.8	SDC-50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected firewall configuration to ascertain whether production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the entity's cloud provider.</p>	No exception noted.
CC6.6	SDC-104	Entity has documented policies and procedures for endpoint security and related controls.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected information security policy and endpoint protection policy to ascertain whether entity has documented policies and procedures for endpoint security and related controls.</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC6.6 CC6.7	SDC-141	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected, for sample endpoints, encryption configuration and password configuration to ascertain whether entity requires that all critical endpoints are encrypted to protect them from unauthorized access.</p>	No exception noted.
CC6.6	SDC-390	Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected asset register to ascertain whether entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.</p>	No exception noted.
CC6.7 C1.1	SDC-49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected encryption status of production databases to ascertain whether entity has set up cryptographic mechanisms to encrypt all production databases that store customer data at rest.</p>	No exception noted.
CC6.7	SDC-51	Entity has set up processes to utilize standard encryption methods, including HTTPS with	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected TLS certificate to ascertain whether</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		the TLS algorithm, to keep transmitted data confidential.	entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.	
CC6.7 CC8.1	SDC-52	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset inventory to ascertain whether entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exception noted.
CC6.7	SDC-100	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected encryption status and firewall configuration for non-prod environment to ascertain whether entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	No exception noted.
CC6.7	SDC-106	Entity has a documented policy to manage encryption and cryptographic protection controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected encryption and cryptographic policy to ascertain whether entity has a documented policy to manage encryption and cryptographic protection controls.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
CC7.1 CC7.2 CC7.3 CC9.1	SDC-56	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vulnerability scans and action plans to ascertain whether entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	No exception noted.
CC7.1 CC7.2 CC7.3	SDC-61	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats	No exception noted.
CC7.1 CC7.2 CC7.3 CC9.1 A1.1	SDC-62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exception noted.
CC7.3	SDC-63	Entity identifies vulnerabilities on the company platform through an annual penetration testing	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest VAPT report to ascertain whether	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		exercise conducted by a qualified third-party service provider.	entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.	
CC7.1 CC7.2 CC7.3	SDC-394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exception noted.
CC7.3 CC7.4 CC7.5	SDC-54	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected list of incidents and noted that there was no security incident reported during the audit period.	No exception noted.
CC7.5 A1.2 A1.3	SDC-392	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected DR policy to ascertain whether entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident	No exception noted.
CC7.5 A1.2 A1.3	SDC-393	Entity has documented policies and procedures that establish guidelines for continuing business	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
		operations and facilitate the application of contingency planning controls.	Inspected business continuity policy and plan to ascertain whether entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	
CC9.1 A1.2	SDC-59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected backup configuration and logs to ascertain whether entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.</p>	No exception noted.
CC9.1 A1.2 A1.3	SDC-60	Entity tests backup information periodically to verify media reliability and information integrity.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected latest back restoration logs to ascertain whether entity tests backup information periodically to verify media reliability and information integrity.</p>	No exception noted.
A1.3	SDC-97	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected BCP plan and test report to ascertain whether entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.</p>	No exception noted.

Information Provided by the Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Internxt	Testing Performed	Results of Tests
C1.1	SDC-70	Entity performs physical and/or logical labelling of information systems as per the guidelines documented policy defined for data classification	<p>Inquired with the management regarding the control activity to ascertain that the control operates as described.</p> <p>Inspected asset management policy and data classification policy to ascertain whether entity performs physical and/or logical labelling of information systems as per the guidelines documented policy defined for data classification</p>	No exception noted.